People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
University of Oum El Bouaghi
Research Laboratory on Computer Science's Complex Systems

CONFERENCE PROCEEDINGS

ICCSA'2021

The Second International Conference on Computer Science's Complex Systems and their Applications

Oum El Bouaghi – Algeria

May 25-26 Th, 2021

Online Conference

Dr. Toufik Marir – Dr. Abdelhabib Bourouis – Dr. Rohallah Benaboud (Eds)

Toufik Marir, Abdelhabib Bourouis and Rohallah Benaboud (Eds.)

ICCSA 2021

2nd International Conference on Computer Science's Complex Systems and their Applications

Oum El Bouaghi, Algeria, May 25-26, 2021

Proceedings

Editors :

Toufik Marir

Research Laboratory on Computer Science's Complex Systems (ReLa(CS)²)
University of Oum El Bouaghi (Algeria)

Abdelhabib Bourouis

Research Laboratory on Computer Science's Complex Systems (ReLa(CS)²)
University of Oum El Bouaghi (Algeria)

Rohallah Benaboud

Research Laboratory on Computer Science's Complex Systems (ReLa(CS)²)
University of Oum El Bouaghi (Algeria)

ISBN 978-9931-9788-0-0

Preface

Complex systems are composed of several interacting components. In fact, these interactions are the source of many properties of complex systems, such as the emergence, the self-organization, the nonlinearity and the adaptation. In addition, these systems are often used to characterize several problems in different fields, like biology, sociology, psychology and economy. They represent an interdisciplinary domain.

Computer science plays two major roles in the context of complex systems. In the one hand, it provides adequate tools to model and simulate such systems. Nowadays, many computer systems can be considered as complex systems, in the other hand. Indeed, the current computer systems are composed of several interacting components where the complex systems' characteristics can emerge.

In this context, the main purpose of the second international conference on computer science's complex systems and their applications (ICCSA'2021), organized by the research laboratory on computer science's complex systems (ReLa(CS)^2) – University of Oum El Bouaghi (Algeria) from May 25th – 26th, 2021, is studying these systems. It brings together academics, industry experts and education leaders from all over the world to discuss incredibly wide range of topics ranging from computer security, computer networks, embedded systems, image and video processing, modelling and simulation and intelligent distributed systems to name a few. Furthermore, after the first successful edition (ICCSA'2016), this edition has the special goal to strengthen its role as a meeting point for the researchers in the field. For this reason, a rigorous double blind review process is applied where each paper is reviewed at least by two experts. In addition, we chose a restricted acceptance rate (about 22%) to ensure good selectivity.

Oum El Bouaghi, Algeria : June 30, 2021

Toufik Marir, Abdelhabib Bourouis and Rohallah Benaboud.

Committees

Our warmest thanks go to our Technical Program Committee (TPC) for their unevaluable work, time and tireless effort. We are most grateful to the reviewers who have so diligently supported the peer review process.

Honorary Chairs

- Pr. Zohir Dibi, Rector of the University of Oum El Bouaghi - Larbi Ben M'Hidi, Algeria
- Dr. Nacer Hebbir, Dean of the SESNV Faculty, University of Oum El Bouaghi - Larbi Ben M'Hidi, Algeria.

General Chair

- Dr. Toufik Marir, Head of ReLa(CS)^2 Laboratory, University of Oum El Bouaghi - Larbi Ben M'Hidi, Algeria.

Organizing Committee chair

- Dr. Zakaria Laboudi, University of Oum El Bouaghi - Larbi Ben M'Hidi, Algeria

Organizing Committee

Amina Zerdani	University of Oum El Bouaghi, Algeria
Asma Saighi	University of Oum El Bouaghi, Algeria
Ayoub Kalach	University of Oum El Bouaghi, Algeria
Cherif Taouch	University of Oum El Bouaghi, Algeria
Hamza Merouani	University of Oum El Bouaghi, Algeria
Kamel Tebessi	University of Oum El Bouaghi, Algeria
Messaoud Djebbar	University of Oum El Bouaghi, Algeria
Mohamed Essadik Chabout	University of Oum El Bouaghi, Algeria
Nour Elhouda Dehimi	University of Oum El Bouaghi, Algeria
Redha Miroud	University of Oum El Bouaghi, Algeria
Salim Zerougui	University of Oum El Bouaghi, Algeria
Sofiane Zaidi	University of Oum El Bouaghi, Algeria
Soumia Zertal	University of Oum El Bouaghi, Algeria

Technical Program Committee chairs

- Dr. Abdelhabib Bourouis University of Oum El Bouaghi, Algeria
- Dr. Rohallah Benaboud University of Oum El Bouaghi, Algeria

Technical Program Committee members

Abbas Cheddad	Blekinge Institute of Technology in Karlskrona, Sweden
Abdeldjalil Gattal	University of Tebessa, Algeria
Abdeldjalil Ouahabi	École polytechnique, University of Tours, France
Abdelhabib Bourouis	University of Oum El Bouaghi, Algeria
Abdelhamid Mammeri	University of Ottawa, Canada
Abdelkarim Amirat	University of Souk Ahras, Algeria
Abdelouahab Moussaoui	University of Setif 1, Algeria
Abdelouahed Gherbi	ÉTS, University of Québec, Canada
Abderrahim Siam	University of Khenchela, Algeria
Abderrahmane Lakas	United Arab Emirates University, United Arab Emirates
Abd-Ed-Daïm Tenachi	University of Oum El Bouaghi, Algeria
Ahmed Korichi	University of Ouargla, Algeria
Asma Maaziz	University of Oum El Bouaghi, Algeria
Asma Saighi	University of Oum El Bouaghi, Algeria
Brahim Nini	University of Oum El Bouaghi, Algeria
Chaabane Lamiche	Université of M'sila, Algeria
Chérif Taouche	University of Oum El Bouaghi, Algeria
CongDuc Pham	University of Pau, France
Djamel Benmerzoug	University of Constantine 2, Algeria
Djamel Nessah	University of Khenchela, Algeria
Djamila Mechta	University of Setif 1, Algeria
Elhillali Kerkouche	University of Jijel, Algeria
Elkamel Merah	University of Khenchela, Algeria
Faiza Belala	University of Constantine 2, Algeria
Farhi Marir	Zayed University, United Arab Emirates
Farid Mokhati	University of Oum El Bouaghi, Algeria
Farida Bouarab-Dahmani	University of Tizi Ouzou, Algeria
Fateh Boutekkouk	University of Oum El Bouaghi, Algeria
Flavien Balbo	Henri Fayol Institute, France
Fouzia Boutaouche	University of Constantine 3, Algeria
Hadj Ahmed Bouarara	University of Saida, Algeria
Hakim Bendjenna	University of Tebessa, Algeria
Hassina Seridi-Bouchelaghem	University of Annaba, Algeria
Hichem Houassi	University of Khenchela, Algeria
Ismail Biskri	University of Québec à trois rivières, Canada
Kamel Karoui	University of Carthage, Tunisia
Karima Boussaha	University of Oum El Bouaghi, Algeria
Kenza Belhouchet	University of Oum El Bouaghi, Algeria
Khadidja Henni	Université TELUQ, Canada
Khalid Ghoul	University of Oum El Bouaghi, Algeria
Lakhdar Derdouri	University of Oum El Bouaghi, Algeria
Lamia Mahnane	University of Annaba, Algeria
Maamar Sedrati	University of Batna 2, Algeria
Mahieddine Djoudi	University of Poitiers, France
Maroua Bouzid-Mouaaddib	University of Caen-Basse Normandie, France
Mahmoud Boufaida	University of Constantine 2, Algeria
Makhlouf Derdour	University of Oum El Bouaghi, Algeria

Meriem Chibani	University of Oum El Bouaghi, Algeria
Mohamed Amin Laouadi	University of Setif 1, Algeria
Mohamed Chaouki Babahenini	University of Biskra, Algeria
Mohamad El Falou	Université Libano-Française, Libanon
Mohamed Hafidi	University of Annaba, Algeria
Mohamed Amine Ferrag	University of Guelma, Algeria
Mohammed Nassim Seghir	ENS de Biotechnologie de Constantine, Algeria
Mohamed Seddik Chebout	University of Oum El Bouaghi, Algeria
Moufida Maimour	University of Lorraine, Nancy, France
Mourad Bouzenada	University of Constantine 2, Algeria
Mourad Oussalah	University of Oulu, Finland
Nacira Ghoualmi-Zine	University of Annaba, Algeria
Nardjes Bouchemal	University Center of Mila, Algeria
Nasreddine Lagraa	University of Laghouat, Algeria
Nour El Houda Dehimi	University of Oum El Bouaghi, Algeria
Okba Kazar	University of Biskra, Algeria
Olivier Boissier	ENS Mines Saint-Etienne, France
Ramdane Maamri	University of Constantine 2, Algeria
Reda Yaich	SystemX Institute for Technological Research, France
Riyadh Baghdadi	Massachusetts Institute of Technology, USA
Rafik Menassel	University of Tebessa, Algeria
Rohallah Benaboud	University of Oum El Bouaghi, Algeria
Salah Merniz	University of Constantine 2, Algeria
Salim Zerrougui	University of Constantine 1, Algeria
Sofia Kouah	University of Oum El Bouaghi, Algeria
Sofiane Zaidi	University of Oum El Bouaghi, Algeria
Soufiane Boulehouache	University of Skikda, Algeria
Soumia Zertal	University of Oum El Bouaghi, Algeria
Tahar Guerram	University of Oum El Bouaghi, Algeria
Tahar Mekhaznia	University of Tebessa, Algeria
Toufik Marir	University of Oum El Bouaghi, Algeria
Toufik Messaoud Maarouk	University of Khenchela, Algeria
Varun Gupta	University of Beira Interior, Portugal
Yacine Lafifi	University of Guelma, Algeria
Youcef Gheraibia	University of York, United Kingdom
Zianou Ahmed Seghir	University of Khenchela, Algeria

Table of Contents

Distributed Secure Services Based on IoT and Blockchain for e-Health remote care

Hamza REFFAD
LRSD Laboratory
University of Sétif-1,
Sétif, 19000 – Algeria
reffadh@yahoo.fr

Abdelatif DJENAOUI
LRSD Laboratory
University of Sétif-1,
Sétif, 19000 – Algeria
hamzadje28@gmail.com

Adel ALTI
LRSD Laboratory
University of Sétif-1,
Sétif, 19000 – Algeria
alti.adel@univ-setif.dz

***Abstract*—Nowadays, the Internet of Thing (IoT) is a potentially powerful solution for health applications. It is a smart technology that provides remote care in real time and requires low latency health data processing and transmission. The large number of connected objects to Cloud can be a problem for low-latency workloads, which is the case of several health mobile applications. To this end, Fog Computing, has emerged, where Cloud computing is extended to the edge of the network to reduce latency and network congestion. It provides a highly virtualized platform that provides health data storage on remote public Cloud servers to which users cannot be fully trusted, especially when we are dealing with sensitive data like health data. In fact, it becomes necessary to rethink a new more robust secure technique. To provide such technique, we proposed a new secure solution called IoToDChain for e-Health mobile application, based on cryptographic techniques especially Elliptic Curve Diffie Hellman-RSA and the Blockchain paradigm. They exchange of a secret key in confidential and robust manner and protect patients' privacy in a mobile-Fog-Cloud environment. The experiments achieved promising results for good data protection against the most known attacks in healthcare systems.**

Keywords—privacy, confidentiality, Blockchain, smart contract, distributed access, RSA-Hashed Diffie-Hellman

I. INTRODUCTION

Countries around the world have been affected by the COVID-19 pandemic since December 2019, and the health care systems are rapidly adapting to the increasing demand for remote treatment. e-Health systems offer remote patient monitoring and share of information (temperature and humidity level, user glucose, user movement states, etc.) between different actors (i.e., physician, patient, and nursing) with various devices (i.e., smartphone, smart-TV, tablet). Hence, it helps to improve the emergency response, diagnosis, and treatment of patient's health remotely. Indeed, physics use intelligent medical equipment and mobile devices (IoT) to collect the patient's health data at home and sends them to the Fog. Then, the Fog sends this data to the Cloud storage service for consultation, evaluation and recommendations by professionals. This process helps professionals understand the behavior of this diseases and gives them a hint about its evolution. As the resources of mobile devices may be limited, applications can impose security requirements on the mobility of tasks and data. Besides, the changes in network behavior and energy levels of mobile devices may require reactive strategies. The health services must be (re-) deployed on the Cloud in real-time to meet a variety of quality service objectives, such as performance and storage capabilities, latency and energy constraints. However, security and privacy still an essential need for healthcare system's success.

Currently, the field of e-Health applications is characterized by heterogeneous mobile devices, as well as sensors transmitting data (IoT), which contribute to the provision of innovative Health Cloud services. All of these on-demand Cloud services (IoToD), provided through APIs or web interfaces. In this context, maintaining a centralized server that supports a large number of concurrent uses can be difficult and relatively expensive. This maintenance cost can be reduced by adopting a decentralized architecture. Despite the importance of e-Health system and their good results, it is necessary to protect the confidentiality of the data, to secure the sharing and to protect the private life of the patients. Therefore, access to shared medical records must be controlled especially when the data are outsourced in the Cloud. Usually, to use a model based on Mobile-Fog-Cloud architecture, a reinforcement of the security measures is mandatory. Thus, the confidentiality, integrity and access control of stored data are among the major challenges raised by external storage. To overcome the challenges mentioned above, cryptography and decentralized techniques are widely adopted to secure sensitive data. In this paper, we propose to design and implement a secure distributed control access approach based on Blockchain and IoT by exchanging data confidentially and protecting patient privacy in a new decentralized Mobile-Fog-Cloud architecture based on cryptography for the transaction of IoT data. Our main contributions are:

- Achieve a strong authentication and secure key sharing between the IoT device characterized by a limited resource in memory and computation. This allows confidential transfer of data between the two services.
- Combine cryptography technologies and Blockchain to strengthen the management of decentralized users-based access control, keep the traceability of data traffic and obtain a level of anonymity offered by the Blockchain and security policies based on smart contract.
- Apply a hybrid Elliptic Curve Diffie Hellman- RSA for secure data sharing between Cloud health services. This scheme allows the implementation of access control according to their identifiers. The authentication is done by a remote proxy/Fog which is a part of the Cloud system.

Our system can effectively resist against the most well-known remote co-allocation attacks in Fog-Cloud and against tampering of control messages. Further, enriching security of health data and deployment location.

The remainder of the paper is structured as follows. Section 2 discusses the related works. Section 3 presents the proposed IoToDChain (IoT on Demand Based on crypto-CHAIN) and the security algorithms. Section 4 illustrates the method proposed by using an illustrative use case in healthcare fields. Section 5 concludes the work.

II. Related Works

Over the last two decades, there have been many research works on the security approaches of Cloud mobile services. They proposed to preserve the confidentiality and privacy of distributed application tasks on mobile devices, Fog, or Cloud to ensure the application security requirements. However, Blockchain has emerged, where a systematic investigation on applications relies on services distribution and decentralized sensitive data security on the mobile device, Fog and Cloud hosts. As well as application in the Cloud uses Blockchain technology to protect users' information. The existing literature has proposed the conceptual underpinnings of Fog and mobile Cloud computing [1]. Zou et al. discussed the benefits and challenges of securing the mobile devices, Fog, and Cloud layers in a hierarchical model [2] but they did not examine in detail their impact on distributed IoT applications and their security. To the best of our knowledge, none of the existing approaches are able to provide decentralized approach to secure and manage a service-based application through user devices to minimize attackers' efficiency. Thus, the confidentiality, integrity and access control of stored data are among the major challenges raised by external storage. For that reason, new authentication technique based-secure communication in the mobile Cloud has been proposed by Jegadeesan et al. [3] to protect the control access of mobile users to the Cloud services. The technique is based on mutual verification between users and Cloud providers where both sides need to provide their legitimacy to each other. Due to the limited storage capacity of mobile devices, mobile users are not able to store the huge details of Cloud services anonymously. Therefore, the technique exchanges only session key once the successful authentication of mobile users to Cloud services occurs which decreases the computational cost. The technique uses a third party known as Trusted Third Party (TTP) to send private keys and public keys for both users and service providers to ensure registration and the authentication phases. The legitimacy of both components is checked via the hashing and cryptographic methods.

Ensuring data integrity and privacy is considered as a major objective to protect the processing data within services on Cloud servers. The new Blockchain technology and a Deep Neural Networks (DNN) model was integrated by Reddy et al. [4] to predict and detect the progression of Diabetic retinopathy disease. This model helps the medical practitioners to detect the first early stages that damage the eye's retina. To classify the extracted features of the disease, the Grey Wolf Optimization (GWO) algorithm was adopted whereas it considers as one of the best Meta heuristics algorithms of optimization in machine learning. The results show that the DNN model provides better detection performance compared to traditional machine learning models in terms of sensitivity, accuracy, recall and specificity. Ali et al. [5] designed an approach that improves the fault detection rate in Cloud-based healthcare services. Body sensors are used for monitoring and diagnosis the illness people in case of emergency cases. However, body sensors increase test fault due to the continuous and redundant tests of patients, which lead to an uncorrected decision from the doctors. The proposed approach successes to decrease the faults (more than 90% of the performance of fault detection rate) compared to previous faults-based approaches. Khare et al. presented a novel classifier model that combines Spider Monkey Optimization (SMO) and Deep Neural Networks (DNN) for detecting the system's intrusions named SMO-DNN [6]. Due to the huge usage of the internet, many malicious systems have developed which cause serious obstacles to the computer and network security. The proposed model showed a high intrusions detection efficiency in terms of accuracy (reach 97%), the precision of 99.5 %, recall between 92.8% and 99.5%, also 92.7 % and 99.6% of F1-score. Further, less training time compared to previous models. Singh et al. presented a comprehensive literature review of the security problems that affect the implementation of Blockchain in sustainable smart cities [7]. Incorporating the Blockchain and artificial intelligence in the smart society concept opens new security suggestions such as the protection of privacy. Moreover, Encryption methods are not sufficient to ensure the protection of security and privacy of the nodes, like hash functions necessitates an improvement by using intelligent search techniques and algorithms.

Various current works have integrated the Blockchain to secure the healthcare application [8, 9, 10, 11, 13, 14], but in our best knowledge, none of them are focusing in protecting the distributed services by adopting Blockchain with hybrid cryptography methods where the services are considered as main components in Cloud computing and any successful attacks occur to them may lead to retrieve users' sensitive data. Authors in [12] have proposed a new proxy to optimize the composition of Cloud service provided in different Cloud providers. However, the main limitation of the proposed proxy is not detecting the malicious communication that occurs between the different services deployed in different services providers. The proposed work for detecting malicious services communication in the Fog based on integrated Blockchain is an improvement of the work in [12], which detects attacks between health services while deployed on the Cloud.

III. Secure Distributed Services Based on Diffie-Hellman-Rsa and Blockchain

This section presents our contribution to secure the sharing and storage of data and preserve the privacy of patients in the e-Health system. The motivation behind proposing new security solution is to control the security aspects of the decentralized data access of an integrating service-based health application, providing a right level of anonymity and keeping distributed service's data safe against the most well-known attacks in health applications and against tampering of control messages. The system architecture of the proposed model with the seven components is shown in Fig. 1 and described as follows.

- **Patient**: includes different types of biomedical information and medical devices used to monitor the vital signs of a patient.
- **Proxy/Fog**: is the healthcare provider such as hospitals, laboratories, and clinics, which associated

to physicians or nurses. They can take care of a relatively large number of patients.

- **Cloud**: it defines as networks of different healthcare services connected with each other by sending and receiving packets. It stores the medical user's data and executes intensive tasks.

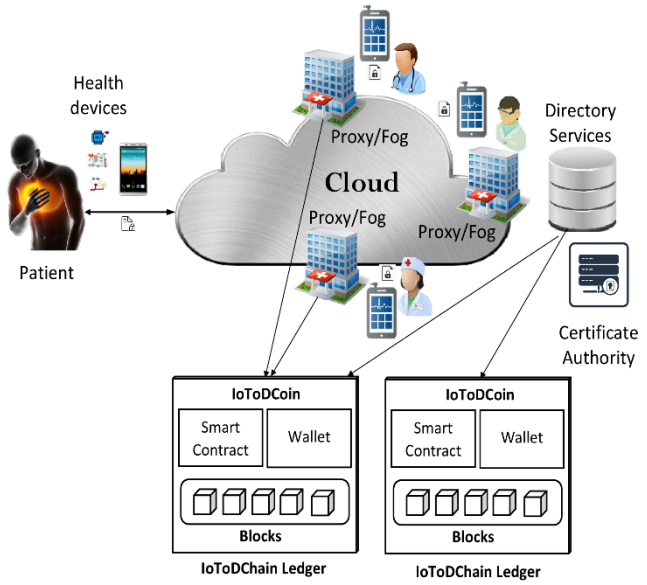


Fig. 1. IoToDChain general architecture.

- **IoToDChain:** plays the role of service provider / service consumer of sensitive health data or both. A service consumer must have the requirements rights to access the data. It also manages a symmetric encryption key to encrypt/decrypt the task's data. This key is used to generate a password and allows a service consumer to check if the latter stores sensitive data. Each service is associated with creation, sharing, reading, and writing transactions. When a service provider wants to send data to another, it will be able to decrypt the message using its private key. Therefore, public-key encryption allows services to exchange encrypted data with common secret key. All exchanges must ensure that the public key that is retrieved is from the task to which we want to send the encrypted information.
  - **IoToDChain Smart contract:** are protocols that facilitate the management of consumer services and data access rights. In IoToDChain, a contract is a stand-alone process to determine if read's request of data needs to be accepted/denied and to manage credits based on the number of objects targeted.
  - **Distributed IoToDChain Ledger:** perform cryptographic hashes of health sensitive data. The ledger is remunerated based on the credits and respects the data access rights of smart contract.
- **Certificate Authority (CA):** allows new mobile users and IoT devices to register with the Blockchain network and enables data signing and encryption.
- **Directory Services:** stores the description of deployed service in all Fog servers.
- **Directory Users/ Devices:** stores the description of deployed mobile users in all fogs.

Throughout the paper, the notation for i[th] registered legal device/service is denoted as D_i and the attacker as A. Table 1 shows the notations used to describe the Diffie-Hellman scheme and their meaning.

TABLE I. NOTATIONS

Notation	*Description*
PK_d	The public key of IoT device/service
PV_d	The private key of a device/service
PK_f	The public key of a proxy/Fog
PV_f	The private key of a proxy/ Fog
msg	A sensed data
E_{msg}	Encrypted-data (data encrypted by RSA-Hash Diffie-Hellman).
D_i	Set of devices/services
Id_i	Identity of the device/service

1) Modeling of our Blockchain: We will first present our records on the Blockchain in the form of a token presenting a pseudo transaction. The Blockchain, in our construction, is used as a distributed, persistent and tamper-proof book. It manages access control messages. In addition, one of the advantages of using the Blockchain is denying access to data by the Cloud. A record (*contained in a block*) in our distributed database is presented in the form of an access authorization token (*designated authorization*) on Blockchain, equivalent to a pseudo crypto-currency.

2) Handling Medical Data Access Contracts: When a patient creates an encrypted data record, add permissions, and download their metadata. The patient information and the account identity information are highly encrypted and can only be accessed with the authorization of the data owner, thereby ensuring data security and personal privacy. We propose to anonymize the request type (write, read, delete, and update) and still gives permissions level of each service and provides a way to set of services grants privileges to perform operations. We define three transactions carried out in the Blockchain:

– $ReadPermission(ID, S)$ is executed by the service's consumer to build a request. As an input, we have an ordered list ID and a corresponding data set S, the latter is chosen as $\sum_1^m s_i id_i$ is the id of the metadata in which the service's consumer is interested in. The function outputs the public and the private keys and the request $Q = \{k_{pub}, E_s\}$ where E_s is the encryption of S.

– The second function is $CheckPermission(Q, P)$ which is executed by the distributed smart contracts when the request is received. This function checks if the required operation is either permitted or not for the service. This function outputs an authorization R.

– Finally, we have the $ReadResponse(k_{priv}, R)$ function, executed by a service consumer when receiving R.

3) Handling Credits: The smart contract updates the credit of the mobile device (or a service). The credit establishes how much the server should trust a device (or a service). When a device (a service) shows malicious behavior once it failed to give the right secret key or attempted any abnormal communication (i.e., transfer malicious packets, service is not among the registered services of the network, the number of communications achieves a certain threshold). When the credit of unauthorized access becomes equal or more than a given threshold, the IoToDChain ledger detects the malicious mobile device (or malicious service). Eventually, its credit will be reduced until it reached zero, the Ledger updates the blacklist table and returns access denied as well as that mobile device (or service) is unable to communicate with any other mobile users (or services). Each smart contract performed both locally and on a distributed Ledger by using Blockchain. In this manner, every mobile device can retrieve the same global list of all accessed health data through the list of smart contracts.

4) The proposed hybrid Elliptic Curve Diffie Hellman-RSA

The scheme generating the secret key of devices in e-Health system is based on hybrid Elliptic Curve Diffie Hellman-RSA by selecting two different prime numbers, applying specific exponential functions and encrypting/decrypting exchanged messages between IoT devices and proxy/Fog.

- **Initialization: Setup ():** The algorithm selects the group G of order n and generator g of G.
- **Diffie Hellman-based secret key generation: generateSecretKey (g): SKu, SKe**

1. An IoT device chooses a random prime number P and computes $h(P)$ using $\frac{e^{P}-e^{-P}}{2}$ and sends it to proxy/Fog.
2. A proxy/Fog chooses a random prime number Q, receives $h(P)$ from a device and extracts P using $\ln\left(h(P)+\sqrt{h(P)^2+1}\right)$ then computes $h(P+Q)$ using $\frac{e^{P+Q}-e^{-(P+Q)}}{2}$ and send it to device.
3. A mobile device receives $h(P+Q)$ from proxy/Fog and extracts Q from $h(P+Q)$ using $\ln\left(h(P+Q)+\sqrt{h(P+Q)^2+1}\right)-P$ and send this value of Q to proxy/Fog.
4. A proxy/Fog authenticates IoT device and chooses a random private prime number pe and computes the public key $PK_f = g^{pe} \bmod Q$ and sends this value to IoT device/service.
5. IoT device/service receives PK_f and chooses a random private prime numbers pu and computes the public key $PK_d = g^{pu} \bmod Q$ and sends this value to user.
6. A mobile device and proxy/Fog compute the secret key (SKd, SKe) using the following equations:

$$SK_f = PK_d{}^{pe} \bmod Q \quad (1)$$

$$SK_d = PK_f{}^{pu} \bmod Q \quad (2)$$

- **RSA-based message encryptions/decryption (msg, P, Q, Sk_d, SK_f) :** we can encrypt a message M as follows:

1. Calculate $\beta = P * SK_f$ and $\alpha = Q * SK_f$.
2. Calculate $N = \beta * \alpha$ and $\varphi(N) = \varphi(\beta) * \varphi(\beta) = (\beta - 1) * (\alpha - 1)$.
3. Choose e such that $1 < e < \varphi(N)$ and e and N are co-prime.
4. Calculate d such that $(d \times e) \bmod \varphi(N) = 1$

Encry_RSA (msg, e, N): chipertext

$$E_{msg} = msg^{e} \bmod N \quad (3)$$

Decry_RSA (Emsg, d, N): cleartext

$$msg = E_{msg}{}^{d} \bmod N \quad (4)$$

IV. Secure Service Data Access and Sharing Scheme

In order to ensure effective access control of sensitive recording and protect patient privacy, we offer a system based specifically on Elliptic Curve Diffie Hellman-RSA encrypt and Blockchain.

*1) **The Registration Phase.*** In this phase, the IoT device D_i intends to become a legal access service and profit services offered by the Fog. The steps that are performed in this phase are:

- D_i uses id_i (@Mac in string format) and selects a random prime number P_i and calculate the value $h(P_i) = \frac{e^{P_i} - e^{-P_i}}{2}$. The values $\{id_i, h(P_i)\}$ are sent to the proxy/Fog in a secure way.
- The proxy/Fog, after receiving $\{id_i , h(P_i)\}$chooses a unique integer Q_i for device D_i
- The proxy/Fog calculates the value $h(Q_i)$ by $\frac{e^{P_i+Q_i} - e^{-(P_i+Q_i)}}{2}$ and sends it to the device.
- D_i after getting $h(Q_i)$, extracts Q_i and stores it with his identifier.

*2) **The login and authentication Phase.*** In order to avail the services of this scheme, IoT device/service and the proxy/Fog agree on the same generator number g. After this, the steps below are executed:

1. First, IoT device/service selects a random prime number P and calculate the value $h(P) = \frac{e^{P}-e^{-P}}{2}$.
2. Then IoT device/service signs an identity id_u and encrypts the value $h(P)$ and the identity id_u by the public key of Fog (PK_f). Then it sends the information to the proxy/Fog.
3. The proxy/Fog decrypts and extracts the information id_d necessary for authentication and P necessary for the calculation of the symmetric key.
4. If the signatures received are correct. Then IoT device/service authenticated successfully. The Fog in turn selects a secure random prime number Q and

extracts P using $\ln\left(h(P)+\sqrt{h(P)^2+1}\right)$. Then, it calculates $h(P+Q)$ using $\frac{e^{P+Q}-e^{-(P+Q)}}{2}$.

5. The Fog encrypts and signs the value $h(P+Q)$ by the public key of IoT device/service (PK_u) and sends it to the user.
6. The user decrypts the message and verifies the validity of the signature. Finally, it calculates the symmetric common key SK_d.

Note that the public parameters are:

- g is the generator point.
- The public keys of Fog and device are: PK_f and PK_d.
- The secure channel is ready to transmit the data generated by the IoT devices/services.

*3) **The Data Encryption Phase.*** The IoT device/service run the $EncrS_K$ (M) algorithm by encrypting the data and sending it to the Fog. Once received, the latter executes the algorithm: Encry_RSA (msg, e, N) = CT, it calculates the data identifier idx = Hash (CT) and transfers the cipher-text to the storage provider where it will be stored and simultaneously the proxy-Fog broadcasts the permission.

*4) **Access permission phase.*** Permission is given by the data signature (proxy/Fog). Indeed, the proxy/Fog generates a permission which is used to authorize a group to access its data in the Cloud. When the physician receives permission to access data, first of all, he authenticates himself on the Cloud with his identifier. The smart contract receives the request and starts the authentication process. If the physician authentication is successful, then the smart contract monitors the access rules. The physician uses his secret key and retrieves the data in clear. **Fig. 2** summarizes the permissions and data access phase.

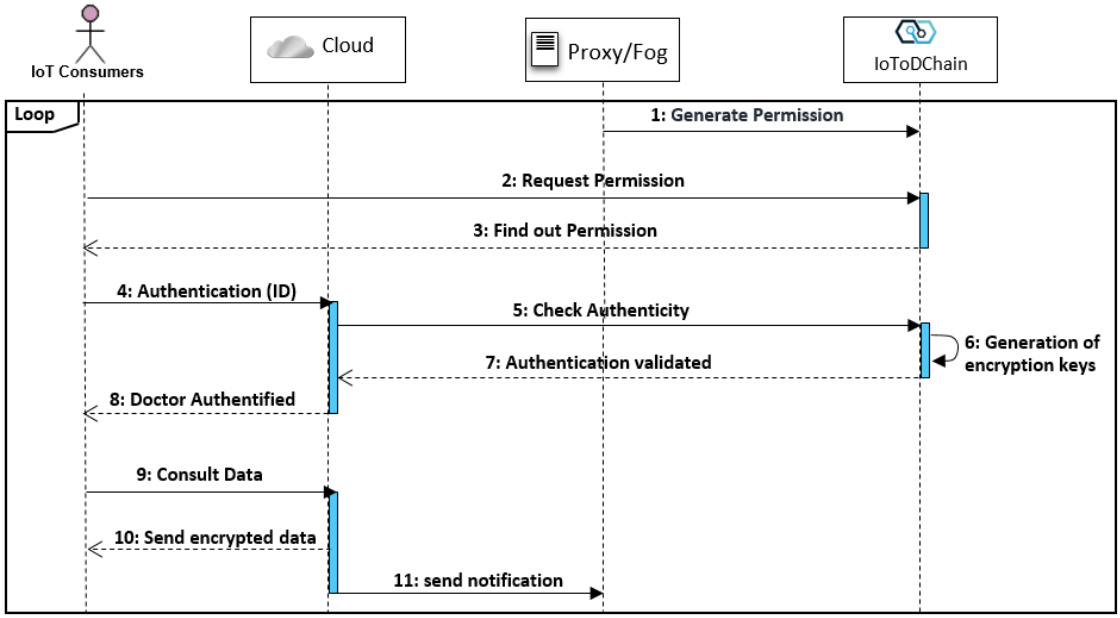


Fig. 2. The permission and data access phase.

V. Security Analaysis And Implementation Results

A. Security Analaysis

Let's assume that there are two parties A and B intend to communicate via unsecure communication channel. We assume that A is Service 1 and B is Service 2 or A is User and B is Secure Fog Proxy. Another party C "Attacker" attempt to intrude the communication between A and B in order to get their shared data. When A encrypts the message that intend to send to B, it must also send the key to decrypt this message (*Secret Decryption Key*). The attacker can get the encrypted message as well as the key to decrypt this message while A sends to B. Diffie-Hellman RSA provides the solution for this situation as follow:

- First, *A* send a public key to B and B also send a public Key to A. The Attacker C cannot see of both the public and private keys of A and B.
- Second, A and B agree on two different prime numbers and generator number. Using the hashed complex exponential functions, the private key of A and B can be constructed. The attacker or any third party cannot find these two numbers.

In order to ensure security and privacy, first of all, the users A and B willing to exchange information need to generate a pair of public and private keys. The public keys have to be exchanged beforehand. The both public keys of A and B are generated using the following equations:

$$PK_A = g^{pa} \bmod Q \quad (5)$$

$$PK_B = g^{pb} \bmod Q \quad (6)$$

After A and B exchanges their public keys. They can calculate the secret key by the following equation:

$$SK_A = PK_B{}^{pu} \ mod \ Q \quad (7)$$

$$SK_B = PK_A{}^{pe} \ mod \ Q \quad (8)$$

They find the same result once the secret keys have been constructed. The same results can be found when (secret key A = secret key B). However, C cannot find the same result because it is practically impossible to get the private number of A and B, more particularly if it is big integer. Moreover, C will be faced with the mathematical problem called the discrete logarithm problem. For example, it is easy to calculate: 315 mod 17 = 6 but it is impossible to find a single number *x* such that *x* Mod 17 = 6. Especially when the private number is longer than 100. Therefore, the calculation will be computationally insolvable. This secret key can be uses with any encryption method.

B. Implementation Results

IoToDChain is implemented using the decentralized Ethereum and Eclipse. The development of IoToDChain is currently in a prototyping phase. The smart contract is compiled and deployed using the *Truffle* framework. It is installed on all the nodes of the network. The application is interacted with Ethereum using the web3j API interface. This API works as modular, secure and lightweight Java library to setup, compile, configure, and deploy smart contracts with clients (nodes) on the Ethereum network.

The prototype is able to secure a variety of IoT services cooperate autonomously, without the need for a third-party trust institution, to form a distributed new proxy/Fog IoToDChain health model shared with all fogs. It transforms the distributed transaction assets into "smart contracts", completes Hash-Diffie Hellman-RSA encryption by Fog computing and secures data storage in the Cloud.

We used our IoToDChain platform to illustrate distributed health system that follow-up diabetes disease for patients. The security management of such application and sensitive communications depends on distributed services in remote providers either in the mobile devices, Fog or in the Cloud platforms. It defines three fundamental actors: patient, nurses and doctors. They are allowed to exchange and share sensitive medical data on the Cloud. The application is built with various services deployed in different nodes and it manipulates patient data and medical information (i.e., *glucose captor service, diabetes assessment service, treatment details service, and insulin injection service*). The application allows patients to send their medical information, which will be posted as message encrypted and signed using Hash-Diffie Hellman-RSA. Patients can include *weight, temperature, glucose and blood pressure*. It allows a doctor and/or a nurse in other sites to track patient updates applied on sensitive and private patient data. Regarding the right of access, we have given permission to access sensitive patient data only to the doctor concerned. **Fig. 3** shows the application with several IoT services. Only agreed doctors must have access to a patient's medical file. However, the access cannot be trusted hence we use IoToDChain platform deployed in the mobile-Fog-Cloud to prevent unauthorized access and control patient's data against malicious attackers.

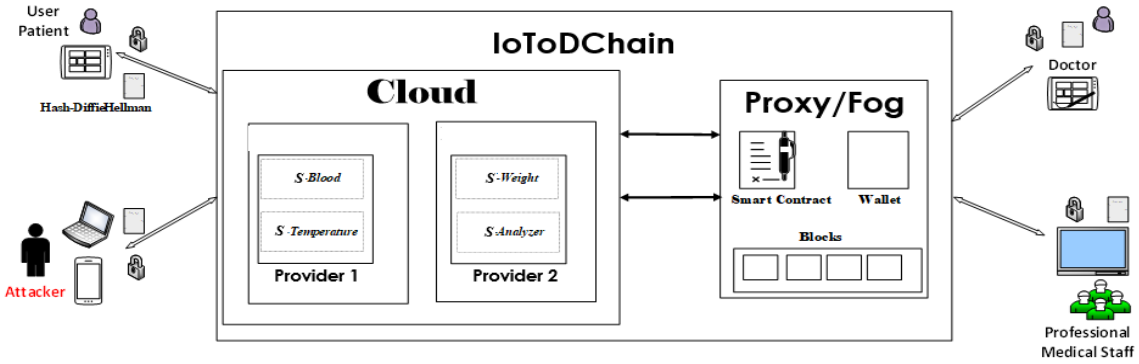


Fig. 3. The architecture of distributed Health care mobile application using IoTODChain

In order to allow the physician to securely access their account and access sensitive patient data, the secure data access sequence is determined as follows:

- First, a system deploys a smart contract on IoToDChain using web3j for the execution of the encryption and decryption algorithms as shown in Fig.4.
- Second, a doctor gets a read permission out from IoToDChain.
- Third, the doctor sends an encrypted request to consult the data with his ID.
- Finally, the Cloud authenticates the doctor, verifies access rights and sends encrypted data.

The validation of the approach has been conducted using a follow-up diabetes disease application. We plan to compare the proposed approach with existing works in near future works.

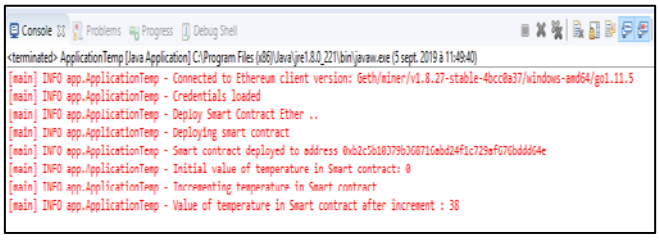


Fig. 4. Dpeloyment of health smart contract in IoToDChain.

VI. Conclusion and Perspectives

With the advent of IoT technology, preserving the security of distributed health applications and handling sensitive data have become a fundamental necessity. In this paper, we presented a secure distributed mobile-Fog-Cloud service approach based on Diffie Hellman-RSA and Blockchain called (IoToDChain) for preserving the privacy of document and health data stored in the Cloud. Due to the access of malevolent users to cloud's services, data integrity and confidentiality can be retrieved by other unauthorized users or external services. Thus, we reinforce the service' data access by adding the smart contract to achieve security of healthcare sensitive tasks using IoToDChain Ledger. Finally, we validate our distributed and innovative approach through a scenario that describes the case study of a diabetic disease follow-up. Prototyping results show that the proposed approach provides good data protection and control access against the most known attacks. However, the time checking complexity must be improved in future work. Our future work focuses on the validation of the proposed architecture by comparing the encryption time with existing approaches, implementing a global framework using real-world health sensors devices, smart objects, and Ethereum.

References

[1] S.Tuli, N. Basumatary, S. S. Gill, M. Kahani, R. C. Arya, G. S. Wander, R. Buyya, HealthFog: "An Ensemble Deep Learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in Integrated IoT and Fog Computing Environments" Future Generation Computer Systems, 2019. https://doi.org/10.1016/j.future.2019.10.043

[2] D. Zou, S. Chen, S. Han, Design of a Practical WSN Based Fingerprint Localization System. Mobile Netw Appl 25, 806–818, 2020. https://doi.org/10.1007/s11036-019-01298-4

[3] S. Jegadeesan, M. Azees, P. Malarvizhi, G. Manogaran, N. Chilamkurti, R. Varatharajan, C. Hsu,. An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications. Sustainable Cities and Society, 49(March), 101-522, 2019. https://doi.org/10.1016/j.scs.2019.101522.

[4] P. K. Reddy, M. S. Kuchay, Y. Mehta, S. K. Mishra, Diabetic ketoacidosis precipitated by COVID-19: a report of two cases and review of literature. Diabetes & Metabolic Syndrome: Clinical Research & Reviews, 14(5), 1459-1462, 2020.
https://doi.org/10.1007/s00125-020-05180-x

[5] S. Ali, H.Yaser, N. Z. Jhanjhi, H. Mamoona, I. Muhammad, N. Anand, S. Saurabh and In-Ho R. Towards Pattern-Based Change Verification Framework for Cloud-Enabled Healthcare Component-Based. IEEE Access 8: 148007-148020, 2020.
https://doi.org/10.1109/ACCESS.2020.3014671

[6] N. Khare, D. Preethi, L. Chiranji, B. Sweta, S. Geeta, S. Saurabh, and Y. Byungun. SMO-DNN: Spider Monkey Optimization and Deep Neural Network Hybrid Classifier Model for Intrusion Detection. Electronics 9, no. 4: 692, 2020.
https://doi.org/10.3390/electronics9040692.

[7] S. Singh, K. Pradip, B. Y. Sharma, S. Mohammad, C. Gi Hwan, and R. In-Ho, Convergence of Blockchain and artificial intelligence in IoT network for the sustainable smart city. Sustainable Cities and Society 63 (2020): 102364, 2020.https://doi.org/10.1016/j.scs.2020.102364

[8] G. Nagasubramanian, R. Kumar, S. Rizwan, P. Amir, Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Computing and Applications, 1. https://doi.org/10.1007/s00521-018-3915-1, 2018.
https://doi.org/10.1016/B978-0-12-819593-2.00004-2

[9] X. Xu, Y. Chen, Y. Yuan, Blockchain-based cloudlet management for multimedia workflow in mobile cloud computing. Multimed Tools Appl 79, 9819–9844, 2020. https://doi.org/10.1007/s11042-019-07900-x

[10] S. Tuli, R. Mahmud, S. Tuli, R. Buyya, The Journal of Systems and Software FogBus : A Blockchain-based Lightweight Framework for Edge and Fog Computing. The Journal of Systems & Software, 154, 22–36, 2019. https://doi.org/10.1016/j.jss.2019.04.050

[11] S. Tanwar, K. Parekh, R. Evans. Blockchain-based electronic healthcare record system for healthcare 4 . 0 applications. Journal of Information Security and Applications, 50, 102407, 2020. https://doi.org/10.1016/j.jisa.2019.102407

[12] H. Reffad, A. Alti, New Approach for Optimal Semantic-Based Context-Aware Cloud Service Composition for ERP, 36(4), 2018. https://doi.org/10.1007/s00354-018-0036-4

[13] X. Liang, , J. Zhao, S. Shetty, J. Liu, D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications." IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC). 2018.
https://doi.org/10.1109/CCGRID.2017.111

A Survey on Identity-based Key Management Schemes in Mobile Ad hoc networks

Kenza Gasmi
ReLa(CS)^2 Laboratory
Oum El Bouaghi University
04000, Oum El Bouaghi, Algeria
kenza.gasmi@univ-oeb.dz

Abdelhabib Bourouis
ReLa(CS)^2 Laboratory
Oum El Bouaghi University
04000, Oum El Bouaghi, Algeria
bourouis.abdelhabib@univ-oeb.dz
ORCID: 0000-0002-4592-4042

Rohallah Benaboud
ReLa(CS)^2 Laboratory
Oum El Bouaghi University
04000, Oum El Bouaghi, Algeria
benaboud.rohallah@univ-oeb.dz
ORCID:0000-0002-6301-2506

***Abstract*—Mobile Ad hoc networks attract more attention over the years, but the security matter of this type of network makes it hard to achieve all of their advantages. Cryptographic key management is the cornerstone for building any robust network security solution. Identity-based cryptography is a promising solution that resists well the key escrow problem which is suitable for Mobile Ad hoc networks. In this paper, we give an overview of the most important identity-based encryption schemes proposed in the last decade; combined with other techniques to enhance it and provide better results for Mobile Ad hoc networks. Hence, we give a comparative analysis to highlight their advantages and weaknesses. This work gives insights into a recent research to point out its interesting features, take advantages of its strength, ovoid its weaknesses and to lay out the future directions in this area.**

***Index Terms*—MANET, key management, identity-based, cryptography, Threshold Cryptography.**

I. Introduction

Without any sort of infrastructure, a mobile ad hoc network (MANET) can manage to establish a robust communication, where wireless mobile nodes cooperate as one to keep the network connected. Each one of the network nodes relies on others to reach a destination where all of them act booth as participants as well as routers. Easy and rapid to deploy, self-organizing, low cost and the size of hosts make this type of networks on demand in all domains where a distribution wireless communication needs to be obtained. MANET is widely employed in military, medicine, natural disaster and several other important areas. However, end-to-end communication caused by the absence of infrastructure, bandwidth-limited, the mobility and the short life of nodes decrease the security of the network. The absence of infrastructure and the limited bandwidth enforce the nodes to communicate through others. An intruder can falsify the communication by modifying or deleting the packets, or even inject false ones. Furthermore, attackers can spy the packets in a passive way by analyzing them then extracting information, or use the active way, so they can interrupt the network operations. The mobility makes the topology changes frequently. The nodes enter and exit the network at any time, making hard to establish trust between network members. The short life caused by limited energy incites the selfish behaving, which causes the reject of messages and leads to not reaching the destination. Moreover, a good security algorithm, which probably requires complicated calculations and a lot of energy, will be difficult to adapt.

Many solutions had been proposed to deal with the security requirements of MANETs, but none of them had reached the security level. One of the top security mechanisms is the cryptographic techniques, which can be an ideal choice to establish a general secure framework in Ad hoc networks. The cryptography is a way of making a secret communication between two parties in the presence of an eavesdropping adversary. The cryptography uses mathematical function and a cryptographic algorithm in a combination with a key to decrypt plain text (clear text) to a cipher-text. It uses mathematical technique to encrypt and decrypt information, so no one can discover it if he is not allowed. Unlike what cryptography does, cryptanalysis seeks to break secure communication using the so called attacks by deciphering ciphers without the knowledge of the used keys. There are two basic types of cryptography based on the nature of used keys and are *Symmetric Key* and *Asymmetric Key*. The former is the oldest and easiest type where the same secret key must be shared by all of the communication members. Knowing this key by an attacker threatens the whole communication. For the later, each member of the communicating groupen uses two different keys or a key pair. One of which everyone knows and called public, and the other must be kept secret and is only known by its owner. For confidentiality purposes, the encryption uses the public key while the decryption uses the private one.

The secrecy of the keys and the strength of the algorithm are the main things that make the data exchange secure. Create, install, update, revoke or even destroy the keys need to be managed. The huge number of keys in a network and the strength of each one of them must be managed using an optimal and a robust mechanism. The key management system is the right mechanism that handles the keying material. Because of the complexity of the key management system, most of the proposed schemes do not target all of its steps.

This work is fully funded by the General Direction of Scientific Research and Technological Development-Algerian Ministry of Higher Education and Scientific Research DGRSDT/MERS.

Generally, they focus just on one of the cryptography types, despite the fact that the two are usually required together.

The leading traditional asymmetric scheme that manages the public-key encryption is the public key infrastructure (PKI). It provides secure communication on an insecure public network and uses a digital signature to verify the identity of the entities. The PKI relies on the security of central control point, called the Certification Authority (CA), that everyone trust. In MANETs, one CA is as applying a single point of failure. If this point is compromised, the security of the entire network will fall down. Another obstacle of using PKI in MANETs is the heavy overhead of transmission and storage of Public Key Certificates (PKCs) [1].

To avoid the upcoming problems within the PKI, identity based cryptography (IBC) can be a good alternative [2] [3]. Here, the asymmetric keys are derived from the user's identity. Thus, there is no need of the CA and the PKCs. Thanks to the reduction in the cost of storage, computation and communication, IBC also adapts to MANETs limited in bandwidth and resources [1]. Instead of CA, another trustworthy authority, called a Private Key Generator (PKG), is needed to generate the private key corresponding to a given identity and can be considered as a single point of failure. Similar to CA in PKI, if the PKG is compromised, the security of the entire network will be exposed. Several revised types of identity-based schemes had been made using multiple authority approaches. Nevertheless, they also caused some other new problems [1].

The threshold cryptography is a complimentary technique to IBC where the secret can be divided into N sub-secrets shared by a group of users. Thus, instead of using one PKG node in IBC, N nodes can play its role.

The rest of the paper is organized as follows. Section II introduces the concept of key management system. Section III recalls briefly some background knowledge. Section IV reviews the most recent ID-dased key management schemes for MANETs in a comprehensive comparative study that highlights strengths and weaknesses. Section V summarizes the weaknesses of the IBC which still pose challenges and require effective solutions. Finally, we conclude this study in Section VI.

II. Key Management System

The establishment of secure communication is crucial in any network. It is a more challenging and hard to achieve task in mobile ad hoc networks than in their wired counterparts. Cryptography is a valuable tool to ensure this goal and implies the use of various small pieces of data known as keys. Keys are themselves sensitive data that need to be securely handled by key management systems (KMS). A KMS is an important process to both traditional and Ad hoc networks when secret communication between any two parties requires handling keys. The use of the keys can be divided in two main types. The first type, that it called symmetric-key, is when all the entities that participate in the communication share the same secret key, where the second uses two different keys per entity. This type is the asymmetric-key. One of its keys is public and used for encryption where the other is secret and used for decryption.

A. Key management stages

Key management has to go through several steps to achieve its goals, either in symmetric as well as in asymmetric systems. This process is summarized in [4] as follows:

1) Users initialization system: This step bootstraps the system. Non-cryptographic operations are included but others are, such as providing identities to the users, verifying user's information, and ensuring the proper software to the key management process.

2) Creating, distributing and installing the keying material: Keys can be created in a centralized or decentralized manner by the parties that are allowed to that could be the users themselves. Keys must be securely distributed to their owners. All parties involved in a communication based on symmetric cryptography must get securely the same key. In asymmetric cryptography, only the authorized party have to receive the private key in a secure way. The public key has to be delivered to any demanding party preserving integrity and authenticity. After the creation and distribution, the keys can then be installed into the nodes.

3) The use of the keying materiel: In this stage, secure communication can be achieved. Using keys to encrypt data and control the exchanging traffic between the network nodes.

4) Updating, revoking, and destroying the keying material: Key management must deal against several threats. Updating keys periodically can avoid attacks that managed to prevail over old ones. Compromised nodes lead to compromised keys that can affect confidentiality, authenticity, and the unauthorized use of keys. In such a case, compromised nodes must be revoked. In some cases, replacement of the keys can be done. Of course, this operation cannot be effective if compromised nodes are under the control of the adversary.

5) Archiving the keying material: This final step may not be always applied. It might be needed only when keys must be saved for auditing purposes, such as in the case of legal proceedings.

B. Categories of Key Management Schemes

Key management schemes can be classified in two main categories: contributory and distributive [5]. A collaborative effort of two or more nodes results in contributory schemes to agree on a key. In distributive schemes, each node generates a key and tries to distribute it to others. In this paper we focus on distributive schemes.

As mentioned before and illustrated in figure 1, asymmetric and symmetric cryptography are the main two cryptographic categories for distributed key management schemes. These two types are generally combined with different techniques to solve specific problems or to get more secure. However, key management in ah doc networks is more challenging than in traditional networks. Key management approaches in traditional networks depend on trusted third parties (TTP) that all of the system nodes trust. The use of a TTP can be achieved

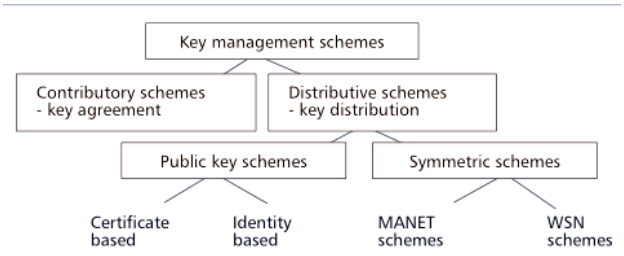


Fig. 1. Classification of key management schemes [5].

in three different ways. In-line TTP, which is an active entity that participates not only in deciding the keying material but during the entire communication as well. On-line TTP is an active trusted entity which participates only in deciding the keying material. Off-line TTP is no longer needed to be part of the system after the distribution of the keys. The keys are distributed in the initialization phase when the system is bootstrap.

The TTPs are important pieces in key management schemes to achieve a secure communicating system in traditional networks. However, it is not always applicable to MANETs, due to their main characteristics and to the lack of trusted infrastructure.

1) Symmetric Key-Based Approach: Keys in this approach are loaded into the nodes before the deployment of the system. Secure communication then can be found during the operation of the network using the secret information that are stocked into the nodes. The use of one common key, a shared key between two or more nodes or the use of a random set of keys to each node are basically the approaches on which the existing solution are based. These approaches can be divide in two categories, being either deterministic or probabilistic schemes.

In a deterministic scheme, the identity of the nodes and the keys loaded on, have a deterministic relationship. Moreover, secure link that exists between any two nodes can be predicted exactly. Several options in choosing the keys are used and the basic alternatives are: one common key for the entire network or each node has a separate key for every other node. For the probabilistic technique, a pool of keys is used, and a bunch of keys that are randomly chosen from this pool, are loaded into each node. Thus, a secure link is built with a certain probability between any two nodes provided by common keys shared between them. The probabilistic scheme namely consists of three phases; key pre-distribution where the pool of P keys is generated along with the keys identifiers. This pool is generated before the deployment of the nodes by a trusted authority. Then, this authority randomly choses K keys among P and installs them on each node along with their identifiers. The size of the key pool is chosen in a way that any random collection of K keys can at least share one key in common with certain probability. The second phase is the shared key-discovery. Nodes start to discover the shared keys with their neighbors. In the case where common keys exist, nodes can then agree on one of them and establish a secure communication. In the opposite case where no common keys exixt, nodes will not be able to establish secure link directly. Note that this phase starts after the installation of the system. The third phase is needed in case of not fully connective system. This phase is called path-key establishment. It is possible that there are no common keys between pair of nodes in the network. In such a situation, nodes without a shared key can get a diect secure link by agreeing on a secrete key using one of the indirect secure paths which are formed by nodes already sharing pairwise keys.

2) Asymmetric Key-Based Approach: The best-known traditional approach of asymmetric cryptography is the public key infrastructure (PKI) where authentic public keys are required to be distributed. A centralized trusted authority or so-called certification authority (CA) guarantees the authenticity of nodes' public keys. In order to do that, this authority makes digital signatures corresponding to the user's public key, using its public/private key pair. Every node in the network is supposed to know its proper public key. Nodes on the network usually send a signed certificate provided by the CA to other parties to confirm their public key when requested. The CA must manage also the expelled nodes, so for any reason certificates can be revoked.

III. Preliminaries

A. Identity-based scheme

In 1984 Shamir in [2], introduced a new scheme that eliminates the need for certificates. To avoid the trusting problems between the parties in the network, their identities serve as mean to create public keys. With this propriety, Shamir proposed an identity based cryptography (IBC). After Shamir proposal, several schemes have been presented based on IBC. Unfortunately, none of them was fully satisfactory. In 2001, Boneh and Franclin in [3], presented an identity-based encryption scheme (IBE) based on properties of bilinear pairings on elliptic curves, which is the first fully functional, efficient and provably secure identity-based encryption scheme. In the same year, Boneh, Lynn and Shacham [6], proposed a basic signature scheme (BLS) using pairings, that has the shortest length among signature schemes in classical cryptography [7]. This type of identity-based cryptography is also named Pairing-based Cryptography (PBC). Based on [3], [6], a number of schemes has been proposed and most of recent proposals for MANETs in the literature use PBC.

The IBC is a subcategory of asymmetric cryptography. Instead of generating a random public/private pair of keys, each party chooses its keys depending on its identity. For example: name, address or telephone number, making sure that it uniquely identifies the party and it is available at any time for others. The need for a certification authority (CA) and public key certificates (PKCs) are eliminated in IBC. Instead, another trustworthy authority, called a Private Key Generator (PKG), is used to generate the private key corresponding to a given identity as illustrated in figure 2. Before sending private keys, the PKG have to verify the validity of the user's identity.

The keys generated by the PKG are a short-lived in general. Hence, as soon as the private key expires its owner must call a key freshness from the PKG. The sender in addition, must not wary about the expiring time of the receiver private key and it can encrypt any message using the public key at any time. The private key shoud stop being freshed as soon as the identity of the user is revoked. A copy of all generated private keys is kept by the PKG. For this reason, if it gets compromised all data can be decrypted. Threshold cryptography can be a solution for this problem.

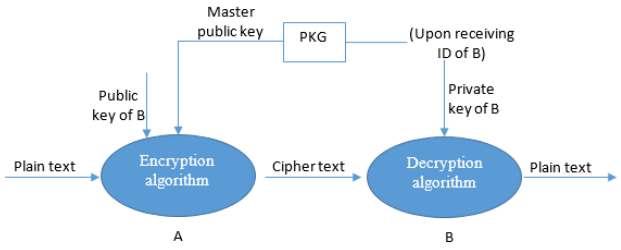


Fig. 2. Identity Based encryption.

B. Threshold cryptography

Despite the great success achieved by the PKI approach, it is difficult to apply in MANETs for many reasons. A centralized CA is not suitable for this type of networks. This authority can be the single point of failure. If it happens that the CA is compromised, all of the system will fall down. In this case, adversary can sign or revoke any certificate and consequently can impersonate any node. The other case is when the CA cannot be accessible. In such a situation, nodes cannot be able to update or change their keys. Moreover, new nodes will be unable to get their certificates. Replicate the CA can solve the availability problem but can lead to other problems as the compromise of any replica can impact the whole system. Another solution is to distribute the CA service among the network nodes. A group of nodes can share the responsibility of the CA in a distributed where the private key is divided into shares and each node can get one. Approaches that require all the network nodes to play the CA role are not feasible because of the dynamic characteristic of the MANETs. For that reason, threshold cryptography can provide the solution. An (n, k) threshold cryptography scheme allows n entities to share the ability to perform a cryptographic operation so that any k entities suffices to perform this peration jointly, whereas it is infeasible for at most $k-1$ entities to do so, even by collusion [8]. Shamir was the first one who came with this idea in 1979 [9]. Its proposal was based on polynomial interpolation. To distribute a secret S among n users, a trust authority chooses a large prime q, and randomly selects a polynomial f over q of degree $k-1$, such that $f(0) = S$. The trust authority computes each user's share using $S_i = f(i) \mod q$ and securely sends the share S_i to user i. Then any k shareholders can reconstruct the secret using the Lagrange interpolation.

IV. ID-Based Key Management in MANETs

In this section, we summarize the most interesting recent proposals in the literature. Table I gives an overview of the basic characteristics of the IBC key management schemes. The IBC is often combined with other techniques for better adaptability. The table II shows the capabilities of the keys generation, update and distribution.

The IBC has several advantages. It is presented as a workable solution against the large number of problems related to the public key infrastructure. The private keys are short and they are easy to generate and store. The public keys are implicitly associated with users' identities, with no need to distribute and to store any certificate or the public key of the certification authority. Thus, eliminate the certificate distribution process, the storage and the transmission of the public keys. However, if the private key generator has been compromised, all the packets protected during the lifetime of the public/private key pair used by this server are also compromised; which makes the PKG valuable target for adversaries.

To eliminate the single-point of failure, excluding the need of a centralized server in IBC, resist mobile adversaries attack, ensure availability of network services, eliminate the interdependency cycle between secure routing and security services, avoiding congestion and to reduce the overhead, the PKG task is distributed among network nodes throw threshold cryptography. Using (t, n) threshold cryptography, only t nodes are needed to obtain requesting node keys, thus resisting to the less connectivity problems. The threshold scheme is also used to secure the key generation, distribution and update, which is shown in Table II. In the (t, n) threshold scheme the value of t must be chosen carefully to ensure security while keeping the service availability, that makes an (n, n) threshold system results the maximum security but leads to poor availability.

Furthermore, to ensure a secure transmission of the IBC parameters and reduce the communication overhead and the computational cost, the pairing-based key agreement techniques are used in several proposals. Based on this method and with a few calculation, each two different nodes can agree on a shared secret key that set up a secure link between all network nodes. Another technique used to communicate in a secure manner is a Self-Organized Key Management Scheme. In this scheme, nodes are able of assuring themselves without any sort of authority. The relationships between the nodes are not known beforehand so without depending on the common authority nodes must establish security relationship among themselves after network formation. The proposed scheme in [15] assumes that every node act as a PKG and the trust relationship is bidirectional. Following that manner, the network nodes can only trust their 1-hop neighbors and using this, a trust secure communication is formed.

To support more flexible cryptographic algorithms, encryption systems and node multiple keys, a new identity-based node key management scheme combined with next generation protected storage of Portable Trusted Platform

TABLE I
SUMMARY OF IDENTITY-BASED KEY MANAGEMENT SCHEMES.

Scheme	Focus on/main features	Key Update	Key Agreement	Weaknesses
[10]	• Threshold secret sharing (To resist mobile adversaries attack and ensure availability of network services) • Bilinear Pairing computation (To reduced communication overhead and computational cost) • Elliptic Curve Cryptography ► Main goal: construction of three level security communication framework through tree and cluster structure Ad hoc networks.	✓	X	• One change needs all system update • Compromising one node threats all lower layer nodes.
[11]	• Threshold cryptography. • Bilinear pairing Cryptography. ► Main goal: eliminating the need of a centralized server.	X	✓	• Uses the hardness of discrete logarithm problem which can lead to computational problems and extensive use of many resources.
[12]	• Bilinear pairing Cryptography. ► Main goal: eliminating the interdependency cycle between secure routing and security services.	✓	X	• One PKG leads to a single point of failure.
[13]	• Threshold secret sharing (To distribute the PKG task). • Bilinear pairing Cryptography. ► Main goal: creating a complete and fully self-organized ID-based key management scheme for MANETs.	✓	X	• Since tne number of ompromised nodes can reach t, the threshold scheme must be $(m, t+1)$ insteadd of (m, t). • Nodes cannot construct functional routes in bigger areas and the system cannot complete all its operations. • The more the threshold t increases, the less the system efficiency will be.
[14]	• Combination of two unique user's identification parameters *id* and *time*. • Threshold cryptography (To distribute the PKG task). ► Main goal: to reduce the possibility of impersonation and enhance the authentication process of user in the network.	✓	X	• Need to communicate with PKGs all the time (consume a lot of energy). • The keys are changed all the time.
[15]	• A Self-Organized Key Management Scheme ► Main goal: to make the nodes capable of ensuring the credibility of themselves when it is needed in order to communicate in a secure manner.	X	✓	• Needs many resources and consumes a lot of energy (share a secret with every other user, which could lead to considerable overhead). • Two successive malicious nodes can easily corrupt the system. • Easy to issue a certificate for a non-existent node, and try to convince the others that such a node does exist in the network.
[16]	• Next generation protected storage of portable trusted platform module (PTPM.next). ► Main goal: To resolve the problems of node multiple keys management and protected storage in MANETs.	X	X	• Intensive computations.
[17]	• Key pool. • Pairing based key generation. • Threshold cryptography (to distribute the PKG task). ► Main goal : eliminating the interdependency cycle between secure routing and security services.	X	✓	• All initial nodes are required to generate the master private key. • Lack of authentication, integrity. . . and so on, before the deployment of the IBC system. • Assumption that initial nodes are not malicious.
[18]	• Detailed implementation of [17].	X	✓	• An (n, n) threshold cryptography. • All initial nodes are required to generate a new PKG.
[19]	• ID + secret value. • Bilinear pairing based cryptography. ► Main goal: encryption, decryption and signatures.	✓	X	• Too much messages to exchange that consumes a lot of energy. • The refreshment of the keys with Short-Term Refreshment requires to replay the whole process.
[20]	• Threshold cryptography. • Multiple variables polynomial. • Intrusion Detect System "IDS" (to select the best nodes to work as the PKG). ► Main goal: creating a distributed hierarchical key management scheme where an optimally selected nodes can updates nodes keys easily.	✓	✓	• Knowing the master secret key of the system exposes the secret keys of all nodes. • Easy to calculate the shared key between two leaf nodes (it is the combination of their identity). • IDS can be a single point of failure.
[21]	• Threshold cryptography. • Group polynomial equation for generating the unique ID for each node. ► Main goal: securely share the secrets, enable a secure and reliable communication, avoid congestion and reduce the overhead.	X	✓	• Needs registration with the home network. • The network administrator is a single point of failure.
[22]	• RSA. • AODV-routing protocol. ► Main goal: Combine data packets and multicasting it in the network.	✓	Each group has its own updated common group key	• Not enough details are given. • One server which is the single point of failure.

TABLE II
SUMMARY OF ID-BASED KEY GENERATION AND DISTRIBUTION SCHEMES.

Scheme	Certification Authority	Master Key pair generated by	PKG	Share of private key transmission	Share update
[10]	X	N nodes in a distributed manner	Three level PKGs	Private channel.	Cluster nodes.
[11]	T PKGs	The initial nodes in a distributed manner	K among N	Private channel	X
[12]	PKG offline	PKG	One PKG	Public channel	PKG
[13]	Distributed PKG	Nodes that participate in the group initialization called founding nodes	Founding nodes in a distributed manner	Not mentioned	PKG
[14]	PKG offline	Not mentioned	K among N	No transmission, each node creates its own key	The nodes themselves.
[15]	X	The nodes themselves	N	No transmission, each node creates its own key	X
[16]	PKG Offline	PKG	One PKG	No transmission, each node creates its own key	X
[17], [18]	PKG Offline	The initial nodes in a distributed manner	Fully distributed	Secret channel	X
[19]	X	The nodes themselves	X	No transmission, each node creates its own key	Not mentioned
[20]	IDS	The root authority.	Multiple PKGs	X	X
[21]	X	Not mentioned	X	X	X
[22]	X	Mentioned brifely	X	X	X

Module (PTPM.next) is proposed in [16]. According to the authors, PTPM is viewed as functionally equivalent to a high-performance USB key. This USB key is used to store, protect and manage a different multiple of keys to support the node multiple keys management schemes. The authors improve PTPM to PTPM.next to support the MANET characteristics.

The hierarchical method has also used in ID-based key management schemes. In this approach, a tree structure is constructed and the depth of the hierarchy is selected. The public/private keys can be deduced from the root to the leaf or in the opposite direction where the threshold cryptography can be used here. This mechanism is used to improve the network security and to reduce traffic and computation costs.

V. WEAKNESSES OF IBC

Even though the many attractive proprieties of IBC to MANET, there are some problems that steel remains. In this section, we will slightly address some of those problems.

Identity Disclosure : the main idea of the IBC is the identity that can be used as the public key. The problem that can be found is the exposition of the identity to all other nodes. In some networks, this can be a serious issue such as battlefield network.

Key Escrow : the PKG that generates the private key knows all the network private keys and can eavesdrop the traffic or impersonate it. Even this feature can be an advantage in some cases; such as military ; but steel undesirable in others.

Key Revocation : key disclosures are very likely in MANETs due to the weak physical protection of nodes. Frequent rekeying is either computational challenging to solve using distributed on-line key generation or useless with off-line key generation.

VI. CONCLUSION

Over the years, several cryptographic techniques had been proposed in the literature for securing Mobile Ad hoc networks. Identity-based cryptography has emerged recently. It is a special form of PKI which eliminates the need for certificates. In this article, we discussed the important identity-based key management schemes for MANATs proposed in the last decade. Most of the proposals manage to enhance this technique by combining it with various mechanisms, so they can improve it and benefit from their advantages to make it more suitable for MANETs. The comparative study we conducted has revealed many advantages together with some drawbacks and challenges that still need to address.

In the area of securing MANETs, the IBC is widely applied and is a promising solution. However, there are no perfect solutions yet because of the unaddressed issues. Therefore, an important step that cryptography and security engineers should focus on, is to explore deeper in these research areas and try to establish a general key management framework.

As a future work, we attempt to survey the large applications of IBC, not only in key management but also in other areas. Also, we will try to take benefits of this work to come up with a new idea choosing the best techniques to give a better solution for securing the MANETs.

REFERENCES

[1] K. Zhao, L. Huang, H. Li, F. Wu, J. Chu, and L. Hu, "A survey on key management of identity-based schemes in mobile ad hoc networks," *Journal of Communications*, vol. 8, no. 11, pp. 768–779, 2013.

[2] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Workshop on the theory and application of cryptographic techniques*. Springer, 1984, pp. 47–53.

[3] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Annual international cryptology conference*. Springer, 2001, pp. 213–229.

[4] F. Anjum and P. Mouchtaris, *Security for wireless ad hoc networks*. John Wiley & Sons, 2007.

[5] H. Anne Marrie, W. Eli, M. Stig F, R. Chunming, K. Oivind, and S. Pal, "A survey of key management in ad-hoc networks," *IEEE Communications surveys & tutorials*, vol. 8, no. 3, pp. 48–66, 2006.

[6] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *International conference on the theory and application of cryptology and information security*. Springer, 2001, pp. 514–532.

[7] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," *IEEE Communications surveys & tutorials*, vol. 14, no. 2, pp. 380–400, 2011.

[8] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE network*, vol. 13, no. 6, pp. 24–30, 1999.

[9] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[10] W. A. Xiong and Y. H. Gong, "Secure and highly efficient three level key management scheme for manet," *WSEAS Transactions on Computers*, vol. 10, no. 1, pp. 6–15, 2011.

[11] A. C. Chan, "Distributed private key generation for identity based cryptosystems in ad hoc networks," *IEEE Wireless Communications Letters*, vol. 1, no. 1, pp. 46–48, 2011.

[12] S. Zhao, R. Kent, and A. Aggarwal, "A key management and secure routing integrated framework for mobile ad-hoc networks," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1046–1061, 2013.

[13] E. da Silva and L. C. P. Albini, "Towards a fully self-organized identity-based key management system for manets," in *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2013, pp. 717–723.

[14] S. Honarbakhsh, L. B. A. Latif, B. Emami *et al.*, "Enhancing security for mobile ad hoc networks by using identity based cryptography," *International Journal of Computer and Communication Engineering*, vol. 3, no. 1, p. 41, 2014.

[15] M. L. Pura and D. Buchs, "A self-organized key management scheme for ad hoc networks based on identity-based cryptography," in *2014 10th International Conference on Communications (COMM)*. IEEE, 2014, pp. 1–4.

[16] G. Yang, J. Liu, and L. Han, "An id-based node key management scheme based on ptpm in manets," *Security and Communication Networks*, vol. 9, no. 15, pp. 2816–2826, 2016.

[17] K. A. Mehr and J. M. Niya, "Securing mobile ad hoc networks using enhanced identity-based cryptography," *ETRI Journal*, vol. 37, no. 3, pp. 512–522, 2015.

[18] K. Adli Mehr and J. Musevi Niya, "Security bootstrapping of mobile ad hoc networks using identity-based cryptography," *Security and Communication Networks*, vol. 9, no. 11, pp. 1374–1383, 2016.

[19] P. Subbulakshmi and S. Vimal, "Secure data packet transmission in manet using enhanced identity-based cryptography (eibc)," *International Journal of New Technologies in Science and Engineering*, vol. 3, no. 12, pp. 35–42, 2016.

[20] F. Wang and S. Hu, "A novel key management scheme for secure mobile ad hoc networks," 2016.

[21] J. Chandrashekar and A. Manoharan, "An identity based key management technique for secure routing in manet," *International Journal of Intelligent Engineering and Systems*, vol. 11, no. 6, pp. 33–43, 2018.

[22] M. S. Rani, R. Rekha, and K. V. N. Sunitha, "Id based multicast secret-key management scheme (skms) in manets," *International Journal of Intelligent Engineering and Systems*, vol. 11, no. 6, pp. 199–208, 2018.

Biometric Image Encryption Scheme based on Modified Double Random Phase Encoding System

Amina Yahi
ETA Laboratory, Department of Electronics
University of Bordj Bou Arreridj
Bordj Bou Arreridj 34030, Algeria
amina.yahi994@gmail.com

Tewfik Bekkouche
ETA Laboratory, Department of Electromechanics
University of Bordj Bou Arreridj
Bordj Bou Arreridj 34030, Algeria
bekkou66@hotmail.com

Mohamed El Hossine Daachi
ETA Laboratory, Department of Electronics
University of Bordj Bou Arreridj
Bordj Bou Arreridj 34030, Algeria
mohamed.daachi@univ-bba.dz

Nacira Diffellah
ETA Laboratory, Department of Electronics
University of Bordj Bou Arreridj
Bordj Bou Arreridj 34030, Algeria
diffellahn@gmail.com

***Abstract*—In this paper, an opto-digital encryption scheme based on a modified Double Random Phase Encoding (DRPE) system is proposed. Two biometric modalities are used in this work which is the face and the corresponding finger print of the same person. Firstly the face biometric image is encrypted chaotically using the permutation-diffusion architecture. Then obtained encrypted face is multiplied element by element by a constructed mask formed by injecting the finger print image within the phase of this mask. The obtained result will be transformed into a frequency domain by the two-dimensional Fourier transform or any of its derivatives, resulting complex image is exactly the encrypted biometric image. Experiment computer simulations confirm the efficiency of this work in terms of histogram analysis, loss data and sensitivity test when compared with existing works.**

Keywords*—*Biometric images, DRPE, Opto-digital, Permutation-diffusion, Finger print, Chaotically, Fourier transform, histogram analysis.

I. INTRODUCTION

Today, in this era of information and communication technology, where we live more digitally than we believe, especially after the global quarantine because of the spread of coronavirus. As a result, unprecedented increase in the use of social media by sharing, sending and receiving of information, even for things that didn't need the use of online connectivity, their digitalization was required, and not optional, as it was before. For example: videoconferences, e-health, e-commerce, online education, online meeting and so on.

Image plays an important role in the data transfer. Given the privacy and the confidentiality of most of them like military images, medical images etc... Thus, image security has become increasingly essential, and a key challenge to protect it from digital attacks such as thefts, espionage, modifications, denigration…

To defeat the problem mentioned above, many researchers invested to develop several secure types of algorithms such as steganography [1,2], watermarking [3,4], and image encryption [5,6]. Since ancient times to today, Image Encryption is considered one of the most effective protection methods, which is defined as the method of transforming the whole image into an unrecognized one [7].

We distinguish two types of encryption domains, spatial domain which is based on changing the pixels positions of the plain image under the control of chaotic sequences [8] and changing their values by means of an XOR operator [9], these two steps named respectively diffusion and confusion.

Regarding image encryption in the frequency domain, it's performed using fast transform algorithms, such as fast Fourier transforms, Hadamard transforms, and Hartley transform [9].

The optical image encryption scheme is essentially based on the famous double random phase encoding (DRPE), by using the discrete Fourier transform (DFT) [9], presented for the first time by Refregier and Javidi [11]. It consists to use two random masks, one in the spatial plane and the other in the Fourier plane, in order to encrypt the primary image into stationary white noise [10, 11]. In order to give more effective results, DRPE has undergone many modifications, such as the use of parametric transforms [12,13] instead of bidirectional FT and their independent parameters are beneficially exploited as an additional secret key. Furthermore, integration of opto-digital hybrid DRPE versions by introducing a scrambling therein the DRPE system with the help of chaotic map [9,14]. Even so, these DRPE versions need more improvement.

In our knowledge , no existing works have proposed schemes of biometric encryption images based on DRPE system, so that, in this paper we have proposed an efficient opto-digital biometric images encryption scheme by modifying the double Random Phase Encoding (DRPE) system, it consists in substituting the first block of the DRPE composed of the first mask applied in the spatial domain and the first Fourier transform or its derivatives by a chaotic encryption in spatial domain applied to the face image, the finger print is used here as a key of encryption. The resulting encrypted image is applied to the second stage of DRPE, where it is multiplied element by element by a constructed mask by introducing the above finger print image within the phase of this mask and finally transforming the result obtained using the DFT to obtain the encrypted image . In order to give more details, we have organized this article as follows: the section 2 presented the proposed encryption and decryption scheme, the third section shows simulation

results and security analysis, finally, section 4 concludes the paper.

II. Proposed encryption/Decryption method

A. PLCM chaotic map

Chaotic maps are known to have attractive cryptographic properties such as high sensitivity to their initial parameters, ergodicity, and pseudo-randomness [13-15]. In our proposed encryption scheme, we exploit the piecewise linear chaotic map (PLCM) proposed in [16] and expressed iteratively as:

$$z_{k+1} = F(z_k, \lambda) = \begin{cases} \frac{z_k}{\lambda}, & 0 \le z_k < \lambda \\ \frac{z_k - \lambda}{0.5 - \lambda}, & \lambda \le z_k < 0.5 \\ F(1 - z_k, \lambda), & 0.5 \le z_k < 1 \end{cases} \quad (1)$$

Where z_0 is the initial condition parameter and $\lambda \in (0,0.5)$ is the control parameter.

B. Encryption scheme

The encryption process is detailed in the following steps:

1. Let P1 be the face image of size (NxN), first we calculate the normalized pixels average value M expressed by the following equation:

$$M = \frac{1}{255}\sum_{ij}^{N} \frac{P1_{ij}}{N \times N} \quad (2)$$

2. Let P2 be the finger print image of size $(N \text{x} N)$, then we calculate the normalized pixels average value MM expressed by the following equation:

$$MM = \frac{1}{255}\sum_{ij}^{N} \frac{P2_{ij}}{N \times N} \quad (3)$$

3. Generate a PLCM chaotic map of size $\left(1 \text{x} N^2\right)$, where :

$$\lambda_{11} = mod\big((\ \lambda_1 + M + MM), 1\big) \quad (4)$$

$$Z_{11}(1) = mod\big((Z_1 + M + MM), 1\big) \quad (5)$$

Where Z_1 is the initial condition parameter and λ_1 is the control parameter of the PLCM chaotic map.

4. As permutation step, reshape P1 into $\left(1xN^2\right)$ and let's name it $V1$, then reorder the pixels of $V1$ according to the chaotic map permutation vector.

5. Re-generate another PLCM chaotic map of the same size, where :

$$\lambda_{22} = mod\big((\lambda_2 + M + MM), 1\big) \quad (6)$$

$$Z_{22}(1) = mod\big((Z_2 + M + MM), 1\big) \quad (7)$$

Where $Z_2$is the initial condition parameter and λ_2 is the control parameter of the second PLCM chaotic map.

And to get values varies between 0 and 255, the equation used is:

$$V2(i) = Z_{22}(i) \times 255 \quad (8)$$

6. As confusion steps, we apply the XOR operator recursively between the vector $V1$ and the vector $V2$ to give a resulting vector VV, according to the following formula:

$$VV(i) = V1(i) \oplus V2(i) \oplus VV(i-1) \quad (9)$$

7. Reshape VV into VVV of size (NxN).
8. Construct the mask by injecting the matrix of fingerprint within the phase of the constructed mask to obtain :

$$mask = e^{j2\pi P2} \quad (10)$$

9. Multiply the matrix *VVV* by the mask element by element to obtain a complex valued matrix *M1*.
10. Transform the obtained result using the discrete fractional Fourier transform (DFrFT) to obtain the encrypted image expressed by :

$$E = F^a(M1)F^b \quad (11)$$

C. Decryption scheme

The decryption process takes exactly the steps of encryption process in inverse manner (Fig. 2).

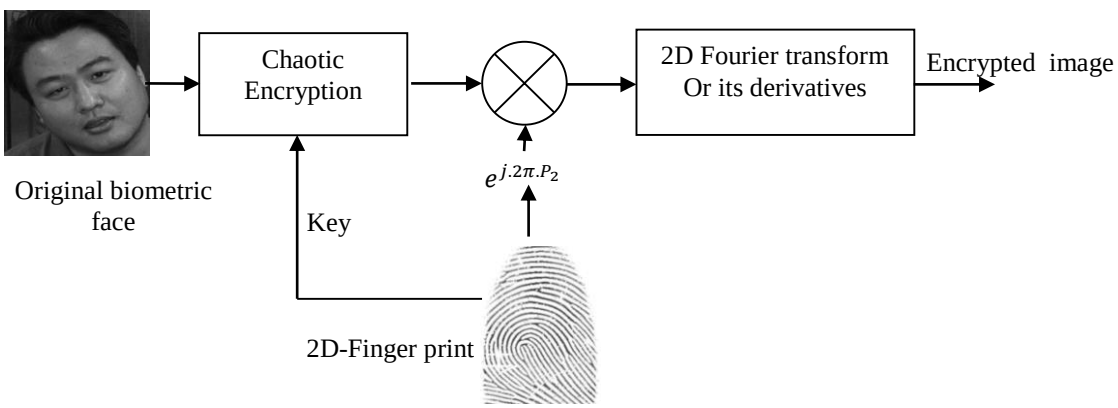


Fig. 1. Proposed encryption scheme.

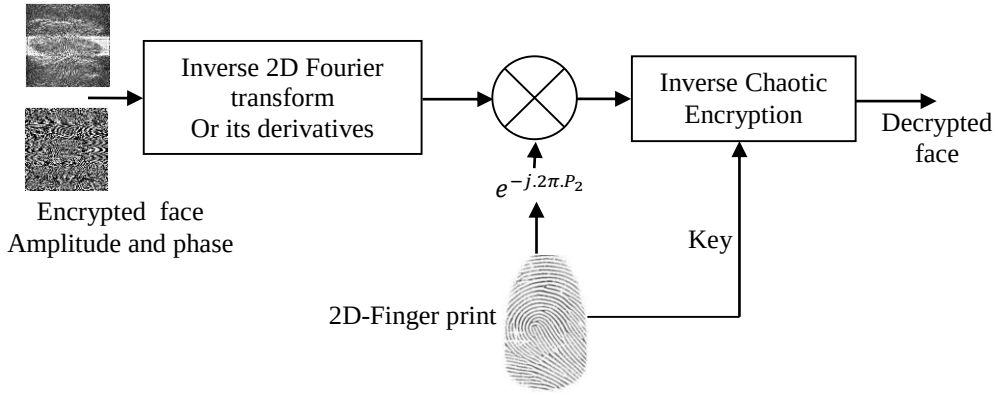


Fig. 2. Proposed decryption scheme.

III. Simulation Results and Security Analysis

The used test images are those of (256×256) from a face data set developed by the center for Signal and Image Processing at Georgia Institute of Technology [17]. The reason why we have chosen it was because it contains a large number of images for each person, and it was used in several research works. The two PLCM chaotic sequences having the following parameters: (λ_1 = 0.2567; Z_1 = 0.1428), (λ_2 = 0.3567; Z_2 = 0.2428), and the fractional orders of the discrete fractional Fourier transform (DFRFT) (a, b) are randomly selected from the interval [0, 1]. The Results of simulations are performed under environment MATLAB 8.1.0.604 (R2013a).To evaluate the proposed method, we have used different metrics: the histograms, the mean square error (MSE) and the standard correlation coefficient which are widely defined in previous works.

A. *Histograms analysis*

Fig. 3. and Fig. 4. show the original images and the result of their encryption and histograms. We note that the histograms of the original images is clearly and completely different, on the other hand, the histograms of amplitude (or phase) of the encrypted images are very similar, which confirm that no information about the original image can be learned by an attacker. Thus, the proposed scheme is robust to histogram analysis.

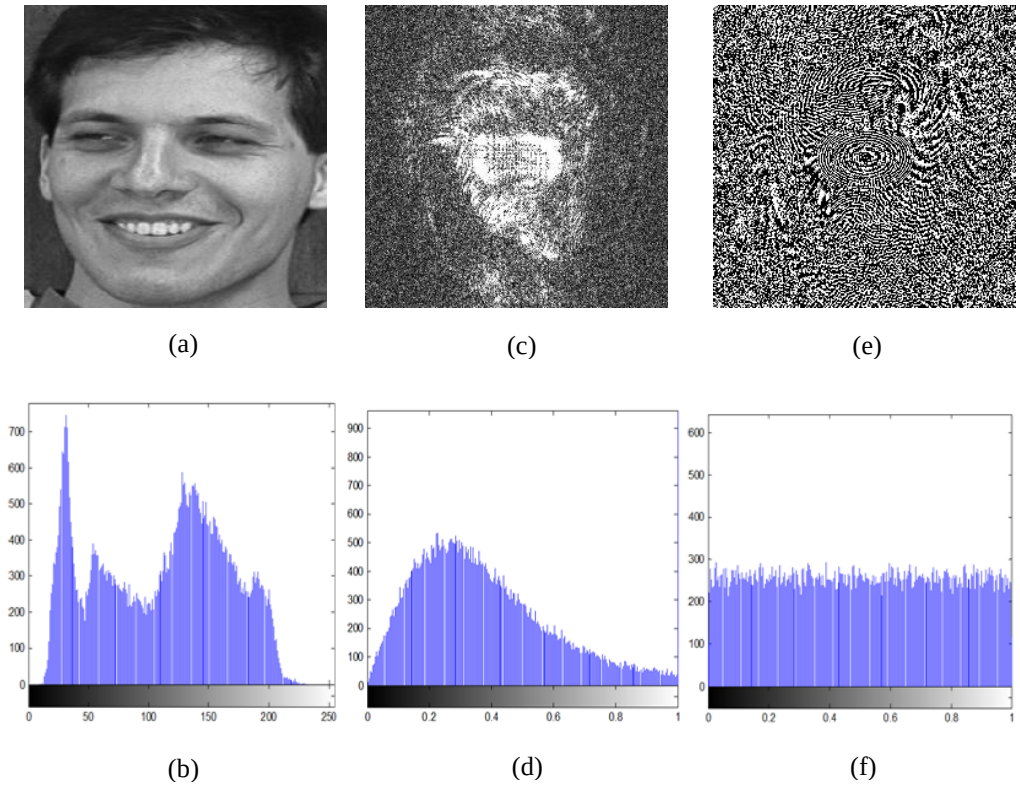


Fig. 3. Histogram analysis of biometric original image 1: The original face image 1 (a), original image histogram (b), the amplitude encrypted image (c), amplitude encrypted image histogram (d), phase encrypted image of (e), phase encrypted image histogram, (f).

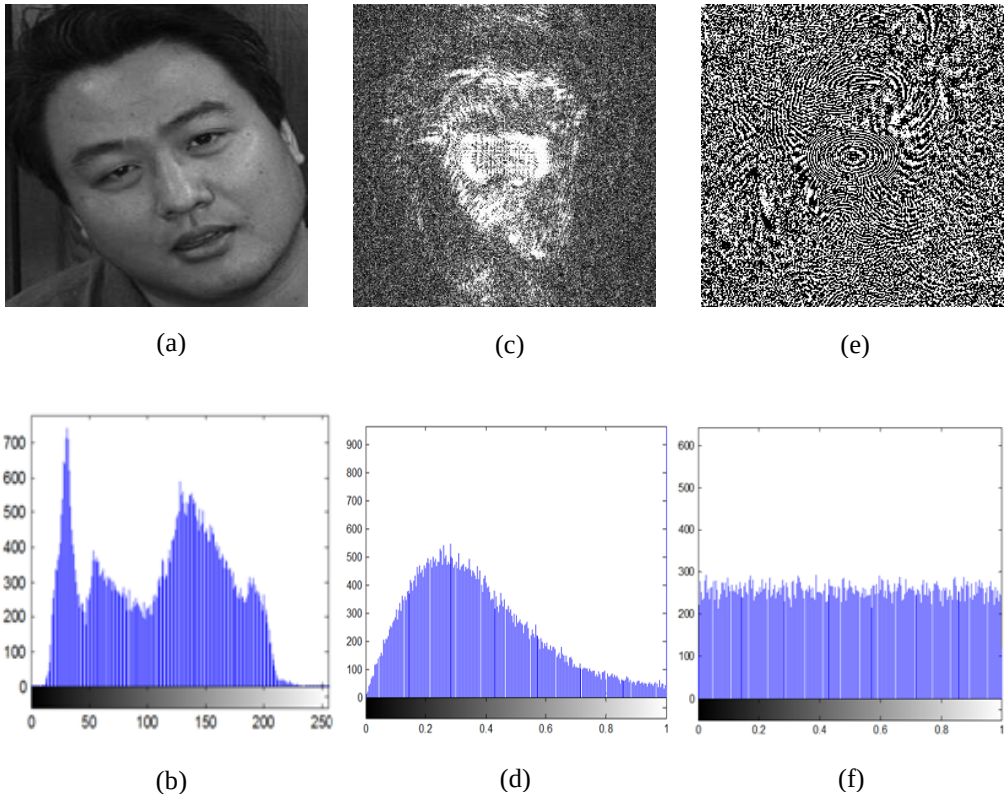


Fig. 4. Histogram analysis of biometric face image 2. The original face image 2 (a), original image histogram (b), the amplitude encrypted image (c), amplitude encrypted image histogram (d), phase encrypted image of (e), the phase encrypted image histogram, (f).

B. Correlation analysis

It is used to calculate the correlation between two images, the plain image and the encrypted image in order to check the degree of similarity between all the pixels on the encrypted image and their opposites on the original image. Results are summarized in TABLE I.

Table. 1. Correlation analysis

File name	Correlation between biometric original and encrypted face images
Face image 1	0.165
Face image 2	0.223

C. Loss data

During image transmission, it is possible that it happen to it several data loss and noise, in order to test the robustness of our method against error transmission, we applied a loss of data to our encrypted images. In the first case we consider a loss data of **25%**, as shown in Fig. 5, we can notice that the decrypted image is still recognizable despite the distortion. Thus, the resistance of the proposed method to data loss.

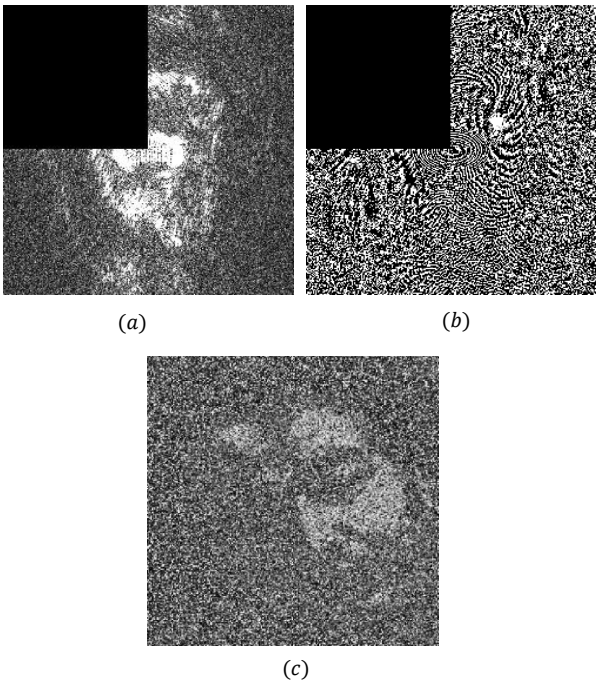
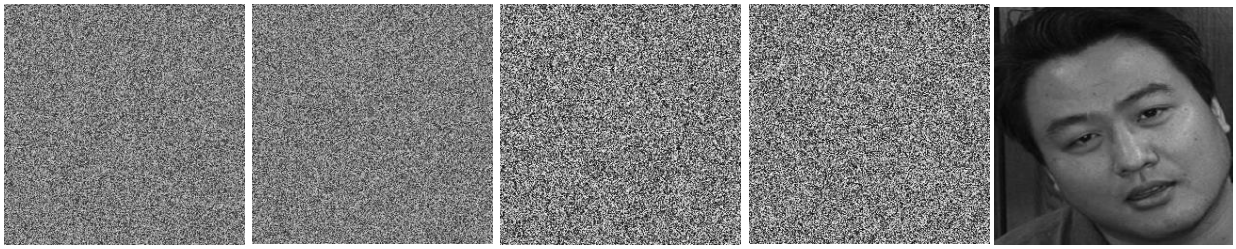


Fig.5. Loss data test: (a) Amplitude encrypted face with 25% loss data (b) Phase encrypted face with 25% loss data (c) The corresponding decrypted face with 25% loss data.

D. Sensitivity analysis



(a) (b) (c) (d) (e)

Fig.6. Sensitivity test: Decrypted face 2 with $(a)\ \lambda'_{11=}\lambda_{11}+10^{-15}$ $(b)\ z'_{11}=z_{11}+10^{-15}$ $(c)\ \lambda'_{22\ =}\lambda_{22}+10^{-15}$ $(d)\ z'_{22}=z_{22}+10^{-15}(e)$ Correct key.

The sensitivity of the secret key is an essential characteristic for a good encryption system, in order to guarantee the security of the latter in the face of several attacks.

Let k_1 be the encryption key of the proposed method, which is composed from the two PLCM chaotic sequences, and the fractional orders a and b of the discrete fractional Fourier transform DFRFT as well as the fingerprint image $k_1(\lambda_{11}, z_{11}, \lambda_{22}, z_{22}, a, b)$, the corresponding decryption key is designed by $k_2(\lambda'_{11}, z'_{11}, \lambda'_{22}, z'_{22}, a', b')$. If the encryption key is exactly the decryption one i.e., $(k_1 = k_2)$ the decrypted image is identical to the original image Fig. 6 (e).

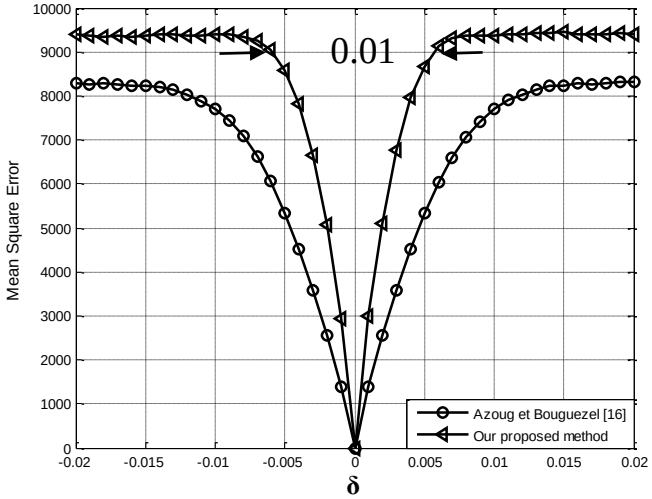


Fig. 7. The value of MSE of our method in terms of the deviation error δ compared with [16].

To test the sensitivity of the encryption key, we make a minor variation in one parameter of the order of 10^{-15} and we set the others parameters at their fixed values. The different cases are depicted in Fig. 5. $(a), (b), (c), (d)$. Obtained results of simulations show that the limit of the appearance of the image decrypted in the clear is of the order of 10^{-16}, this confirms the high sensitivity of the proposed method which is of the order of 10^{-15} for the different parameters of the encryption key. In regards to The sensitivity of the encryption key to the fractional order parameters of the DFRFT, we make a modification δ which varies between -0.02 and 0.02 in the two fractional parameters a and b, then we compute the mean square error (MSE).

From Fig. 7, we can notice that the proposed method present a big sensitivity against encryption key errors and prove their superiority when compared with the method of the reference [16].

E. Key space

The image encryption method is secure if it has the largest possible encryption key space, regarding our method we have the first key with four parameters, the precision of each one is of 10^{15}, the second key is the two fractional parameters a and b, the space of this latter is $1/0.01$ Whereas the number of modifications possible in the finger print image is not considered. Thus, the total key space is $10^{15\times4} \times 100 \times 100 = 10^{64} \cong 2^{192}$, and this indicates that is sufficiently strong against the brute-force attack. , and widely sufficient compared to the value required in cryptosystems [18].

F. Statistical tests analysis

The statistical tests are used in order to study the randomness of random and pseudorandom number generators. NIST is one of the most famous and efficient randomness tests, it calculates the p-value, wich must be ≥ 0.01. table 2 shows the results of the 15 tests of Nist, we can observe that all the tests are passed.

Table .2. NIST results

Tests	P-value	Results
Frequency	0.88	passed
BlockFrequency	1.00	passed
Runs	0.49	passed
LongestRunsOfOnes	0.24	Passed
Rank	0.85	Passed
Spectral	0.04	Passed
Non Overlapping Template Matching	0.24	passed
Overlapping Template Matching	0.12	passed
Universal	0.57	Passed
Linear Complexity	0.48	Passed
Serial	0.43	Passed
Approximate Entropy	0.99	passed
Cumulative Sums	0.33	Passed
Random Excursions	0.26	Passed
Random Excursions Variant	0.75	Passed

IV. CONCLUSION

Nowadays, the number of digital images is widely used in several online applications. The aim of this study is to ameliorate their security and privacy by developing an opto-digital encryption algorithm based on a revised DRPE system. Our proposed algorithm combines both the encryption in the spatial domain and the frequency domain on two biometric identities, the face as the secret image and the supposed corresponding fingerprint of the same person as a secret key. The results of the simulation using the MATLAB environment, in comparison with the state of the art algorithms have demonstrated superior performance, especially in term of key space and key sensitivity.

The data set used for the evaluation phase developed by the center for Signal and Image Processing at Georgia Institute of Technology [17]. The reason why we have chosen it was because that contains a large number of images for each person it was used in several research works.

As future works, we aim to improve even more this proposed encryption method.

REFERENCES

[1] C. Wang, H. Wang, Y. Ji, "Multi-bit wavelength coding phase-shift-keying optical steganography based on amplified spontaneous emission noise," Opt. Commun. 407, 1–8 (2018).

[2] R.G. Zhou, J.Luo, X.A.Liu, C.Zhu , L.Wei, X. Zhang, "A novel quantum image steganography scheme based on LSB," Int. J.Theor. Phys, 57(1), 1–16 (2018).

[3] L.Cao, C.Men, R.Ji, "Nonlinear scrambling-based reversible watermarking for 2d-vector maps. Vis. Comput,"29(3), 231–237(2013).

[4] Q.Luong, "A blind image watermarking using multiresolution visibility map," J. Glob. Optim, 49(3), 435–448 (2011).

[5] M. Kaur, V.Kumar, "Fourier-mellin moment-based intertwining map for image encryption," Mod. Phys. Lett, B 32(9), 1850115 (2018).

[6] L. Huang, S. Cai, M. Xiao, X. Xiong, "A simple chaotic map-based image encryption system using both plaintext related permutation and diffusion," Entropy, vol. 535 (2018), pp. 20(7),

[7] D. Herbadji, A. Belmeguenai, N. Derouiche, H. Liu, "Colour image encryption scheme based on enhanced quadratic chaotic map," IET Image Processing., vol. 14(2020), pp. 40-52.

[8] C. E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, Vol. 28(1949), no. 4, pp. 656–715.

[9] T. Bekkouche, « Développement et implémentation des techniques de cryptage des données basées sur les transformés discrètes," Doctorat these in Electronics, Setif university, vol. 103(2018).

[10] P. Refregier, B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett., vol. 20(1995), pp. 767–769.

[11] B. Javidi, A. Sergent, G. Zhang, L. Guibert, "Fault tolerance properties of a double phase encoding encryption technique," Opt. Eng., vol. 36(1997), pp. 992–998.

[12] R. Matthews, "On the derivation of a chaotic encryption algorithm," Cryptologia, vol. 4 (1989), pp. 29–42.

[13] H. Zhou, X. Ling, " Problems with the chaotic inverse system encryption approach, " IEEE Trans. Circ. Syst, vol. 44 (1997), pp. 268–271.

[14] T. Bekkouche, S. Bouguezel, " A recursive nonlinear pre-encryption for opto-digital double random phase encoding," Optik., vol. 158 (2018), pp. 940-950.

[15] A. Baranovsky, D. Daems, "Design of one-dimensional chaotic maps with prescribed statistical Properties," International Journal of Bifurcation and Chaos, Vol. 5(1995), no. 6, pp. 1585–1598.

[16] S.E. Azoug, S. Bouguezel, "A non-linear preprocessing for opto-digital image encryption using multiple-parameter discrete fractional Fourier transform," Opt. Commun, vol. 359 (2016), pp. 85–94.

[17] Georgia Tech face database, available at: http://www.anefian.com/research/face_reco.htm.

[18] G. Alvarez, S.Li, "Some basic cryptographic requirements for chaos based cryptosystems," Int. J. Bifurcation Chaos vol. 16 (2006), pp. 2129–2151.

SIRAT[a] : a Real-Time Indexing Arabic Text Editor Based on the Extraction of Keywords

Tahar Dilekh
LAMIE Laboratory Batna 2 University
Computer Science Department
University of Batna 2
Batna, Algeria
tahar.dilekh@univ-batna2.dz

Saber Benharzallah
LAMIE Laboratory Batna 2 University
Computer Science Department
University of Batna 2
Batna, Algeria
s.benharzallah@univ-batna2.dz

Ayoub Mokeddem
Computer Science Department
University of Batna 2
Batna, Algeria
a.mokeddem@univ-batna2.dz

***Abstract*— Indexing stage in information retrieval process has a great importance as an essential tool for the performance of recall and precision. Despite the many studies that have been done on the indexing conducted in the last few decades, to our knowledge, no study has investigated whether indexing real-time based on keywords extraction is efficient to perform of recall and precision. Moreover, relatively fewer Arabic text indexing studies are currently available despite the enormous efforts put together to satisfy the needs of the growing number of Arabic internet users. This paper suggests a method for Arabic text indexing based on keywords extraction. The proposed method consists of two stages. The first stage conducts a real-time indexing. The second stage is a keywords extraction and updating of initial index taking into account the output of keywords extraction process. We illustrate application and the performance of this method of indexing using an Arabic text editor (SIRAT) developed and designed for this aim. We also illustrate the process of building a new form of Arabic corpus appropriate to conduct the necessary experiments. Our findings show that SIRAT successfully identifies the keywords most relevant to the document. Finally, the main contribution of this experiment is to demonstrate the effectiveness of this method compared to other methods. In addition, the paper proposes a solution to issues and deficiencies Arabic language processing suffers from, especially regarding corpora building and keywords extraction evaluation systems.**

Keywords—NLP[b], Arabic text indexing, Real-Time indexing, Arabic keywords extraction, Arabic information retrieval system.

I. INTRODUCTION

The vast availability of information made it particularly challenging for users to obtain and find relevant and useful information. In this context, Information Retrieval Systems (IRS) have emerged as a tool to address this problem. IRS consists of two stages: the «indexing» and the «search» stages. In the first stage, the descriptors are extracted from documents and prepared to facilitate and accelerate the search process in the second stage. Currently, IRS benefit from the indexing processes, most of which remains under-performing in the extraction of accurate descriptors that contribute to improving the quality of these systems including extracting the semantic of these descriptors. This remains a challenging task of automatic indexing that often requires words or sentences (keywords or keyphrases) as appropriate descriptors of texts. Despite the many studies that have been done on the indexing conducted in the last few decades, to our knowledge, no study has investigated whether indexing real-time based on keywords extraction is efficient to perform of recall and precision. As well as, while the literature consists of many studies concerning various natural languages, there are relatively fewer studies on Arabic language, where the complex grammatical and morphological features of this language make the task of automatic processing even more challenging. In addition to the scarcity and size limitation of required Arabic corpus. Thus, this paper suggests a new type of indexing to contribute to improving the quality of future IRS. The proposed method of indexing consists of two stages. The first stage conducts a real-time indexing where one document is the indexing module. This type of indexing refers to the indexing process that begins directly after the writing of each unit ends. The output of this process give a rise to an initial index. The second stage – under this method- is a keywords extraction and updating of initial index taking into account the output of keywords extraction process. The output of this process leads to a final index of each document. We also illustrate implementing and the performance of this method of indexing using SIRAT, an Arabic text editor, developed and designed for this reason. We also illustrate the process of building a new form of Arabic corpus appropriate to conduct the necessary evaluations. Thus, this study contributes to two key areas of the literature. First, it offers application of SIRAT that have been developed to show the extent to which the integration of a real-time indexer and a keywords extractor into text editors is effective in improving the indexing. Second, the study is conducted on Arabic texts, which contributes to the enrichment and development of Arabic language processing tools. More specifically, to overcome the scarcity and size limitation of the required Arabic corpus.

The remainder of the paper is organized as follows. Section 2 offers an account of the main developments and recent advances of Arabic keywords extraction literature. Section 3 identifies the main characteristics of Arabic language followed by an illustration of the proposed approach in Section 4. Section 5 illustrate implemented applications and analyze the result. Section 6 concludes.

II. LITERATURE REVIEW

Keywords (descriptors) are a subset of words or phrases that can describe the meaning of a document, where several natural language processing applications can benefit from keywords. Unfortunately, most documents do not contain these words. On the other hand, adding high-quality keywords manually is costly, time-consuming, and error-prone. Therefore, this domain has emerged to develop novel algorithms and systems designed to extract keywords automatically.

Keywords extraction has many applications and therefore there are numerous studies that suggest algorithms for approaching that problem [5] [9] [1] [12] [11] [4] [7] [15] [8] [19] [20]. While the majority of these studies deal with the

[a] **S**emantic **I**nformation **R**etrieval for **A**rabic **T**ext project.

[b] **N**atural **L**anguage Processing

English text, there are relatively fewer studies on Arabic language. We present some work related to the automatic Arabic keywords extraction, which helps to improve the quality of Arabic indexing systems.

[7] presented the KP-Miner (KeyPhrases-Miner) system to extract keyphrases from both English and Arabic documents of varied length. This system does not need to be trained on a particular document set in order to achieve its task (i.e. unsupervised learning). It also has the advantage of being configurable as the rules and heuristics adopted by the system are related to the general nature of documents and keyphrases. In general, Experiments and comparison studies with widely used systems suggest that KP-Miner is effective and efficient.

[10] introduced AKEA, a keyphrase extraction - unsupervised- algorithm for single Arabic documents. They relied on heuristics that collaborate linguistic patterns based on Part-Of-Speech (POS) tags, statistical knowledge and the internal structural pattern of terms. They employed the usage of Arabic Wikipedia to improve the ranking of candidate keyphrases by adding a confidence score if the candidate exists as an indexed Wikipedia concept. Experimental results have shown that the performance of AKEA outperforms other unsupervised algorithms as it has reported higher precision values.

[13] presented a keyword extraction system for Arabic documents using term co-occurrence statistical information. In case the co-occurrence of a term is in the biasness degree, then the term is important and it is likely to be a key word. The biasness degree of the terms and the set of frequent terms are measured using $\chi 2$. Therefore, terms with high $\chi 2$ values are likely to be keywords. This technique showed an acceptable performance compared to other techniques.

[14] presented a supervised learning technique for extracting keyphrases of Arabic documents. The extractor is supplied with linguistic knowledge to enhance its efficiency instead of relying only on statistical information such as term frequency and distance. An annotated Arabic corpus is used to extract the required lexical features of the document words. The knowledge also includes syntactic rules based on part of speech tags and allowed word sequences to extract the candidate keyphrases. The experiments carried out show the effectiveness of this method to extract Arabic keyphrases.

[6] presented a framework for extracting keyphrases from Arabic news documents. It relies on supervised learning, Naïve Bayes in particular, to extract keyphrases. The final set of keyphrases is chosen from the set of phrases that have high probabilities of being keyphrases.

Various experiments have shown the effectiveness of these methods to extract Arabic keywords in varying percentages. However, while supervised techniques are costly and limited by the type of language resources used, unsupervised techniques suffer from the best semantic cover for the documents.

III. Characteristics of the Arabic Language

The complex grammatical and morphological features of the Arabic language make the task of automatically processing more difficult. Among these features, we highlight the following:

- Arabic scripts have diacritics to represent the short vowels, which are marks above or below the letters. However, these diacritics have been disappearing in most contemporary writings, and readers are expected to fill in the missing diacritics through their knowledge of the language. The absence of diacritics from contemporary Arabic texts makes the automatic processing a difficult task.
- Morphological analysis is a complex procedure because Arabic is an agglutinative language.
- Arabic is a highly inflectional and derivational language where many of the nouns and verbs are derived from the same root. This latter is based on more than 150 patterns, which makes them more complex and difficult to handle.

IV. The Architecture of SIRAT

As emphasised in the introduction above, we have designed and developed an Arabic text editor (Figure1) that extracts the keywords and makes Real-Time indexing that is based on:

- An Real-Time indexing module.
- An Arabic keywords extract module for the automatic extraction of keywords and updating of initial index.

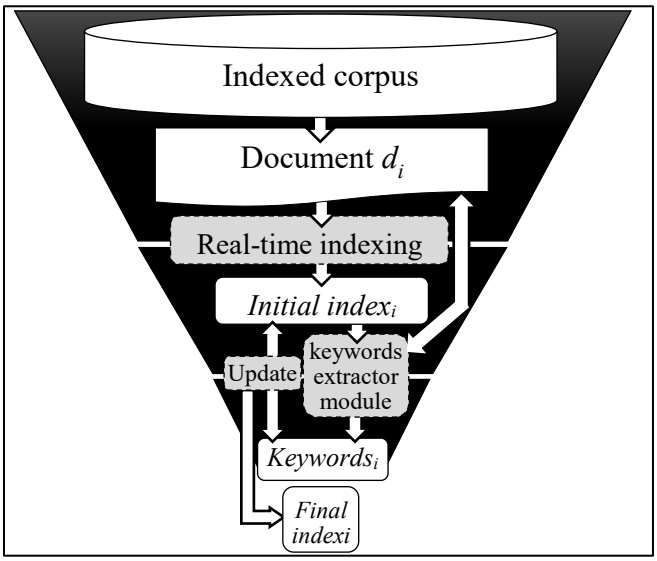


Fig. 1. The architecture of SIRAT

With the possibility of the intervention of the human expert to select the relevant keywords and updating the index of a document.

A. Real-time Indexing Module

Indexing is the process of representing the given text into the list of informative terms, which reflects its content in order to optimize speed and performance in finding relevant documents for a search query.

This module conducts an automatic indexing where one document is the indexing unit. This type of indexing refers to the indexing process that begins directly after the writing of each unit ends. The output of this process give a rise to an initial index (Figure 2).

The automatic indexing of Arabic texts had dominated most of the research literature in Arabic text retrieval. In our study, we followed the approach due to [2] [21] to create the index with some modifications, which we discuss in the next

section. This method has proved to be effective in improving the process of indexing Arabic documents.

We have implemented the algorithm of figure 2 to obtain, as output, the $index_i$.

```
Input : document di ∈ corpus
Output : Indexi
Procedure indexing (var tf_type)
      being
            Encoding ();
            Normalize ();
            Removing_stop_words ();
            Stemming ();
            If (tf_type = tf) then
                  Weighting(tf);
            Else
                  Weighting(tf-idf);
            End
      end
begin
   For di
      If (i = 1) then
            Call indexing (tf);
      Else
            Call indexing (tf-idf);
      end
   end
end.
```

Fig. 2. Real-Time Indexing Algorithm

This real-time indexing algorithm takes as input a document d_i belonging to the corpus. Then, it applies the set of treatments described as following:

1) Encoding

The corpus and queries can be encoded differently, making them incomparable. In order to standardize the documents with the queries, we must reuse converting tools between different encodings systems. Thus, everything would beconvertedintoUTF-16 encoding in our case, because it allows the representation of letters and symbols in a wide range of languages, including Arabic.

2) Normalization

Normalization involves the following steps:

- Remove punctuation;
- Remove the Tatweel '-'.
- Remove diacritics (primarily weak vowels);
- Replace the 'آ' by the 'ا';
- Replace the 'إ' or the 'أ' initial by Alif nu 'ا';
- Replace the 'ى' final by the 'ي';
- Replace the 'ىء' of order by the 'ئ';
- Replace the 'ة' final by the 'ه'.

3) Removing stop words

The removal of stop words has the advantage of reducing the number of indexing terms and may reduce the recall rate. We use a list of stop words to remove stop words.

4) Stemming

We used a hybrid method, as proposed by [2], to extract the roots of the words and use them as index terms. This combines the application of three previously used techniques, which deal with three key issues related to Arabic stemming including affix removal proposed by [18], dictionaries [3] and morphological analysis [16]. This method has been found to be effective in indexing process compared to other methods.

5) Term frequency and weighting

Several statistical measure are available to assign weights to words of a document in a corpus. Currently, TF-IDF is one of the most popular term-weighting procedure. TF-IDF value increases proportionally to the number of times a word appears in the document and is offset by the frequency of the word in the corpus, which helps to adjust for the fact that some words appear more frequently in general.

In our study, we used TF-IDF that combine the definitions of term frequency and inverse document frequency, to produce a composite weight for each term in each document. The TF-IDF weighting procedure assigns a weight to term t in document d given by

$$tf - idf_{t,d} = tf_{i,j} * idf_i \quad (1)$$

where

- $tf_{i,j}$: the number of times that term i occurs in document j.
- $idf_i = \log \frac{|D|}{|\{d_i : t_j \in d_j\}|}$
- $|D|$ total number of documents in the corpus.
- $|\{d_i : t_j \in d_j\}|$: number of documents where the term t appears (i.e., tf(t,d) ≠ 0).

Our automatic indexing unit deals differently with the first document added to the corpus (Figure 2). Since there are no documents available prior to the first document to compute $tf - idf_{t,d}$, we only count a $tf_{i,j}$ value.

The automatic indexing unit constructs an *initial index* for every document of every corpus. The output of this unit is an *initial index* for each document. The main motivation behind constructing initial indexes is to allow the expert intervention in the creation of index later.

B. Keywords Extraction Module

We have adopted a hybrid method of extracting keywords, where linguistics and statistical techniques are used to construct this module. The automatic keyword extraction module proposes the list of candidate words. This list is limited to twelve keywords, each consisting of at most five words.

We based on a supervised learning approach which consists of two phases:

- The training phase in which we create a model using the training data; these consist of documents with expert assigned keywords (Section V.B).
- The extraction phase, we use the model created in the training phase and applies it to the testing data.

In the extraction phase, we adopt the results of the automatic indexing module, where we retrieve the index words with the highest weights.

Then, we add, if possible, to each index word, from original text, two nearest neighbor words on the right and two

others on the left while ensuring that this five -word string does not contain Arabic punctuation marks in between words (as shown in the example above - figure 3).

Stage	Yes/No	If no, why?
1. ***Input:*** في تقريرها السنوي حول الجمهورية الجزائرية الديمقراطية الشعبية أن ... (In its annual report on the democratic and popular republic of Algeria that …)	-	
2. ***Selected word from the result of the indexing module*** في تقريرها السنوي حول الجمهورية الجزائرية الديمقراطية الشعبية أن...	Yes	
3. ***Add 1st right word*** في تقريرها السنوي حول الجمهورية الجزائرية الديمقراطية الشعبية أن...	Yes	
4. ***Add 2nd right word*** في تقريرها السنوي حول الجمهورية الجزائرية الديمقراطية الشعبية أن...	No	Stop word
5. ***Add 1st left word*** في تقريرها السنوي حول الجمهورية الجزائرية الديمقراطية الشعبية أن...	Yes	
6. ***Add 2nd left word*** في تقريرها السنوي حول الجمهورية الجزائرية الديمقراطية الشعبية أن...	Yes	
7. ***Output:*** الجمهورية الجزائرية الديمقراطية الشعبية (The democratic and popular republic of Algeria)		

Fig. 3. An example of the keywords extraction process

Otherwise, we just take the number of words between two punctuations. We also give priority to a noun phrase or nominal phrase by setting terms for the candidate words in the following order:

- Begin with "ال" letters and end with "ي" ,"ة" or "ء" letters.
- Begin with "ال" letters.
- End with "ي" ,"ة" or "ء" letters.
- Ordinary words.

Then we assign weights to these candidates by calculating two values:

- TF-IDF calculates the frequency of a given keyword at the current document (TF) and frequency of the keyword in the corpus of documents (IDF). TF-IDF for keyword K in document D is calculated using the formula shown in Equation (2) [1].
- The First occurrence weight is calculated as the number of words that precedes the keyword's first appearance divided by the total number of words in that document.

$$TF - IDF = \frac{freq(K,D)}{size(D)} * \log_2(\frac{df(K)}{N}) \quad (2)$$

Where:

- $freq(K,D)$ is the number of times K occurs in D.
- $size(D)$ is the number of words in D.
- $df(K)$ is the number of documents containing K in the corpus.
- N is the size of the corpus.

After calculating the weights of candidate keywords, we determine whether a given candidate word is qualified to be a keyword (P[K]) or not (P[NK]). These two probabilities are calculated as shown in Equations (3) [1] and (4) [1] respectively:

$$P[K] = \frac{K}{K+NK} * P_{TF-IDF}[t/k] * P_{distance}[d/k] \quad (3)$$

$$P[NK] = \frac{NK}{NK+K} * P_{TF-IDF}[t/nk] * P_{distance}[d/nk] \quad (4)$$

Where:

- t is $TF - IDF$
- d is distance or First Occurrence value.
- K is the number of positive keywords in the training data.
- NK is the number of negative keywords in the training data.
- Identify applicable funding agency here. If none, delete this text box.

The importance of a candidate keyword is calculated using Rank as equation 5 [1]:

$$Rank = \frac{P[K]}{P[K]+P[NK]} \quad (5)$$

1) Unit of updating initial index

The role of this unit is to update an initial index of a document by taking into account the keywords generated by the keywords extraction module. The expert's opinions can be accounted for by updating the weights of the selected keywords and assigning to them higher values. This phase concludes with the integration of this initial index into the document, and saving it to an object file in order to exploit it later.

V. IMPLEMENTED APPLICATIONS AND RESULT

To implement our idea that we designed, we developed an Arabic text editor that contains a real-time indexing module and a keywords extraction module. In addition, we worked on building a suitable new form of Arabic training data (corpus), which contains keywords proposed by a human expert, to conduct the necessary experiments.

A. Arabic Text Editor

We first developed an Arabic text editor (Figure 4), which -in addition to the regular functions as text editor-, is provided with the automatic indexing option to editor's users. We have adopted the design of real-time automatic indexing module described above (Figure 1) to add this option.

As discussed above, we deal differently with the first document added to the corpus, where there are no other documents, so it only counts a $tf_{i,j}$ value. We then integrate the keyword extraction module, which is based on the results obtained from the automatic indexing module and proposes some keywords.

[a] http://www.aljazeera.net/encyclopedia. Uploaded on November 16, 2017.

[b] JEC: Al Jazeera Encyclopedia Corpus.

Finally, the index is updated. The output of this editor is an object file that contains the processed text and the generated document index.

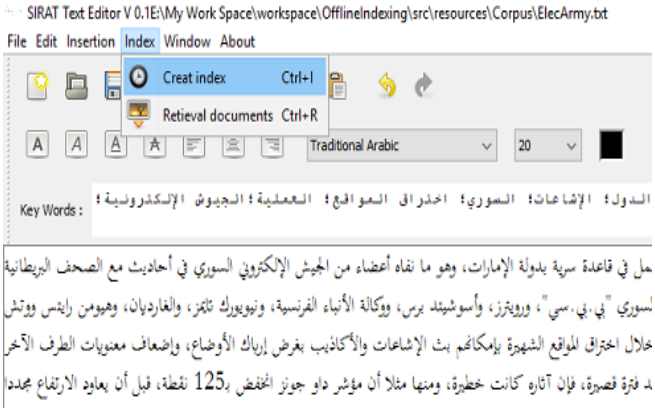


Fig. 4. Arabic Text Editor "SIRAT"

B. *New Arabic corpus form*

To study the efficiency of the proposed Editor, it was necessary to obtain a test corpus consisting of an Arabic data set which consists of documents that would meet a set of necessary and sufficient features for testing. We have developed a program to build an Arabic corpus, through the organization of a number of web pages of Al Jazeera's website[a] (JEC)[b], in a new corpus form (Figure 5) that is different from the usual ones, by appending keywords suggested by the human expert (Al Jazeera journalists) to the end of documents. This allows evaluating the performance of the automatic keywords extraction module. In addition, we have taken into account the set of rules used globally in the building of such corpus, especially those provided by (TREC) [17].

<DOC>
<DOCNO> ALJAZEERA-243 <ENDDOCNO>
<ENDHEADLINE> منطقة القبائل الجزائرية <HEADLINE>
<ENDDATELINE> المصدر : الجزيرة,مواقع إلكترونية <DATELINE>
<TEXT>
منطقة تقع شرق الجزائر العاصمة وتضم ست ولايات، هي تيزي وزو وبجاية وبومرداس والبويرة وسطيف وبرج بوعريريج، وكانت معقلا لعدد من الثورات. الموقع تقع القبائل شرق الجزائر العاصمة في منطقة أغلب تضاريسها جبلية تنفتح على البحر الأبيض المتوسط. تنقسم المنطقة إلى القبائل الكبرى التي تضم تيزي وزو وأجزاء من ولايتي بومرداس والبويرة، والقبائل الصغرى التي تضم ولاية بجاية وشمال سطيف
...
من أبرز الشخصيات السياسية التي ولدت في المنطقة حسين آيت أحمد من مواليد أغسطس/آب 1926 بعين الحمام بولاية تيزي وزو، وتوفي في ديسمبر/كانون الأول 2015، ويعد أحد كبار قادة الثورة الجزائرية وزعيم حزب جبهة القوى الاشتراكية أقدم حزب معارض في الجزائر. أنجبت المنطقة عام 1922 كريم بلقاسم الذي توفي عام 1970 بألمانيا، وهو أحد أبرز قادة الثورة الجزائرية وصار من المعارضين السياسيين للنظام الجزائري بعد الاستقلال.
<ENDTEXT>
<KEYWORDS> الجزائر؛ منطقة القبائل؛ تيزي وزو؛ بومرداس؛ بجاية؛ البويرة؛ سطيف؛ برج بوعريريج؛ البحر الأبيض المتوسط؛ الأمازيغ؛ وزارة الداخلية؛ فاطمة أنسومر؛ محمد المقراني؛ حسين آيت أحمد؛ جبهة القوى الاشتراكية؛ كريم بلقاسم؛ <ENDKEYWORDS>
<ENDDOC>

Fig. 5. New Arabic corpus form

Thus we were able to obtain an Arabic corpus containing 2416 documents. The vocabulary number of this corpus is 1475148 words, of which 133474 different words (i.e. 9.03% of the total words).

According to Zipf's Law, which is concerned with the distribution of words across documents, the range, and high light the importance of the corpus words. Figure 6 illustrates the JEC curve (in red color represented by symbols (+)) and Zipf's curve (in green color represented by symbols (x)). The Figure suggests that JEC curve is very close to Zipf's curve. Furthermore, according to some other criteria [19], our new form corpus is very rich and qualified to use as a test collection for keywords extraction system quality.

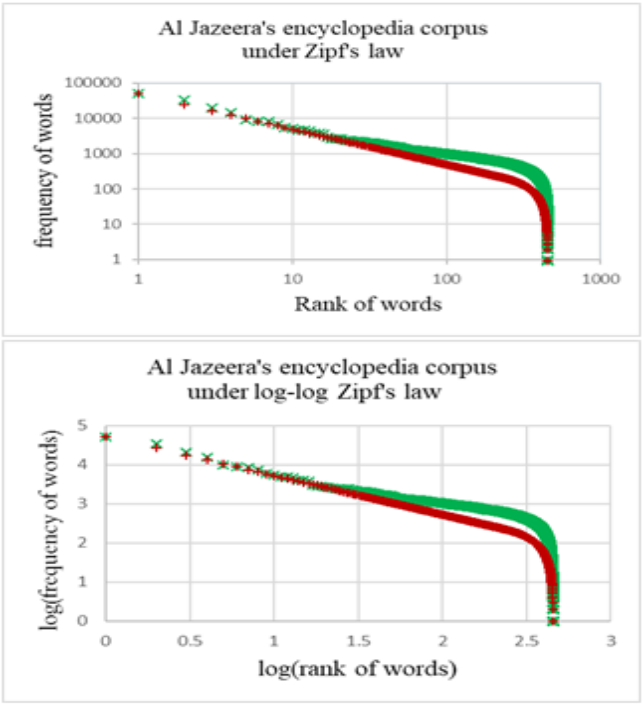


Fig. 6. Curve JEC according to Zipf's law curve

This new format enables us to benefit from, among other things:

- The Contribution to building a system for keywords systems evaluation, where we have been able to perform extracting experiments using the corpus documents, compare the results of these systems with the available keywords.
- The Contribution to building a system for IR systems evaluation, which enables researchers to test the effectiveness of their applications.

C. *Result*

In this paper we have two interesting results. The first one is related to our new method of indexing Arabic texts (RT+KE: Real-Time + Keyword Extraction) and the second one is related to the corpora building and keywords extraction evaluation systems.

In the first result of this study, and to evaluate our new method (RT+KE) of indexing performance in Arabic information retrieval. A series of experiments was conducted to show the effect of this method with the hybrid method (HY) [2] in retrieval performance.

We conducted those several experiments using the OIRDA application [2] and endowed it with RT+KE method, and we plot the recall-precision curve. (Figure 7) represents a comparison between these two methods of indexing.

These results show that RT+KE method of indexing is more effective than the HY method [2]. One can observe this behavior in Figure 7; RT+KE indexing curve representing accuracy of retrieval based on recall points is often above the HY curve. We obtain 60% average accuracy with RT+KE method and 59% with HY method.

Also, these results show that the method RT+KE can better determine the semantic core of a word, and therefore it increases the performance of IR.

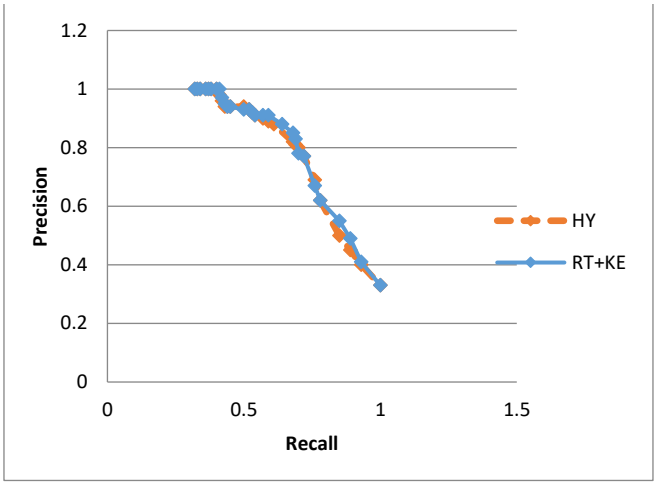


Fig. 7. Curves recall-precision of the two methods of indexing HY et RT+KE.

In the second result of this study, we have divided the corpus as a training documents and a testing documents (Table 1). The before last column of Table 1 shows the average number of keywords assigned to documents and the last column shows the average number of matched keywords between SIRAT generated keywords and JEC keywords.

TABLE I. JEC DISTRIBUTIONS AND MATCHED KEYWORDS

Dataset	total docs	Training docs	Testing docs	Avg of keywords	Avg of matched keywords
JEC	2416	1610	806	12.5	3.56 + 1.92

The aim of our experiments is to evaluate our approach of Arabic keywords extraction performance that we integrated in SIRAT. We conducted experiment using the SIRAT application in which we compare between SIRAT generated keywords and those of new corpus. The average number of matches is calculated by averaging the number of matched keywords for every document and then dividing by the number of documents. Result show the accuracy of SIRAT compared to other studies [7] [10] [13] [14] [6].

SIRAT suffers from problems, especially in the case where the editor cannot identify the descriptors that are relevant the most to the document, the aspect this editor must improve and find a viable solution to.

VI. CONCLUSION

The main objective of this study is to show the effects of integrated of real-time indexing module in an Arabic text editor tool, which require the automatic indexing, on keywords extraction system performance. Therefore, we recommend integrating this model into word processing tools in order to allow the editor to contribute effectively to build a high quality keywords while accounting for the drawbacks and shortcomings of this model. This study also proposes a solution to problems and deficiencies that Arabic language processing suffers from, especially regarding corpus building by developing an application framework for the building and development of corpora. In addition, the paper suggests a solution to reduce deficiencies keywords extraction evaluation systems suffer from, which enable researchers to test their indexing and keywords extraction algorithms. In the future work, we also plan to investigate the effects of use the partial index in which generated by SIRAT, on the general indexing process performance, and thus, on the information retrieval system performance.

REFERENCES

[1] I. H. Witten, G. W. Paynter, E. Frank, C. Gutwin, and C. G. Nevill-Manning, KEA: Practical Automated Keyphrase Extraction, in: Design and Usability of Digital Libraries: Case Studies in the Asia Pacific, (ed. Yin-Leng Theng and Schubert Foo), IGI Global, 2005, pp. 129–152.

[2] T. Dilekh and A. Behloul, Implementation of a New Hybrid Method for Stemming of Arabic Text, International Journal of Computer Applications 46, 8, (2012) 14–19.

[3] I.A.Al - Kharashi and M. W. Evens, Comparing words, stems, and roots as index terms in an Arabic Information Retrieval system, J. of the American Society for Information Science 45, 8 (1994) 548-560.

[4] O. Medelyan and I. Witten, Domain-independent automatic keyphrase indexing with small training sets, Journal of the American Society for Information Science and Technology 59, 7 (2008), 1026–1040.

[5] P.D. Turney, Learning algorithms for keyphrase extraction, Information Retrieval 2, 4 (2000), 303–336.

[6] R. Duwairi and M. Hedaya, Automatic keyphrase extraction for Arabic news documents based on KEA system, J. of Intelligent and Fuzzy Systems 30, 4 (2016) 2101–2110.

[7] S. R. El-Beltagy and A. Rafea, KP-Miner: A keyphrase extraction system for English and Arabic documents, J. Information Systems, Elsevier 34, 1 (2009) 132–144.

[8] Y.Kang,P.Delir-Haghighi and F. Burstein, CFinder: An intelligent key concept finder from text to ontology, Expert Systems with Applications 41, 9 (2014) 4494– 4505.

[9] Y. Matsuo and M. Ishizuka, Keyword extraction from a single document suing word co-occurrence statistical information, International Journal on Artificial Intelligence Tools 13, 1 (2004), 157–169.

[10] E. Amer and K. Foad, AKEA: An Arabic keyphrase extraction algorithm, Proc. the International Conference on Advanced Intelligent Systems and Informatics 2016. (AISI'2016), Lecture Notes in Advances in Intelligent Systems and Computing, Springer 533 (2017) 137–146.

[11] T. Nguyen and M. Kan, Keyphrase extraction in scientific publications, Proc. 10th International Conference on Asian Digital Libraries, (ICADL2007), Lecture Notes in Computer Science, Springer 4822 (2007) 317–326.

[12] J. Wang, H. Peng, J. Hu and J. Zhang, Ensemble learning for keyphrase extraction from scientific documents, Proc. Third International Symposium on Neural Networks, (ISNN 2006), Lecture Notes in Computer Science, Springer 3971 (2006) 1267–1272.

[13] M. Al-kabi, H. Al-belaili, B. Abul-huda, and A. H. Wahbeh, Keyword Extraction Based on Word Co-Occurrence Statistical Information for Arabic Text, Abhath Al-Yarmouk: Basic Science & Engineering, 22, 1 (2013) 75–95.

[14] T. El-Shishtawy and A. Al-sammak, Arabic Keyphrase Extraction using Linguistic knowledge and Machine Learning Techniques, arXiv preprint arXiv: 1203.4605 (2012) 1–8

[15] K. Sarkar, M. Nasipuri and S. Ghose, Machine learning based keyphrase extraction: Comparing decision trees, naïve Bayes and artificial neural networks, The Journal of Information Processing Systems, 8, 4 (2012), 693–712

[16] K. Beesley,Arabic morphological analysis on the Internet, Proc. the 6th International Conference and Exhibition on Multi-lingual Computing, Cambridge, UK, 1998.

[17] Y. Kadri and J. Y. Nie, Effective stemming for Arabic information retrieval, Proc. the challenge of arabic for nLPmt, international conf. at the British computer Society (BcS), 2006, pp. 68–74.

[18] E. M. Voorhees, Overview of TREC 2003, Proc. in Trec, 2003, pp. 1‑13.

[19] N. Firoozeh, A. Nazarenko, F. Alizon, and B. Daille, “Keyword extraction: Issues and methods,” Nat. Lang. Eng., vol. 26, no. 3, pp. 259–291, May 2020, doi: 10.1017/S1351324919000457.

[20] H. Benghuzzi and M. M. Elsheh, “An Investigation of Keywords Extraction from Textual Documents using Word2Vec and Decision Tree,” Int. J. Comput. Sci. Inf. Secur., vol. 18, no. 5, pp. 13–18, 2020.

[21] T. Dilekh, S. Benharzallah, and A. Behloul, “The impact of online indexing in improving Arabic information retrieval systems,” Inform., vol. 42, no. 4, pp. 607–616, 2018, doi: 10.31449/inf.v42i4.2297.

Evaluation of ANN, ICA-ANN and PSO-ANN predicting ability in the prediction of CO_2 emissions during the calcination of cement raw material

Yakoub Boukhari
Chemistry Department
Ziane Achour University
Djelfa, Algeria
jacoubchimie@yahoo.fr

***Abstract*—Cement industry releases large amounts of carbon dioxide CO_2 as by-product to the atmosphere during the calcination of cement raw material. In fact, the calcination is a complex process and not completely understood. The amount of CO_2 emitted varies with the grain size, chemical composition, burning temperature and time to pass through the kiln during calcination process. However, due to interaction of several parameters, it is not easy to establish accurate mathematic model to calculate the real amount of CO_2 emission. Moreover, using the laboratory experiments to determine the amount of CO_2 emissions are not usually easy, time-consuming, expensive and require good quality of reagents and equipments. To overcome the above problems, artificial neural network (ANN), ANN optimised by imperialist competitive algorithm (ICA-ANN), ANN optimised by particle swarm optimization (PSO-ANN) are applied to predict amount of CO_2 emissions. A comparative accuracy of these tools is evaluated based on the coefficient of determination R^2, R^2 adjusted, mean absolute percentage error (MAPE) and scatter index (SI).**

The results obtained are promising and demonstrate that all proposed tools represent a good alternative for the prediction of CO_2 emission with adequate accuracy. PSO and ICA are capable to improve the predicting accuracy of ANN. In addition, PSO-ANN can predict slightly better than ICA-ANN. Based on testing data, the results obtained show that 98.61%, 98.18% and 97.5% of experimental data are explained by PSO-ANN, ICA-ANN and ANN, respectively with average relative error less than 1.41% and SI less than 0.1.

Keywords—CO_2 emissions, calcination process, artificial neural network, imperialist competitive algorithm, particle swarm optimization

I. INTRODUCTION

The cement is used extensively in a diversity of construction projects. The one of the most important step in the cement production process is clinker calcination process of raw materials. The calcination of raw materials is produced in cement kilns at high temperature. In fact, the calcination process is a complex thermo-chemical reaction, and at the same time, it is greatly influenced by heat transfer, mass transfer from inside particle to reaction interface, chemical reaction and experimental conditions [1]. It is complicated process due to complex interactions of the influencing parameters between them [2]. In fact, the calcination process is a complex process and not completely understood.

The main by-product of clinker calcination process of raw materials is CO_2 emitted from thermal chemical decomposition reaction of limestone [3]. The amount of CO_2 emissions during calcination of raw materials is very important and it has strong influence in determining cement quality. The main oxides present in in the raw materials are CaO, SiO_2, MgO, Al_2O_3 and Fe_2O_3 [6]. These oxides have very significant role in determining the amount of CO_2 emissions during calcination. The amount of CO_2 emissions vary with their grain size, chemical composition and burning time. However, the influence of these parameters on an amount of CO_2 emissions is still not clear. Due to the complexity of calcination process, it is very difficult to account the amount of CO_2 emissions by traditional mathematical methods. Moreover, using the laboratory experiments to determine the amount of CO_2 emissions are not usually easy, time-consuming, expensive and require good quality of reagents and equipments.

For decades, intelligence methods are widely used in several domain to predict the behavior of complex phenomena [4,5]. The objective of present study is to evaluate the predicting ability of artificial neural network (ANN), ANN optimised by imperialist competitive algorithm (ICA-ANN) and ANN optimised by particle swarm optimization (PSO-ANN) in the prediction of CO_2 emissions during the calcination of cement raw material. These models do not need to understand the process behavior for extracting prior knowledge and have strong capability to adapt to system variation. Due to their advantages, ANN, PSO-ANN, ICA-ANN are widely used to solve a diversity of complex problems in many fields. ANN is a very effective tool for predicting the pitting corrosion [7] and velocity of sound in liquid water [8]. PSO-ANN is also successfully applied for predicting of cobalt leaching rate from waste lithium-ion batteries [9] and solar space heating system parameters [10]. ICA-ANN is successfully applied as intelligence models to predict maximum surface settlement caused by tunnelling with higher reliability [11] and oil flow rate of the reservoir [12].

The present paper is organised as follows: Section 2 describes briefly the artificial intelligence tools used to predict the target. Section 3 presents the used materials and methods. Section 4 presents and discuss predicting results. Finally, Section 5 presents our conclusions.

II. BRIEF DESCRIPTION OF ARTIFICIAL INTELLIGENCE TOOLS

A. Artificial neural network (ANN)

Artificial neural network is inspired from the biological nervous system within the human brain [13]. It is the most popular intelligence tools because it is able to predict the output of complex nonlinear relationships among variables in

a wide range of areas. It is composed of input layer, output layer and at least one intermediate layers called hidden layers. Each layer contain one or more nodes arranged (neurons). The neurons in each layer are fully connected with neurons in the subsequent layer. There are no links between neurons in the same layer. The neuron mainly consists of weight, bias and activation functions. The weight, bias factors are adjusted and optimised at every iteration by Levenberg Marquardt (LM) based back propagation (BP) during training process [14]. The cost function used by ANN during leanining process mean square error (MSE). It is used to measure the difference between the predicted output and the desired output.

The number of neurons in the input layer and the output layer equal the number of input and output variables in the data, respectively. Whereas, there are no general rules to determine the suitable number of hidden nodes and number of its neurons. The common way is to set a relative large number of neurons at the beginning, and then reduce it gradually until the desired error are achieved. There are some cases where the ANN tool has the disadvantages of slow learning convergence, local optima trapped instead of global optimal solution [15]. PSO and ICA are proposed to overcome the previous shortcomings of ANN and to improve its applications.

B. Imperialist Competitive Algorithm-Artificial Neural Network (ICA-ANN)

As mentioned previously, despite the popularity of ANN in prediction complex system, it still has the possibility to fall in a local optimum. Hence, Imperialist Competitive Algorithm is combined with ANN to find the global optimal and avoid premature convergence toward local.

The imperialist competitive algorithm ICA is a new optimization algorithm which is inspired by the imperialistic competition processes of human [16]. ICA algorithm is applied to update the weights and biases during the training process in order to improve efficiency of ANN. Recently, it is very attractive [17] and widely applied to solve discrete optimization problems due to its good convergence rate and better global optima finding. ICA algorithm start by initial randomly population called countries. In reality, there are two groups of countries which are imperialists and colonies regarding their power. The most powerful countries with the minimum best cost are chosen as imperialists, whereas the weakest countries are taken as colonies of theses imperialists. The imperialist and their colonies are united together to construct the initial empires. ICA algorithm begins an iterative process to arrive at optimal solutions after some number of decades or generations.

Three main operators of ICA are assimilation, revolution and competition [18]. In assimilation, each colony starts to moves to their corresponding imperialist in order to develop its position. During the movement, the colony can attain great power (lower cost) compared to its imperialist. This procedure is called revolution. In this case, their positions will be exchanged and the empire has a new imperialist. At the next step, imperialist competition starts and the weakest empires is eliminated from the competition. At the end, only one of these empires is remained and all the other countries are their colonies. The remaining empire presents the optimal solution. The most important ICA parameters are number of countries, number of imperialists, number of decades.

C. Particle Swarm Optimization-Artificial Neural Network (PSO-ANN)

Similar to ICA, Particle Swarm Optimization (PSO) is combined with ANN to form powerful tools and to adjust its setting parameters. PSO is a popular algorithm due to its competitive performance and easy implementation [19]. It is inspired by natural phenomena of birds flocking or schooling fish while searching for food sources. In the natural, birds randomly move in groups and work together by sharing information to achieve a nearest food source. Each bird tries to follow the bird which is nearest to the food. Bird searching for food updates both its speed and position. This process is repeated iteratively until the source of food is found. After a sufficient number of iterations, all birds will eventually discover the nearest path from the nest to the food source. The nearest path is the desired solution [20]. PSO is more attractive because of its quick convergence and only few parameters adjustments are required [21]. The performance of PSO is related principally to the number of particle, number of iterations.

III. MATERIALS AND METHODS

A. Materials and experiments:

In the present study, CO_2 emission is considered as a function of chemical composition, grain size and time exposed. The raw materials are blended and preheated to around 300°C to remove water combined in the hydration products and then up to 850° C to remove impurities, which can affect the cement quality.

Four different grain size distribution (71, 125, 250 and 350 µm) of raw materials used are selected separately. The chemical composition and mix proportions of four raw materials used are summarised in Table I. Finally, each mixture of raw materials with gain size are burned in the laboratory furnace at 1000° C for different times 5, 10, 15, 20, 30 min. The amount of CO_2 emissions is calculated before and after burning of each mixture of raw materials at 1000 °C.

TABLE I. CHEMICAL COMPOSITION (% BY WEIGHT) FOR EACH RAW

Raw Materials	**Oxides**				
	SiO_2	CaO	MgO	Fe_2O_3	Al_2O_3
Material 1	12,38	80,28	1,38	1,69	4,27
Material 1	3,96	92,62	0,99	0,65	1,78
Material 1	14,06	78,69	1,35	1,68	4,22
Material 1	14,16	78,04	1,36	2,21	4,23

B. Dataset collection

The dataset extracted from the experimentation is collected in a table of 80 rows and 8 columns. Each row in this table presents an experiment. From 1 to 7 columns are inputs where the last column is output. The size particle, time exposed, SiO_2(%), CaO (%), MgO (%), Fe_2O_3 (%), Al_2O_3 (%) are inputs and the amount of CO_2 emissions is the output.

The total dataset are randomly divided into two sets: training and testing. For each algorithm, 75% of dataset is used for training while the remaining 25% (unseen dataset) of dataset are kept out to evaluate the generalisation ability. The most common performance criterion used to evaluate the accuracy of each algorithm are the coefficient of determination R^2 R^2 adjusted, the mean absolute percentage

error (MAPE) and the scatter index (SI). The tool performance is perfect when value of R^2 is very close to 1, while value of MAPE are very close 0. The predictive accuracy is excellent when SI is inferior of 0.1; good if SI among 0.1 and 0.2; and bad if SI more than 0.3. [22].

IV. Results and Discussion

In fact, selecting an optimal settings parameters of each intelligence methods tools during training stage is a challenging task. The trial-and-error method is considered as best method to find the optimal settings parameters [23]. It is applied in this study to determine different setting parameters.

A. *ANN results*

It is well known, that ANN has ability to learn the relationship between inputs and outputs in the presence sufficient number of hidden layer and neurons with suitable transfer functions [7]. After trying various ANN parameters during the training phase, the more appropriate structure parameters of ANN are determined as listed in Table II.

TABLE II. ANN PARAMETERS

Parameters	Values
Number of hidden layer	1
Neuron number in hidden layer	12
Transfer function for hidden layer	transig
Transfer function for output layer	purelin
Training Algorithm	LM based BP

The comparison between experimental and predicted CO_2 emissions values obtained by ANN for training and testing phases are shown in Figure 1 and Figure 2, respectively. The results obtained clearly indicate that ANN performs best with all ANN parameters selected. It is clear from these figures that experimental CO_2 emissions is positively correlated with predicted ones in both phases. In addition, linear fit lines and line of equality (y=x) are perfectly aligned with almost dataset points. The value of R_2 training and testing phases are respectively 0.9896, and 0.9763.

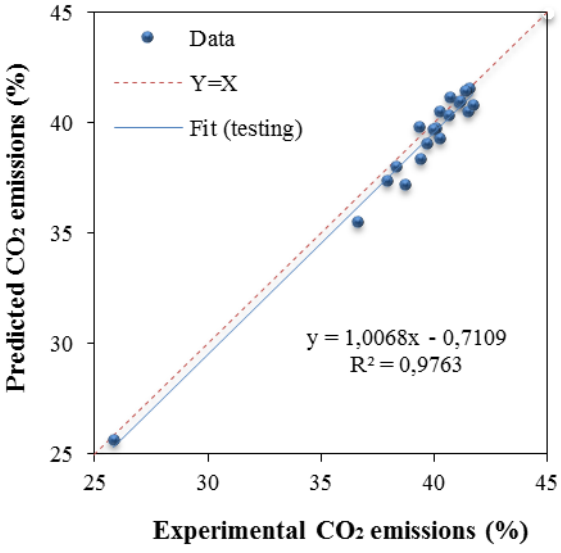


Fig. 1. Comparison between predicted and experimental CO_2 emissions in testing phase

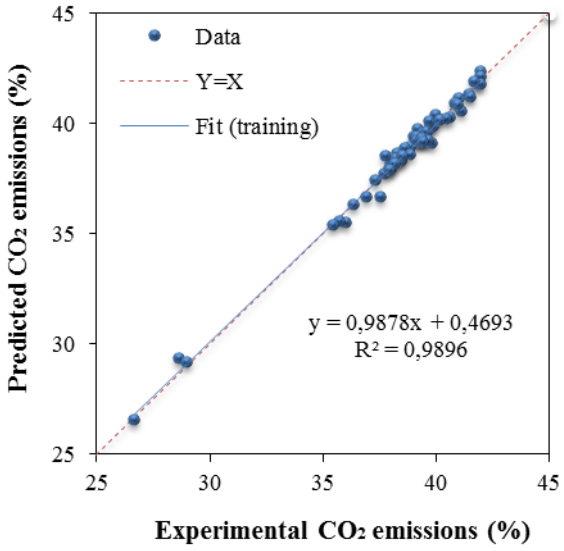


Fig. 2. Comparison between predicted and experimental CO_2 emissions in training phase

The distribution of the relative error obtained ANN during training and testing phases is illustrated in Figure 3. It is clear from Figure 3 that the relative error values are nearly spread around the zero line. The average relative error for training phase is 0.58% while it is 1.41% for testing phase. While the maximum error for training phase is 2.36% and for testing phase is 4.02%. These low values of MAPE are indicative of very small difference between experimental of CO_2 emissions and predicted ones.

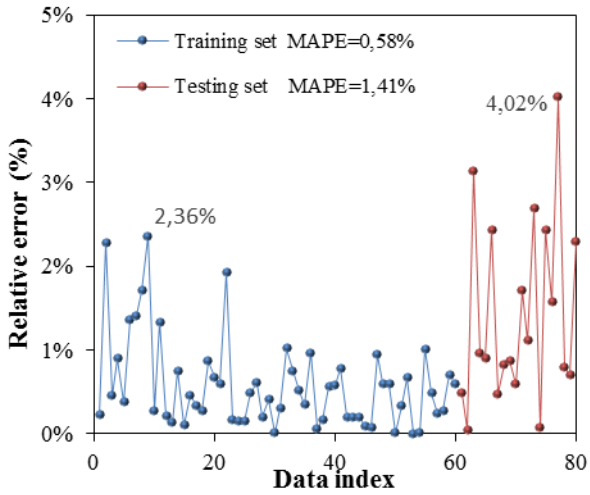


Fig. 3. Distribution of the relative error obtained ANN during training and testing phases

The results illustrated in Figure 3 confirm that ANN has good generalisation capability and can predicts the amounts of CO_2 emissions adequately, as indicated by the low value of MAPE equal to 1.41%, high value R^2 equal to 0.9763.

From Table III, the values of R^2 adjusted indicate that ANN is able to predict approximately 98.94% of training dataset and 97.50% of testing dataset. The values of SI less than 0.1 obtained in both phases mean adequate predictive capability. The high accuracy of ANN is usually due to its

flexible architecture and its excellent performance in solving the nonlinear mapping between the inputs and outputs.

TABLE III. PERFORMANCE CRITERIA

Parameters	R^2 adj	SI
Training phase	98.94%	97.50%
Testing phase	0.0076	0.0176

B. PSO-ANN results

The PSO algorithm is used to train and optimise weights and biases of previously ANN architecture to form powerful tool. The objective of using the same architecture is to evaluate the capability optimising of PSO algorithm. The optimal parameter configuration of PSO-ANN utilised are summarises in Table IV.

TABLE IV. PSO-ANN PARAMETERS

Parameters	Values
Number of particle	14
Number of iteration	16
Acceleration constant (C_1=C_2)	1.5
Number of hidden layer	1
Neuron number in hidden layer	12
Transfer function for hidden layer	transig
Transfer function for output layer	purelin
Training Algorithm	LM based BP

The predicted values of CO_2 emissions obtained from PSO-ANN are compared with the experimental ones for training phase and testing phase as shown in Figure 4 et Figure 5, respectively. It is clear that almost points are very closely clustered around the line of equality (y=x) and lied exactly linear fit. Moreover, the linear fit is sloped with an angle close to 45° that means strong linear relationships between to predicted and experimental dataset.

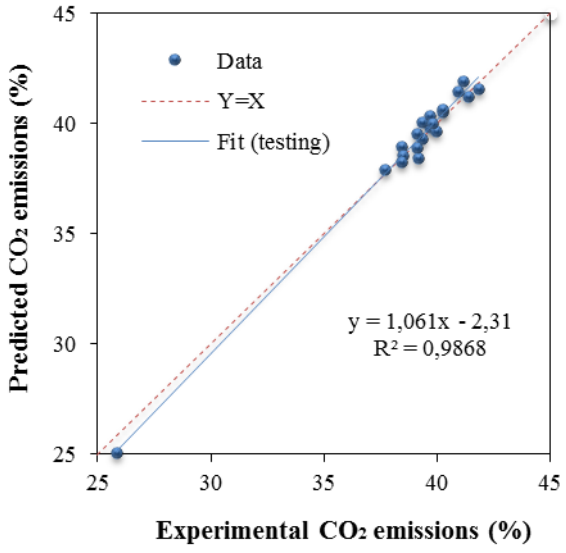


Fig. 4. Comparison between predicted and experimental CO_2 emissions in testing phase

PSO-ANN can achieve R^2 of 0.9870 in the training phase and 0.9868 in the testing phase. The R2 values close to 1 mean that the predicted CO_2 emissions are very close to the real experimental values. The R^2 mean that less than 1.4% of testing dataset and training dataset can not explain by PSO-ANN.

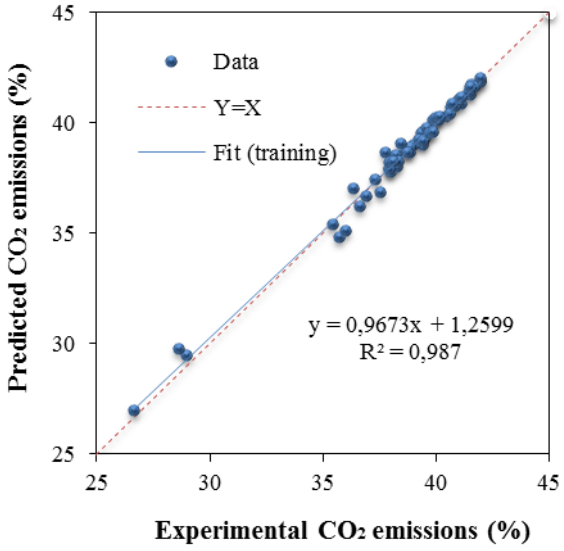


Fig. 5. Comparison between predicted and experimental CO_2 emissions in training phase

The distribution of the relative error obtained during training and testing phases are plotted in Figure 6. It is observed that almost of points are tightly concentrated near to line zero. The relative errors are relatively less in both phases, where the maximum error not exceed 3.15% in training phase and 3.17% in testing phase. The average relative error for training and testing are 0.6% and 0.97%, respectively.

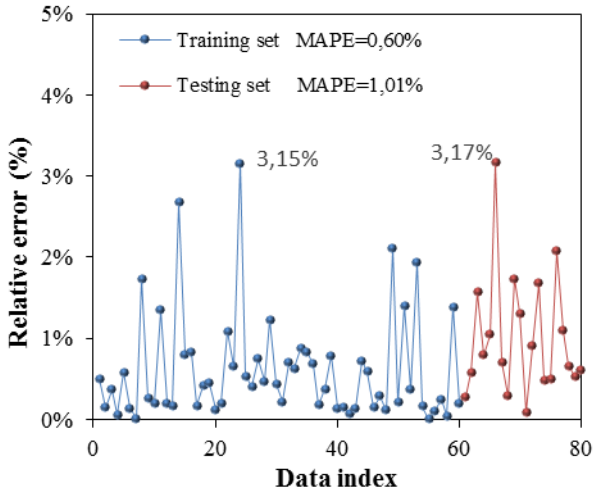


Fig. 6. Distribution of the relative error obtained PSO-ANN during training and testing phases

The prediction results approve the feasibility of the PSO-ANN and show the good generalization capability. As reported in Table V, the values of R^2 adjusted mean that PSO-ANN can predicted 98.6 % of total dataset correctly. In addition, the SI values less tha 0.1 reflect the excellent predicting ability of amount of CO_2 emissions.

TABLE V. PERFORMANCE CRITERIA

Parameters	R^2 adj	SI
Training phase	98.70%	0.0088
Testing phase	98.68%	0.0114

The high performance of PSO-ANN is explained by the capability of PSO to find the global optimum solution and optimum structure of ANN and high capability of ANN to learn by example during training process. In summary, PSO-ANN tool is very useful in predicting the amount of CO_2 emissions with very high value R^2 and very low value of MAPE.

C. ICA-ANN results

Similar to previous case, ICA is also used for optimising the weights and bias values in ANN. The best parameters values of ICA utilised during training process to optimise and to improve the prediction performance accuracy of ANN are shown in Table VI.

TABLE VI. ICA-NN PARAMETERS

Parameters	Values
Number of countries	14
Number of initial imperialists	16
Number of decades	1.5
Number of hidden layer	1
Neuron number in hidden layer	12
Transfer function for hidden layer	transig
Transfer function for output layer	purelin
Training Algorithm	LM based BP

The capability of ICA-ANN to predict amount of CO_2 emissions during calcination process is shown in Figure 7 and Figure 8.

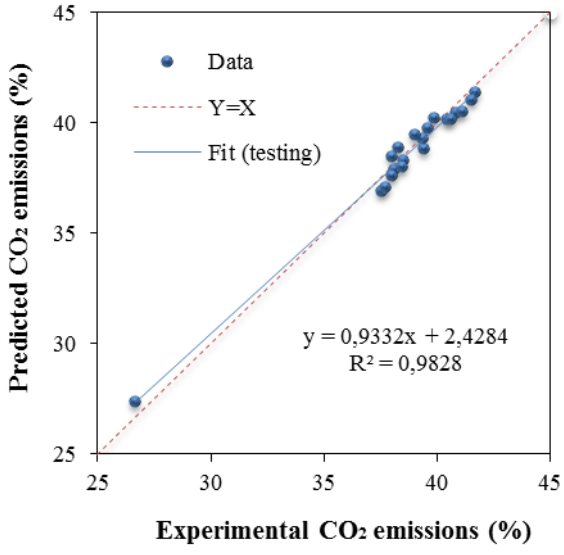


Fig. 7. Comparison between predicted and experimental CO_2 emissions in testing phase

The plots clearly illustrate that almost of dataset in training and testing phases fall on a linear fit which is mostly overlapped with line of line of equality (y=x). The R^2 value are high for both phases and are near to one, reflecting strong linear relationships between predicted amount of CO_2 emissions and experimental ones. The values of R^2 reveal that more than 98% of testing and training dataset are predicted perfectly by ICA-ANN.

The accuracy of amount of CO_2 emissions prediction of ICA-ANN is shown in Figure 9. It is clear, the dispersion of points dataset is quite close to the line zero. The relative error is almost low in the slip range of 0 to 2.51% in both phases. ICA-ANN is capable of providing average relative error values equal to 0.6% and 1.12% for training and testing phases, respectively. These values illustrate that the CO_2 emissions predicted are very close to the real experimental ones.

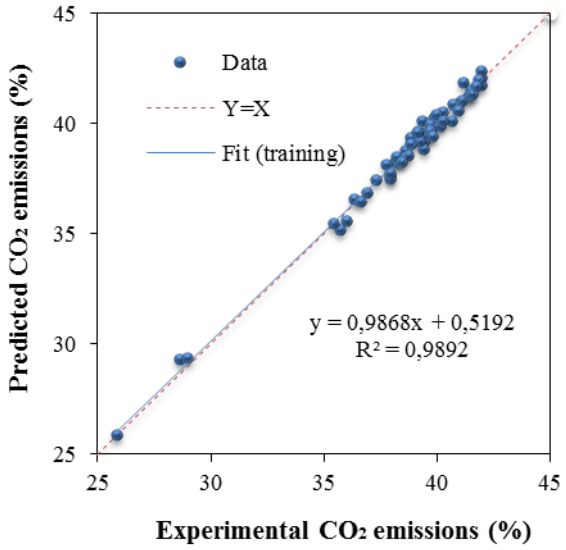


Fig. 8. Comparison between predicted and experimental CO_2 emissions in training phase

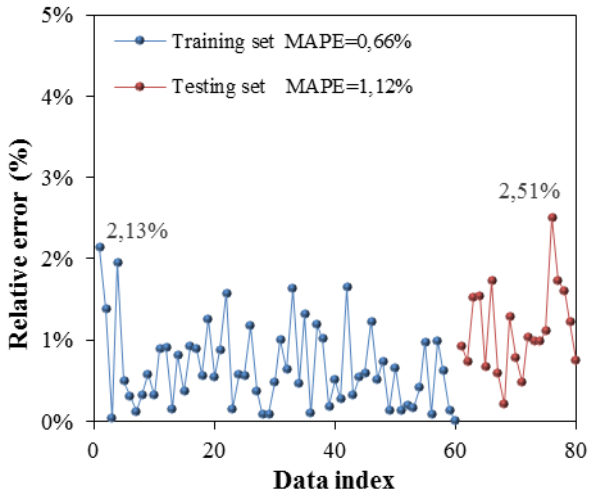


Fig. 9. Distribution of the relative error obtained by ICA-ANN during training and testing phases

The distribution of the relative error obtained by ICA-ANN during training and testing phases is shown in Figure 9. It is clear, the dispersion of points dataset is quite close to the

line zero. The relative error is almost low in the slip range of 0 to 2.51% in both phases. ICA-ANN is capable of providing average relative error values equal to 0.6% and 1.12% for training and testing phases, respectively. These values illustrate that the amount of CO_2 emissions predicted by ICA-ANN are very close to the real experimental ones.

The performance criteria for both phases are illustrated in Table VII. The adjusted R2 adjusted indicate that only 1.08% of training and 1.72% of testing dataset are not explained by this model. The values of SI that are less than 0.1 signify excellent capability of predicting.

TABLE VII. PERFORMANCE CRITERIA

Parameters	R^2 adj	SI
Training phase	98.92%	0.008
Testing phase	98.28%	0.0118

Results obtained reveal that ICA-ANN can produce excellent predicting results with high values of R^2 and low values of MAPE. The high accuracy of ICA-ANN is mostly due to its great capability of optimizing and the self -adaptive learning ability of ANN.

D. Comparison between different tools

Based on testing dataset, ANN non-optimised is compared to PSO-ANN, ICA-ANN to evaluate predicting ability of each tool in the prediction of CO_2 emissions during the calcination of cement raw material and the capacity of PSO and ICA in optimising of parameters of ANN. This comparison is presented in Figures 10.

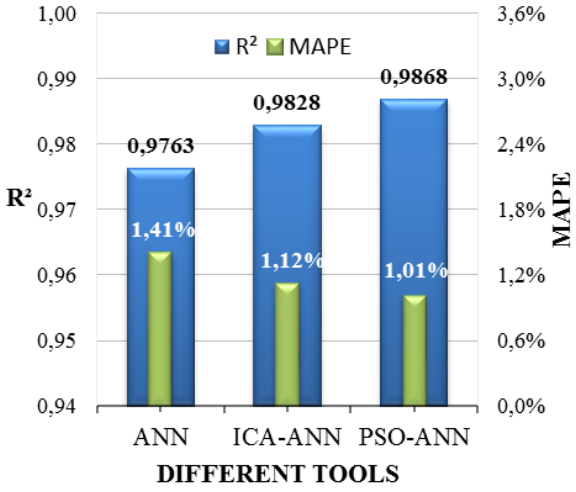


Fig. 10. Comparison between PSOANN, ICA-ANN and ANN in term of R^2 and MAPE

Firstly, PSO-ANN, ICA-ANN and ANN act as robust and powerful tools in predicting of amount of CO_2 emissions and can generate good accuracy. As can be seen from Figure 10, using PSO and ICA for optimising weight and bias can lead to a good predicting ability on result compared to simple ANN. For PSO-ANN, the values of R_2 and MAPE are 0.9763 and 1.14%, respectively whereas after combining ANN with PSO the value of R_2 and MAPE become 0.9868 and 1.01%, respectively. A similar improvement is observed with ICA-ANN. The results reveal the highest prediction capacity of PSO-ANN compared to ICA-ANN and ANN. Furthermore, the ANN efficiency is less than ICA-ANN by according to the results obtained via R_2 and MAPE. The predicting ability of ANN, ICA-ANN and PSO-ANN are as excellent as expected and they can reveal the real relationship between the influencing parameters and target. Based on testing dataset, the results obtained show that 1.39%, 1.82% and 2.50% of experimental dataset are not explained by PSO-ANN, ICA-ANN and ANN, respectively with average relative error less than 1.41% and SI less than 0.1.

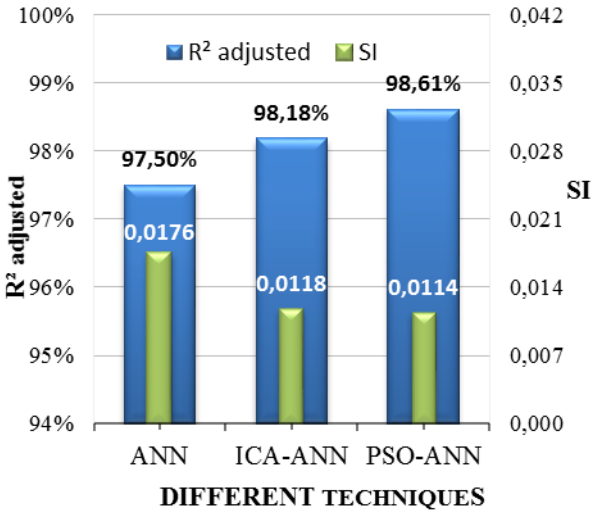


Fig. 11. Comparison between PSOANN, ICA-ANN and ANN in term of SI and R^2 adjusted

V. CONCLUSION

In present paper, PSO-ANN, ICA-ANN and ANN tools are proposed, and their prediction performances of amount of CO_2 emissions is evaluated through a comparison with the experimental ones. Based on testing dataset, the results obtained demonstrate that all tools proposed are very useful tools for fast prediction of amount of CO_2 emissions with high generalization performance. Using PSO and ICA for optimising weight and bias can lead to a good predicting ability on result compared to simple ANN. Based on the same neural network architecture, PSO-ANN has highest predicting ability with comparative high value of R^2 and less value of MAPE, followed ICA-ANN, while slightly less performance is seen in the case of ANN non optimised.

Based on testing dataset, the results obtained show that 98.61%, 98.18% and 97.5% of experimental dataset are explained by PSO-ANN, ICA-ANN and ANN, respectively with average relative error less than 1.41% and SI less than 0.1. Finally, the results obtained are promising and demonstrate that all proposed tools represent a good alternative for the prediction CO_2 emission during the calcination of cement raw material with excellent accuracy.

REFERENCES

[1] F. García-Labiano, A. Abad, L. F. Diego, P. Gayán, and J. Adánez, "Calcination of calcium–based so rbents at pressure in a broad range of CO_2 concentrations," Chem. Eng. Sci, vol. 57, pp. 2381-2393, July 2002.

[2] G. D. Silcox, J. C. Kramlich, and D. W. Pershing, "A mathematical model for the flash calcination of dispersed $CaCO_3$ and Ca(OH) particles," Ind. Eng. Chem. Res, vol. 28, pp. 155-160, February 1989.

[3] H. Mikulčić, E. Berg, M. Vujanović, P. Priesching, L. Perković, R. Tatschl, and N. Duić, "Numerical modelling of calcination reaction mechanism for cement production," Chem. Eng. Sci, vol. 69, pp. 607-615, February 2012.

[4] Y. Boukhari, M. N. Boucherit, M. Zaabat, S. Amzert and K. Brahimi, "Artificial intelligence to predict inhibition performance of pitting corrosion," J. Fundam. Appl. Sci. vol. 9, pp. 308-322, January 2017.

[5] A. M. Abubakar, E. Behravesh, H. Rezapouraghdam, and S. B. Yildiz, "Applying artificial intelligence technique to predict knowledge hiding behavior," Int. J. Inf. Manag. Sci, vol. pp. 45-57, December 2019.

[6] Z. Cao, L. Shen, J. Zhao, L. Liu, S. Zhong, and Y. Yang, "Modeling the dynamic mechanism between cement CO_2 emissions and clinker quality to realize low-carbon cement". Resour. Conserv. Recycl, vol. 113, pp. 116-126, October 2016.

[7] M. N. Boucherit, S. A. Amzert, F. Arbaoui, Y. Boukhari, A. Brahimi, and A. Younsi, "Modelling input data interactions for the optimization of artificial neural networks used in the prediction of pitting corrosionn," Anti-Corros. Methods. Mater, vol. 66, pp. 369-378, July 2019.

[8] H. Nowruzi and H. Ghassemi, "Using artificial neural network to predict velocity of sound in liquid water as a function of ambient temperature, electrical and magnetic fields," J. Ocean. Eng. Sci, vol. 1, pp. 203-211, September 2016.

[9] H. Ebrahimzade, G. R. Khayati, and M. Schaffie, "PSO–ANN-based prediction of cobalt leaching rate from waste lithium-ion batteries," J. Mater. Cycles. Waste. Manag, vol. 22, pp. 228–239, October 2019.

[10] B. Jamali, M. Rasekh, F. Jamadi, R. Gandomkar, and F. Makiabadi, "Using PSO-GA algorithm for training artificial neural network to forecast solar space heating system parameters," Appl. Therm. Eng, vol. 147, pp. 647-660, January 2019.

[11] M. R. Moghaddasi, and M. Noorian-Bidgoli, "ICA-ANN, ANN and multiple regression models for prediction of surface settlement caused by tunnelling," Tunn. Undergr. Space Technol, vol. 79, pp. 197-209, September 2018.

[12] M. A. Ahmadi, M. Ebadi, A. Shokrollahi, S. Mohammad, and J. Majidi, "Evolving artificial neural network and imperialist competitive algorithm for prediction oil flow rate of the reservoir," Appl. Soft Comput, vol. 13, pp. 1085-1098, February 2013.

[13] E. Heidari, M. A. Sobati, and S. Movahedirad, "Accurate prediction of nanofluid viscosity using a multilayer perceptron artificial neural network (MLP-ANN), Chemom. Intell. Lab. Syst, vol. 155, pp. 73–85, July 2016.

[14] P. Amani, and K. Vajravelu, "Intelligent modeling of rheological and thermophysical properties of green covalently functionalized graphene nanofluids containing na-noplatelets", Int. J. Heat. Mass. Transf, vol. 120, pp. 95–105, May 2018.

[15] A. M. Adrian, A. Utamima, and K. J. Wang, "A comparative study of GA, PSO and ACO for solving construction site layout optimization," KSCE J. Civ. Eng, vol. 19, pp. 520–527, March 2015.

[16] M. Abdollahia, A. Isazadehb, and D. Abdollahic, "Imperialist competitive algorithm for solving systems of nonlinear equations," Comput. Math. with Appl, vol. 65, pp. 1894-1908, August 2013.

[17] D. Peri, "Hybridization of the imperialist competitive algorithm and local search with application to ship design optimization," Comput. Ind. Eng, vol. 137, pp. 106069, November 2019..

[18] D. J. Armaghani, M. Koopialipoor, A. Marto, and S. Yagizd, "Application of several optimization techniques for estimating TBM advance rate in granitic rocks," J. Rock. Mech. Geotech. Eng, vol. 1, pp. 779-789, August 2019.

[19] X. Xia, L. Gui, and Z-H. Zhanc, "A multi-swarm particle swarm optimization algorithm based on dynamical topology and purposeful detecting," Appl. Soft Comput, vol. 67, pp. 126-140, June 2018.

[20] Q. Cui, Q. Li, G. Li, Z. Li, X. Han, H. P. Lee, Y. Liang, B. Wang, J. Jiang, and C. Wu, "Globally-optimal prediction-based adaptive mutation particle swarm optimization," Inf. Sci, vol. 418–419, pp. 186-217. December 2017.

[21] P. S. You, "An efficient computational approach for railway booking problems," Eur. J. Oper. Res, vol. 185, pp. 811–824, 2008.

[22] R. J. Stone, R.J. (1993). Improved statistical procedure for the evaluation of solar radiation estimation models. Solar Energy, 51(4): 289-291.

[23] Hill, D.J., and Minsker, B.S., 2010.Anomaly detection in streaming environmental sensor data: a data-driven modeling approach. Environ. Model. Softw. 25, 1014–10 22.

Bandwidth Provision through Disjoint Multipath RPL in the IoMT

Souhila Kettouche
RELA(CS)^2 labs
Larbi Ben M'hidi University
Oum El Bouaghi, Algeria
souhila.kettouche@gmail.com

Moufida Maimour
Lorraine University, CNRS, CRAN
F-54000 Nancy, France
moufida.maimour@univ-lorraine.fr

Lakhdar Derdouri
RELA(CS)^2 labs
Larbi Ben M'hidi University
Oum El Bouaghi, Algeria
derdouril@yahoo.fr

***Abstract*—Internet of Multimedia Things (IoMT) is one extensively current topic of the Internet of Things (IoT) due to the immersive growth of multimedia applications in several fields. In LowPower and Lossy Networks (LLNs) where sensor nodes are a key component, providing a satisfactory quality of service (QoS) as well as a user quality of experience (QoE) for such applications is a challenging task. In fact, high bandwidth and substantial computation resources are required. To provide sufficient bandwidth to handle these high data rate applications, we propose to extend RPL to enable for simultaneous use of disjoint multiple paths. This is done on top of the already maintained DODAG structure with the least induced overhead. Furthermore, we suggest applying a low-complexity encoding method on the captured images. Based on both QoS and QoE metrics, we evaluate the performance of our disjoint multipath RPL (DM-RPL) for real video clip transmission using the IoT-LAB testbed. Our results show that multipath provides more bandwidth as the PDR is increased. Video quality is further improved thanks to the adopted data reduction at the source. All of this translates into less energy being consumed.**

***Index Terms*—Internet of Multimedia Things (IoMT) ; RPL ; Multipath routing ; Visual data transmission ; Performance evaluation ; QoE ; QoS ; Contiki OS ; IoT-Lab.**

I. Introduction

The IoMT has undergone an unprecedented development these last years. This is confirmed by the massive use of multimedia applications in various fields such as smart homes and industrial monitoring. However, IoMT has stringent requirements compared to traditional IoT in terms of quality of service (QoS) as well as quality of experience (QoE). When it comes to handle multimedia applications characterised by their high data rate in wireless sensor networks (WSN), one of the basic building blocks of the IoT, the problem becomes more challenging because of their constrained resources.

RPL [1] is the IETF standardised IPv6 Routing Protocol for low-power and lossy networks (LLNs) where directed-oriented acyclic graphs (DODAG) rooted at the sink are maintained. An objective function is used by each node to select its preferred parent toward the root node. Two objective functions namely, *ETX* [2] (default) and *OF0* (hops number) are predefined. Despite the fact that RPL almost meets the requirements of LLNs to handle scalar data routing, it is still far from being able to allow real time streaming of video flows as it was mainly designed for low data traffic network [3]. To handle multimedia applications, some researchers proposed new objective functions based on energy [4], [5] or free bandwidth [6]. The proposed objective functions allow better behaviour when compared to predefined ones. However, the performance evaluation in both [4] and [6] does not consider real video traffic and the user QoE is not evaluated either. As for [5], simulations are based on H. 264 multimedia trace [7]. Nonetheless, H. 264 compression is not adapted to low-power video sensors [8]. Besides, the user QoE has not been assessed.

Multipath routing [9] has emerged in the last decades as a promising solution to provide sufficient bandwidth to handle high data rate flows. Extending RPL to allow for multipath routing has already been considered in the literature mainly to balance traffic among bottleneck nodes [10]–[12], improve data transmission reliability through replication [13] or mitigate congestion [14], [15]. The above multipath extensions are targeted to scalar data reporting and mostly make use of braided (non-disjoint) paths. More recently, authors of [16] leverage the RPL multi-instance opportunity to build multiple paths to enhance video delivery in the IoMT. A priority-based strategy is implemented where high priority frames are routed via the instance maintained using link quality as a metric and the low priority ones via the instance with the shortest path. They mainly showed by simulation that the disjoint multipath is more suitable to video delivery when compared to single and non-disjoint RPL variants.

Since a wireless network capacity is limited even with multipath routing, it still remains difficult to provide sufficient bandwidth able to satisfy the requirements of data intensive applications such as IoMT ones. Low complexity in-network data reduction is more than necessary to lower transmissions and the corresponding energy expenditure. Widely used standard video encoding techniques based on motion estimation algorithms such as MPEG-4, H.263 or H.264 are not suitable for sensor nodes [8].

In this paper, we aim to handle video delivery in the IoMT by addressing both facets of bandwidth scarcity problem. First, we propose a new algorithm to obtain disjoint multiple paths in RPL. Our extension do not leverage the multi-instance opportunity provided by RPL as in [16]. Instead, it uses existing RPL control messages to insure disjointness through

the use of the IDs of the last hop nodes toward the DODAG root. Second, we make use of low-complexity video encoding more adapted to LLNs to reduce the amount of transmitted data. Our performance evaluation considers both QoS and QoE metrics and is carried on a real WSN testbed (IoT-LAB [17]). To the best of our knowledge, this is the first work that evaluates video transmission using multipath RPL on top of a real testbed with real video streams emulation. In this paper, we begin by presenting our disjoint multipath RPL (DM-RPL) protocol in Section II. Afterwards, the compression method is presented in Section III. The experimental scenario and the obtained results are discussed in Section IV before concluding.

II. Disjoint Multipath RPL (DM-RPL)

The IoMT is made of a large number of small low-power devices that integrate sensors with on-board processing and wireless communication capabilities. Some of these devices ideally placed at strategic positions, are equipped by video cameras to provide richer and more informative data on an area of interest. These sensor nodes are generally in charge of reporting information to a central gateway called the *Sink*. This delivery model is known as *convergecast* or multipoint to point communication.

A WSN can be modelled as a unidirected connected graph $G(V, E)$ composed of a set of sensor nodes V and a set of links E. We consider the use of RPL to establish and maintain a DODAG structure rooted at the Sink $r \in V$ according to an appropriate objective function. This is achieved through the use of ICMPv6 packets called *DODAG Information Objects* (DIO). Based on the DODAG structure, each node v maintains a list of parents, one of which is designated as the preferred parent noted $\pi(v)$. A node willing to transmit data to the Sink, sends packets to its preferred parent. Let $T(V, E_T)$ be the spanning tree of G, rooted at the Sink (r), obtained by considering only links to preferred parents in the RPL DODAG rooted at r. We define the *depth* of a node (d) as the length (number of hops) of its tree path to the root. The tree root has a depth $d(r) = 0$ and a non-root node $v \in T$ has a depth $d(v) = d(\pi(v)) + 1$. We call a *subtree* each tree rooted at a node $v \in T$ where $\pi(v) = r$ or equivalently $d(v) = 1$. The subtree rooted at v is noted T_v and v is designated as a *subroot*.

When dealing with high data rate applications, it is worth remembering the important limitations of LLNs. The available bandwidth is insufficient with respect to the requirements of these applications. In an attempt to provide additional bandwidth, we suggest to leverage simultaneous transmissions on multiple disjoint paths. To do so, we propose to extend monopath RPL to allow for simultaneous use of multiple disjoint paths without incurring much more overhead. The resulting protocol is called Disjoint Multipath RPL (DM-RPL).

Paths disjointness from two nodes u and v to r using tree T child-parent links is guaranteed if these nodes belong to two different subtrees i.e. $u \in T_{t_u}$ and $v \in T_{t_v}$ with $t_u \neq t_v$. For a given source s, the default path is the one that follows the preferred parent at each hop. To get other paths that

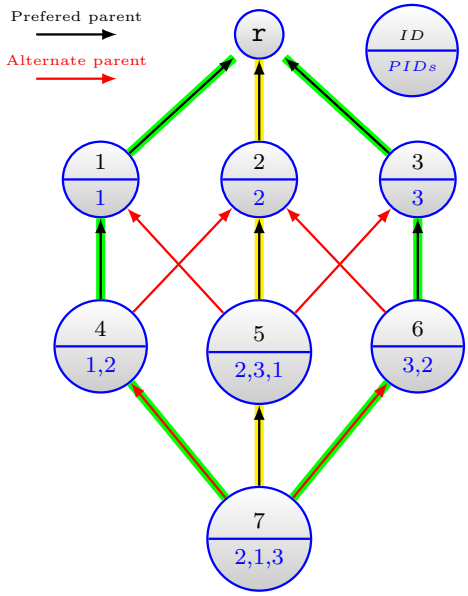


Fig. 1: Illustrative example

are disjoint, the source has to choose alternate parents that belong to different subtrees. In order to enable a node to identify the subtree to which belong each of its parents, one need to propagate the ID of each subroot downward. This is achieved by piggybacking this information in a field of DIO messages intended for this purpose we call PID (Path ID). It is initialised to zero in the initial DIO advertised by the DODAG root. Upon the reception of a DIO message from the DODAG root, a subroot inserts its ID in the PID field before advertising the obtained DIO to its neighbours. When a regular node (other than root and subroots) receives a DIO message with non-zero PID field, it broadcasts it as it is. Based on the DIO information, a regular node updates its parents list as suggested by default RPL except that it records the PID of each of them. When the above process converges, each node in G will learn the ID of its subroot which is the last crossed node before last hop as well as the potential parents leading to the root via disjoint paths.

Figure 1 illustrates how DM-RPL maintains multiple disjoint paths based on the DODAG structure and the subroot ID propagation downward using DIO messages. The DODAG root r broadcasts a DIO message with a zeroed PID field. Each of the subroots i.e. nodes 1, 2 and 3, chooses r as its preferred parent and puts its own ID in the PID field before broadcasting the resulting DIO. The other nodes (4, 5, 6 and 7), on the reception of a DIO, update the list of their parents. In each lower part of the circle representing a node, is given the list of the PIDs maintained where the first is the one related to the preferred parent. As depicted, node 4, for instance, has two disjoint paths via 1 and 2 respectively. For node 7, there are three possible paths highlighted in yellow for the primary one (via the preferred parent) and in green for the two alternative paths.

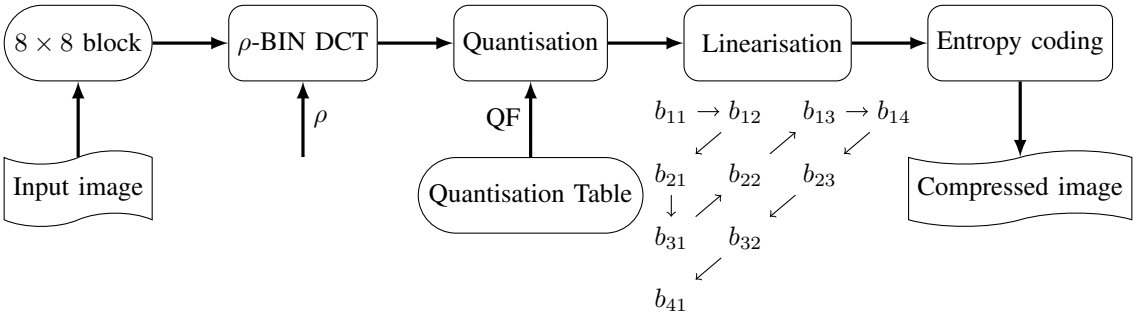


Fig. 2: M-frame block encoding sequence ($\rho = 4$).

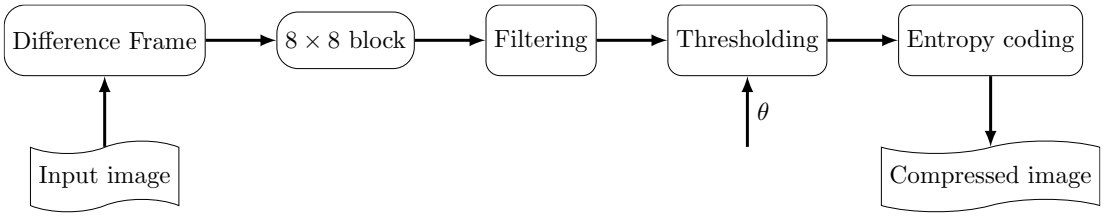


Fig. 3: S-frame encoding sequence

III. Low Complexity Video Compression

Since an LLN network capacity is limited even when multiple paths are involved, it still remains difficult to provide sufficient bandwidth able to satisfy the requirements of data intensive applications such IoMT ones. Having sensors to deliver all the captured visual data is inefficient and has to be avoided. Authors of [18] showed that multipath routing allows to double the overall throughput. However, an acceptable video quality was difficult to obtain even when capturing and transmitting at only 6 fps a grey-scale low resolution video clip compressed using MPEG-4. As a result, in-network data reduction is more than necessary to lower transmissions and the corresponding energy expenditure. As already stated, MPEG-4 is not suitable for sensor nodes. Even JPEG low complexity still image compression algorithm is not very beneficial in terms of power consumption. This is mainly due to the discrete cosine transform (DCT) stage which consumes at least 60% of the whole power encoder [19], [20]. In order to suite the constrained nature of processing resources of low-power motes, we suggest to use a low complexity image compression provided by SenseVid [21], a video transmission and evaluation tool that considers LLNs specific characteristics.

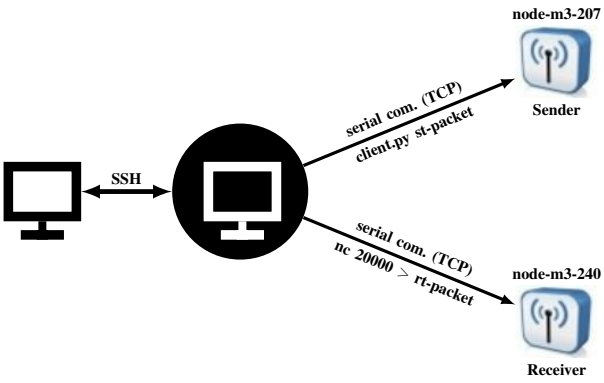
A captured image is either intra-coded (M-frame) or inter-coded with respect to the previous M-frame in which case it is referred to as an S-frame. Whether a given frame is M- or S-encoded depends on the GOP coefficient (g). If $MSE \leq g^2$ where MSE is the mean square error with respect to the previous M-frame, then the frame is S-encoded ; otherwise, it is M-encoded. When $g = 0$ then all the frames are M-encoded. Increasing its value results in more S-frames and thus reduces the data rate. In what follows the process of encoding is detailed for each frame type.

A. Main Frame Encoding

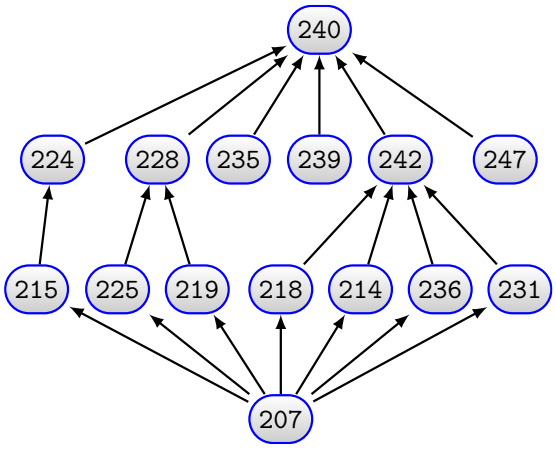
Figure 2 shows the different steps of an M-frame encoding process. First, the image is decomposed into blocks of 8×8. Then, a fast pruned DCT called binDCT-C [22] is applied on each block with a triangular pattern [23]. Only coefficients located at the upper left triangle of side length $\rho \leq 8$ are considered. The resulting DCT block coefficients are quantised using the JPEG standard quantisation matrix. Trade-off between quality level and compression rate can be obtained by selecting a proper quality factor (QF) that allows adjusting the quantisation matrix values. An image visual quality ranges from the poorest ($QF = 1$) to the best quality ($QF = 100$). The obtained block is then linearised following a zigzag scan before applying a lossless entropy encoding.

B. Secondary Frame Encoding

As shown in Figure 3, a secondary frame is inter-coded with respect to the previous main frame i.e. only blocks of the difference between the current frame and the previous M-frame are considered. To further save video sensors and network resources, a filtering and a thresholding operations are consecutively applied. Difference blocks with the least values that satisfy $\sum d_{ij}^2/64 \leq 650$ are ignored. The retained blocks with difference values less than θ are zeroed. θ is the *threshold similarity* parameter provided by the user. Finally, a lossless entropy encoding is applied on the resulting non-null blocks. Note that since not all blocks are transmitted, blocks sequences have to be specified in the packet header. The sequence number of the first block of a packet is given as it is. A subsequent sequence is encoded using the difference with the respect to the previous one.



(a) IoT-LAB interface with SenseVid.



(b) Tree Sample.

Fig. 4: IoT-lab Experiment Setup

IV. Experiment Results

Our experiments are made using IoT-LAB [17], a very large scale open experimental IoT testbed composed of 2728 static and mobile nodes distributed over six different sites in France (Strasbourg, Grenoble, Lille, Paris Saclay and Lyon). Three types of nodes, equipped with different micro-controllers and wireless communication chips, are provided namely, M3, A8 and WSN430 nodes. IoT-LAB can be accessed through a web portal or using provided command-line tools. Additionally, it offers a hosted environment on SSH front-ends with pre-installed command-line Tools and target architectures cross-compiler tool chains. It allows to retrieve experiments results and to access devices serial ports.

In order to assess the performances of our disjoint multipath routing, we extended the RPL implementation provided in the Contiki IPv6 network stack. The last two bytes of the IPv6 address of a node in IoT-LAB testbeds are used as an ID. Its uniqueness is ensured by the fact that only the last 16 bits are varied in the IPv6 address assignment and subnetting. In DM-RPL, this 16-bit ID is used to identify possible disjoint paths. The unused 7^{th} (*Flags*) and 8^{th} (*Reserved*) bytes of the DIO packet are chosen to constitute the PID field.

To carry out our experiments, we used M3 nodes[1] installed in the F4 corridor of Grenoble site. Figure 4b shows the 15 used nodes and represents a possible tree structure in which the links are those connecting each node to its best parent. Since IoT-LAB does not provide video sensors, we emulate the transmission of a real video clip (by the node 207 to the root 240) using a traffic trace file (*st-packet*) generated by SenseVid. As shown by Figure 4a, a python script (*client.py*) gives transmission instructions to the source node. The RPL-UDP sender and receiver modules are modified to enable the former to send packets according to the instructions and the latter to retrieve the list of received packets to be stored in a receiver trace file (*rt-packet*). Based on this latter, SenseVid reconstructs the video received images and generates QoE video related metrics, namely, PSNR and SSIM. The PSNR between the sent and the received, possibly distorted video frame is computed using :

$$PSNR = 20\ log\ \frac{V_{peak}}{MSE}$$

where MSE is the mean square error and V_{peak} is the maximum possible pixel value. The SSIM metric is computed as follows :

$$SSIM = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \times \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \times \frac{\sigma_{xy} + C_2/2}{\sigma_x\sigma_y + C_2/2}$$

where x and y are two non negative image signals, μ_x, σ_x and μ_y, σ_y are the mean and standard deviation of x and y respectively. σ_{xy} is the sample cross-covariance between x and y. $C_1 = 6.5025$ and $C_2 = 58.5225$.

We compare the performance of DM-RPL with default RPL and focus on the impact of increasing images frequency capture on their real time transmission. To do so and coping with LLNs constraints, we consider the transmission a given number ranging from 9 to 18 grey-scale images extracted from the original 300 ones of the hall monitor video clip [24]. Moreover, these images are down-sampled to a resolution of 128×128. We consider transmitting images encoded independently of each other (M-encoded) as well as the case of including some S-frames where the GOP coefficient g is set to 15 in order to reduce the data transmission rate as shown in Table I. Used parameters are regrouped in Table II. Each experiment is repeated at least 10 times to avoid fluctuation and obtained results are presented using box plots to show the distribution of obtained values of the metric of concern. A segment and a small black square inside each rectangle shows the median and the mean values respectively.

Although, our multipath extension allows to build more paths, we conducted our experiments using only two paths.

[1] https://www.iot-lab.info/docs/boards/iot-lab-m3/

TABLE I: Transmitted video characteristics

Images number	ref. PSNR (dB)		ref. SSIM		compression ratio (bpp)		transmission rate (Kbps)		packets to send		Frames sequence when $g = 15$
	$g = 0$	$g = 15$	$g = 0$	$g = 15$	$g = 0$	$g = 15$	$g = 0$	$g = 15$	$g = 0$	$g = 15$	
9	29.50	28.52	0.9081	0.8980	0.66	0.57	7.8	6.73	99	90	MMMMSMSMS
12	29.50	28.81	0.9010	0.8997	0.66	0.57	10.40	8.98	132	116	MMMMMSMMSMSM
15	29.50	28.05	0.9077	0.8959	0.66	0.52	13.01	10.32	165	140	MSMMMMSMSMSMSSM
18	29.51	28.31	0.9078	0.8960	0.66	0.51	15.6	11.94	198	162	MSMMMSMSSMSMSMSSMM

TABLE II: Experimental Setup

Number of sensors	15 (including the root)
Testbed site	INRIA Grenoble
Experiment duration	10 min
operating system	Contiki OS
Sensors type	M3 open nodes
Packet maximum payload	128 Bytes
Transport protocol	UDP
Routing protocol	(IPv6) RPL ,DM-RPL
RPL objective function	ETX
DIO maximum interval	17.5 min
DIO minimum interval	4 sec
MAC	CSMA / link-layer bursts
Radio Duty Cycling	ContikiMAC
Channel check rates (Hz)	128
transmission power	0 dbm
reception sensitivity	101 dBm
Video duration	12 seconds
Frame resolution	128x128
Number of captured images	9, 12, 15, 18
GOP Coefficient (g)	0, 15
Quality Factor	5
DCT	Triangular BIN DCT
DCT triangle side length ρ	8
Entropy coder	Exponential-Golomb (EG)

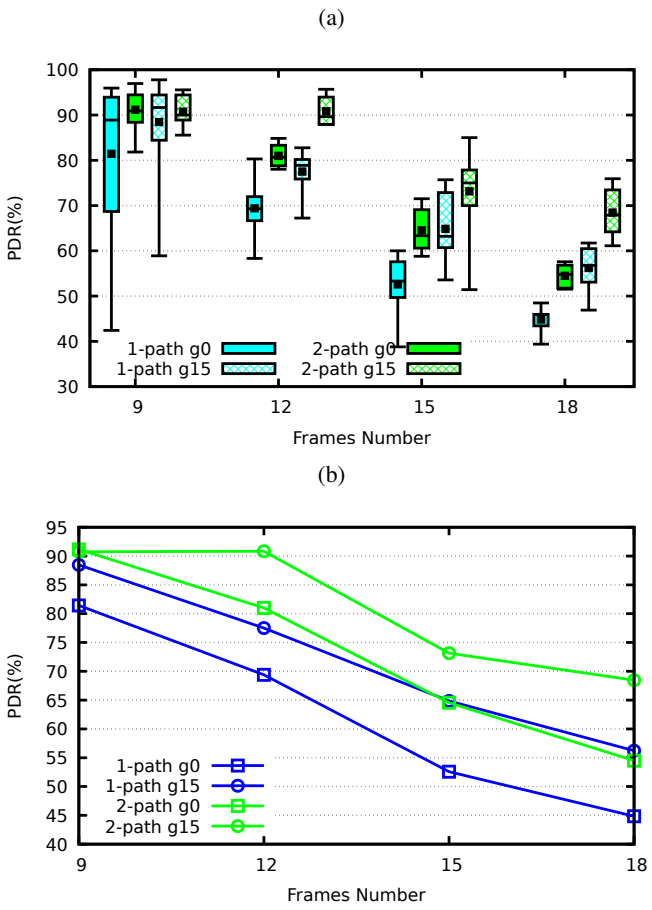
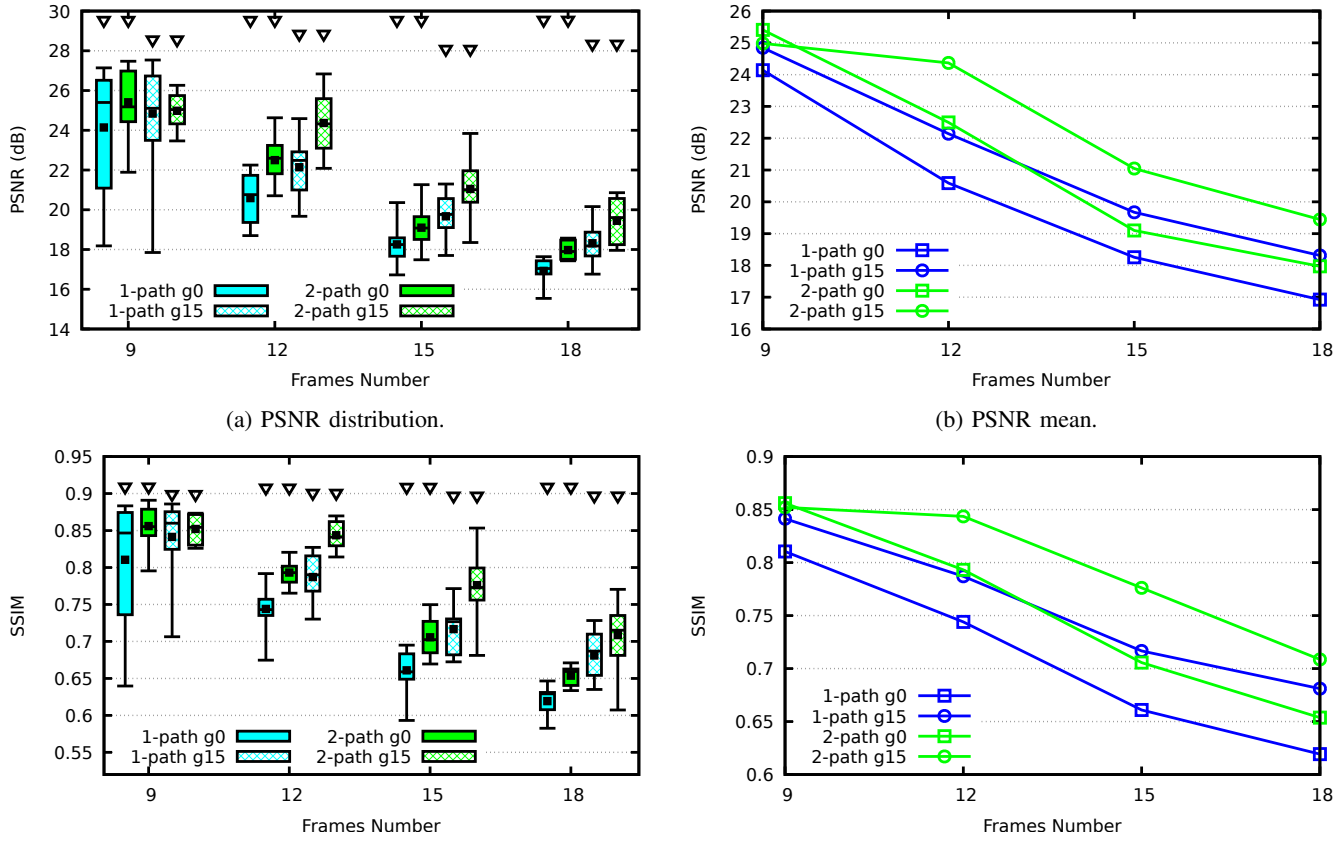


Fig. 5: PDR (a) distribution and (b) mean values

The obtained results and lessons learnt using two paths can be generalised to more paths and are expected for a future work. We first consider the packet delivery ratio (PDR) obtained by RPL (1-path) and DM-RPL (2-path) with the two sequences of frames ($g0$ and $g15$). As expected, Figure 5 shows a decreasing PDR when increasing the number of images to transmit due to a higher number of packets to transmit in a limited time window. Based on the mean PDR, DM-RPL outperforms RPL regardless of the transmission rate. DM-RPL is able to provide more bandwidth thanks to splitting the data flow on the two disjoint paths. Reducing the required bandwidth by inter-coding some of the frames ($g = 15$) allows to achieve better performances in terms of PDR when compared to the case where all frames are intra-coded ($g = 0$). This observation is valid for both RPL and DM-RPL.

Transmission rate reduction thanks to the introduction of S-frames leads to lower quality of images when compared to the use of only M-frames as shown by the obtained reference PSNR and SSIM given in Table I. Hence, the quality of the received images has to be considered in the evaluation. Figure 6 shows both mean and distribution plots of the obtained PSNR and SSIM of the received images as reconstructed by SenseVid considering the incurred packet losses. Triangles in the candles curves depict the reference PSNR and SSIM. Once again, the quality is getting worse when increasing the transmission rate. The images quality is still fair ($PSNR > 20$) for the evaluated schemes provided that the number of frames does not exceed 12. When using two paths along with more data reduction (2-path, $g15$), the quality remains acceptable even for the highest rate i.e. 18 frames captured and transmitted in real time. Note that the obtained PSNRs and SSIMs are higher when $g = 15$ compared to $g = 0$ even if the corresponding reference values are better in the latter case.

Figure 7 shows samples of the frame 3 when 12 images are captured and transmitted. The rightmost image is the one transmitted by the source. The others are those received by the Sink when using the four evaluated schemes. Data reduction



(a) PSNR distribution.

(b) PSNR mean.

(c) SSIM distribution.

(d) SSIM mean.

Fig. 6: Obtained Images Quality

strategy is profitable mainly when two paths are used where both PSNR and SSIM are improved.

Figure 8 plots the average consumed power for the different evaluated schemes when varying the number of captured frames. The results show that DM-RPL exhibits lower energy consumption compares to RPL. This is due to the fact that in DM-RPL, the traffic load is balanced on two paths. Thus, experimenting a lower number of packet losses which reduces the amount of MAC level retransmissions leading to lower energy expenditure.

V. Conclusion

In an attempt to handle multimedia traffic in constrained LLNs, we propose to extend RPL such that multiple disjoint paths can be maintained and used by video sensors. Moreover, we leverage low complexity compression techniques to cope with limited sensors resources. We carried out experiments using real WSN testbed and real video clip transmission. Both QoS (PDR and energy) and QoE (PSNR and SSIM) were adopted to assess the added value of our proposal. We mainly showed that using two paths allows to provide more bandwidth such that the amount of successful transmissions is improved. Our used data reduction technique allows additionally for better images quality. Energy consumption is also improved.

Despite the obtained results, there is still a way to go to enhance the received images quality mainly when increasing the capture frequency. As a future work, we expect to improve our multipath strategy to obtain the best paths possible. Moreover, advanced encoding techniques with better optimised rate-distortion have to be investigated. Transmission strategies involving interleaving techniques are under study. Finally, advanced methods for image reconstruction with denoising and deblurring are to be explored.

Acknowledgement. Authors thank FIT IoT-LAB project for providing testbed and tools to perform this paper experiments.

References

[1] R. Alexander, A. Brandt, J. Vasseur, J. Hui, K. Pister, P. Thubert, P. Levis, R. Struik, R. Kelsey, and T. Winter, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550, Mar. 2012. [Online]. Available: https://rfc-editor.org/rfc/rfc6550.txt

[2] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *Proceedings of the 9th ACM International Conference on Mobile Computing and Networking (MobiCom '03)*, San Diego, California, September 2003.

[3] S. Kettouche, M. Maimour, and L. Derdouri, "Qoe-based performance evaluation of video transmission using rpl in the iomt," in *2019 7th Mediterranean Congress of Telecommunications (CMT)*, Oct 2019, pp. 1–4.

(a) Transmitted frame PSNR=29.530 SSIM=0.907 (b) 1-path, g=0 PSNR=20.1803 SSIM=0.747 (c) 2-path, g=0 PSNR=22.1850 SSIM=0.802 (d) 1-path, g=15 PSNR=19.819 SSIM=0.767 (e) 2-path, g=15 PSNR=24.319 SSIM=0.850

Fig. 7: Sample images for frame 3 when 12 frames are captured.

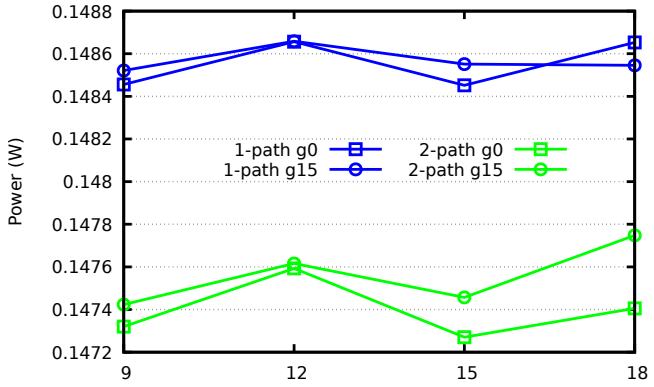


Fig. 8: Mean Power Consumption

[4] S. A. Alvi, G. A. Shah, and W. Mahmood, "Energy efficient green routing protocol for internet of multimedia things," in *2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*. IEEE, 2015, pp. 1–6.

[5] F. Mortazavi and M. Khansari, "An energy-aware rpl routing protocol for internet of multimedia things," in *Proceedings of the International Conference on Smart Cities and Internet of Things*, ser. SCIOT '18. New York, NY, USA: ACM, 2018, pp. 11:1–11:6. [Online]. Available: http://doi.acm.org/10.1145/3269961.3269965

[6] H. Bouzebiba and M. Lehsaini, "Freebw-rpl: A new rpl protocol objective function for internet of multimedia things," *Wireless Personal Communications*, pp. 1–21, 2020.

[7] P. Seeling, M. Reisslein, and B. Kulapala, "Network performance evaluation using frame size and quality traces of single-layer and two-layer video: A tutorial," *Communications Surveys Tutorials, IEEE*, vol. 6, no. 3, pp. 58–78, Third 2004.

[8] B. A. B. Sarif, M. Pourazad, P. Nasiopoulos, and V. C. M. Leung, "A study on the power consumption of H.264/AVC-based video sensor network," *International Journal of Distributed Sensor Networks*, vol. 11, no. 10, p. 304787, 2015. [Online]. Available: https://doi.org/10.1155/2015/304787

[9] M. Maimour, "Interference-aware multipath routing for WSNs: Overview and performance evaluation," *Applied Computing and Informatics*, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2210832717303009

[10] O. Iova, F. Theoleyre, and T. Noel, "Exploiting multiple parents in RPL to improve both the network lifetime and its stability," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 610–616.

[11] M. N. Moghadam and H. Taheri, "High throughput load balanced multipath routing in homogeneous wireless sensor networks," in *2014 22nd Iranian Conference on Electrical Engineering (ICEE)*. IEEE, 2014, pp. 1516–1521.

[12] L. Zhu, R. Wang, and H. Yang, "Multi-path data distribution mechanism based on rpl for energy consumption and time delay," *Information*, vol. 8, no. 4, p. 124, 2017.

[13] T. Lagos Jenschke, R.-A. Koutsiamanis, G. Z. Papadopoulos, and N. Montavont, "ODeSe: On-demand selection for multi-path RPL networks," vol. 114, 2021.

[14] M. A. Lodhi, A. Rehman, M. M. Khan, M. Asfand-e yar, and F. B. Hussain, "Transient multipath routing protocol for low power and lossy networks." *KSII Transactions on Internet & Information Systems*, vol. 11, no. 4, 2017.

[15] Z. Wang, L. Zhang, Z. Zheng, and J. Wang, "Energy balancing RPL protocol with multipath for wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 11, no. 5, pp. 1085–1100, 2018.

[16] I. Bouacheria, Z. Bidai, B. Kechar, and F. Sailhan, "Leveraging multi-instance rpl routing protocol to enhance the video traffic delivery in iomt," *Wireless Personal Communications*, pp. 1–30, 2020.

[17] C. Adjih, E. Baccelli, E. Fleury, G. Harter, N. Mitton, T. Noel, R. Pissard-Gibollet, F. Saint-Marcel, G. Schreiner, J. Vandaele *et al.*, "Fit iot-lab: A large scale open experimental iot testbed," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. IEEE, 2015, pp. 459–464.

[18] Z. Bidai and M. Maimour, "Interference-aware multipath routing protocol for video transmission over zigbee wireless sensor networks," in *the 4th International Conference on Multimedia Computing and Systems*, IEEE, Ed. Marrakesh, Morocco: IEEE, April 14-16 2014.

[19] C. N. Taylor, D. Panigrahi, and S. Dey, "Design of an adaptive architecture for energy efficient wireless image communication," in *Embedded processor design challenges*. Springer, 2002, pp. 260–273.

[20] "Energy efficient image coding techniques for low power sensor nodes: A review," *Ain Shams Engineering Journal*, vol. 9, no. 4, pp. 2961 – 2972, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2090447917301247

[21] M. Maimour, "Sensevid: A traffic trace based tool for qoe video transmission assessment dedicated to wireless video sensor networks," *Simulation Modelling Practice and Theory*, vol. 87, pp. 120–137, September 2018.

[22] J. Liang and T. D. Tran, "A fast multiplierless approximations of the dct with the lifting scheme," *IEEE Transactions on Signal Processing*, vol. 49, no. 2, pp. 3032–3044, December 2001.

[23] A. Mammeri, A. Khoumsi, D. Ziou, and B. Hadjou, "Modeling and adapting jpeg to the energy requirements of VSN," in *Computer Communications and Networks, 2008. ICCCN '08. Proceedings of 17th International Conference on*, 2008, pp. 1–6.

[24] "Yuv video sequences." [Online]. Available: http://trace.eas.asu.edu/yuv/index.html

Modularity maximization to find community structure in complex networks

Bilal SAOUD
dept. Electrical engineering
University of Bouira
Bouira, Algeria
bilal340@gmail.com

***Abstract*—Complex networks have in generally communities. These communities are very important. Network's communities represent sets of nodes, which are very connected. In this research, we developed a new method to find the community structure in networks. Our method is based on flower pollination algorithm (FPA) witch is used in the splitting process. The splitting of networks in our method maximizes a function of quality called modularity. We provide a general framework for implementing our new method to find community structure in networks. We present the effectiveness of our method by comparison with some known methods on computer-generated and real-world networks.**

***Index Terms*—Community detection, Networks, Flower pollination algorithm, Normalized mutual information, Modularity**

I. Introduction

Many systems can be represented by network or graphs, which makes them very powerful structure. A network G is defined by two sets [1]. The first set is vertex set V (node set) and the second is edge set E. Vertexes share relationships between them. Relationships are represented by edges. In general, the number of nodes is $|V| = n$ and edges is $|E| = m$. Euler's solution of the Seven Bridges of Königsberg problem is considered to be the first use of networks to represent systems [2]. Today networks are used to illustrate several systems. For instance, in social network, which is an interaction between entities (persons, groups of persons, organizations, web sites, ...), can be represented by a network with two sets V and E. Vertexes stand for entities (for example persons) and edges stand for relationships between entities (for examples between persons). Analyzing and understanding a network leads to understand better the system. Among features that can help to understand the structure of a network, we can find the community structure.

Community structure exists in networks and it gives more information about the network. For instance, we can understand very well the system, which is represented by a network, by finding its community structure and the relationship between communities. In addition, networks can represent many systems like social networks, electric networks, biological networks, etc. It is vital to develop new methods to find network's communities. When we analyze networks by studying relationships between nodes we can get extra information about networks and systems. In general, nodes in the same community have common properties or insure similar tasks in network. Basically, a network has parts that are more densely connected than other parts. In other words, the nodes in these parts share many edges between them. These parts of nodes and edges are called communities (clusters). Finally, many studies have been done around networks and how to find community structure.

Many community structure detection methods have been developed [3]. According to the type of network, we can find methods for uniparitie/bipartite networks, weighted/unweighted networks and directed/undirected networks. Furthermore, methods can be classified into different classes such as hierarchical methods (merging or splitting), methods that are based on maximization of an objective function. Some methods find disjoint communities, where intersection between communities is empty. However, other methods were designed to find overlapping communities, for instance the method in [4], where the intersection between communities is not empty.

In this paper, we address the problem of finding community structure in networks. We present a new method to discover community structure in unweighted and undirected networks. Our method is based on nature-inspired metaheuristics algorithm. We have developed our method based on the pollination process of flowers [9]. Our method is an hierarchical one. It is based on the splitting of a given network $G(V, E)$, which models a system. Splitting step in our method is done by the flower pollination algorithm (FPA) [9] in order to optimize the function of quality called modularity Q. The process of splitting will be stopped when the graph G has been disconnected, which means that each node of G represents a community. Finally, our method builds a dendrogram and finds the the most optimal community structure $\pi = \{c_1, ..., c_k\}$, such as $\bigcup_{i=1}^{k} = V$ and $c_i \neq \emptyset$, $c_i \cap c_j = \emptyset$ (for $i, j = 1 : k$).

The paper is organized as follows. The concept of FPA is presented in Section II. Our approach is detailed in Section III. Experimental results and discussions are given in Section IV. Finally, Section V concludes the paper.

II. FPA Presentation

Flower pollination is an interesting phenomena in nature. Based on the studying flower pollination process, a new algorithm of optimization was designed by Yang in [9]. The algorithm has been named Flower Pollination Algorithm (FPA). In nature pollination can be abiotic form or biotic form. In general, 90% of flower have biotic pollination where the pollen is transferred by animals (pollinator) like insects. Biotic pollination by bees for instance can be done at long distance.

FPA has three steps [9] described in the following:

- In the first step, the algorithm initializes its parameters and generate the initial population. The best solution is found also in the first step.
- The second step, flowers in population start doing pollination in d-dimensional search (solution space). Flowers can choose a local or global pollination at every iteration in the search space. The algorithm switch between local pollination and global pollination based on probability $p \in [0, 1]$. Flowers location represent the vector of solutions vector and the value of objective function for every solutions is estimated. According to the value of objective function the new solution is evaluated and updated at every iteration and the best solution will may be improved.
- In the final step, the algorithm stops after some iterations and the best solution will be selected.

FPA can converge very fast and can escape the problem of local minima because it makes the long distances movement based on levy flight [10]. FPA can be used to solve diffrent problems like in [8].

III. A new method to find communities in networks

In this section, we present our hierarchical method to discover community structure in networks. Hierarchical methods can be divisive or agglomerative. Our method is hierarchical divisive method. Network is divided by our method based on the maximization of the function of quality called modularity [6]. Our method is designed to find community structure in networks with only a single type of vertex and undirected, unweighted edge.

We can measure the strength of a community structure by the function of quality called modularity [6]. Modularity function Q is based on the observed edges fraction $e(c_i)$ within communities and the expected edges fraction $a(c_i)$ within the same communities, $Q = \sum_{c_i} e(c_i) - a(c_i)^2$. Modularity can be estimated for undirected and unweighted graph $G(V, E)$ as:

$$Q = \frac{1}{2m} \sum_i \sum_j (A[i,j] - P[i,j]) \delta(c_i, c_j) \qquad (1)$$

where n is the number of nodes in G $(n = |V|)$, m is the number of edges in G $(m = |E|)$ and the community structure is $\pi = \{c_1, ..., c_k\}$. $A_{n,n}$ represents the adjacency matrix of $G(V, E)$. For any vertex $i \in V$, d_i is the degree of node i and c_i its community. The matrix A takes two values 1 or 0 if there is an edge between node i and j then $A[i, j] = 1$ or $A[i, j] = 0$ if there is not a connection between i and j. $P_{n,n}$ represents the adjacency matrix that corresponds null model. In the null model the probability of an existing edge between vertexes i and j is $P_{i,j} = \frac{d_i \times d_j}{2m}$. Finally, δ function is given as follows:

$$\delta(c_i, c_j) = \begin{cases} 1 \; if \; c_i = c_j \\ 0 \; otherwise \end{cases} \qquad (2)$$

Values of Q are between 0 and 1. Q closer to 1 indicates stronger community structures. According to Clauset et al. [6], a value above about 0.3 is a good indicator of significant community structure in a network.

Let $G(V, E)$ be an undirected and unweighted network, where $V = (v_1, ..., v_n)$ is the set of vertexes, $E = (e_1, e_2, ..., e_m)$ is the set of edges. The goal of our community detection method is to partition the network G into k communities (groups): $\pi = \{c_1, c_2, ..., c_k\}$, where $c_i \neq \emptyset$, $c_i \cap c_j = \emptyset$, $(i = 1 : k, j = 1 : k)$ and $V = \bigcup_{i=1}^{k} c_i$. In addition, our method finds the community structure π of the network G with the greatest value of modularity Q. To reach this goal, we used a FPA. Our method splits $G(V, E)$ into two new networks G_1 and G_2. Nodes of each new network represent a community. Nodes of G_1 represent a community c_1 and nodes of G_2 represent a community c_2. The splitting is based on FPA in order to maximize the value of modularity function Q. Then, G_1 and G_2 will be split until the network G has been disconnected. At the end of our method each node in $G(V, E)$ represents a community. Finally, we get a dendrogram for our method and the community structure will be chosen based on value of modularity Q or the number of communities.

The general algorithm of our method to find community structure is as follows:

Algorithm 1: The algorithm of our method

Data: $G(V, E)$
Result: dendrogram
1 $\pi = FPA()$, find a partition π based on FPA;
2 Divide G based π, $G = G_1 + G_2$;
3 Update the matrix of merge M for a final dendrogram;
4 Go to *Steps 1* for each graph G_1 and G_2;
5 Return the final dendrogram;

Fig. 1 shows the dendrogram that was built by our method on Zachary's Karate Club network [11]. Our method gave a community structure with two communities, which were separated by vertical lines on dendrogram. Labels of dendrogram are nodes (members of Zachary's Karate Club). The community structure that was found by our method on the same network is also represented in Fig. 2. In this figure, communities' nodes have different colors and shapes.

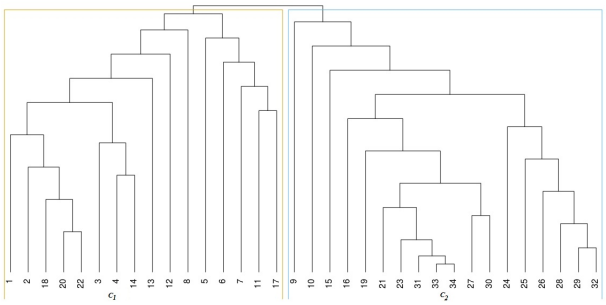


Fig. 1. The dendrogram of Zachary's Karate Club network created by our method.

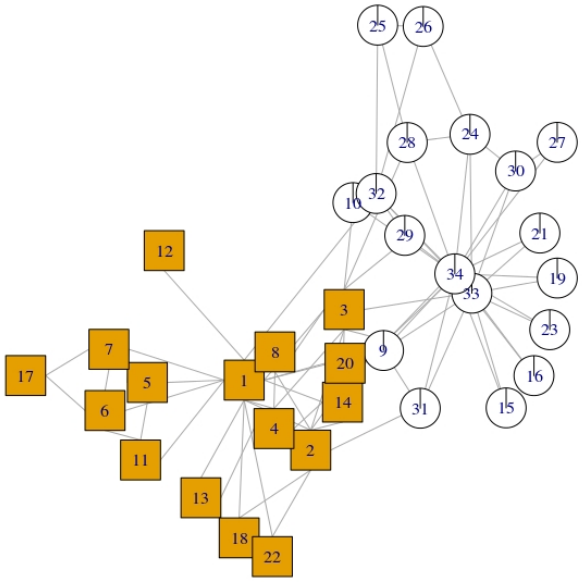


Fig. 2. Zachary's karate club network community structure is detected by our method.

IV. Experiments and Results

To evaluate our method to find community structures in networks, we have tested it on computer-generated and several real networks (Zackary's Karate Club [11], American College Football [5], Dolphins [16], Books about US Politics [17], Jazz musicians [18], Word adjacencies [19] and Les Miserables [20]). We have compared our method with some well-known methods: fast greedy method [6], label propagation method [7], and infomap method [12].

A. Normalized Mutual Information

The comparison of our method with other methods is done based on the normalized mutual information (NMI) function [13]. The NMI is a powerful function to compare a community structure that was founded by methods with the real community structure. The value of NMI is based on defining a confusion matrix N, where the rows represent the real communities, and the columns represent the found communities. N_{ij} is the number of nodes in the real community that appears in the found community j. For two partitions A and B, the partition A represents the real partition with c_A communities and B represents the found partition with c_B communities, The normalized mutual information (NMI) is estimated as follows:

$$NMI(A,B) = \frac{-2\sum_{i=1}^{c_A}\sum_{j=1}^{c_B} N_{ij}\log(\frac{NijN}{N_{i.}N_{.j}})}{\sum_{i=1}^{c_A} N_{i.}\log(\frac{N_i}{N}) + \sum_{j=1}^{c_B} N_{.j}\log(\frac{N_{.j}}{N})} \quad (3)$$

NMI values are in the range $[0,1]$. Partitions A and B are identical if $NMI(A,B) = 1$.

B. Dataset based on computer-generated networks

Our method is tested on computer-generated networks benchmark proposed by Lancichinetti et al. [14]. The benchmark parameters are the number of nodes N, the exponents γ and β of the degree and community size distribution respectively (both distributions are power laws), the number of average degree $\langle k\rangle$, number of communities N_c, and the mixing parameter μ. Each node shares a fraction $(1-\mu)$ of its links with other nodes of its community and a fraction μ with the other nodes of the network.

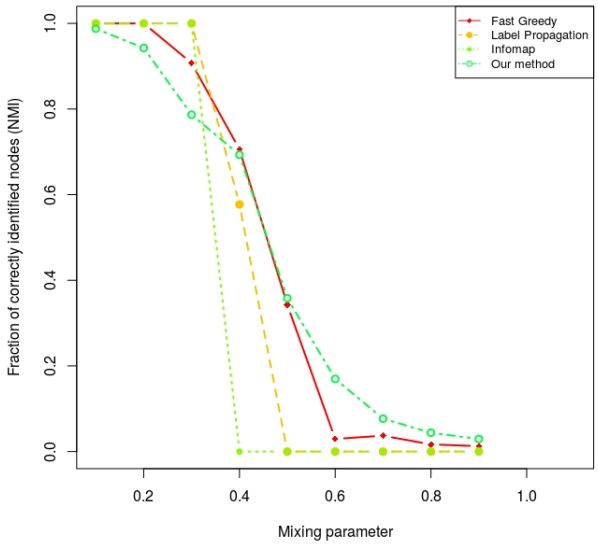


Fig. 3. NMI vs. mixing parameter μ.

Fig. 3 shows the variation of the NMI obtained by our method, fast greedy method, label propagation method and infomap method on the benchmarks networks, with the parameters: mixing parameter μ between 0.1 and 0.9, $\langle k\rangle = 16$, $\gamma = 3$, $\beta = 2$, $N = 128$ and $N_c = 4$.
The value of NMI obtained by our method is high when μ changes from 0 to 0.5 and the same thing with other methods. At this range, nodes share many edges with nodes of its community that makes the community structure very clear and easy to find. Methods could group the most nodes in the correct communities when the mixing parameter μ is in $[0, 0.5]$. When μ is in $[0.5 - 0.9]$ range, it is difficult for all methods to find the true community structure. At this range

nodes share few edges with nodes of its community and many edges with nodes from other communities, which makes the community structure unclear and difficult to find. However, our method is still more accurate than the other methods. Our method evaluates the community structure at each step of splitting process and at the end our method selects the best community structure based on modularity value. From Fig. 3, we see that our method can discover community structure better than fast greedy, label propagation method and infomap method when μ is greater than 0.5.

Fig. 4 illustrates the result of our method on network generated by computer with mixing parameter $\mu = 0.8$. Fig. 4 shows the different communities that were found by our method. On this network with a mixing parameter $\mu = 0.8$, our method found a community structure (π) with eight communities ($\pi = \{c_1, c_2, ..., c_8\}$). Dendrogram labels stand for nodes. In this example, we have a network with 128 nodes. We mention that the community structure can be found by breaking the dendrogram (Fig. 4) at different levels [15]. In our case, we have chosen to break the dendrogram at the level which maximizes the modularity function.

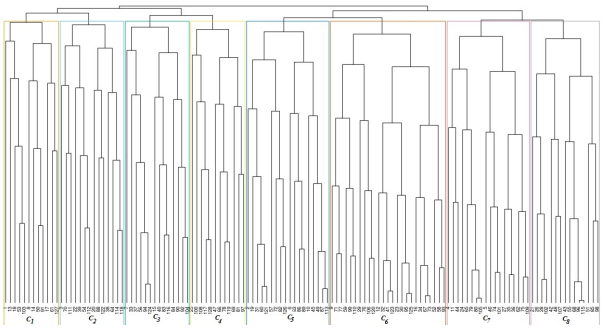


Fig. 4. The dendrogram and community structure by our method on computer generated network with mixing parameter $\mu = 0.8$.

C. Dataset based on real networks

In this section, we give the simulation results of our method, fast greedy, label propagation and infomap on real networks. We considered some real networks drawn from disparate fields (Zachary [11], Dolphins [16], Football [5] and Books about US politics [17]), where the community structure is known, which made them suitable to evaluate community detection methods.

1) Zachary's club network [11] is a real network that corresponds to a social network of friendships between 34 members of a karate club at a university in the United States in the 1970 ($n = 34$ and $m = 78$). The network has two clusters.
2) Dolphins Network [16] is an undirected social network of frequent associations between 62 dolphins in a community living off Doubtful Sound, New Zealand. This network ($n = 62$ and $m = 159$) has two communities.
3) College football network [5] represents the schedule of Division I Games for the year 2000 season. This network is made of 115 teams (nodes) and 613 edges. It is divided into 12 groups.
4) Books about US politics Network [17] is a network of books about US politics published around the time of the 2004 presidential election and sold by the online bookseller Amazon.com. Edges between books represent frequent purchasing of books by the same buyers. Compiled by Valdis Krebs. Books network has three communities.

Table I gives obtained results on networks. In this table, for each network we have estimated the value of modularity function according to equation 1, NMI values (according to equation 3) and we have mentioned the number of communities. As can be seen from Tables 1, methods find community structure with different number of communities. According to NMI values, our method can regroup the most nodes in the correct communities on Zachary's karate club, dolphin social network, American college football and books about US politics. On Zachary's karate club our method finds the same real community structure. On dolphin social network our method grouped more than 80% of nodes in the correct communities. Our method grouped 78% and 52% of nodes in correct communities on American college football and books about US politics respectively. The value of modularity by our method on these networks was above 0.3.

Fig. 5 and Fig. 6 show the community structure that was found by our method on Dolphins network and Books about US politics network. Each label represents a node and edges stand for the relationship between nodes. The community structure that was found by our method was represented by different shapes and colors. Nodes of the same community are represented by the same color and shape. Form these Fig. 5 and Fig. 6, we can see that nodes in the same community are more connected between them and have a few connection with nodes from other communities.

We evaluated the performance of our method with other different real networks without a known community structure. A brief description of these networks is given below.

- Jazz network is a collaborative network [18], which represents the association between jazz musicians. The jazz musicians are represented by nodes and edge existing between nodes just if two musicians played together. The network has $n = 198$ nodes and $m = 2742$ edges.
- Word adjacencies network represents the adjacency network of common adjectives and nouns in the novel *David Copperfield by Charles Dickens* [19]. It has $n = 112$ nodes and $m = 425$ edges.
- Les Miserables network is co-appearance network of characters in the novel *Les Miserables* [20]. The network has $n = 77$ nodes and $m = 254$ edges.

Table II gives results of our method, fast greedy, label

TABLE I
PERFORMANCE RESULTS ON REAL NETWORKS WITH KNOWN COMMUNITY STRUCTURE.

Methods	Karate			Dolphins			Football			Books		
	$\|c\|$	NMI	Q	$\|c\|$	NMI	Q	$\|c\|$	NMI	Q	$\|c\|$	NMI	Q
$Fast\ greedy$	3	0.69	0.38	4	0.55	0.49	6	0.70	0.54	4	0.53	0.50
$Label\ propagation$	4	0.70	0.41	3	0.76	0.48	11	0.85	0.58	3	0.50	0.47
$Infomap$	3	0.50	0.40	5	0.53	0.52	12	0.91	0.60	6	0.49	0.52
$Our\ method$	2	1	0.37	2	0.81	0.38	10	0.78	0.51	2	0.52	0.43

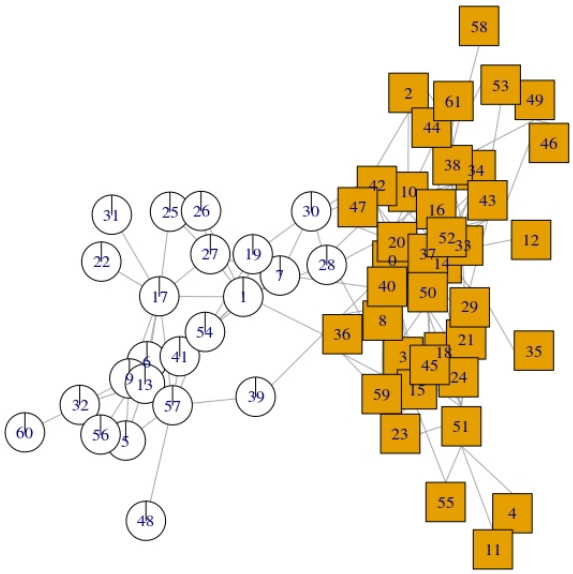


Fig. 5. Community structure of Dolphins network detected by our method and represented by different colors and shapes.

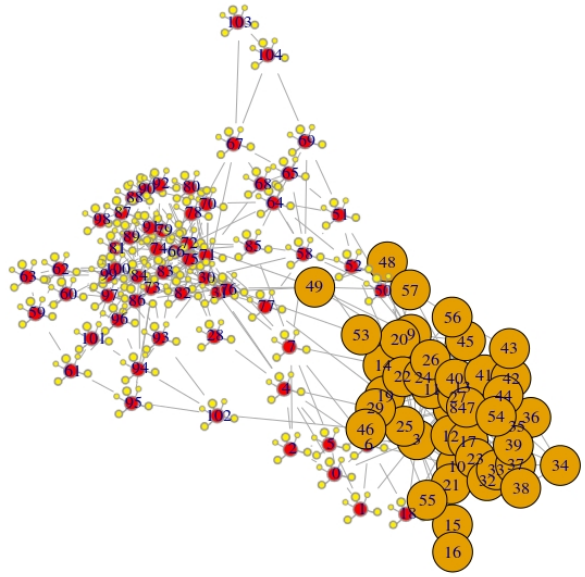


Fig. 6. Community structure of Books about US politics network detected by our method and represented by different colors and shapes.

propagation and Infomap. The number of communities and the estimated value of modularity were mentioned in Table II. From Table II, we can see that our method finds community structures with a high value of modularity. It is difficult to compare methods between them because we do not have a reference (a known community structure).

Fig. 7 shows the dendrogram, that was built by our method, and the community structure for Jazz network. Community structure that was found by our method has three communities. Labels of dendrogram represent nodes.

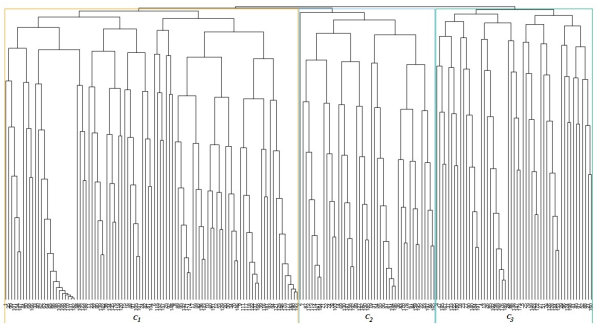


Fig. 7. The deprogram of Jazz network and the community structure by our method.

V. CONCLUSION AND FUTURE WORK

A new hierarchical method to discover the community structure for unweighted and undirected networks was presented in this paper. Our new method was developed based on maximization of function of modularity by FPA. Results obtained on computer-generated networks and real benchmark networks prove the efficiency of our method in terms of finding community structures with high values of modularity and accuracy.

Our method can be tested on large scale networks. We can develop it to find community structure in weighted or directed network. It can be extended to find overlapping communities.

REFERENCES

[1] MEJ. Newman, " Networks: an introduction," Oxford university press, 2010.

[2] B. Hopkins, RJ. Wilson, "The truth about Königsberg," The College Mathematics Journal, 35(3), pp. 198-207, 2004.

TABLE II
PERFORMANCE RESULTS ON REAL NETWORKS WITH UNKNOWN COMMUNITY STRUCTURE.

Methods	Jazz		Word adjacencies		Miserables	
	$\|c\|$	Q	$\|c\|$	Q	$\|c\|$	Q
Fast greedy	4	0.438	7	0.294	5	0.500
Label propagation	2	0.281	1	0	4	0.475
Infomap	7	0.280	2	0.009	9	0.546
Our method	3	0.346	6	0.264	7	0.505

[3] S. Fortunato, "Community detection in graphs," Phys Rep. 486, pp. 75-174, 2010.
[4] J. Chen, M. Liu, X. Liu, "Research on of overlapping community detection algorithm based on tag influence," Cluster Computing, 22(3), pp. 6669-6679, 2019.
[5] M. Girvan, MEJ. Newman, "Community structure in social and biological networks," Proc Natl Acad Sci USA, 99, pp. 7821-7826, 2002.
[6] A. Clauset, MEJ. Newman, C. Moore, "Finding community structure in very large networks," Phys Rev, 70, 66111, 2004.
[7] U. Raghavan, R. Albert, S. Kumara, "Near linear time algorithm to detect community structures in large-scale networks," Phys. Rev, E 76, 036106, 2007.
[8] G. Zhou, R. Wang, Y. Zhou, "Flower pollination algorithm with runway balance strategy for the aircraft landing scheduling problem," Cluster Computing, 21(3), pp. 1543-1560, 2018.
[9] XS. Yang, "Flower pollination algorithm for global optimization," in: Unconventional Computation and Natural Computation, Lecture Notes in Computer Science, 7445, pp. 240-249, 2012.
[10] E. Emary, HM.Zawbaa, M. Sharawi, "Impact of Lvy flight on modern meta-heuristic optimizers," Appl Soft Comput, 75, pp. 775-789, 2019.
[11] WW. Zachary : "An information flow model for conflict and fission in small groups," J Anthropol Res. 33, pp. 452-473, 1977.
[12] M. Rosvall, C. T. Bergstrom, "Maps of random walks on complex networks reveal community structure," Proceedings of the National Academy of Sciences of the United States of America, 105, pp. 1118-1123, 2008.
[13] L. Danon, A. Diaz-guilera, J. Duch, A. Arenas, "Comparing community structure identification," J Stat Mech, P09008, 2005.
[14] A. Lancichinetti, S. Fortunato, F. Radicchi, "Benchmark graphs for testing community detection algorithms," Phys. Rev. E 78, 046110, 2008.
[15] J. Abonyi, B. Feil, "Cluster analysis for data mining and system identification," Springer Science and Business Media, 2007.
[16] D. Lusseau, K. Schneider, O.J. Boisseau, P. Haase, E. Slooten, S.M. Dawson, "The bottlenose dolphin community of doubtful sound features a large proportion of long-lasting associations," Behav Ecol Sociobiol, 54, pp. 396-405, 2003.
[17] V. Krebs, unpublished, http://www.orgnet.com, 2019.
[18] P. M. Gleiser, L. Danon, "Community structure in jazz," Advances in Complex Systems, 6(4), pp. 565-573, 2003.
[19] MEJ. Newman, "Finding community structure in networks using the eigenvectors of matrices," Phys. Rev, E 74, 036104, 2006.
[20] D. E. Knuth, "The Stanford GraphBase: A Platform for Combinatorial Computing," Addison-Wesley, Reading, MA, 1993.

Behavioural verification of limited resources systems under true concurrency semantics

1st Bouneb. Messaouda
Department of mathematics and computer science
EL Arbi Ben Mhidi University
Oum El Bouaghi, Algeria
bounebm.univ@gmail.com

2nd Saidouni. Djamel Eddine
Department of computer science
Abed El Hamid Mehri Constantine2
Constantine, Algeria
saidounid@hotmail.com

***Abstract*—In this paper we propose a true concurrency semantics for limited resources systems using K-bounded Petri net as modeling formalism and maximality labeled transition system (MLTS) as semantics model. Indeed the model of MLTS expresses clearly the semantics of true parallelism of concurrent systems. The proposed operational maximality semantics for K-bounded Petri nets makes it possible to interpret any K-bounded Petri net in terms of MLTS. Through an example we show the interest of the proposed semantics in comparison with the interleaving semantics and the ST semantics. The comparison concerns the preservation of true concurrency and the reduction of the size of the semantics model. Furthermore, we will show that expected CTL properties may be verified on the corresponding maximality labeled transition system of a modeled system using our developed tool.**

***Index Terms*—Formal verification, maximality labeled transitions system, concurrent systems, K-bounded Petri net**

I. Introduction

Formal verification of complex systems is now a major issue in many areas. Indeed, the use of methods of specification and formal verification, assisted by powerful computer tools make the analysis of these systems reliable and guarantees a good compromise between cost and performance. The Petri net model is a graphical and mathematical modelling tool used to specify clearly concurrent systems behaviours. The marking graph associated to the Petri net is used to check the properties of the specified system. Indeed this markings graph is seen as a labeled transition system (LTS). However, the model of LTS is an interleaved model that makes abstraction of the parallel execution of transitions. To clarify the ideas, we recall the example of the two Petri nets of Figures 1.(a) and Figure 1.(b) presented in [1] [2]. The Petri net of Figure 1.(a) represents a system able of executing the transitions t_1 and t_2 in parallel, while the Petri net of Figure 1.(b) represents a system which executes either the transition t_1 then t_3 or the transition t_2 then t_4.

The marking graphs corresponding to the Petri net of Figure 1.(a) and Figure 1.(b) are given respectively by Figure 2.(a) and Figure 2.(b). When the transitions t_1 and t_4 are labeled by the action a and the transitions t_2 and t_3 by the action b, we remark that these marking graphs are isomorphic. Consequently, the parallel execution of the actions a and b

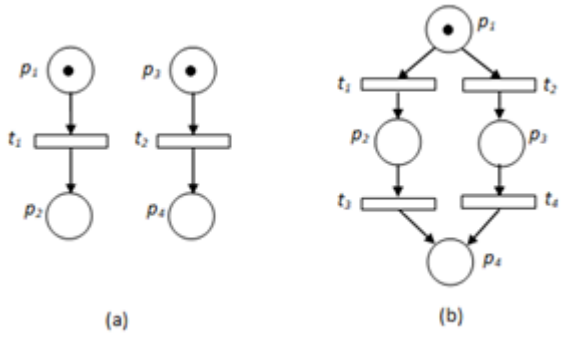


Fig. 1. Ordinary Petri net.

is interpreted as the interleaved execution of these two actions in time.

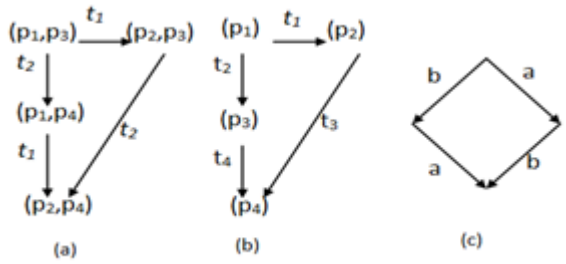


Fig. 2. Interleaving semantics.

This result is acceptable under the assumption that the firing of each transition corresponds to the execution of an indivisible action with zero duration (structural and temporal atomicity of the actions). This hypothesis is far from acceptable in the reality.

In order to accept the results of the verification, it is imperative that the constraints imposed by the real world are taken into account both by the specification and by the underlying semantic model. To support our claim, let us now reconsider that the transition t_1 (resp. t_4) consists of two sequential transitions t_{1-1} followed by t_{1-2} (resp t_{4-1} followed by t_{4-2}), the transitions t_{1-1} and t_{4-1} are labeled by the action

a_1 while the transitions t_{1-2} and t_{4-2} are labeled by the action a_2. The refined Petri nets as well as their labeled transitions systems are represented in Figure 3. It is clear that the behaviours of these two Petri nets are different. Indeed, in the first system, the execution of action b may occur between the execution of actions a_1 and a_2, which is not possible in the second system.

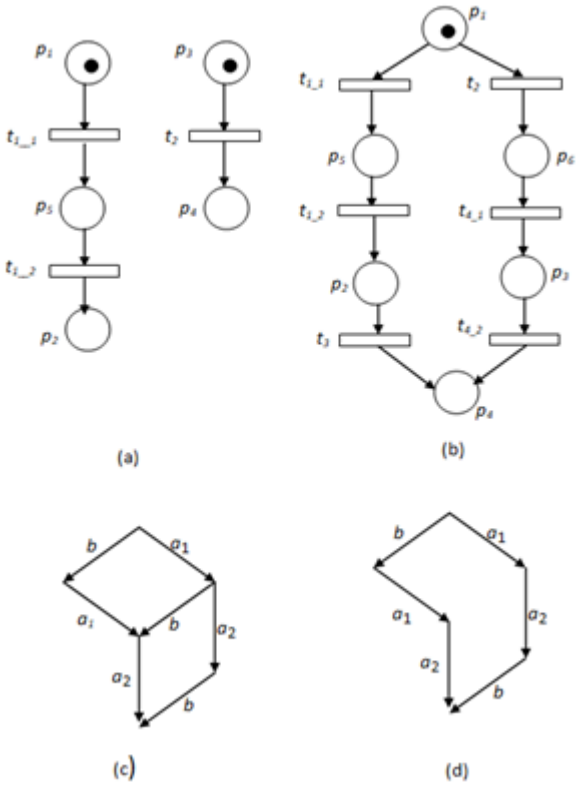


Fig. 3. No structural atomicity of actions.

Taking into account the non-atomicity of actions in a system has been deeply studied in the literature through the definition of several semantics supporting the concept of action refinement [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16]. Considering such semantics allows a hierarchical design of the systems by refining actions (actions are seen as abstract processes). Another interest of these semantics is the characterization of parallel executions of non-instantaneous actions.

Among these semantics, we can cite the maximality semantics. Which has been defined by Devillers and Vogler [10] [17]. In this context, maximality bissimulation relation has been defined and proved to be coarsest relation preserved by action refinement.

In underlying semantics models of Petri net and event structures, a system with infinite behaviour needs an infinite set of events, which makes the underlying structures interesting just for theoretical point of view [10] [17].

Dealing with implementability, another model named maximality based labeled transition system has been defined in the literature and used for expressing the semantics of process algebras and Petri net with the hypothesis that actions are not necessary atomic, i.e. actions are abstractions of finite processes and may elapse on time [18] [1] [19] [2] [20]. The main interest of maximality labeled transition system model is that it can be implemented and used in verification.

To more show the interest of the maximality semantics, we take the same example of the figure 1 while applying the method of generating the MLTS for the Petri nets proposed in [1]. So we get from the start two completely different MLTS that exactly reflect the behaviour described by the Petri nets.

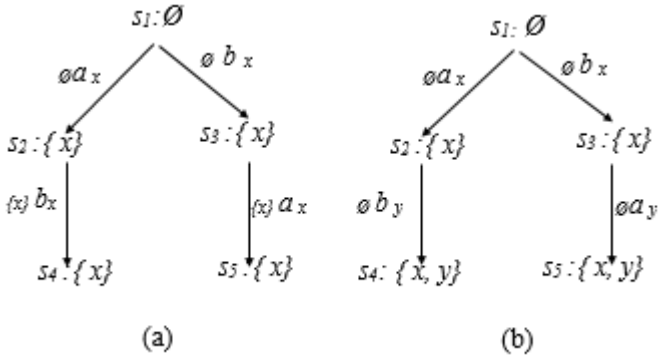


Fig. 4. Maximality semantics.

For the MLTS of figure 4.(a) actions a and b are executed sequentially a then b or b then a. For example for the first branch of this MLTS the start of execution of action a is identified by x, this action is executed independently of any other action, hence the association of the empty set to the cause of the transition $s_1 \xrightarrow{\emptyset a_x} s_2$. However the start of the execution of the action b from state s_2 is caused by the end of the execution of the action a hence the association of the set $\{x\}$ to the set of causes of the transition $s_2 \xrightarrow{\{x\} b_x} s_2$ and the event name x is re-used to identify the start of execution the action b. For the MLTS of figure 4.(b) actions a and b are clearly executed in parallel. The actions a and b are executed independently of any other action. The set $\{x, y\}$ in states s_4, s_5 indicated that there is two actions executed in parallel one is identified by x and the other by y.

In this paper we are interested by limited resources systems, while using the model of K-bounded Petri net as a modelling formalism, indeed the model of K-bounded Petri net is an intuitive model to represent the limitation of resources in a system. To deal with concurrency in the system behaviour we propose an operational maximality semantics that translates any K-bounded Petri net to maximality labeled transition systems.

The proposed semantics is concretized by the development of a software tool named MOS-KBPN for (Maximality Operational Semantics for K-Bounded Petri Net). Consequently we can take advantage of different results developed around the model of maximality labeled transition system.

Through a classic example of a limited buffer producer consumer paradigm, we show the interest of the proposed semantics in comparison to the interleaving semantics and the ST semantics. The comparison concerns the preservation of true concurrency and the reduction of the size of the semantics model. Furthermore, we will show that the properties of good behaviour of system can be verified on the corresponding maximality labeled transition system using our developed tool.

In addition, as we have mentioned to take advantage of the results developed around the model of maximality labeled transition system, we have applied on the fly reduction method to the maximality labeled transition system generated from a K-bounded Petri net which is proposed in [19] [22]. This method is based on the transitions aggregation, which contributes considerably to the reduction of the size of the semantics model.

II. Maximality-based labeled transition system

Definition 2.1: Let $\mathcal{H}$ be a countable set of event names. Let $\mathbb{L}$ be an alphabet ranging over by $a, b, ...$ In practice a label is a name of an action. A maximality-based labeled transition system of support $\mathcal{H}$ is a fivefold $(\rho, \varphi, \mu, \xi, \theta)$ with: $\rho = \langle S, TR, \alpha, \beta, s_0 \rangle$ is a transition system such that:

- *S* is the set of states in which the system may be found, this set can be finite or infinite.
- *TR* is the set of transitions indicating the change of states which the system can do; this set can be finite or infinite.
- α and β are two applications of *TR* in *S* such that for any transition $tr \in TR$: $\alpha(tr)$ is the origin of the transition *tr* and $\beta(tr)$ is its goal.
- s_0 is the initial state of the transition system ρ.
- (ρ, φ) is a system of transitions labeled by the function φ on $\mathbb{L}$, called support of (ρ, φ). $(\varphi : TR \longrightarrow \mathbb{L})$.
- $\theta : S \longrightarrow 2^{\mathcal{H}}$ is a function which associates to each state a finite set of maximal event names, with the assumption that $\theta(s_0) = \emptyset$.[1]
- $\mu : TR \longrightarrow 2^{\mathcal{H}}$ is a function which associates to each transition a finite set of event names corresponding to the actions which began their execution and their terminations cause the execution of this transition.
- $\xi : TR \longrightarrow \mathcal{H}$ is a function which associates to each transition the event name identifying its occurrence.

Where each transition $tr \in TR$ satisfies the condition, $\mu(tr) \subseteq \theta(\alpha(tr))$, $\xi(tr) \notin \theta(\alpha(tr)) - \mu(tr)$ and $\theta(\beta(tr)) = (\theta(\alpha(tr)) - \mu(tr)) \cup \{\xi(tr)\}$.
The last condition avoids the consideration of imaginary systems. In fact:

- The condition $\mu(tr) \subseteq \theta(\alpha(tr))$ ensures that the execution of the transition tr is only conditioned by the termination of a subset of actions potentially in execution in the state $\alpha(tr)$.
- The condition $\xi(tr) \notin \theta(\alpha(tr)) - \mu(tr)$ ensures that the event name $\xi(tr)$ indexing the transition tr does not refer to any action remaining potentially in execution in the resulting state $\beta(tr)$.
- As the set of event names $\mu(tr)$ is related to actions such that their termination constitute a condition for the execution of the transition tr, then the condition $\theta(\beta(tr)) = (\theta(\alpha(tr)) - \mu(tr)) \cup \{\xi(tr)\}$ ensures that the set of maximal events in the state $\beta(tr)$ is the one in the state $\alpha(tr)$ from which the set $\mu(tr)$ is removed and the event name $\xi(tr)$ is added.

[1] $2^{\mathcal{H}}$ denotes the part sets of $\mathcal{H}$.

III. Maximality semantics for ordinary Petri net

In this section we recall the maximality approach for ordinary Petri net, proposed in [1]. Consider the example of the

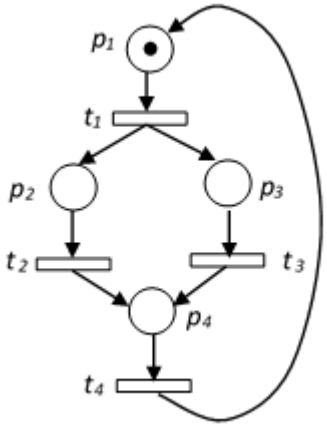


Fig. 5. Marked Petri net.

marked Petri net of Figure 5. After the firing of the transition t_1, it is evident that the execution of the transitions t_2 and t_3 are conditioned by the end of the action linked to the transition t_1. To capture this causal dependence between the firing of transitions, we consider that the tokens produced by the firing of the transition t_1 are bound to this transition, namely the token in place p_2 and the token in place p_3. We can remark that, in the initial state, the token in p_1 is not bound to any transition, this token is said to be free in this state. In the case where the transition t_2 is fired, it could be deduced that the action associated with the firing of t_1 has finished. As a result, the token in p_3 will become free. Resulting marking after the firing of the transition t_2 is given in Figure 6.(c).

To distinguish between free and bound tokens in a place, we can imagine that a place is composed of two separated parts. The left part contains free tokens while the right one will contain bound tokens. In a place, the number of free tokens will be noted by $\mathcal{FT}$, while bound tokens set will be noted by $\mathcal{BT}$. Each bound token identifies an action that is potentially in execution (this token is a maximal event). For example, in the configuration C_2 of Figure 6, the right part $\mathcal{BT}$ of the place p_2 contains a bound token of the firing $\emptyset t_1 x$, which means that $\mathcal{BT}_2 = \{(1, t_1, x)\}$.

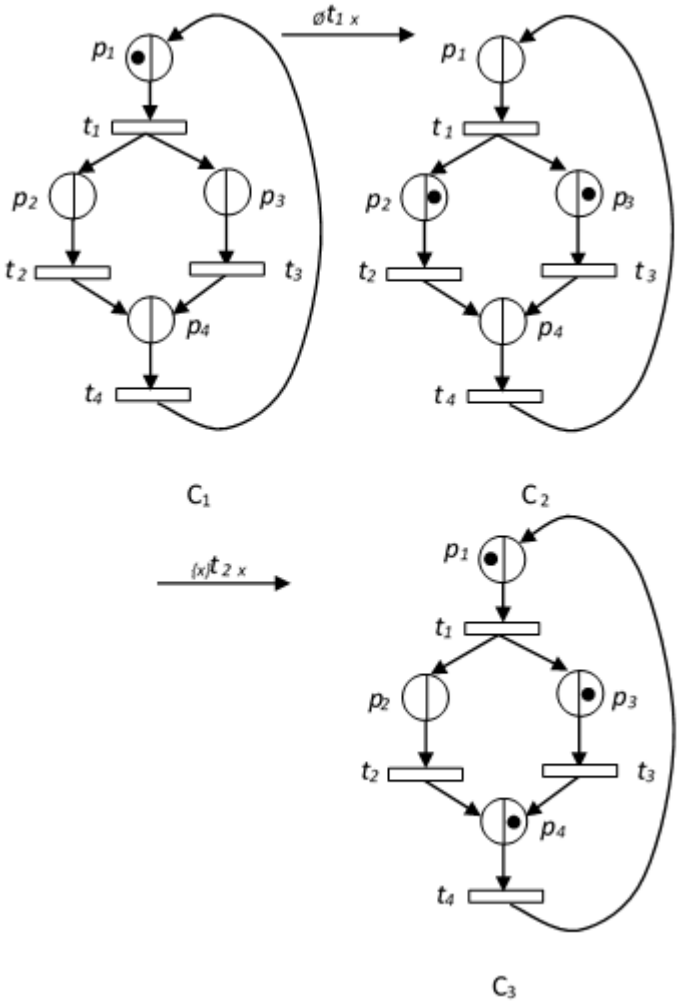


Fig. 6. Free tokens and bound tokens in a marking.

IV. Maximality Semantics for k-bounded Petri net

Through an example we explain the idea behind the proposed maximality semantics for K-bounded Petri nets. Let the Petri net of Figure 7. The tokens in p_1 are not bound to any transition, these tokens are said to be free (see Figure 8.(a)). In the case when the transition t_1 is launched, a bound token is produced in the place p_2.

By firing the transition t_1, we will obtain the marked Petri net of Figure 8.(b). From this marking, it can be seen that transition t_1 can be launched again. The firing of this transition will lead to the configuration of Figure 8.(c). From this configuration, the transition t_1 can not be fired again because the place p_2 is 2-bounded $(k = 2)$.

The maximality labeled transition system of Figure 9 corresponds to the petri net of Figure 7.

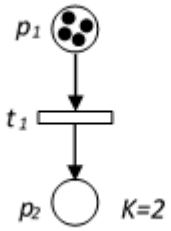


Fig. 7. Modelling of auto-concurrency.

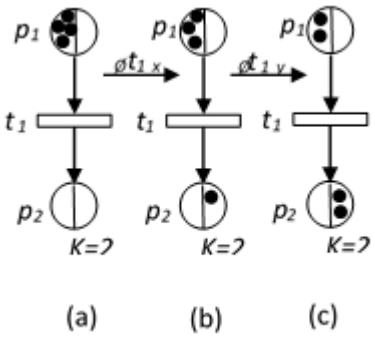


Fig. 8. Evolution of Petri net.

V. Operational maximality semantics for K-bounded Petri net

A. Preliminary definitions:

Definition 5.1: A K-bounded Petri net is a fivefold (P, T, W^-, W^+, K) where:

- P : is a finite set of places.
- T : is a finite set of transitions such that: $P \cap T = \emptyset$.
- $W^- : P \times T \longrightarrow \mathbb{N}$ is the matrix of preconditions.
- $W^+ : P \times T \longrightarrow \mathbb{N}$ is the matrix of postconditions.
- $K : P \longrightarrow \mathbb{N}^+$ is a function defining the limit capacity of places. $K(p) = k$ denotes the fact that the place p can't contain more than k tokens.

Definition 5.2: A labeled system $\Sigma = (P, T, W^-, W^+, K, \lambda)$ is a K-bounded Petri net in which all

Fig. 9. MLTS in the case of parallelism.

transitions are labeled by actions such that $\lambda : T \longrightarrow L$ is a labeling function.

Definition 5.3: Let (P, T, W^-, W^+, K) be a K-bounded Petri net with a marking M:

- $\forall p \in P$, $M(p)$ is a pair $(\mathcal{FT}, \mathcal{BT})$ such that $\mathcal{FT} \in \mathbb{N}$ and $\mathcal{BT} = \{bt / bt \in \mathbb{N} \times T \times \mathcal{H}\}$ denote the number of free tokens and the set (possibly empty) of bound tokens in the place p, respectively.
- Let p be a place such that $M(p) = (\mathcal{FT}, \mathcal{BT})$ where $\mathcal{BT} = \{(n_1, t_1, x_1), ..., (n_m, t_m, x_m)\}$. The set of event names in p is given by a function $\delta^\bullet : P \longrightarrow 2^{\mathcal{H}}$, $\delta^\bullet(p) = \{x_1, x_2, .., x_m\}$.
- The set of maximal event names in M is the set of all event names identifying bound tokens in the marking M. Formally, the function δ will be used to calculate this set and it can be defined as:
  $\delta : \{M : M\, a\, marking\, of\, the\, Petri\, net\} \longrightarrow 2^{\mathcal{H}}$ such that $\delta(M) = \cup_{p \in P} \delta^\bullet(p)$.
- Let $X \subset \mathcal{H}$ be a finite set of maximal event names of actions which terminated their execution. The operation of transforming bound tokens defined by X to free tokens in the marking M is defined by the inductive function $makefree$ as follows :
  - $makefree(\{x_1, x_2, ..., x_m\}, M) = makefree(\{x_2, ..., x_m\}, makefree(\{x_1\}, M))$
  - $makefree(\{x\}, M) = M'$ such that for all $p \in P$, if $M(p) = (\mathcal{FT}, \mathcal{BT})$ then:
    - If there is $(n, t, x) \in \mathcal{BT}$ then $M'(p) = (\mathcal{FT} + n, \mathcal{BT} - \{(n, t, x)\})$ (Conversion of n bound tokens identified by the event name x to free tokens).
    - Otherwise, $M'(p) = M(p)$.
- $\mid M(p) \mid = \mathcal{FT} + \sum_{i=1}^{m} n_i$ such that $M(p) = (\mathcal{FT}, \mathcal{BT})$ with $\mathcal{BT} = \{(n_1, t_1, x_1), ..., (n_m, t_m, x_m)\}$.
- Let t be a transition of T; t is said to be enabled by the marking M iff $\mid M(p) \mid \geq W^-(p, t)$ for all $p \in P$. And $\mid M(p) \mid - W^-(p, t) + W^+(p, t) \leq k$ if p is K-bouned place $(K(p) = k)$. The set of all transitions enabled by the marking M will be noted $enabled(M)$.
- The marking M is said minimal for the firing of the transition t iff $\mid M(p) \mid = W^-(p, t)$ for all $p \in P$.
- Let M_1 and M_2 be two markings of the K-bounded Petri net (P, T, W^-, W^+, K). $M_1 \subseteq M_2$ iff $\forall p \in P$, if $M_1(p) = (\mathcal{FT}_1, \mathcal{BT}_1)$ and $M_2(p) = (\mathcal{FT}_2, \mathcal{BT}_2)$ then $\mathcal{FT}_1 \leq \mathcal{FT}_2$ and $\mathcal{BT}_1 \subseteq \mathcal{BT}_2$ such that the relation $\subseteq$ is extended to bound tokens sets as follows: $\mathcal{BT}_1 \subseteq \mathcal{BT}_2$ iff $\forall (n_1, t, x) \in \mathcal{BT}_1, \exists (n_2, t, x) \in \mathcal{BT}_2$ such that $n_1 \leq n_2$.
- Let M_1 and M_2 be two markings of the K-bounded Petri net (P, T, W^-, W^+, K) such that $M_1 \subseteq M_2$. The difference $M_2 - M_1$ is a marking M_3 $(M_2 - M_1 = M_3)$ such that, for all $p \in P$, if $M_1(p) = (\mathcal{FT}_1, \mathcal{BT}_1)$ and $M_2(p) = (\mathcal{FT}_2, \mathcal{BT}_2)$ then $M_3(p) = (\mathcal{FT}_3, \mathcal{BT}_3)$ with $\mathcal{FT}_3 = \mathcal{FT}_2 - \mathcal{FT}_1$ and $\forall (n_1, t, x) \in \mathcal{BT}_1$, $(n_2, t, x) \in \mathcal{BT}_2$, if $n_1 \neq n_2$ then $(n_2 - n_1, t, x) \in \mathcal{BT}_3$.
- $Min(M, t) = \{M' / M' \subseteq M$ and M' is minimal for the firing of $t\}$.
- $get : 2^{\mathcal{H}} \longrightarrow \mathcal{H}$ is a function such that for any $A \in 2^{\mathcal{H}}$, $get(A) \in A$. The function get chooses in a unique manner an element of A (an event name).

B. Semantic rule

The operational semantics of labeled Petri nets allowing the generation of a maximality-based labeled transition systems is defined by:

$$\frac{t \in T \wedge t \in enabled(M_1), M_3 \in Min(M_1, t)}{M_1 \xrightarrow{E\,\lambda(t)_x} M_2}$$ such that:

- $E = \delta(M_3), M_4 = makefree(E, M_1 - M_3)$
- For any $p \in P$ with $M_4(p) = (\mathcal{FT}_4, \mathcal{BT}_4)$, $M_2(p) = (\mathcal{FT}_4, \mathcal{BT}_2)$ where:
  $\mathcal{BT}_2 = \mathcal{BT}_4 \cup \{(W^+(p, t), t, x) / W^+(p, t) \neq 0\}$
- $x = get(\mathcal{H} - (\delta(makefree(E, M_1))))$

VI. On the fly reduction method for maximality labeled transition system

In this section we recall the approach that generates an on-the-fly reduced MLTS modulo a maximality bisimulation relation proposed for ordinary Petri net in [19].

For explanation we consider the example of Figure 10. In the initial state (state s_1) of the maximality-based labeled transition system of Figure 10.(b), no action is running, from where the association of the empty set with this state. From state s_1, actions a and b can start their execution independently, their starts are respectively identified by event names x and y. a and b can be launched in any order. The set $\{x\}$ (resp. $\{y\}$) in state s_2 (resp. s_3) stipulates that the action a (resp. b) are potentially under execution in this state. $\{x, y\}$ in s_4 shows that actions a and b can be executed simultaneously.

Note that when the system is in state s_2, while the action a has not been terminated yet, the only evolution concerns the start of b. However, when a terminates, we can start the action b caused by a or the action b which is independent from the end of a. Resulting states are respectively s_4 and s_5. We can observe that from state s_5, the start of b is always possible. However, the same ending constraint of a is imposed for the execution of b at the level of state s_4. Note that causal dependence between execution of b across from the action a is captured by the consumption of the produced token coming from the transition t_1 during the firing of t_2 in the Petri net.

Notice that from state s_2, transitions leading respectively to states s_4 and s_5 are due to the firing of the same transition t_2. In the first firing, the token of the initial marking is used whereas in the second firing, the used token is that produced by the firing of t_1. On the other hand, such as we noted above, the derivation by b leading to state s_4 is not conditioned by the end of the action a, while the derivation leading to state s_5 is conditioned by the end of a. In [19] it is clearly proved

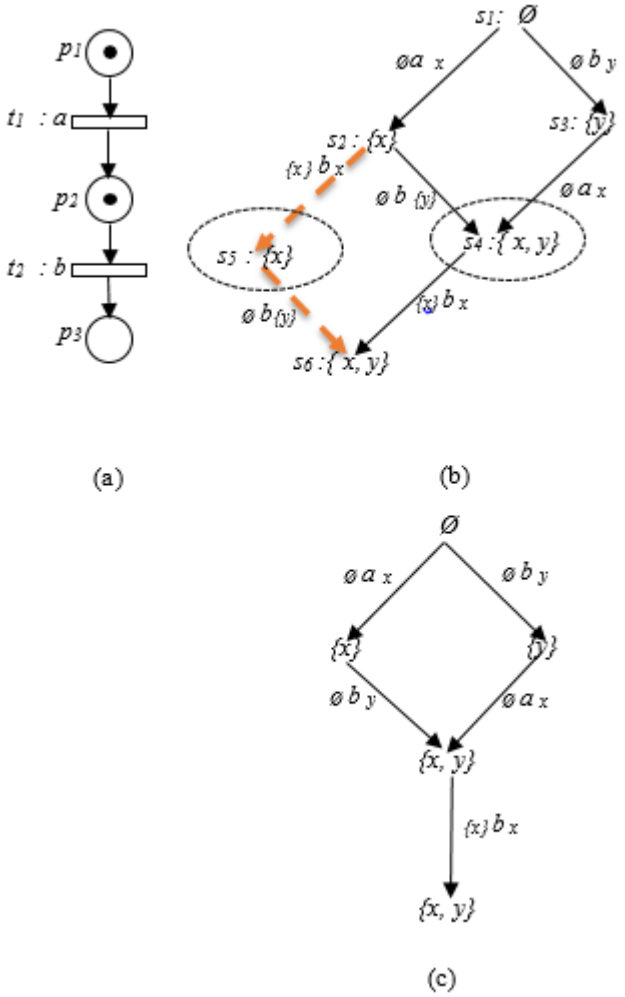


Fig. 10. Example MLTS reduction.

that states s_4 and s_5 are maximally bisimilar which means that is possible to omit the derivations $s_2 \longrightarrow s_5 \longrightarrow s_6$ in the maximality-based labeled transition system.

As we have previously mentioned, to take advantage of the results developed around the model of maximality labeled transition system, maximality bisimulation relations defined on maximality labeled transitions system for ordinary Petri net will be extended in this paper to K-bounded Petri net.

Definition 6.1: Let $Mark$ be a set of markings, T a set of transitions and $\longrightarrow$ a derivation relation between markings which is previously explained.

1) Let $\Re \subseteq 2^{Marq} \times 2^{Marq} \times \mathcal{F}$. the relation $\Re$ is sais maximality bisimulation relation according to a set of transitions of K-bounded Petri net bisimulation relation according to a set of transitions iff: $\forall \left(M_i, M_i^{'}, Id_{A_i}\right) \in \Re$, $A_i \subseteq \delta\left(M_i\right)$ et $A_i \subseteq \delta\left(M_i^{'}\right)$.
   a) If $M_i \overset{E_i t_i x}{\longrightarrow} M_j$ then $\exists\ M_i^{'} \overset{E_i^{'} t_i y}{\longrightarrow} M_j^{'}$ / $\forall u \in A_i$ if $u \notin E_i$ then $u \notin E_i^{'}$ and for $z = get\left(\mathcal{M} - \left(\left(\delta\left(M_i\right) - E_i\right) \cup \left(\delta\left(M_i^{'}\right) - E_i^{'}\right)\right)\right)$: $\left(M_j\left[z/x\right], M_j^{'}\left[z/y\right], Id_{A_{i+1}}\right) \in \Re /\ A_{i+1} = \left(A_i - E_i\right) \cup \{z\}$.
   b) If $M_i^{'} \overset{E_i^{'} t_i y}{\longrightarrow} M_j^{'}$ then $\exists\ M_i \overset{E_i t_i x}{\longrightarrow} M_j$ /$\forall u \in A_i$ if $u \notin E_i^{'}$ then $u \notin E_i$ and for $z = get\left(\mathcal{M} - \left(\left(\delta\left(M_i\right) - E_i\right) \cup \left(\delta\left(M_i^{'}\right) - E_i^{'}\right)\right)\right)$: $\left(M_j\left[z/x\right], M_j^{'}\left[z/y\right], Id_{A_{i+1}}\right) \in \Re /\ A_{i+1} = \left(A_i - E_i^{'}\right) \cup \{z\}$.
2) Let $\Sigma_1 = \left(P_1, T, W_1^-, W_1^+, K1, M_0^1, \lambda_1\right)$, $\Sigma_2 = \left(P_2, T, W_2^-, W_2^+, M_0^2, \lambda_2\right)$, two labeled systems with initial marking. Σ_1, Σ_2 are said to be maximally bisimilar according to T noted $\Sigma_1 \approx_m^T \Sigma_2$ if and only if there exists a maximality bisimulation relation $\Re$ according to Tsuch that / $\left(M_0^1, M_0^2, \emptyset\right) \in \Re$.
3) $M_1 \approx_m^T /f\ \ M_2$ note that $(M_1, M_2, f) \in \Re$.

In this paper we will apply the same approach to reduce on the fly the maximality labled transition system generated from K-bounded Petri net. For this we keep the same operational semantics by modifying the semantics of the function Min.

In this case, a minimal marking for the firing of a transition t is considered as an element of the set $Min\left(M, t\right)$ only if for each place of this marking, bound tokens are only taken in the case when the free part does not satisfy the pre-condition of this transition. Therefore, we can ensure that a transition t will be executed sequentially after a transition t' if it cannot be executed independently with this same transition t'.

Formally, $Min\left(M, t\right)$ is the set of markings $M' \subseteq M$ such that for any place p where $M\left(p\right) = \left(FT, BT\right)$, $M'\left(p\right)$ is defined as follows:

$$M'\left(p\right) = \begin{cases} \left(W^-\left(p, t\right), \emptyset\right) & if\ \mathcal{FT} \geq W^-\left(p, t\right) \\ \left(\mathcal{FT}, \mathcal{BT}'\right) & otherwise \end{cases}$$

With: $\mathcal{BT}' \subseteq \mathcal{BT}$ and $\mid \mathcal{BT}' \mid = W^-\left(p, t\right) - \mathcal{FT}$

VII. Case study

Consider two processes, one called producer and the other consumer. The producer produces data and deposits them in the buffer. The consumer process take a produced data from the buffer and consumes them. When modelling the system, the buffer capacity will be represented by a K-bounded place. The modelling of this example in terms of K-bounded Petri net is given by the Figure 11.

For $k = 1$, the labeled transition system corresponding to the marking graph generated from this Petri net is depicted in Figure 12, it contains 8 states, 12 transitions. At this level we notice that this model is unable to model possible parallel execution of production and consumption operations.

The maximality labeled transition system which corresponds to this Petri net is depicted in Figure 13. Indeed in order to concretize our theoretical study we have

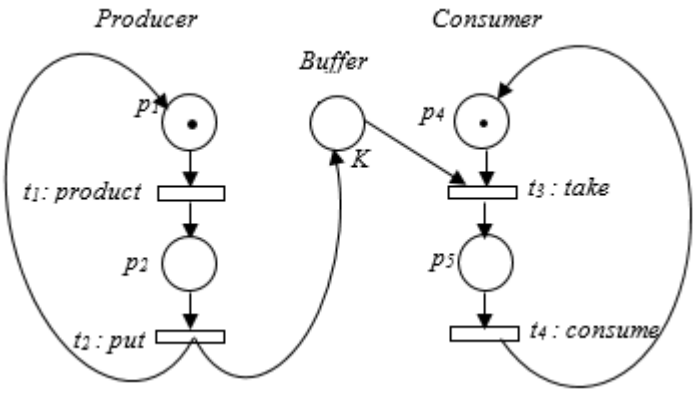


Fig. 11. Producer/consumer.

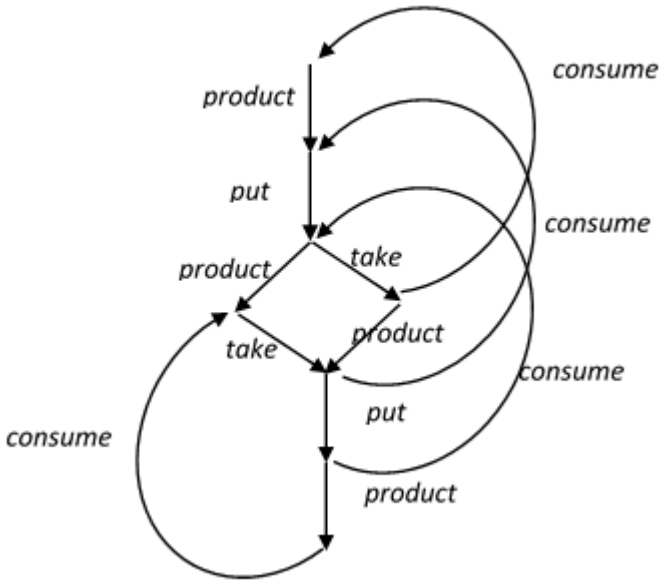


Fig. 12. Labeled transitions system for producer/ consumer.

developed a software tool named MOS-KPN for (Maximality Operational Semantics for K-Bounded Petri Net) this tool interprets any K-bounded Petri net to a MLTS. We have used this tool to generate the MLTS corresponding to the example of producer consumer. This MLTS contains 18 states and 26 transitions, but we can clearly see that the MLTS model represents parallelism and causality with reliability, for example in state s_5 the set $\{0, 1\}$ means that the actions product and take are under execution in this state. The properties of the good functioning of the system are specified in terms of CTL logic and verified using our developed tool.

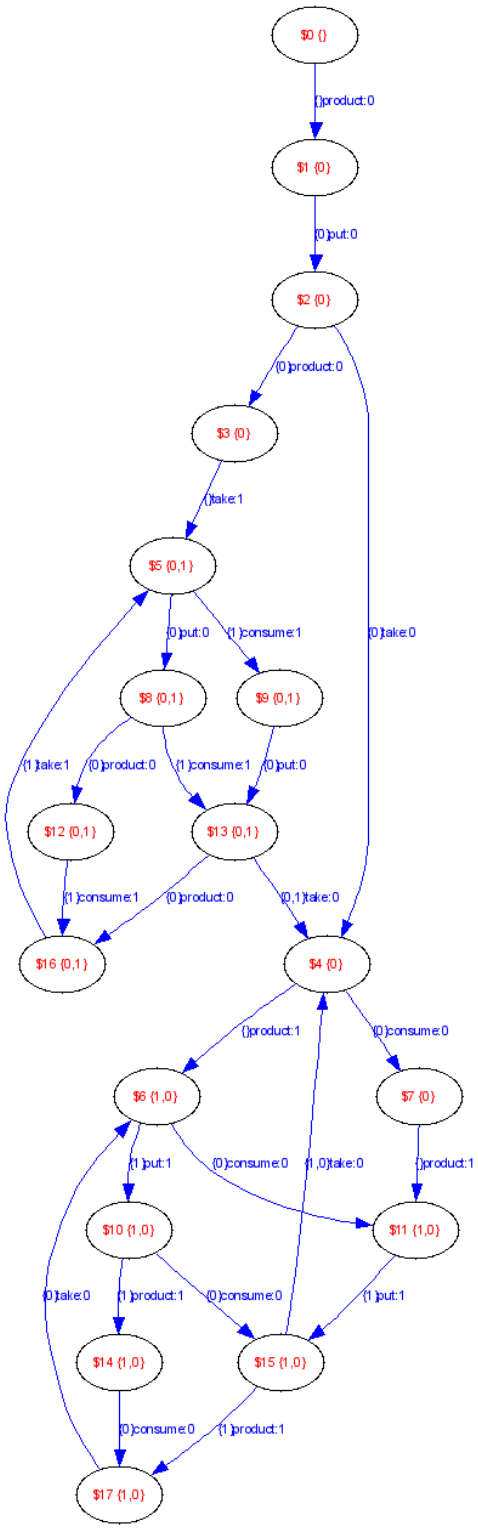


Fig. 13. Maximality labeled transitions system for producer/consumer.

A. *Verification*

- Safety properties:

- If the buffer is full the producer produced or waiting $AGput \Rightarrow EX(product\, or\, (not(put)))$
- If the buffer is empty then the consumer waiting or consuming. $AG\, take \Rightarrow EX(consume\, or\, (not(take)))$

- Liveness properties :
  - If the producer can produce then it produces. $AG\, take \Rightarrow EX\, product$
  - If the consumer can consume then it consumes. $AG\, put \Rightarrow EX(take\, or\, consume)$

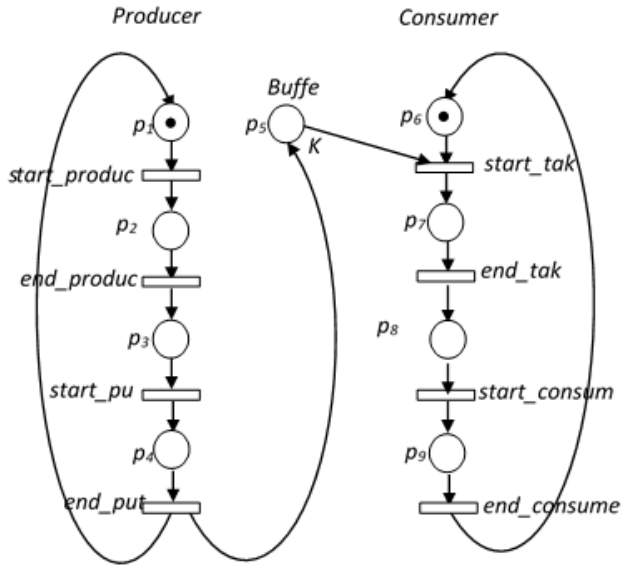


Fig. 14. Petri net with producer/consumer after refinement.

To capture the true concurrency under an interleaving semantics each transition may be splitted into two sequential actions, the start and the end actions like in the ST semantics. So, we consider now the Petri net of Figure 14 and we vary the capacity of buffer k. Then we compare the results obtained with the MLTS. We find that with the labeled transition system (LTS) the number of states and transition is very greater that of MLTS. In this case the reader can understand that the MLTS model represents causality and true parallelism with simplicity and reliability but with a minimum number of states. The obtained results are summarized in Table I.

Now we applied the reduction method proposed in [19] [22] to generate the MLTS for the Petri net of Figure 14 which contributes more to the reduction of the size of the semantics model. All with the change of the number of producers and consumers. The obtained results are summarized in Table II.

VIII. Conclusion

In this paper we have proposed an operational method for the generating of maximality labeled transition system associated to K-bounded Petri net. Noting that the K-bounded Petri net model is the most appropriate for modelling systems with limited resources. Consequently, the properties relating to the good functioning of a system specified by a K-bounded Petri net can be verified on its corresponding maximality labeled transition system. On the other hand, the structure of the maximality labeled transition system integrates information about the parallel execution of actions. This structure allows us to express more easily the properties related to the parallel execution of actions. At the end, we have applied the obtained results to the example of the producer / consumer with limited buffer capacity. Furthermore we have extended the on the fly reduction method for MLTS proposed in [19] [22] to K-bounded Petri net which contribute to the reduction of the number of states and transitions. Through this example we have shown the interest of our approach for the modeling and verifying concurrent systems with limited resources. This result may be extended to the work about recursive Petri net presented in [21] [22] [24].

TABLE I
Number of states and transitions of LTS and MLTS

Buffer	**LTS**		**MLTS**		**reduction rate**	
k	$N°s$	$N°T$	$N°S$	$N°T$	$s\%$	$T\%$
1	125	285	18	26	$85,60\%$	$90,74\%$
2	249	621	30	51	$87,95\%$	$91,78\%$
3	433	1161	42	76	$90,30\%$	$93,45\%$
4	693	1967	54	101	$92,20\%$	$94,86\%$
5	1048	3115	66	126	$93,70\%$	$95,95\%$
6	1548	4690	78	151	$94,86\%$	$96,78\%$
7	2126	6787	90	176	$95,76\%$	$97,40\%$
8	2896	9510	102	201	$96,47\%$	$97,88\%$
9	3855	12973	114	226	$97,04\%$	$98,25\%$
10	5031	17299	126	251	$97,49\%$	$98,54\%$

TABLE II
Number of states and transitions of MLTS before and after reduction for K=10

$N°$	$N°$	MLTS before		MLTS after		reduction rate	
P	C	$N°s$	$N°T$	$N°S$	$N°T$	$s\%$	$T\%$
1	1	126	251	108	206	$14,28\%$	$19,92\%$
2	1	448	1322	297	844	$33,70\%$	$36,15\%$
2	2	1930	7612	1321	4855	$31,55\%$	$36,21\%$
3	1	1342	5102	757	2822	$43,59\%$	$44,68\%$
3	2	7600	36751	4193	19187	$44,82\%$	$47,79\%$
3	3	31986	31986	17836	17836	$44,23\%$	$48,43\%$
4	1	3920	18166	1861	8456	$52,52\%$	$53,45\%$
4	2	28178	159320	12431	66944	$55,88\%$	$57,98\%$
5	1	11416	61898	4511	23750	$60,48\%$	$57,98\%$
6	1	33150	204226	10931	64180	$67,02\%$	$68,57\%$

References

[1] D.E. Saidouni, N. Belala, and M. Bouneb. Using maximality- based labeled transitions as model for petri nets. In The International Arab Conference on Information Technology(ACIT).2008a.

[2] D. E. Saidouni, N Belala, and M. Bouneb. Using maximality- based labeled transitions as model for petri nets. The International Arab Journal of Information Technology (IAJIT),2009a. 6(5):441–446.

[3] G Boudol and I Castellani. Concurrency and atomicity. TCS,1988. 59:1–60.

[4] P. Darondeau and P. Degano. Causal trees. in ICALP'89, LNCS, Springer-Verlag,1989. 372:234–248.

[5] R. J. Van Glabbeek. The refinement theorem for st-bisimulation semantics. in IFIP Working Conference on Programming Concepts and Methods, North-Holland.1990.
[6] L. Aceto and M. Hennessy. Adding action refinement to finite process algebra. in ICALP91, LNCS Springer-Verlag,1991. Pages 506–519.
[7] E Best, R Devillers, A Kiehn, and L. Pomello. Concurrent bisimulations in petri nets. Acta Informatica,1991. 28:231–264.
[8] P. Degano and R. Gorrieri. Atomic refinement in process description languages. in A. Tarlecki, ed., Mathematical Foundations of Computer Science, LNCS, Springer-Verlag,1991. 520:121–130.
[9] W Janssen, M. Poel, and J. Zwiers. Action systems and action refinement in the development of parallel systems. CONCUR91, LNCS, Springer-Verlag,1991. 527:298–316.
[10] R. Devillers. Maximality preservation and the st-idea for action refinement. in G. Rozenberg, ed., Advances in Petri Nets, LNCS Springer-Verlag, 1992. 609:108–151.
[11] D. Andrews, J Groote, and C. Middelburg. Workshop on semantics of specification languages. Workshops in Computing, Springer-Verlag,1993. Pages 289–303.
[12] D. Hogrefe and S. Leue. IFIP TC6/WG6.1, 7th Int. Conf. on Formal Description Techniques (FORTE94), Chapman , Hall,1994. Pages 293–308.
[13] J.P. Courtiat and D.E. Saidouni. Action refinement in lotos. in A. Danthine, G. Leduc and P. Wolpe, eds, Protocol Specification, Testing and Verification (PSTV93), NorthHolland,1994a. Pages 341–354.
[14] D.E. Saidouni and J.P. Courtiat. Syntactic action refinement in presence of multiway synchronization. Semantics of Specification Languages,1994b. Pages 289–303.
[15] Gorrieri R and Laneve C. Split and st bisimulation semantics.1995. Pages 272-288.
[16] Gruska D.P. Bounded concurrency.1997.
[17] W. Vogler. Bisimulation and action refinement. TCS.1993.
[18] D.E. Saidouni. Maximality semantic: Application to actions refinement in LOTOS. PhD thesis, PhD thesis., LAAS-CNRS, 7 av. du Colonel Roche, 31077 Toulouse Cedex France.1996.
[19] D. E Saidouni, N Belala, and M. Bouneb. Aggregation of transitions in marking graph generation based on maximality semantics for petri nets. In Verification and Evalution of Computer and Communication systems (VECOS). 2008b.
[20] D. E Saidouni, N Belala, and M Bouneb. Maximality-based structural operational semantics for petri nets. In 2nd Mediterranean Conference on Intelligent Systems and Automation (CISA).2009b.
[21] D. E. Saidouni, M. Bouneb, J. M. Ilie. Maximality Semantic For Recursive Petri Net. European Council for Modelling and Simulation (ECMS) :2013. Pages 544-550
[22] M Bouneb, D. E Saidouni, and J. M. Ilie. A reduced maximality labeled transition system generation for recursive petri nets. In Journal of formal aspect of computing, Springer,November 2015. Number Volume 27, Issue 56, pp 951-973.
[23] M. Bouneb, D. E. Saidouni. Hierarchical Design Method for Multi-Agent Systems. International Journal of Agent Technologies and Systems (IJATS).2015.IGI Global 7(2): pages 105-134.
[24] M. Bouneb, D. E. Saidouni, J. M. Ilie. Hierarchical System Design Using Refinable Recursive Petri Net. Journal of Computing and Informatics.2018. 37(3):pages 635-655.

Training Cellular Automata with Extended Neighborhood for Edge Detection

Safia Djemame
Computer Science Department
Ferhat Abbes University, Setif-1
Setif, Algeria
Djemame@univ-setif.dz

***Abstract*—Edge detection refers to the process of identifying and locating sharp discontinuities in an image. Since edge detection is in the forefront of image processing for object detection, it has attracted much attention from scientific research. More accurate results and less time consuming are there still the main issues when extracting edges from images. To cope with this challenge, we propose a complex system: Cellular Automata (CA) that has proven high performances in image processing domain. Unlike previous works, which used in majority Von Neumann or Moore neighborhood, We use a particular kind of CA, with extended Moore neighborhood. This allows a large exploration of the search space. We trained a QPSO algorithm for extracting the adequante subset of rules. Experiments were carried on several images from Mathworks and Berkeley dataset. Visual and numerical results show that our CA provides excellent performances, and edges with high accuracy.**

***Index Terms*—Artificial intelligence, Complex systems, Cellular Automata, Rule selection, Image Processing, Edge detection.**

I. Introduction

Edge detection is one of the fundamental image processing tasks that has been widely investigated since technology allowed people to digitally process visual data. Information about edges is the basis of many computer vision systems such as object recognition, pattern classification, robotic vision and medical diagnosis [1] . The quality of detected edges has a direct and high influence on the performance of mentioned systems.
There are many ways to perform edge detection. However, the majority of methods may be grouped into two categories [2]:

* Gradient-based edge detection: the gradient method detects the edges by looking for the maximum and minimum in the first derivative of the image.
* Laplacian-based edge detection: the Laplacian method searches for zero crossings in the second derivative of the image to find edges. An edge has the one-dimensional shape of a ramp, and calculating the derivative of the image can highlight its location [3] .

The main techniques used in the literature for edge detection are Canny [4] , Sobel, Deriche, Prewitt, Roberts edge detectors and Laplacian of Gaussian (LoG).
Given the importance of edge detection, many different methods were introduced to overcome different problems that occur in classical methods. Our research focuses on Cellular Automata, a complex system that presents interesting properties in solving image processing problems, due to its simplicity and local interactions.
This study focuses on edge detection based on Cellular Automata. Cellular Automata, introduced by John Von Neumann [5] in the 1950's, is a spatially and temporally discrete dynamical system composed of cells arranged in a lattice. Each cell can be in one of a finite number of states. The transition between states is dependent on the cell value, the state of its neighbourhood and the transition rule. The most characteristic feature of CA is that using simple rules interacting with a local neighbourhood can produce very complex behaviour.
Image is viewed as a two dimensional CA model with initial configuration in which each pixel is represented by a cell and the pixel value is represented by the state of the cell. So, any updating rule can be applied once in an image at a particular time and its intensity of the pixels change simultaneously in the successive time interval. Due to this kind of behavior, CA model influences a large application in image processing.
Based on the above idea, many algorithms have been developed for edge detection, however this is still a challenging and an unsolved problem.
In this paper, we propose a CA with extended Moore neighborhood, which allows to have larger set of transition rules to explore. Among these rules, we extract the subset which gives better results for edge detection than some traditional methods.
The remaining parts of this paper are organized as follows. In Section 2, we present a brief overview of CA. Related works are presented in Section 3. In section 4, we explain the proposed method. In section 5, we present and discuss the obtained results for a set of images. Finally the paper is concluded in Section 6.

II. Overview of Cellular Automata

Cellular automata (CA) are mathematical models for systems consisting of large numbers of simple identical components with local interactions. The simple components act together to produce complex emergent global behavior [6] .

Cellular automata perform complex computation with high degree of efficiency and robustness. They are especially suitable for modeling natural systems that can be described as massive collections of simple objects interacting locally with each other [7]. Cellular automata is called cellular, because it is made up cells like points in the lattice and it is called automata, because it follows a simple local rule [8] . Each cell can assume a state from finite set of states. The cells update their states synchronously on discrete steps according to a local rule. The new state of each cell depends on the previous states of a set of cells, including the cell itself, and constitutes its neighborhood [9].

Formally, Cellular Automata is quadruples (d, S, N,I):

* The integer d is the dimension of the space the CA will work on,
* S = $s_1, s_2, ..., s_k$ is a finite set of states,
* The neighborhood N is a v-tuple of distinct vectors of Z^d
* N = ($x_1, x_2, ..., x_v$): the Xi 's are the relative positions of the neighbor cells with respect to a given center cell,
* f : $S^v \rightarrow S$ is the local transition rule.

The states of all cells in the lattice are described by a configuration. A configuration can be described as the state of the whole lattice. The rule and the initial configuration of the CA specify the evolution of CA that tells how each configuration is changed in one step.

The reason behind the popularity of cellular automata can be traced to their simplicity, and to the enormous potential they hold in modeling complex systems. Cellular automata can be viewed as a simple model of a spatially extended decentralized system made up of a number of individual components (cells). The communication between cells is limited to local interaction. Each individual cell is in a specific state which changes over time depending on the states of its local neighbors. The overall structure can be viewed as a parallel processing device. However, this simple structure when iterated several times produces complex patterns displaying the potential to simulate different sophisticated natural phenomena [7] .

A. Neighborhood structure

The neighborhood of a cell, called the core cell (or central cell), made up of the core cell and those surrounding cells whose states determine the next state of the core cell. There are different neighborhood structures for cellular automata.The two most commonly used neighborhoods are Von Neumann and Moore neighborhood, shown in "Fig. 1".

Von Neumann neighborhood has five cells, consisting of the cell and its four immediate non-diagonal neighbors and has a radius of 1. The radius of a neighborhood is defined to be the maximum distance from the core cell, horizontally or vertically, to cells in the neighborhood.

Moore neighborhood has nine cells, consisting of the cell and its eight surrounding neighbors and has a radius of 1. Extended Moore neighborhood composed of the same cells as the Moore neighborhood, but the radius of neighbourhood is increased to 2. In this paper, we explore the abilities of a 2D-CA with extended Moore neighborhood (25 cells), to extract efficiently edges on an image.

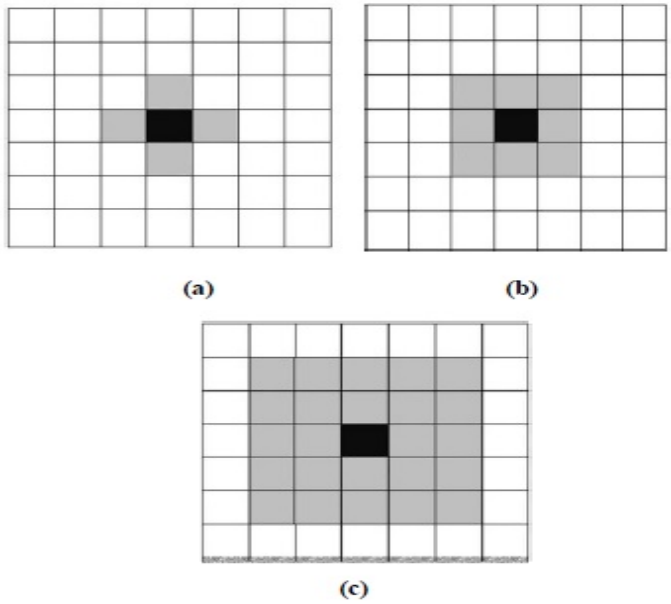


Fig. 1. Neighborhood models (a)Von Neumann (b) Moore (c) Extended Moore.

B. Relationship of 2D CA with image

An image may be described as a two-dimensional function *I*, $I = f(x, y)$, where x and y are spatial coordinates. Amplitude of f at any pair of coordinates (x, y) is called intensity I or gray value of the image. When spatial coordinates and amplitude values are all finite, discrete quantities, the image is called digital image. The digital image I is represented by a single 2- dimensional integer array for a gray scale image and a series of three 2- dimensional arrays for each color bands. As the digital image is a two-dimensional array of $m*n$ pixels, so we are interested in two- dimensional CA model. An image is viewed as a two dimensional CA where each cell represents a pixel in the image and the intensity of the pixel is represented by the state of that cell. The color values of the pixels are updated synchronously at a discrete time step. So very less time is required to solve any image processing task.

III. Related Works

The most characteristic feature of CA is that using simple rules interacting with a local neighbourhood can produce very complex behaviour. Many researchers have investigated the possibility of using Cellular Automata for image processing. [10], [11] and a few focused on edge detection with either binary, greyscale or colour images as inputs. The linear set of rules applied to binary images were recently investigated by several authors. Qadir and Khan [12] divided all 512 rules for Moore neighbourhood into three groups depending on their ability to detect edges. However, they did not cover the different behaviour of rules or compared them. Uguz et. al. [13] focused on the benefits of implementation of the

transition function in the form of matrix multiplication. They have presented the results for four rules but focused more on the speed benefits.

Aydogan [14] formulated a cellular neural network based edge detection of 2D data. Diwakar et. al. [15] presented an application of totalistic rules with Moore neighbourhood for edge detection. Wongthanavasu and Sadananda [16] proposed a Weighted Cellular Automata method (WCA) based on von Neumann neighbourhood that can deal with both binary and greyscale images and can be implemented efficiently and it does not require selection of rules or any user input. Djemame et. al. [17] presented a method using a Continuous Cellular Automata for edge detection.

Chang et. al. [18] proposed a method, where an Orientation Information Measure is used to process a greyscale image into binary, and then a Cellular Automata with semi-neighbourhood is used to detect edges. Chen and Yan [19] presented a method that combines the diffusion model with CA.

Recently, a lot of attentions were attracted to the work of Rosin [20]. He proposed to use a Sequential Floating Forward Search (SFFS), which is a deterministic algorithm, to search for the best set of rules that would allow performing different tasks like denoising, thinning and finding the convex hull. Later he proposed an extension of his method [21] to tackle edge detection. This method can generate edge intensity images with simultaneous removal of impulse noise. However, this method is relatively time-consuming since processing has to be done for a set of 255 images.

In opposite to deterministic SFFS, a heuristic can be applied, with most interest presented in Genetic Algorithms. An example of searching for an optimal packet of rules is presented in work of Batouche et. al. [22] and Slatnia et. al. [23]. Similarly to Rosin's method, they searched for a set of rules that would change the central pixel state, but they did not restrict them to central white pixel. Their publications claim that great results can be obtained using only a single rule. Djemame and Batouche [24] used Particle Swarm Optimization heuristic to determine the best rules without enumerating the complete search space.

Apart from simple cellular automata, Fuzzy Cellular Automata-based edge detector has also been studied because it incorporates fuzzy logic into transition rules, which results in a good performance when used for greyscale images [25], [26]. Patel and More incorporated fuzzy logic and cellular learning automata [27]. Sinaie et. al. presented a method for enhancement of 65 edges acquired by fuzzy edge detector [28]. Some others CA-based methods have been developed to focus on grey and color image [29], [30], [31].

IV. Proposed Approach

This work target finding a discrete uniform CA that performs edge detection. A choice is established to use a CA as model, its lattice has as initial configuration the input image, and in one-time iteration the computed lattice represents the output edge image. The reason behind these choices is to attend an edge detector of fast performance. Unlike the precedent works which use Von Neumann or Moore neighborhood, we explore the use of CA with extended Moore neighbor model (of radius r=2).

A. Neighborhood Configuration

Our binary CA has 25 neighbor cells (extended Moore neighbor model), so the number of possible neighbor configurations is $2^{25} = 33554432$. The possible number of CA that can be conceived using combination of these configurations is $2^{33554432}$. Our problem is to find the rules that perform edge detection the best within this large number of CA. A choice is established to only use CA with linear rules (only one neighbor configuration rule for each CA) which is beneficial in terms of computational performance of the CA and the substantial reduction in the search space to 33554432.

The rule convention shown in "Fig. 2" is used to designate

1048576	2097152	4194304	8388608	16777216
524288	64	128	256	512
262144	32	1	2	1024
131072	16	8	4	2048
65536	32768	16384	8192	4096

Fig. 2. The rule convention model

rules. The number within each box represents the rule number associated with a neighbor configuration that only has that particular neighbor. So, if the next state of a cell depends only on its present state, it is represented as Rule 1. Similarly, if the next state of a cell is dependent only on its bottom neighbor, then it is represented as Rule 8 and so on. These twenty-five rules are known as fundamental/basic rules. All linear rules are derived using these basic rules which are expressed as the sum of the basic rules. For example, Rule 71, Rule 130, Rule 262176 can be expressed as follows:

$$Rule71 = Rule64 \oplus Rule4 \oplus Rule2 \oplus Rule1$$
$$Rule130 = Rule128 \oplus Rule2$$
$$Rule262176 = Rule262144 \oplus Rule32$$

Likewise, we can express all the possible 33554432 linear rules CA.

B. The Transition Rule

The transition function of our CA switches the state of each white cell to black only if the neighbor cells defined by its rule are white. The black cells are unchanged. The boundary conditions for our CA is set arbitrarily to use white boundary conditions, where all border cells are considered white. Later experimentation proven that this choice produces better results. The steps implementing this CA are:

- Iterate on each pixel of the input image, if this pixel is white,
- iterate on each of its neighbors and check if all of them are white.
- If all of them are white it changes the pixel to black.

It is found that a code optimization can be applied to the algorithm. The value of the output pixel can be computed using "(1)":

$$P_{t+1} = P_t \wedge (\neg N_1 \neg N_2) \neg N_n \tag{1}$$

P_{t+1} is the new logical value of the pixel (True for white, False for black).
P_t is the original value of the pixel.
n is the number of rule neighbors.
N_i is the value of the N_i neighbor.
From this we can deduce the matrixial logical calculation of the whole image "(2)":

$$Img_{t+1} = Img_t ANDNOT(Shift(Img_t, N_1), ..., NOT(Shift(Img_t, N_n))) \tag{2}$$

Img_t is the input image as a logical matrix. Img_{t+1} is the output image as a logical matrix.
AND, OR are matrixial logical operators that do the respective logical operation $\wedge$,$\vee$ between each two corresponding elements of the matrixes.
NOT is matrixial logical operators that do logical $\neg$for each element of the matrix.
Shift(Img_t, N_i) is a function that returns the matrix Img_t shifted in both x,y direction by x_i, y_j the positions of the neighbor i relative to the core cell.

C. The method

In this section, the proposed method is discussed. A digital image is assumed to be a two dimensional array of $(m * n)$ pixels, each with a particular gray value or color. An image can be considered as the lattice configuration of a 2D CA where each cell corresponds to an image pixel, and the possible states are the different gray values or colors.
As the possible values of transition rules are a huge number (about $2^{33554432}$), we used an optimization algorithm based on a quantum PSO metaheuristic (QPSO), to extract the subset of rules, capable to give a satisfactory result. The algorithm is detailed in [32].

We take advantage of the calculating faculties of the CA, to transform the initial configurations defined by a numerical image lattice as discrete input data in order to find its edges. The search space is defined by all the transition rules of the CA. The evolutionary process trained by QPSO has the effect of extracting the subset of rules which leads to an edge detection with good quality. In this context, a rule is a particle of the swarm, and the best rule which gives rise to a good segmentation corresponds to the particle with the best fitness. In this algorithm, the input image and the ground-truth image are uploaded. The QPSO process is initialized by setting the number of iterations and the swarm size. At the beginning of the process, the value of parameter beta is set to 1.0; then, it is linearly decreased during the execution of the algorithm. Beta is the only parameter tuned automatically in the QPSO process. QPSO has relatively better performance by varying linearly the value of beta from 1.0 to 0.5 in order to balance between exploration and exploitation. The particles are randomly initialized in the search space. Each particle of the swarm (a rule) is converted in binary representation and applied on the input image pixel by pixel, according to the transition function defined in (Eq. 2). For each particle, an output image is obtained. The quality of edge detection is measured by evaluating two fitness functions: SSIM and RMSE. The best position is identified. The mean of the best positions mbest is computed. For each particle,the new position X is computed. The fitness of the new particle is evaluated, and the new rule is applied on the image. The process is repeated until reaching a predefined maximum number of iterations. At the end of the algorithm, the best rule, the best segmentation and the best fitness are displayed.

V. Experimental Results

In this section, we present the results of the evolutionary algorithm in the search process, and the results of the extracted rules on different images.
Experiments were carried on several test images from Mathworks and the database of Berkeley University. In this paper, we illustrate some examples: Cameraman, Lena, X-ray images from Mathworks and swan, church, woman, bird and plane images from Berkeley database.
After dozens of experiments, we observed that six rules appeared most frequently than others and allowed extracting good edges after only one application on the input image. The rules identified were rule 38, rule 42, rule 175, rule 935, rule 1273, rule 1511. It is important to note that once the best rules emerge, they may be directly applied to an image, quickly leading to the desired result.

The results in "Fig. 3","Fig. 4" and "Fig. 5", clearly demonstrate that rules 38, 42, 175, 935, 1273, and 1511 extracted by the QPSO algorithm, produce satisfactory results. Edges are continuous, clean and fine. They are one pixel wide. The external contour is accurate, continuous and without noise. The rules provide good edges with a fine level of details.

A. Images with Ground Truth

In this section, we present five images with their hand-made ground truth, provided from the Berkeley database: woman, plane, swan, bird and church. Figures "Fig. 6","Fig. 7", "Fig. 8","Fig. 9" and "Fig. 10" show the edges after application of rules 38, 42, 175, 935, 1273, 1511. We can easily conclude that the edges provided by the CA rules are very satisfactory, with a high visual quality. They provide a great level of continuity and smoothness. Edges are fine and accurate.

B. Fitness fuctions

In order to evaluate the quality of edges produced by a CA rule, we need a function that measures how close are the

Fig. 3. Edge detection of Cameraman image. a) Original image b) Binary image c) Rule 38 d) Rule 42 e) Rule 175 f) Rule 935 g) Rule 1273 h) Rule 1511

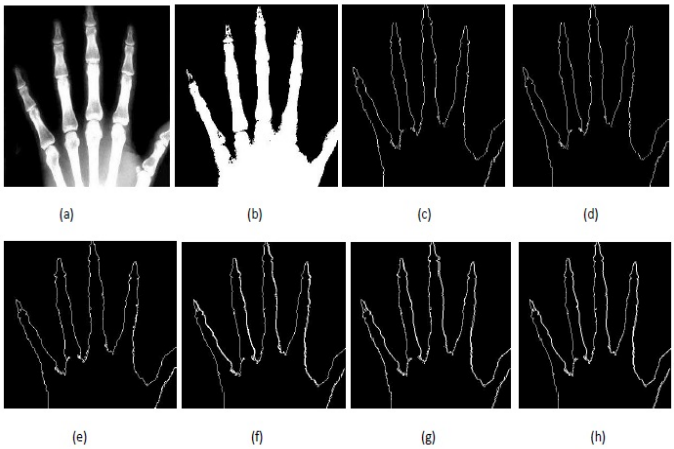


Fig. 4. Edge detection of X-ray image. a) Original image b) Binary image c) Rule 38 d) Rule 42 e) Rule 175 f) Rule 935 g) Rule 1273 h) Rule 1511

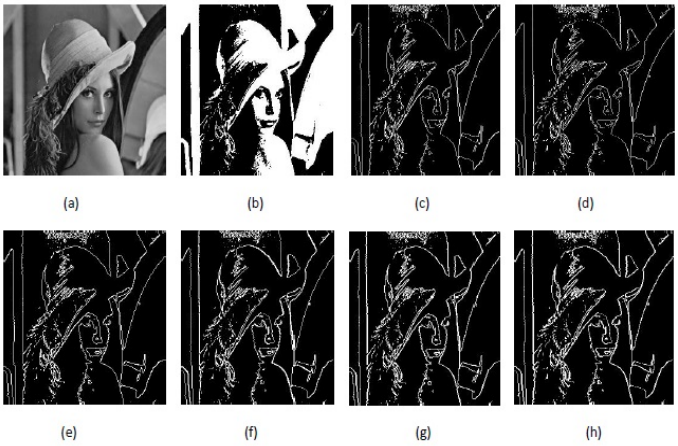


Fig. 5. Edge detection of Lena image. a) Original image b) Binary image c) Rule 38 d) Rule 42 e) Rule 175 f) Rule 935 g) Rule 1273 h) Rule 1511

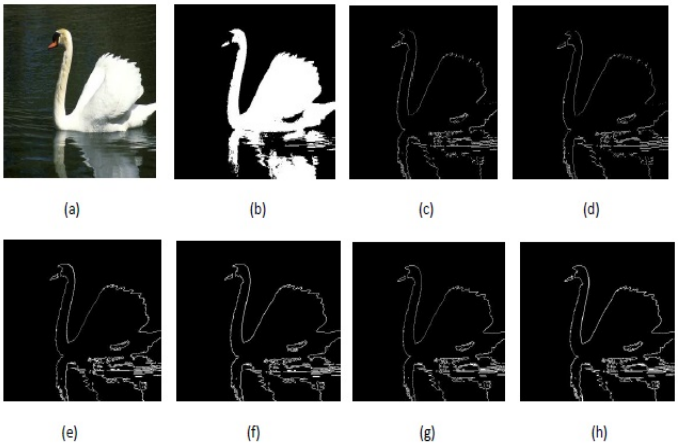


Fig. 6. Edge detection of Swan image. a) Original image b) Binary image c) Rule 38 d) Rule 42 e) Rule 175 f) Rule 935 g) Rule 1273 h) Rule 1511

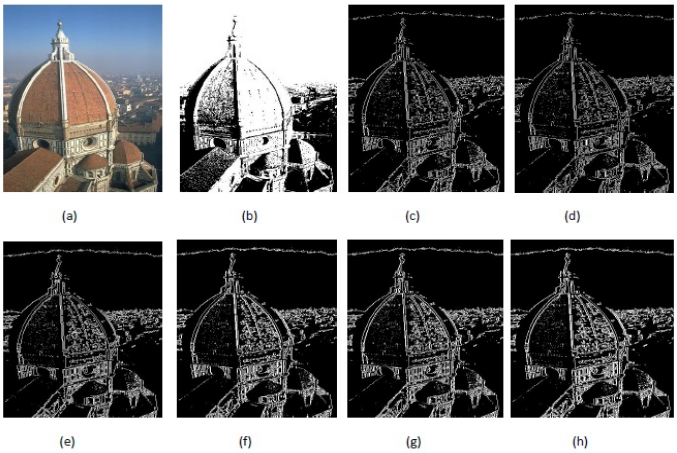


Fig. 7. Edge detection of church image. a) Original image b) Binary image c) Rule 38 d) Rule 42 e) Rule 175 f) Rule 935 g) Rule 1273 h) Rule 1511

results produced by this CA to the ground truth.

Whichever optimization method is used, an objective function is required, and its quality obviously has a crucial effect on the final results. In this work, We considered two fitness functions: the Structural Similarity Index (SSIM) and Root-Mean-Square Error (RMSE). The role of these functions is to measure the difference of quality between the CA resulting image and the reference image.

For images with more intensity values, the RMSE between the input and target image is a straightforward measure. However, it is well known that RMSE values have limitations. In particular, given that they do not involve inter-pixel relationships they often do not capture perceptual similarity.

SSIM measures the image similarity taking into account three independent channels including luminance, contrast and structure [33]. It is the well suited measure for gray level images. The SSIM metric between two images x and y is defined as

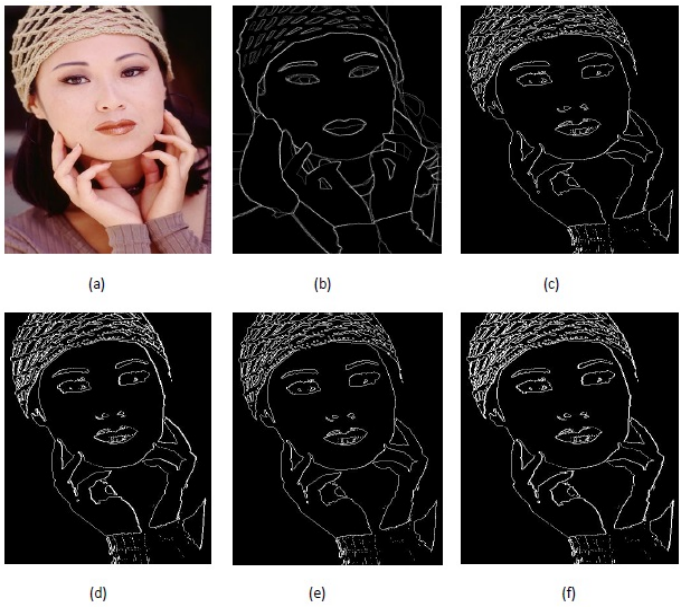


Fig. 8. Edge detection of woman image. a) Original image b) Ground truth c) Rule 175 d) Rule 935 e) Rule 1273 f) Rule 1511

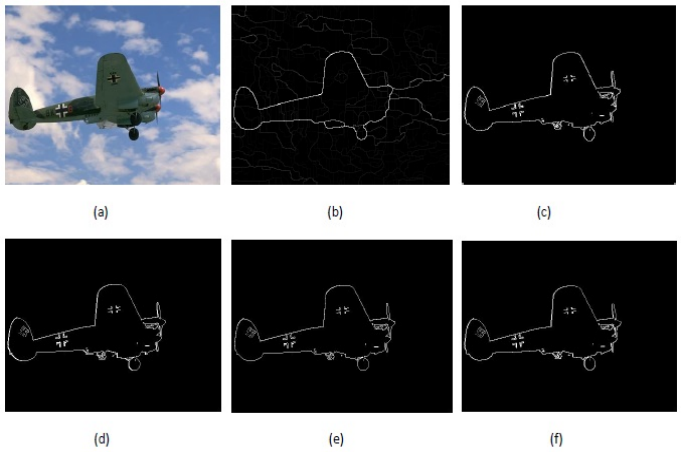


Fig. 9. Edge detection of plane image. a) Original image b) Ground truth c) Rule 175 d) Rule 935 e) Rule 1273 f) Rule 1511

"(3)" :

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (3)$$

where $\mu_x, \mu_y, \sigma_x^2, \sigma_y^2, \sigma_{xy}$ are the mean of x, the mean of y, the variance of x, the variance of y, and the covariance of x and y, respectively. Following [33], C_1 is set to $(0.01 * 255)^2$ and $C_2 = (0.03 * 255)^2$.
The RMSE is calculated according to "(4)":

$$RMSE = \sqrt{\frac{1}{MN}\sum_{r=0}^{M-1}\sum_{c=0}^{N-1}[E(r,c) - O(r,c)]^2} \quad (4)$$

where $O(r,c)$ is the original image (in our case, the ground-truth image) and $E(r,c)$ is the reconstructed image.

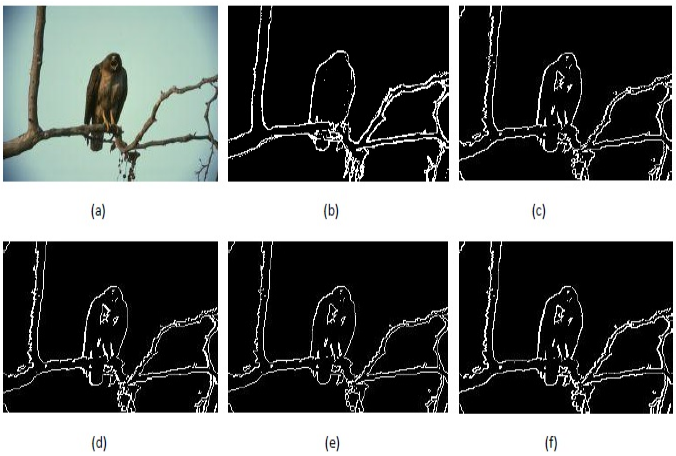


Fig. 10. Edge detection of bird image. a) Original image b) Ground truth c) Rule 175 d) Rule 935 e) Rule 1273 f) Rule 1511

"Tab. I" shows the best fitness values obtained for Woman, Bird, and Plane input images. For each image, they are tested using the fitness functions RMSE and SSIM. The best fitness values are collected in the table. The numerical results clearly show that rules 175, 935, 1273 and 1511 provide high performances and very good values of fitness. They consolidate the visual results obtained by these rules.

VI. Conclusion

This paper presents a novel method of edge detection based on a cellular automata with extended Moore neighborhood. Although the rule space have become larger, we used an evolutionary algorithm to extract the optimal rules which provide the best results. This process allowed to extract a subset of simple rules which produce very good edges in only one iteration. Experiments are carried on several images, from Mathworks, and comparisons are made with images from Berkeley database which have ground truth edges. The visual results show that the extracted rules enhance the contrast of the output images, and smoothes the edge of the objects present in the image. The fitness values of SSIM and RMSE are calculated and confirm the good quality of obtained results.

Possible future research directions could be extended to search about rules that perform image denoising, or exploring quantum metaheuristics for optimizing huge sets of rules.

References

[1] M. Juneja and P. S. Sandhu, "Performance evaluation of edge detection techniques for images in spatial domain". International journal of computer theory and Engineering, 1(5), 614, 2009.
[2] D. Ziou and S. Tabbone, "Edge detection techniques-an overview". Pattern Recognition and Image Analysis, (8) , 537—559, 1998.
[3] S. Amrogowicz, Y. Zhao, Y. Zhao, "An edge detection method using outer Totalistic Cellular Automata". Neurocomputing, 214, 643-653, 2016.
[4] J. Canny, "A computational approach to edge detection". IEEE Transactions on pattern analysis and machine intelligence, (6), 678–698, 1986.
[5] A. W. Burks (Ed.), Theory of Self-Reproducing Automata, University of Illinois Press, Champaign, IL, USA, 1966.

TABLE I
FITNESS VALUES FOR IMAGES: WOMAN, BIRD AND PLANE

	Rule 175		**Rule 935**		**Rule 1273**		**Rule 1511**	
	RMSE	***SSIM***	***RMSE***	***SSIM***	***RMSE***	***SSIM***	***RMSE***	***SSIM***
Woman	0.213	0.99	0.216	0.99	0.221	0.99	0.211	0.99
Bird	0.118	0.99	0.127	0.99	0.124	0.99	0.115	0.99
Plane	0.021	0.99	0.022	0.99	0.021	0.99	0.021	0.99

[6] J. Mohammed, and D. R. Nayak, "An efficient edge detection technique by two dimensional rectangular cellular automata". In International Conference on Information Communication and Embedded Systems (ICICES2014) (pp. 1-4),2014.

[7] N. H. Packard and S. Wolfram, "Two-Dimensional Cellular Automata", Journal of Statistical Physics, 38(2), 901–946, 1985.

[8] E. Fredkin, "Digital Machine: A Informational Process Based on Reversible Cellular Automata". Physica D, 45(7), 254–270, 1990.

[9] J. Kari, "Reversability of 2D Cellular Automata is Undecidable", Physica D, 45(7), 379–385, 1990.

[10] N.R. Silva, P. Ween, B.D. Baets and O.M. Bruno, "Improved texture image classification through the use of a corrosion-inspired cellular automaton", Neurocomputing, Part C, 1560–1572, 2015.

[11] Y.G. Yang , S. Tian, H. Lei, Y.H. Zhou and W.M. Shi, "Novel quantum image encryption using one-dimensional quantum cellular automata", Information Sciences, 257–270, 2016.

[12] F. Qadir and K.A. Khan, Investigations of Cellular Automata Linear Rules for Edge Detection, "International Journal of Computer Network and Information Security", 4(3), 47–53, 2012.

[13] S. Uguz, U. Sahin and F. Sahin, "Uniform Cellular Automata Linear Rules for Edge Detection", in: 2013 IEEE International Conference on Systems, Man, and Cybernetics, 2945–2950, 2013.

[14] D. Aydogan, "CNNEDGEPOT: CNN based edge detection of 2D near surface potential field data", Computers and Geosciences, (46),1–8, 2012.

[15] M. Diwakar, P.K. Pate and K. Gupta, "Cellular Automata Based Edge Detection for Brain Tumor", in: 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 53–59, 2013.

[16] S. Wongthanavasu and R. Sadananda, "A CA-Based Edge Operator and its Performance Evaluation", Journal of Visual Communication and Image Representation, 14(2), 83–96, 2003.

[17] S. Djemame, O. Djidel and M. Batouche "Image Segmentation using Continuous Cellular Automata", in: 10th International Symposium on Programming and Systems (ISPS), 94–99, 2011.

[18] C.L. Chang, Y.J. Zhang and Y.Y. Gdong, "Cellular Automata for Edge Detection of Images", Proceedings of the Third International Conference on Machine Learning and Cybernetics, 3830–3834, 2004.

[19] Y. Chen and Z. Yan, A Cellular Automatic Method for the Edge Detection of Images, in: D.-S. Huang, I. Wunsch, DonaldC., D. Levine, K.-H. Jo (Eds.), Advanced Intelligent Computing Theories and Applications. With Aspects of Artificial Intelligence, Vol. 5227 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 935–942, 2008.

[20] P.L. Rosin, "Training Cellular Automata for Image Processing", IEEE Transactions on Image Processing,15(7), 2076–2087, 2006.

[21] P.L. Rosin, "Image Processing using 3D-State Cellular Automata", Computer Vision and Image Understanding, 114(7),790–802, 2010.

[22] M. Batouche, S. Meshoul and A. Abbassene, On Solving Edge Detection by Emergence, in: M. Ali, R. Dapoigny (Eds.), Advances in Applied Artificial Intelligence, Vol. 4031 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 800–808, 2006.

[23] S. Slatnia, M. Batouche and K.E. Melkemi, Evolutionary Cellular Automata Based-Approach for Edge Detection, in: F. Masulli, S. Mitra, G. Pasi (Eds.), Applications of Fuzzy Sets Theory, Vol. 4578 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 404–411, 2007.

[24] S. Djemame and M. Batouche, "Combining Cellular Automata and Particle Swarm Optimization for Edge Detection", International Journal of Computer Applications, 57(14), 16–22, 2012.

[25] M. Mraz, N. Zimic, I. Lapanja and I. Bajec, "Fuzzy Cellular Automata: from Theory to Applications", in: IEEE International Conference on Tools with Artificial Intelligence, 320–323, 2000.

[26] K. Zhang, Z. Li and X.O. Zhao, "Edge Detection of Images based on Fuzzy Cellular Automata", in: Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, (2), 289–294, 2007.

[27] D. K. Patel, S. A. More, "Edge Ddetection Technique by Fuzzy Logic and Cellular Learning Automata using Fuzzy Image Processing", in: International Conference on Computer Communication and Informatics (ICCCI), 1–6, 2013.

[28] S. Sinaie, A. Ghanizadeh, E.M. Majd and S. M. Shamsuddin, A Hybrid Edge Detection Method Based on Fuzzy Set Theory and Cellular Learning Automata, in: International Conference on Computational Science and Its Applications, ICCSA 09., 208–214, 2009.

[29] P. Doll´ar and C. L. Zitnick, Structured Forests for Fast Edge Detection, in: ICCV, International Conference on Computer Vision, 2013.

[30] M. H. Mofrad, S. Sadeghi, A. Rezvanian and M. R. Meybodi, "Cellular edge detection: Combining cellular automata and cellular learning automata", International Journal of Electronics and Communications,69(9), 1282–1290, 2015.

[31] M. Han, X. Yang and Y. Jiang, "An extreme learning machine based on cellular automata of edge detection for remote sensing images". Neurocomputing , 198, 27–34, 2016.

[32] S. Djemame, M. Batouche, H. Oulhadj and P. Siarry, "Solving reverse emergence with quantum PSO, application to image processing". Soft Computing, 23, 6921–6935, 2019.

[33] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity". IEEE Transactions on Image Processing, 13(4),600–612, 2004.

Using Association Rules for Ontology Enrichment

Dr Khaled Benali

Department of Mathematics and Computer Science, University of Tahri Mohammed Bechar UTMB
Bechar, Algeria
benali.khaled@univ-bechar.dz

***Abstract*—An ontology is a formal description of knowledge as a set of concepts within a domain and the relationships that hold between them. At the same time, data mining techniques are used to discover hidden structures in large databases. In particular, Association Rules are used to discover implicative trends among items in a transactional database. In this context, we propose to develop a method to enrich existing ontologies with the identification of new semantic relationships between concepts in order to have a better coverage of domain knowledge. The enrichment process is realized by association rules discovered by applying the Apriori algorithm. We demonstrate the applicability of this method using an existing ontology.**

***Index Terms*— Apriori; Association Rules; Data Mining; knowledge; Ontology; Ontology Enrichment**

I. INTRODUCTION

ONTOLOGY , a branch of artificial intelligence, is a formal representation of concepts in a particular domain and the relationships amongst those concepts. In more simplified words, Ontology is the knowledge representation of a domain of interest [1]. Ontologies are regularly subject to updates and changes. The realization of these updates is a costly and tedious task because it mobilizes one or more experts in the field to identify and classify new vocabulary elements in the ontology.

In order to speed up the process of evolution and enrichment, fairly recent research has focused on the implementation of semi-automatic and automatic ontology enrichment techniques. The majority of the approaches cited in the literature, often based on statistical or linguistic tools, have focused on adding new concepts and / or existing relationships between them.

Ontologies can be joined with data mining. Data Mining techniques are used to discover non-trivial, implicit, unknown, potentially useful and understandable models from a large set of data. The idea of data mining is to extract hidden knowledge from a bunch of available data. Various forms of knowledge can be learned from data: they can be in the form of rules, models, regularities, concepts, etc... There are several techniques for extracting knowledge: Association rules, Decision trees, Neural networks, Clustering, etc...

The Association Rules (AR) technique is a practical means widely used in the field of knowledge searches, and which has been the subject of several researches to improve its implementation. The main advantage of the association rules lies in its clarity and simplicity of implementation.

In this article, we propose a new approach for enriching an existing ontology by the use of association rules using the Apriori algorithm applied to a database.

The remainder of this paper is organized as follows: in the next section, we present an overview of related approaches to our field of research. In section 3, we present the steps of the development of our approach. Finally, we conclude the article with a conclusion and an overview of the work in progress.

II. RELATED WORK

The use of ontologies with the integration of association rules has undergone a major evolution with the aim of choosing the right techniques to extract and benefit from useful knowledge while facilitating the use and processing of the information obtained. In this section, we will present some approaches that use association rules and ontologies to solve different problems. We divided our research into four trends of research areas (See Table 1):

1. Association rules guided by ontologies and rule schemas.
2. Evaluation of association rules based on ontologies.
3. Classification of association rules based on ontologies.
4. Association rules for enriching of ontologies.

A. The first trend: Association rules guided by ontologies and rule schemas

There are a few works that use association rules guided by ontologies and rules schema. Among these works, we find:

In this thesis [2], the author proposes to model the user's knowledge using a formalism similar to that of association rules, called Rule Schemas. These define, the user's expectations regarding the association rules produced. For the modeling of domain knowledge, the author proposes to use a domain ontology. A "rule schema" allows to express knowledge on the form of the sought rules. It allows to combine the constraints on the attributes with the concepts described in the ontology in order to select only the interesting association rules.

The thesis [3] presents the representation of knowledge by ontologies and rule schemas in the same way as that proposed in the previous approach with a considerable improvement of the Data Mining processing process. The contribution of this approach is to introduce from the start the filtering of useful attributes and concepts and the generation only of useful association rules, based on rule schemas previously chosen by the expert in the field.

B. The second trend: Evaluation of association rules based on ontologies

Many works use ontologies for the evaluation of association rules. Among these works, we cite:

In [4], the authors propose a new approach for the evaluation of association rules. This approach is based on two components: the domain ontology, used for calculating the semantic distance between two items, and the preferences of the user modeling his points of view in relation to the domain. This approach assesses the relevance of pairs of items. Therefore, the semantic distance indicating how close two items are semantically, each type of relationship being weighted differently and the expert's knowledge represent the two components used to guide the process during the selection phase of item sets.

In [5] the authors proposed to create significant partitions in all of the extracted association rules. The approach is based on the combination of knowledge from an ontology with the objective measure of reliability.

In the article [6], the authors present a new method for discovering association rules using an ontology to solve the problems expressed. They present data mining based on ontology on a medical database containing clinical data on patients. The proposed ontology-based data mining algorithm makes rules more intuitive, attractive, and understandable, eliminates waste and unnecessary rules, and, as a minor result, dramatically reduces the execution time of the Apriori algorithm.

The authors of [7] propose an integrated framework for the extraction of multilevel association rules based on constraints using an ontology. The system makes it possible to define a set of constraints specific to a domain by using the ontology to filter the instances used in the process of exploring association rules. This method can improve the quality of the rules of the associations extracted in terms of relevance and comprehensibility. The main advantages of this framework can be summarized in terms of scalability and flexibility.

C. The third trend: classification of association rules based on ontologies

Other works use ontologies for the classification of association rules. Among these works, we cite:

In [8], the authors propose a new approach for classifying association rules according to their conceptual distance, which has been defined on the basis of ontological distance. The proposed classification algorithm helps the user to identify interesting association rules, in particular expected and unexpected rules. This algorithm uses a fuzzy light ontology to calculate the distance between the antecedent and the consequence of the rules on which the classification is based. More the conceptual distance is large, more the rule presents a high interest.

In [9], the authors propose an approach for classifying association rules using the SWETO ontology (Semantic Web Technology Evaluation Ontology). The user has a Web user interface through which he can enter the two entities in which he wishes to find associations, he can also customize his classification criteria by specifying other criteria such as "Favor rare or common associations", "Favor popular or unpopular associations" and "Favor short or long associations", the associations are stored in an Oracle database.

The authors of [10] propose a measure of interest based on an ontology to encode the usefulness of a rule in order to be able to select and classify rules according to their importance using the Apriori algorithm. The proposed approach is based on the semantic calculation of the similarity between two items i1, i2 using on the measure of [11] which is based on the location of the concepts as well as their common ancestor in the ontological hierarchy.

D. The fourth trend: Association rules for enriching of ontologies

Several works use association rules for the enrichment of ontologies. Among these works, we cite:

The author of [12] presents a process of enriching of an existing mammography ontology. This process focuses on conceptual and relational enrichment. Conceptual enrichment is based on the introduction of new concepts. For relational enrichment, the proposed method is based on the extraction of associations between the terms of a domain database.

The principle of this article [13] is based on the deployment of a Minimum Generic Base of association rules (MGB) between terms containing only associations between non-redundant terms, in order to enrich an ontology existing domain and lead to a conceptual network. This network integrates two types of knowledge, namely: semantic knowledge from the initial ontology and implicit knowledge from the generic MGB base, illustrated by the association rules between terms. This ontology enrichment approach is proposed to apply it to real data relating to dystonia disease.

The authors of [14] propose to set up a system using sequential patterns in order to extract the candidate terms for enrichment, and to correlate them to the ontological structure.

For more details on the research work in this section see the article [15].

It appears that the fourth group corresponds to our approach (Association rules for enriching of ontologies) but with other techniques mentioned above. Our approach is the first research that uses Apriori algorithm for ontology enrichment.

Table 1: Summary of related work.

Source	Objective	Results	Issue	Trend of approach
[2]	Pruning; Compliance research; Research for interesting AR	Ontology & Rule schemas	Application of operators for the comparison between AR and rule schemas	**Association rules guided by ontologies and rule schemas**
[3]	Search for useful AR; Reduced cost and execution time	Ontology & Rule schemas	Filtering of useful attributes and concepts. Generation of useful AR	
[4]	Evaluation of AR	Evaluated AR	Semantic distance calculation based on ontology and user interest.	
[5]	Evaluation of AR	Evaluated AR	Extraction of AR; Creation of significant partitions in AR	**Evaluation of association rules based on ontologies**
[6]	Evaluation of AR	Evaluated AR Medical ontology	Discovery of RA. Elimination of unnecessary AR	
[7]	Evaluation and improvement of AR	Ontology	Extraction of multi-level AR. Define the constraints. Filter the instances	
[8]	Ranking of AR	Ontology	Calculation of the conceptual distance based on an ontology	**Classification of association rules based on ontologies**
[9]	Ranking of AR	Ontology	Calculate the classification of ARs based on the context of items in the ontology	
[10]	Ranking of AR	Ontology	Calculation of the Semantic distance based on an ontology	
[12]	Conceptual and relational enrichment of existing mammography ontology	Updated Ontology	Establish new ARs; Ontology enrichment	
[13]	Enrichment of ontology by the minimum generic base of AR	Updated Ontology	Development of the generic AR database; Enrichment of ontology	**Association rules for enriching of ontologies**
[14]	Enrichment of ontology by sequential patterns	Updated Ontology	Extraction of sequential patterns; Enrichment of ontology	

III. PROPOSED APPROACH

The proposed approach consists in using the association rules for the enrichment of an existing ontology, by applying the Apriori algorithm. Our approach goes through the following steps (see Fig .1):

1. Collect and assemble the information in a Database;
2. Application of the apriori algorithm [16] on the Database in order to extract the association rules;
3. Enrichment of the ontology by new concepts using the ARs extracted from the previous step.

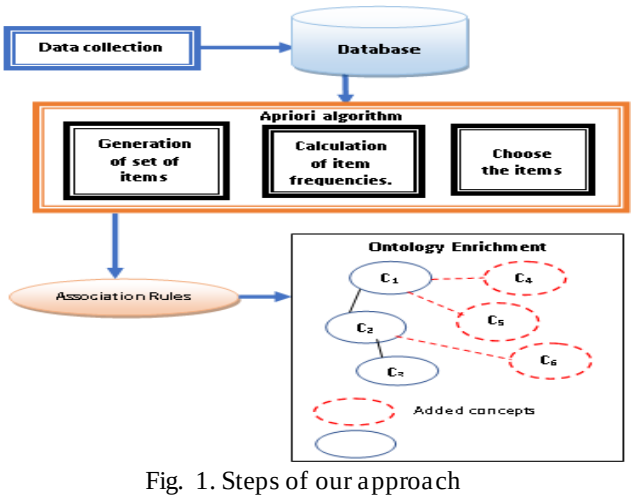


Fig. 1. Steps of our approach

A. Collect and assemble the information in a Database

A.1- "Vêtements" ontology

For the ontology, we used an existing ontology called "Vêtements ontology" which contains the different types of clothes in a store (see Fig 2). This ontology is characterized by a well-structured and fairly compact hierarchy. It contains 104 classes linked by subsumption links and properties.

A.2. Save the results in a database

After collecting the data, we must save the results in a database to apply the Apriori algorithm on this database. The database consists of a set of transactions T described through a set of attributes (items) I. We consider that T = {T1, T2,…, Tn} is the set of n transactions, and I = {I1, I2, ..., Im} is the set of m attributes.

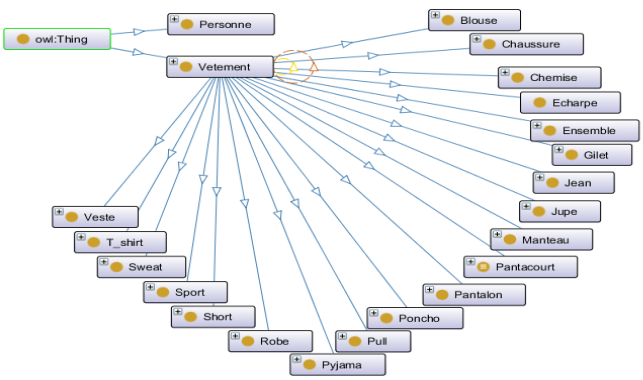


Fig. 2. "Vêtements" Ontology.

B. Apriori algorithm

Association rules help uncover correlations between pages. Deriving association rules from data was first formulated and is called the "market basket problem" [17]. Given a set of elements and a large collection of transactions that are set (baskets) of elements, one can find relationships between the confinements of various elements within these baskets. In addition to the supermarket scenario, other examples of using association rules are users visiting WWW pages, in which the structure and its contents can be optimized.

The strength of the association will be measured by:

A. Support: The support of a rule is defined by:

The number of transactions containing X and Y items / Total number of transactions.

B. Confidence: The confidence of a rule is defined by:

The number of transactions containing X and Y items / Number of transactions containing X product.

B.1- Justification for using apriori algorithm

The Apriori algorithm is one of the most basic and popular algorithms for association rules mining. Agrawal and Srikant proposed the Apriori algorithm in 1994 et al [16]. Until now, this algorithm is the most used and developed by the researcher [18]. Because of the simple process of this algorithm, the advantage of this algorithm is more comfortable to learn, understand, and implemented; this is the reason this algorithm is called the most basic algorithm for association rules Apriori operates on databases containing transactions (for example collection of objects brought by customers, or details of website traffic) [19].

The Apriori algorithm (see Fig. 3) is the most supervised and important algorithm for retrieving frequent itemsets. It goes through the following steps:

- Generating a set of items;
- Frequency of item sets calculation;
- Keeping item sets with minimal support: frequent itemsets;
- Generating and keeping only the rules with minimal trust.

$L_1 = \{\text{large 1-itemsets}\}$;
for ($k = 2$; $L_{k-1} \neq \emptyset$; k++) **do begin**
  C_k = apriori-gen(L_{k-1}); // New candidates
  forall transactions $t \in \mathcal{D}$ **do begin**
    C_t = subset(C_k, t); // Candidates contained in t
    forall candidates $c \in C_t$ **do**
      c.count++;
  end
  $L_k = \{c \in C_k \mid c.\text{count} \geq \text{minsup}\}$
end
Answer = $\bigcup_k L_k$;

Fig. 3. Apriori Algorithm [16]

Note that the C_k data (and L_k) is a set of records containing two fields:

- *"itemset"* this field contains the subset of items;
- *"count"* this field contains the frequency of this set in the transaction database.

B.2- Results of the application of the apriori algorithm on the Database

After collecting the information in a given database and extracting the sequential patterns. We apply the apriori algorithm on these patterns. Table 2 shows the transaction data.

Table 2: Representation of transaction data (partie 1)

	Robe_longue	Pull	T_shirt	Ballerines	Salopette
T1	1	0	0	1	0
T2	0	1	0	0	0
T3	0	0	1	0	1
T4	0	0	0	0	0
T5	0	0	0	0	0
T6	0	0	0	0	0
T7	1	0	0	1	0
T8	1	0	0	1	0
T9	0	0	0	0	0
T10	0	0	0	0	0
T11	0	0	0	0	0
T12	0	0	0	0	0

Table 2: Representation of transaction data (partie 2)

Chaussette	Pyjama	baskets	Pantoufle	Jean_slim	Manteau	Echarpe
0	0	0	0	0	0	0
0	0	0	0	1	0	0
0	0	0	0	0	0	0
1	0	1	0	0	0	0
0	1	0	1	0	0	0
0	0	0	0	0	1	1
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	1	1
1	0	1	0	0	0	0
1	0	1	0	0	0	0
0	1	0	1	0	0	0

The following tables (Table 3, Table 4, Table 5 and Table 6) represent rules support and confidence for levels 1, 2, 3 and 12 respectively.

Table 3. The Support and Confidence of Level 1 rules

Rule	Level	Support	Confidence
Robe_longue → pull	1	0	0
Robe_longue → T_shirt	1	0	0
Robe_longue →ballerine	1	0.25	1
Robe_longue → salopettes	1	0	0
Robe_longue → chaussette	1	0	0
Robe_longue → pyjama	1	0	0
Robe_longue → baskets	1	0	0
Robe_longue → pantoufle	1	0	0
Robe_longue → jean_slim	1	0	0
Robe_longue → manteaux	1	0	0
Robe_longue → écharpe	1	0	0

Table 4. The Support and Confidence of Level 2 rules

Rule	Level	Support	Confidence
Pull → Robe_longue	2	0	0
Pull → T_shirt	2	0	0
Pull → ballerine	2	0	0
Pull → salopette	2	0	0
Pull → chaussette	2	0	0
Pull → pyjama	2	0	0
Pull → baskets	2	0	0
Pull → pantoufle	2	0	0
Pull → jean_slim	2	0.083	1
Pull → manteau	2	0	0
Pull → écharpe	2	0	0

Table 5. The Support and Confidence of Level 3 rules

Rule	Level	Support	Confidence
T_Shirt → pull	3	0	0
T_Shirt→Robe_longue	3	0	0
T_Shirt → ballerine	3	0	0
T_Shirt → salopettes	3	0.083	1
T_Shirt → chaussette	3	0	0
T_Shirt → pyjama	3	0	0
T_Shirt → baskets	3	0	0
T_Shirt → pantoufle	3	0	0
T_Shirt → jean_slim	3	0	0
T_Shirt → manteau	3	0	0
T_Shirt → écharpe	3	0	0

Table 6. The Support and Confidence of Level 12 rules

Rule	Level	Support	Confidence
Echarpe→Robe_longue	12	0	0
Echarpe → T_shirt	12	0	0
Echarpe → ballerine	12	0	0
Echarpe → salopette	12	0	0
Echarpe → chaussette	12	0	0
Echarpe → pyjama	12	0	0
Echarpe → baskets	12	0	0
Echarpe → pantoufle	12	0	0
Echarpe → jean_slim	12	0	0
Echarpe → manteau	12	0.16	1
Echarpe → pull	12	0	0

C. *Ontology Enrichment*

The process of enriching an ontology can be divided into two stages: A phase of research of new concepts and a phase of placement of these concepts.

C.1. Research of new concepts

The determined AR: X → Y try to bring together, in a certain way, the candidate concepts X, Y in ontology through association → without naming the relationships. For example, if a rule defines an implication between two concepts "Robe" and "Ballerines" (Dress, Ballerinas) whose support and confidence are respectively higher than the Min_Sup and Min_Conf thresholds, then these two concepts will be associated in the ontology. The transaction table is independent of the ontology, therefore it is possible to find terms that are absent in the ontology.

C.2. Placement of new concepts

This step consists in placing the candidate concepts while preserving the coherence of the pre-established concepts in the initial ontology. The addition of these concepts is not random. This allows not to add conceptual redundancies.

IV. IMPLEMENTATION

To automate the process of our approach, we have produced a software in Java language, which exploits the SQL transaction database. For the implementation of the different datasets used for enriching the ontology, we opted the following development tools:

- NetBeans[1] which is an open source development environment used by programmers to write, compile, debug and deploy programs.
- JENA[2] is an open source working environment in Java, for building semantic web applications. JENA allows you to manipulate RDF, RDFS, OWL and SPARQL documents.
- Microsoft SQL Server Management Studio[3] is a visual database design tool that integrates SQL development, administration, database design, creation and maintenance in a transparent environment for the database system.
- Protégé tool[4] is an open source platform that provides a suite of tools for building knowledge bases and ontologies. Its graphical interface allowing to easily define classes and organize them in class / subclass hierarchy.

A. *"Vêtement" Ontology*

The Figure 4 represents the components of our used ontology.

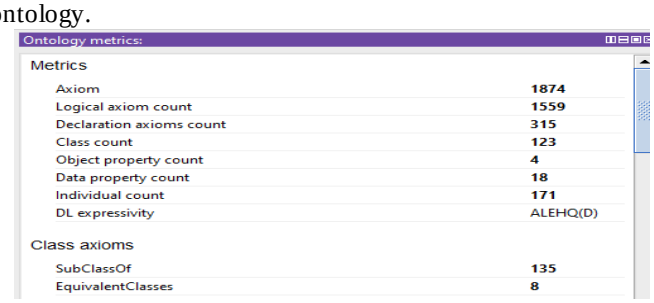
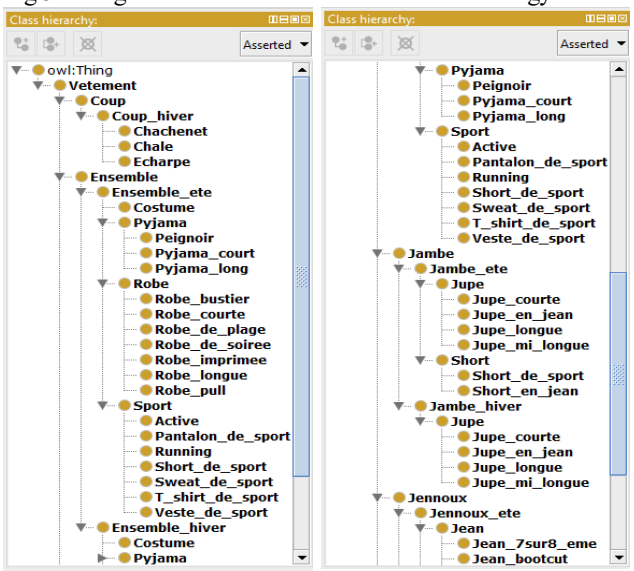


Fig 4. The components of "Vêtements" Ontology

The ontology "Vêtements" consists of 104 classes (see fig 5 and fig 6) illustrated below, they are found in the tab "Class" which is intended for the creation of classes and allows you to manage a tree of classes.

Fig.5 The general classes of "Vêtements" Ontology



[1] https://netbeans.apache.org/download/index.html

[2] https://jena.apache.org

[3] https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver15

[4] https://protege.stanford.edu

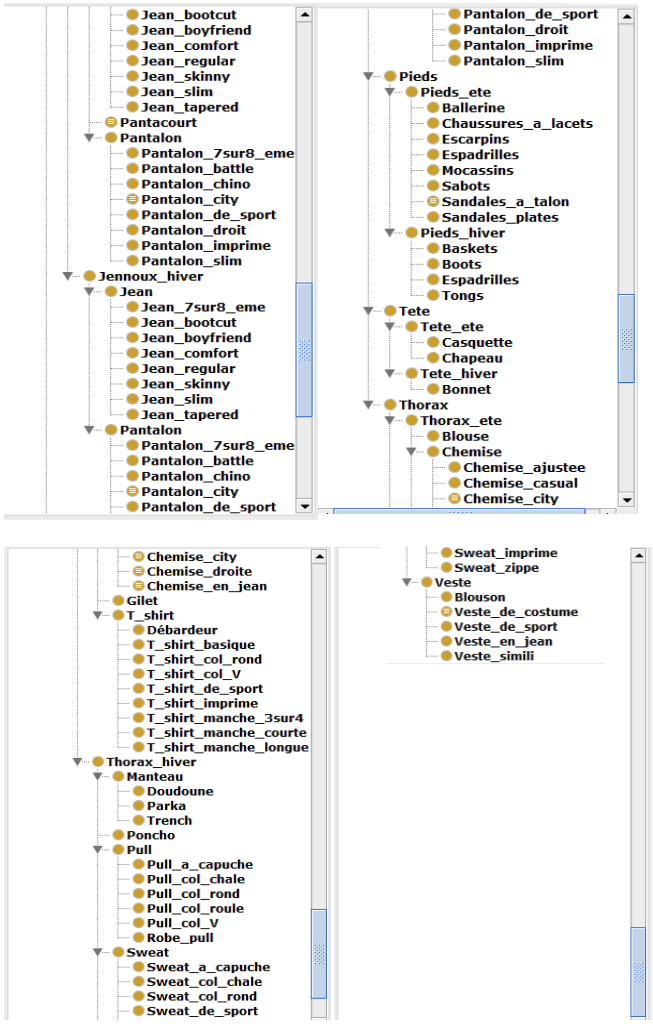


Fig 6. General hierarchy of "Vêtements ontology"

The ontology consists of a few properties, they are found in the 'Data properties' tab (see fig 7).

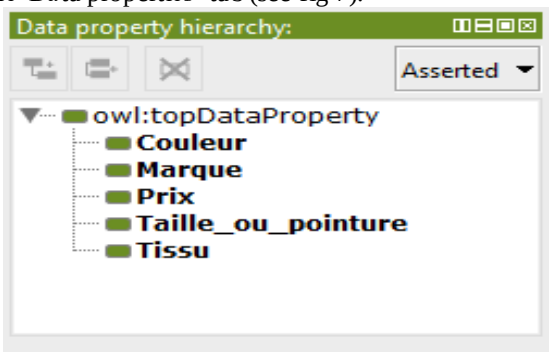


Fig 7. Properties of our ontology

The ontology consists of a few relationships (see fig 8), they are found in the 'Object properties' tab.

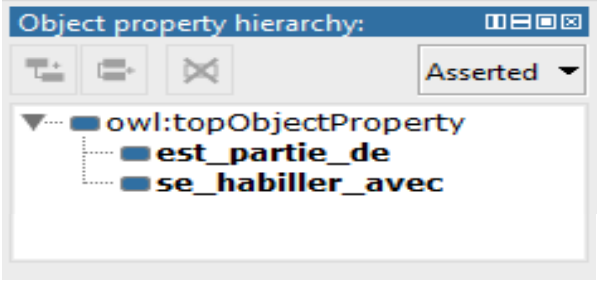


Fig 8. A part of relationships of our ontology

The ontology contains instances (see fig 9), they are found in the "Individuals" tab.

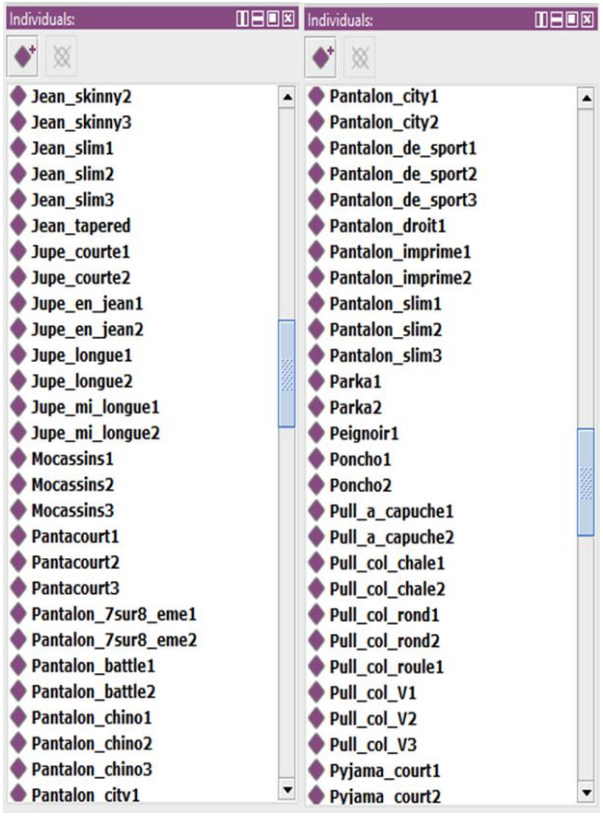


Fig 9. A part of ontology instances

B. *Connection of Protege with NetBeans by Jena*

To establish the connection between Protégé and Netbeans, you must first load all the library (.jar file) and define the general ontology link (found in the ontology) with the following instruction:

Public static final String uri_Ontologie= "http://www.owl-ontologies.com/Vetement.owl";

And the local path of ontology by the following instruction: final String CheminOwl= "D:\\Ontology\\vetement.owl"; Then create a list (ArrayList) to load the tree ontology (jTree) and display it by the following instruction:

jTree_Ontologie.setEnabled(true);

C. *Creation of the database in Microsoft SQL server*

The first step is to create a new database (fig 10) like the following figure:

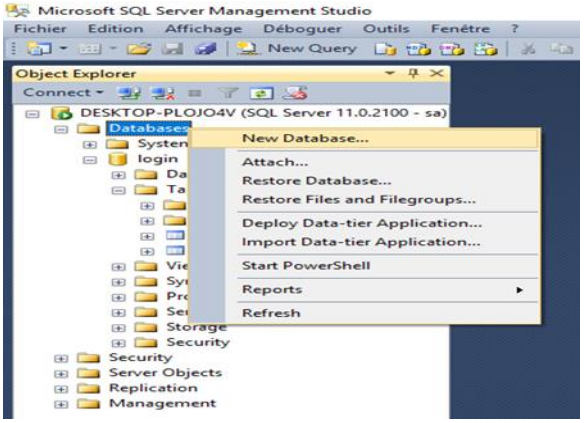


Fig. 10. Creation of a new database

Then right click on the "table" node and choose "new

table" (fig 11), after naming it we right click on the table and choose "Edit Top 200 Rows".

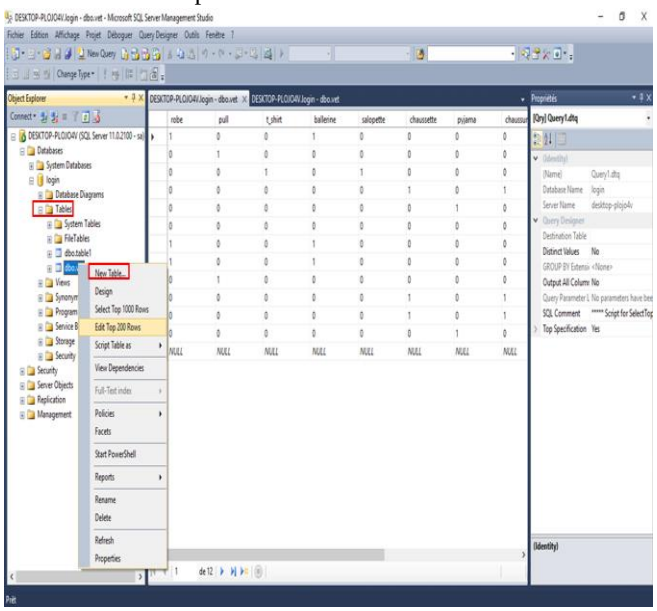


Fig. 11. Creation of a new table.

D. Connection of Microsoft SQL server with Netbeans

Once the database is created, the connection is made by the following instructions:

Class.forName("com.microsoft.sqlserver.jdbc.SQLServer Driver");

String url ="jdbc:sqlserver://localhost:1433; databaseName=login; user=sa; password=0000";

Connection con= DriverManager.getConnection(url);

E. Development of the interface under NetBeans

For the development of our application, we chose the JAVA language for many reasons:

Java is such a fast language and can be used for a heavy application (online games, image processing software, video encoding, etc.).

- Java is organized, it contains well designed and well distributed classes.
- Java is free.
- Java is portable.
- It is compatible with the JENA API, which allows us to manipulate, browse and model OWL documents.

The figure (Figure 12) below shows the main interface of our application « OnERA Acces ».

Fig. 12. Main interface "OnERA Access".

The figure (fig 13) below presents the application processing space.

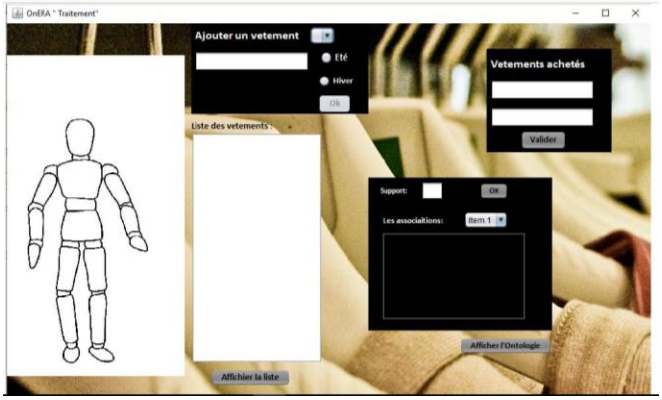


Fig. 13. Processing area of the "OnERA Processing" application.

Step 1. Loading the table and adding a garment

To load the table found in Microsoft SQL Server containing the list of clothes on which the apriori algorithm is applied, just click on the "Display the list" button. And to add a new garment, just click on the body part in the drawing and choose the type of season (Summer or winter) then enter the name of this garment, finally click OK.

The figure (Figure 14) below shows these treatments

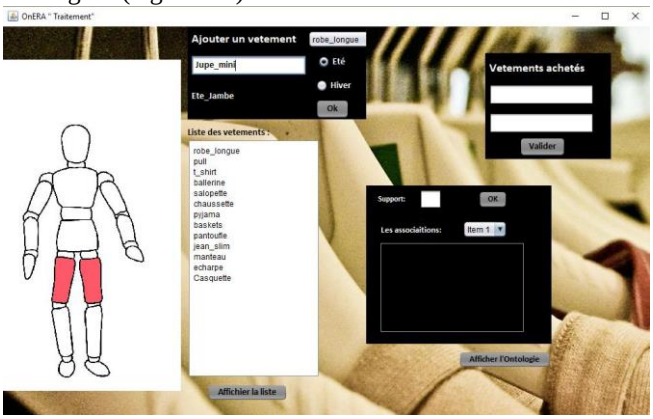


Fig. 14. Loading the table and adding a garment

Step 2. Recording a purchase

To register a purchase, choose the two items of clothes from the list and click on Validate. These two clothes will be registered with the value '1' in the database.

The figure (Figure 15) below presents this treatment.

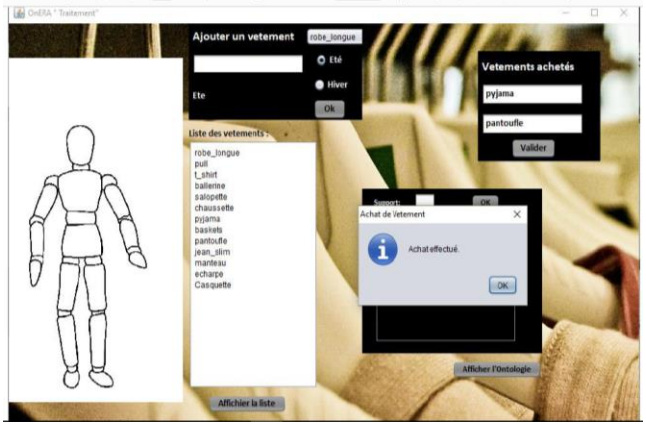


Fig. 15. Recording a purchase

Step 3. Application of the APRIORI algorithm

To extract the association rules, enter the Min support, and click OK (Figure 16).

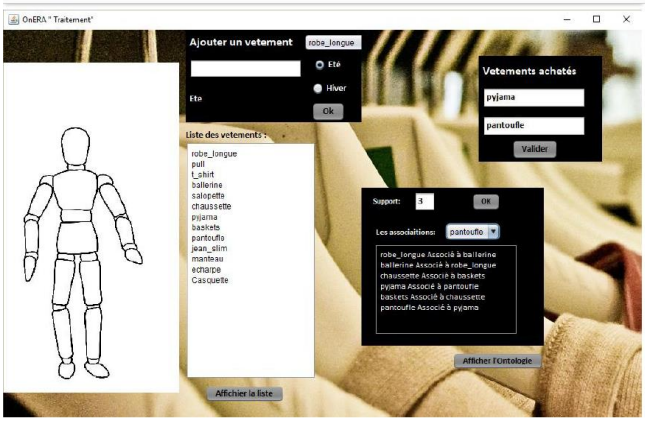


Fig. 16. Application of the APRIORI algorithm and extraction of RAs

Step 4. Loading the "Vêtements" ontology

To display the ontology just click on the button "display the ontology" then on "Load the ontology" (figure 17).

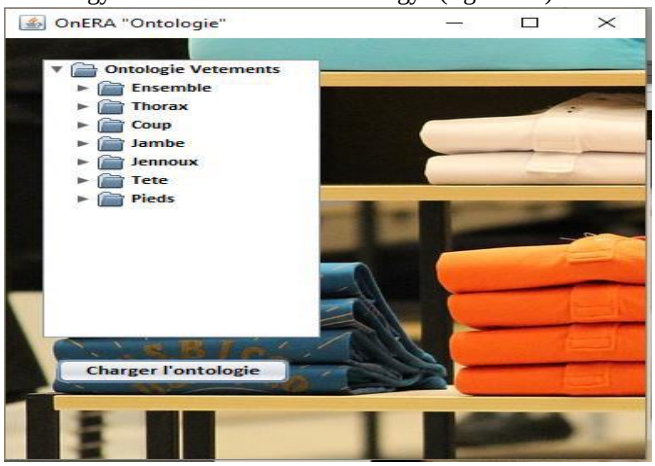


Fig. 17. Loading the "Vêtements" ontology

Step 5. Enrichment result in the Protege tool

After the application of the APRIORI algorithm, new concepts will be added (figure 18).

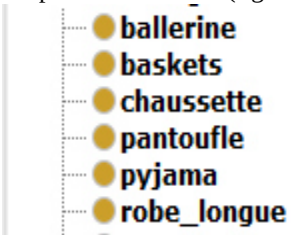


Fig. 18. Enrichment result in the Protege tool.

V. CONCLUSION

In this paper, we have attempted to demonstrate the potential impact of association rules on ontology enrichment. The algorithm applied on a database that we used for the extraction of RA is the APRIORI algorithm. This algorithm has allowed us to enrich the ontology, by adding new concepts.

We used an existing domain ontology that represents the knowledge found in a clothing store. Once the application of the APRIORI algorithm is validated, the obtained results enrich our ontology. After using our approach, we can say that our approach allows for giving accurate results and facilitates the enrichment of ontologies.

When implementing our approach, we used the basic Apriori algorithm to find the association rules. However, many algorithms are proposed for this research. The choice of algorithm depends on the context studied. An improvement can be added to our work. We can also extend our work to other functional areas (finance, maintenance, logistics, etc.) to extract the knowledge hidden in the data history.

REFERENCES

[1] Pundlik, S, S Jori, J Kapure, A Gaikwad and S Valunj. Survey paper on Ontology as a driving force". In International Journal of Inventive Engineering and Sciences, 2(12), 2014, 2137–2141.

[2] Marinica Claudia Association Rule Interactive Postprocessing using Rule Schemas and Ontologies -ARIPSO, Doctoral dissertation, Artificial Intelligence. –Université de Nantes, 2010.

[3] Dahmani Djilali. Fouille des règles d'association guidée par des ontologies et des schémas de règles : Application au domaine de la production SONATRACH/ AVAL , Magister en informatique Spécialité : Modélisation, Optimisation et Evaluation des performances des systèmes (MOEPS) Université des Sciences et de la Technologie d'Oran «Mohamed Boudiaf», 2011.

[4] Ana Cristina, Bicharra Garcia and Inhauma Ferraz. From data to knowledge mining, Artificial Intelligence for Engineering Design, Analysis and Manufacturing. -2009.- 4: Vol. 23. - pp.427 – 441.

[5] Mansingh Gunjan, Osei-Bryson Kweku-Muata and Reichgelt Han , Using Ontologies to Facilitate Postprocessing of Association Rules by Domain Experts, Information Sciences 181. - 2011. - pp.419–434.

[6] Mahmoodi Sayed Abbas, Mirzaie Kamal and Mahmoud Seyed Mostafa, Article, A new algorithm to extract hidden rules of gastric cancer data based on ontology, SpringerPlus, University Yazd, Iran 2016.

[7] Bellandi Andrea, Barbara Furletti, Valerio Grossi, and Andrea Romei. Ontology-driven association rule extraction: A case study. Contexts and Ontologies Representation and Reasoning, page 10, 2007.

[8] Hamani Mohamed Said, Maamrib Ramdane and Kissoumc Yacine Unexpected rules using a conceptual distance based on fuzzy ontology, Journal of King Saud University - Computer and Information Sciences. -January 2014.

[9] Narayana, Varma and Govardhan. An improved technique for ranking semantic associations, International Journal of Web & Semantic Technology. - 2013. - Vol. 4. - pp. 93- 106.

[10] Razan Paul, Tudor Groza and Hunter Jane. Semantic interestingness measures for discovering association rules in the skeletal dysplasia domain, Journal of Biomedical Semantics. - 2014. - 8 : Vol. 5. - pp. 1-13.

[11] Wu Zhibiao and Palmer Martha. Verb semantics and lexical selection, 32nd Annual Meeting of The Association for Computational Linguistics. - Las Cruces 1994. - pp. 133-138.

[12] Idoudi Rihab. Fouille de connaissances en diagnostic mammographique par ontologie et règles d'association, thèse/ IMT Atlantique Université de Bretagne Loire pour obtenir le grade de DOCTEUR, 2018.

[13] Chiraz Latiri, Lamia Ben Ghezaiel — Mohamed Ben Ahmed — Neziha Gouider-Khouja, Article d'Enrichissement d'ontologie par une base générique minimale de règles associatives, Application aux maladies neurologiques : Les dystonies, TUNIS 2010.

[14] Di Jorio Lisa, Abrouk Lylia and Fiot Céline, Article, Enrichissement d'ontologie basé sur les motifs séquentiels, 2007. - lirmm-00176073.

[15] Murtaza S., Ahmed S.. Impact of the Semantic Web mining by using different techniques-A Survey. International Journal of Science and Innovative Research, Vol. 01 Issue 02, December 2020.

[16] Agrawal R and Srikant R. Fast algorithms for mining association rules in large databases. Proceedings of the 20th VLDB Conference Santiago, Chile, 478–499 p.

[17] Agrawal R., Imielinski T and Swami A. Mining Association Rules between Sets of Items in Large Databases. Proceedings of the 1993 ACM SIGMOD International Conference on Management of Data, Washington DC, 207-216 p.

[18] Deo WICAKSONO, Muhammad Ihsan JAMBAK and Danny Matthew SAPUTRA. The Comparison of Apriori Algorithm with Preprocessing and FP-Growth Algorithm for Finding Frequent Data Pattern in Association Rule. Advances in Intelligent Systems Research, volume 172 Sriwijaya International Conference on Information Technology and Its Applications (SICONIAN 2019).

[19] Sai S.C Review of Web Usage Mining using Apriori Algorithm. Published in International Journal of Trend in Research and Development (IJTRD), 32-35 p, ISSN: 2394-9333, Special Issue | ASAT in CS'17 , March 2017.

On the Drivers' Behavior Evaluation using Vehicular Networks

Tahar Bendouma*, Abdou El Karim Tahari*, Chaker Abdelaziz Kerrache*, Mama Chima Boukhelkhal†, Rekaia Bendouma†, Nasreddine Lagraa*
*Laboratoire d'Informatique et de Mathématiques, Université Amar Telidji de Laghouat, Laghouat, Algeria
†Department of Computer Science, Université Amar Telidji de Laghouat, Laghouat, Algeria
Email: * t.bendouma,k.tahari,ch.kerrache,n.lagraa}@lagh-univ.dz;
†{m.boukhalkhal.inf,r.bendouma.inf}@lagh-univ.dz

***Abstract*—With the emergence of connected and intelligent vehicles, various research projects aiming at reducing traffic accidents by detecting driver behavior have also emerged. These vehicles are generally equipped with cameras and sensors that can be used to detect driver's fatigue, drowsiness, and distraction using different technologies and a multitude of classification techniques. In this work, we propose a new real-time driver behavior-detection technique based on vehicle-to-vehicle communication (V2V) and by exploiting the information carried by the periodically exchanged messages known as Cooperative Awareness Message (CAM) that are a part of the European ETSI-ITS standard (or Basic safety message BSM in the US standard). These information include the vehicle's current speed, the average speed, the position, the acceleration, to name a few. In our proposal, each vehicle can classify its neighbors (normal, aggressive) according to its driver's driving style. An audio or video message can be then generated to warn the driver of any vehicle presenting a danger. Simulations conduct in both rural and urban environments depict that our proposal called "Vehicular Ad-Hoc Network Exchange Message (VanetExM)" can determine the state of the driver with a relatively high success rate and low overhead.**

***Index Terms*—VANET, Driver behavior, Safety Message, V2V communication, Road Safety.**

I. Introduction

According to World Health Organization (WHO), every year the lives of approximately 1.35 million people are lost as a result of a road traffic crash, and between 20 and 50 million more people suffer from non-fatal injuries, with many incurring a disability as a result of these injuries [1]. This means that every 24 second one death is registered on road [2]. furthermore, Road traffic crashes cost to most of the countries more than 3% of their gross domestic product (GDP) [1]. It is estimated that fatal and nonfatal crash injuries will cost the world economy approximately $1.8 trillion dollars from 2015–2030 [3]. One of the most important goals of Intelligent Transport Systems (ITS) is to prevent accidents and improve the safety on roads.

Moreover, The National Highway Transportation Safety Administration (NHTSA) reported that between 94% to 96% of all motor vehicle accidents are the result of human error [4]. That is what made driver behavior detection one of the interesting fields of Intelligent Transport Systems. Many factors can affect the behavior of the driver including the fatigue, alcohol, distraction, reckless or careless, experience, environment and vehicle condition, as well as the physiological and the psychological state of the driver. The real-time capturing of all these data requires various types of sensors which are the key factor of all driver detection systems. The captured information is then passed through computer application models to classify the driver behavior. Several methods have been used to detect the abnormal driver behavior among which: Neural Network [5], Kalmen filter [6], Hidden Markov Model [7], Gaussian Mixture Model [8], Smartphone based [9], [10], Fuzzy Logic [11] and K-means [12]. Recently, with the emergence of Vehicular ad-hoc network (VANET), which characterized by high mobility and permanently changes of network topology and the ability of vehicles to communicate with each other and with infrastructure, the real-time analysis of driver behavior became much more attractive research problem.

In the last years, tremendous efforts have been devoted to the study of driver behavior and various research works have approached the problem of detecting abnormal human driver behavior with the aid of capturing and analyzing the driver's face and the vehicle's dynamics via image and video processing. However, the traditional methods are not capable of capturing complex temporal features of driving behaviors [13]. Other works [14] propose the utilization of accelerometers and gyro-sensors built into smartphones for detecting driving behavior. Yet, the Smartphone-based methods suffer from the inability to detect the aggressive driving cases. The authors of [15] developed non-intrusive driver behavior detection system using a context-aware system in VANET to detect abnormal behaviors exhibited by drivers, and to send warnings to other vehicles on the road so as to prevent accidents from happening. A key limitation of the all above research works is that each vehicle can detect only the abnormal behavior of its driver but not the behaviors of the neighboring vehicles.

In this paper, we propose a novel and efficient method for real-time detection of abnormal driving behavior using the periodically inter-vehicle exchanged messages. The main contributions of this paper are twofold: (1) we propose a method based on exploiting the information included or added to periodically exchanged messages (Cooperative Awareness Message CAM or Basic safety message BSM) like acceleration, location, velocity, braking for detecting the driver

behaviors. (2) Alarm the driver or other vehicles by warning messages via wireless communication technology in VANETs.

The rest of this paper is organized as follows. Section II describes the components of the behavior detection system. Section III explain the proposed approach for detecting abnormal driving and alert the driver of vehicle and neighboring vehicles about this dangerous driving which can decrease accident occurring probability. Section IV shows and discusses the experimental results, and finally, Section V concludes the paper.

II. Driver's behavior detection systems

In the last 10 years different commercial and research systems have been proposed to analyze the driver's behavior, to evaluate the driver's performance, and to assist and help drivers during the driving process [16]. All these systems share a common paradigm called "Driving Monitoring System (DMS)". DMSs are generally classified into In-Vehicle Data Recording Systems and Real-time Monitoring Systems [17] where these latter are the most important ones. In this paper, we propose an extension of the classical behavior detection system (c.f, Fig. 1). This system is divided into three units. The first is the Input Unit and is used to capture the different information concerning the driver and the vehicle, this information will then be processed by the second unit called Treatment Unit which also takes the decision according to the degree of risk and transmits it to the third unit called Output Unit as a simple alert or action.

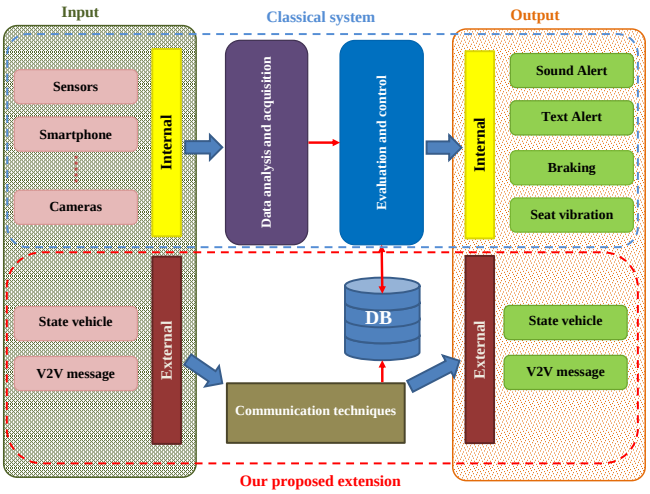


Fig. 1. The components of the behavior detection system

A. System input

Sensors are the key factor of behavior detecting systems. The information can be captured by:

- *Cameras*: Driver behavior is mainly monitored by a camera, and therefore, this approach is known as video-based measurement. Cameras can be used for detecting driver fatigue and drowsiness by observing abnormal behavior associated with eyes movement, facial expression, and head position.
- *Smartphone*: The development of smartphones over the past decade has provided a permanent and mobile source of computation and processing. Moreover, all new smartphones are equipped with a wide range of sensors such as accelerometer, gyroscope, magnetometer, and many other sensors [14].
- *Physiological sensors:* The driver's physiological signals come from human organs such as the brain, eyes, muscles, and heart [18], which can indicate the level of fatigue and vigilance on real-time. This also includes Brain activity which can be captured by electroencephalography (EEG) or near-infrared spectroscopy (NIRS), Eyes activity, measured by ElectroOculoGraphy (EOG), Muscle activity; by ElectroMyoGraphy (EMG), and heart activity by ElectroCardioGraphy (ECG). The methods which use this type of sensors are known as Bio-signal-based methods [13]
- *Sensors on board of the vehicle*: On-board measurement sensors are used to collect a number of indicators deployed to determine the level of vigilance / drowsiness of the driver, this approach is based on measurement and detection of Steering wheel movement (SWM), Vehicle deviation and position [19] and Vehicle speed and acceleration [20].

B. Treatment unit

As shown in Figure 1, internal infrastructure of a behavior detection system is generally composed of two main modules with communication technique to send and receive (to exchange) messages of type V2V or vehicle-to infrastructure. The two modules are:

- *Data analysis and acquisition module*: This module receives data from the different sensors which form a network and communicate with the coordinator network to send the data. The measured signals are then filtered and transformed to eliminate any noise and nuisance that may affect the quality of the sensed data.
- *Evaluation and control module*: The signals are received by the acquisition module undergo in a first step, a noise filtering and unwanted signals discarding phases. In the second step, the signals are processed to extract the main characteristics which reflect the different states of the target application. (e.g. driver's cognitive states). These characteristics can be extracted using learning machine and classification algorithms.

At each identified condition, an appropriate timely action is triggered. This action can be an alarm or a buzz inside the vehicle to alert or wake up the driver. In some cases, the system can take control of the vehicle in order to accelerate or stop the vehicle.

C. System output

After the data processing and the risk assessment phases, the results will be either internal or external (sending warning

messages to other vehicles) or both at the same time. Internal outputs include alerts that is displayed in the dashboard as text or audible to attract the driver's attention in the event of drowsiness or distraction. Other systems combine the alerts with actions like seat vibration to wake the driver up if he has not responded to an alert or make the decision instead if he is not conscious (drunk driver for instance) by a speed decrease or braking (c.f, Fig. 2).

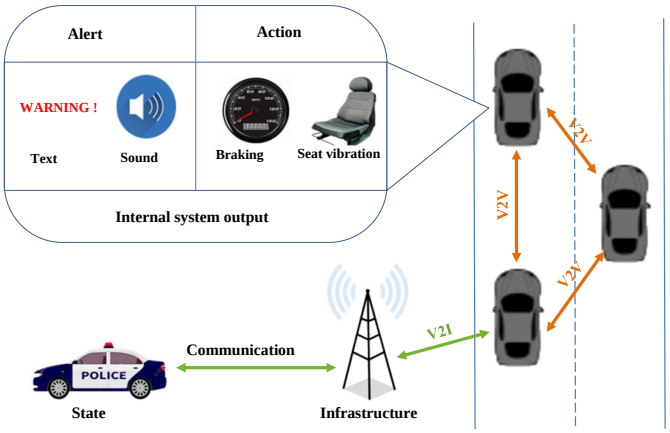


Fig. 2. System output

III. Our proposal

Vehicular Networks are deployed primarily to increase the safety of road users. One of the safety aspects is to detect the behavior and state of the driver. Our approach consists of exploiting the inter-vehicular communications and especially the periodically exchanged messages (CAM/BSM) in order to create a state on each vehicle and thus detect the style of driving and dangerous behavior. Thus, by using the information contained in these messages, it is possible to estimate the driver's condition from his speed, acceleration braking, frequent lane change, etc.

A. Technique description

We consider that our VANET network consists of nodes which communicate with each other using the V2V type in Ad-hoc mode. Each vehicle periodically sends a CAM type message every Δ milliseconds when $\Delta \in$ [100ms, 1000ms], i.e. with a frequency ranging from 1Hz to 10Hz. This message contains information about the vehicle such as its position and speed. After receiving these messages, a processing is done by each vehicle individually to determine the behavior of each neighboring driver. It should be noted that we have avoided using the judgments of others for security reasons in order to avoid collaborative attacks which will have serious consequences. The basic idea is to calculate the difference between the current speed (SC) and the average speed (SA) of a vehicle. Both information must be included in the CAM message and since the average speed does not exist in the standard message [21], then it is imperative to modify the standard CAM message in order to meet the requirements of the proposal protocol as shown in Fig. 3.

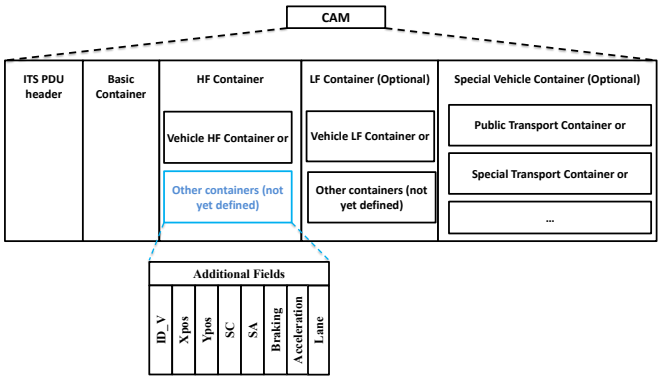


Fig. 3. The Modified CAM formats

The additional fields used in our protocol are:

- **ID_V**: Source identity.
- **Xpos**, **Ypos**: Source position.
- **SC**: the current speed of the source.
- **SA**: the average speed of a vehicle on each lane during a period *T*.
- **Lane**: Lane type (Slow, Medium, Fast, City).
- **Braking**: brake indicator.
- **Acceleration**: acceleration indicator.

To include it in the CAM message, each vehicle calculates its average speed using the following equation for short periods:

$$VM = \frac{1}{N} * \sum_{i=1}^{N} V_i \tag{1}$$

when N is number of captured speeds in a given interval and Vi is the i^{th} captured speeds.
But in case when the period is large, it is better to use the weighted average using the following equation:

$$VM_{(\Delta t+1)} = \alpha VM_{\Delta t} + (1-\alpha)VA_{(\Delta t+1)} \tag{2}$$

when $\alpha \in [0, 1]$
Knowing that each driver has his own driving style which differs depending on the situation, we have chosen to insert the associated average speed (SA) for each type of lane in both freeway and urban environments. For the sake of simplicity, we have limited the number of lanes to three. Thus, we have four speeds integrated in the message associated with (S (00), M (01), F (10), C (11)) with: 'S' is the slow channel, 'M' is the medium channel, 'F' is the fast lane and C is city. Each node receiving a CAM message executes VanetExM algorithm 1. Therefore, in the case when the current speed is slower or faster than the permissible lane speed, the system sends recommendations to the driver of the concerned vehicle to change the lane or adjust the speed according to each case (see Algorithm. 2). In the other case (when the current speed corresponds to the permissible speed on the lane), the system will try to detect abnormal driver behavior based on braking frequency, acceleration frequency, deviation, and the average speed. If an abnormal behavior of neighboring vehicle detected the system warn the driver (see Algorithm. 3).

Algorithm 1 VanetExM Algorithm

VanetExM(_)
Lane: char (S, M, F, C)
ID_V: Integer
SC, SA: Long
Xpos, Ypos: Float
Braking, Acceleration: Boolean
while vehicle receive CAM message from neighbor *i* **Do**
if (Lane = S **and** SC = 40)**or** (Lane = M **and** (SC<40 **or** SC $>$ 80)) **or** (Lane = F **and** (SC $<$ 80**or** SC $>$ 200)) **then**
Warning (ID_V, SC, 'F');
else
if (Lane = S **and** SC $<$ 40) **or** (Lane = M **and** (SC $>$ 40 **or** SC $<$ 80)) **or** (Lane = F **and** (SC $>$80 **or** SC $<$ 200)) **or** (Lane = C **and** SC $<$ 60) **then**
Detection (ID_V, SC, SA, Braking,Acceleration, Xpos)
else if (Lane = C **and** SC $>$ 60) **then**
Warning (ID_V, SC, 'C');
end if
end if
EndWhile

Algorithm 2 Warning

Warning($ID\_V, SC, Road$)
if Road = 'F' **then**
if SC $>$ 0 **and** SC $<$ 40 **then**
Send (ID_V, "You must change your lane to the slow");
else
if SC $>$ 40 **and** SC $<$ 80 **then**
Send (ID_V, "You must change your lane to the medium");
else
Send (ID_V, "You must change your lane to the fast");
end if
end if
else
Send (ID_V, "You are in the city your speed must not exceed");
end if

Algorithm 3 Detection

Detection($ID\_V, SC, SA, Braking, Acceleration, Xpos$)
$\text{Act}_{\text{abnormal}}$=(frequency_Braking = high) **or** (frequency_Acceleration= high)
Dev = ($\Delta x > Deviation\_threshold$)
if $|SC - SA| > Speedthreshold$ **then**
if SC $>$ SA **then**
if Dev = True **then**
Write ("Vehicle",ID_V," its driver may be drunk");
else if $\text{Act}_{\text{abnormal}}$= = True **then**
Write ("Vehicle",ID_V," its driver behaves aggressively");
else if $\text{Act}_{\text{abnormal}}$= True **then**
Write ("Vehicle",ID_V," its driver may be sleepy or tired");
end if
else
Write ("Vehicle",ID_V," its driver behaves normally");
end if

IV. Performance Evaluation

To evaluate the performance of our proposal with Network Simulator **NS2** we have considered two scenarios where in the first one we use a urban model and a freeway model is used in the second. The simulation parameters are described in the table I:

- **Ratio of abnormal vehicles detected**:

Fig. 4 represents the ratio of detected abnormal vehicles in respect of the total number of vehicles, we observe that this ratio increases with the increase in the number of nodes. This can generally be explained by the fact that in a dense network, we have more neighbors and consequently, we receive more messages helping to increase the detection ratio. However, with a density of 25 vehicles, we can see that there is a decrease in this ratio, which is due to packet losses linked to the nature of the wireless medium or to the location of certain isolated nodes .

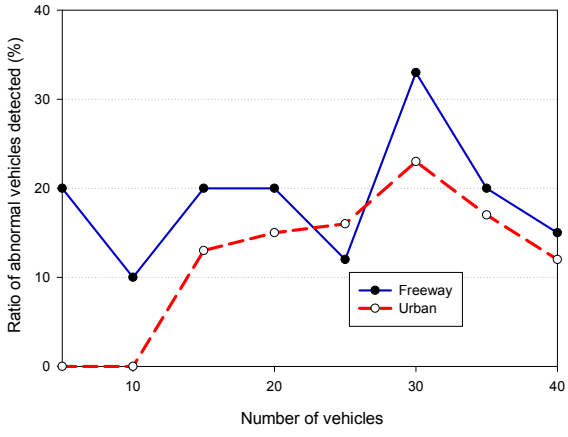


Fig. 4. Ratio of abnormal vehicles detected with respect to the total number of vehicles

TABLE I
SIMULATION PARAMETERS

Parameter	Scenario 1	Scenario 2
Channel type	Channel / WirelessChannel	Channel / WirelessChannel
Protocol	Mac/802.11p	Mac/802.11p
Transmission range	250 m	250 m
Mobility model	Freeway	Manhattan
Number of nodes	[5 – 40]	[5 – 40]
Road length	1.1 Km	–
Packet length	512 Bytes	512 Bytes
Simulation time	100 seconds	100 seconds
Number of intersections	–	3x3

- **Number of generated warning messages**:

Fig. 5 illustrates the performance of the number of generated warning messages compared to the number of vehicles. It can be observed for the two models (Urban and Freeway) that the number of generated warning messages increases with the increase in the number of nodes. The number of warning messages reaches a maximum of 125 in the freeway. On the other hand, it reaches 27 warning messages for the urban scenario. We attribute this increase to the fact that with the increase in the number of nodes in the network, there will be more neighbors. Therefore, each node will detect, in the normal case, all the normal vehicles within its range, and this explains the increase in the number of warning messages. In addition, we notice that the number of warning messages increases more on the freeway than in the city, because in an urban environment, the disconnection is frequent since there are more obstacles and changes of direction (lane), something which decreases the ratio of correctly received messages.

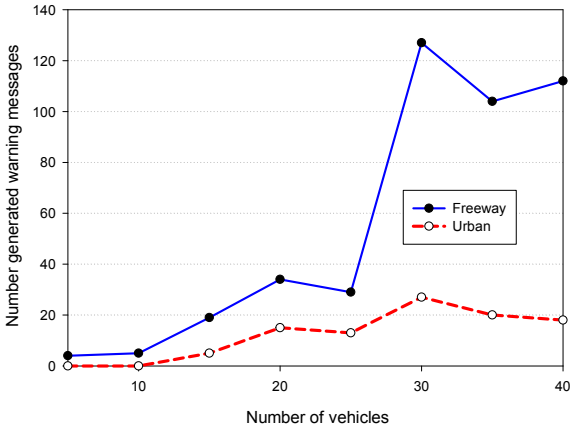


Fig. 5. Number of generated warning messages with respect to the total number of vehicles

- **Number of vehicles that reacted**:

The generation of a warning messages in the normal case should be followed by corrective action of the situation. Fig. 6 represents the number of vehicles which reacted after warning messages according to the number of vehicles.

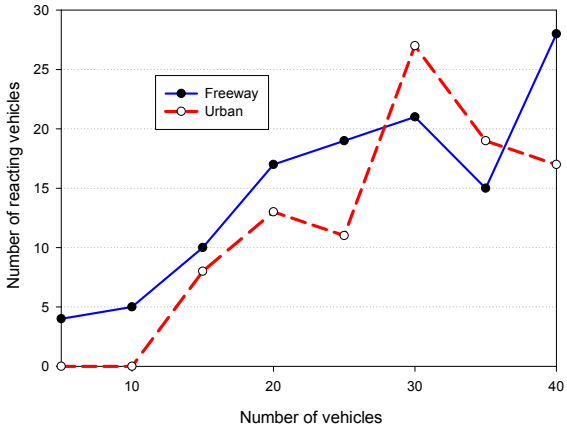


Fig. 6. Number of reacting vehicles with respect to the total number of vehicles

The shape of the curve can have the same explanation of the above curves. Thus, the number of abnormal nodes and the number of reactions increase proportionally with the number of nodes in the network. On the other hand, we justify the decrease for a density of 25 and 35 by the decrease of the abnormal nodes in the network which reacted after warning messages during the simulation time.

- **Ratio of positive faults**:

The ratio of positive faults represents the number of false generated warning messages.

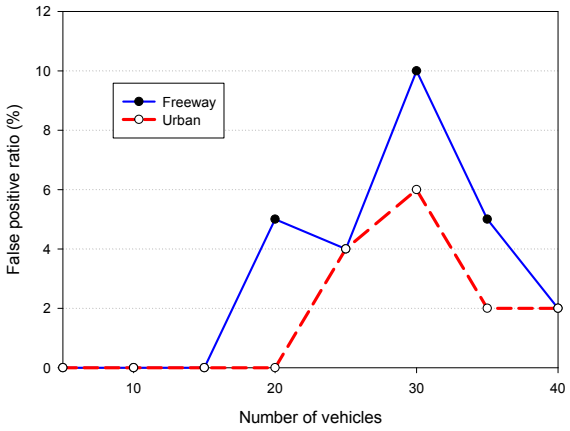


Fig. 7. False positive ration with respect to the total number of vehicles

Fig. 7 shows that this rate is between 0% and 10% of all the abnormal nodes reported. The rate of positive faults reaches its maximum of 10% when the abnormal nodes present more than 20% in our network, which represents 2% of the density. So, the algorithm is overall very reliable.

V. Conclusion

Monitoring and detecting abnormal driver behavior is an important task for improving road safety and preventing accidents. In this context, we presented in this paper our driver behavior detection protocol which uses inter-vehicle communications. This approach made it possible to detect two ”normal or abnormal” behaviors while driving and to classify the abnormal behavior as drowsy, drunk, or aggressive drivers on the fly. In the case of abnormal behavior, the vehicle generates a warning message to reduce the potential undesired damages. The performance evaluation results of our approach called Vehicular Ad-Hoc Network Exchange Message ”VanetExM” in both urban and freeway environments demonstrated the ability of the proposed algorithm to infer driver behavior using readings from different sensors over time and messages received from other vehicles.

As a future work, we plan to run realtime testbeds using smartphones as a mean of inter-vehicles communications to further asses and improve our proposal.

References

[1] World Health Organization. Global status report on road safety 2018: Summary (No. WHO/NMH/NVI/18.20). World Health Organization, 2018.

[2] Association for Safe International Road Travel. Road traffic Injuries: the facts. [cited 2021 March 07]. Available from URL: https://www.asirt.org/safe-travel/road-safety-facts/

[3] Chen S, Kuhn M, Prettner K, Bloom DE. The global macroeconomic burden of road injuries: estimates and projections for 166 countries. The Lancet Plane Health, 1;3(9): pp 390–398, 2019.

[4] Singh, S. Critical reasons for crashes investigated in the National Motor Vehicle Crash Causation Survey. (Traffic Safety Facts Crash-Stats. Report No. DOT HS 812 115). Washington, DC: National Highway Traffic Safety Administration, 2015.

[5] Shahverdy, M., Fathy, M., Berangi, R., Sabokrou, M. Driver behavior detection and classification using deep convolutional neural networks. Expert Systems with Applications, 149, 113240, 2020.

[6] V. Rin and C. Nuthong. Front moving vehicle detection and tracking with Kalman filter. In 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS), pages 304 - 310, 2019.

[7] Yao, Y., Zhao, X., Wu, Y., Zhang, Y., Rong, J. Clustering driver behavior using dynamic time warping and hidden Markov model. Journal of Intelligent Transportation Systems, pp 1-14, 2020.

[8] Indrabayu, R. Y. Bakti, I. S. Areni, and A. A. Prayogi. Vehicle detection and tracking using gaussian mixture model and Kalman filter. In 2016 International Conference on Computational Intelligence and Cybernetics, pages 115 -119, 2016.

[9] Munaf Najim Al-Din. Driver behavior detection techniques: A survey. International Journal of Applied Engineering Research, 13, 06 2018.

[10] A. Kashevnik, I. Lashkov, and A. Gurtov. Methodology and mobile application for driver behavior analysis and accident prevention. IEEE Transactions on Intelligent Transportation Systems, 21(6): 2427 - 2436, 2020.

[11] Aksjonov, A., Nedoma, P., Vodovozov, V., Petlenkov, E., Herrmann, M. Detection and evaluation of driver distraction using machine learning and fuzzy logic. IEEE Transactions on Intelligent Transportation Systems, 20(6), 2048-2059, 2018.

[12] M. H. Baccour, F. Driewer, E. Kasneci and W. Rosenstiel, ”Camera-Based Eye Blink Detection Algorithm for Assessing Driver Drowsiness,” 2019 IEEE Intelligent Vehicles Symposium (IV), Paris, France, pp. 987-993, 2019.

[13] M. H. Alkinani, W. Z. Khan and Q. Arshad, ”Detecting Human Driver Inattentive and Aggressive Driving Behavior Using Deep Learning: Recent Advances, Requirements and Open Challenges,” in IEEE Access, vol. 8, pp. 105008-105030, 2020.

[14] Steinbach, E. (2013). Android Smartphone Application for Driving Style Recognition Android Smartphone Applikation für Fahrstilerkennung. 2013.

[15] Al-Sultan, S., Al-Bayatti, A. H., Zedan, H. Context-aware driver behavior detection system in intelligent transportation systems. IEEE transactions on vehicular technology, 62(9), 4264-4275, 2013.

[16] Kang, H. B. Various approaches for driver and driving behavior monitoring: A review. In Proceedings of the IEEE International Conference on Computer Vision Workshops (pp. 616-623), 2013.

[17] Bergasa, L. M., Nuevo, J., Sotelo, M. A., Barea, R., Lopez, M. E. Real-time system for monitoring driver vigilance. IEEE Transactions on Intelligent Transportation Systems, 7(1), 63-77, 2006.

[18] X. Zhu, W. Zheng, B. Lu, X. Chen, S. Chen, and C. Wang. Eog-based drowsiness detection using convolutional neural networks. In 2014 International Joint Conference on Neural Networks (IJCNN), pages 128-134, 2014.

[19] Pia M. Forsman, Bryan J. Vila, Robert A. Short, Christopher G. Mott, and Hans P.A. Van Dongen. Efficient driver drowsiness detection at moderate levels of drowsiness. Accident Analysis Prevention, 50: 341 - 350, 2013.

[20] Zhijun Chen, Chaozhong Wu, Ming Zhong, Nengchao Lyu, and Zhen Huang. Identification of common features of vehicle motion under drowsy/distracted driving: A case study in wuhan, china. Accident Analysis Prevention, 81 :251 - 259, 2015.

[21] ETSI EN 302 890-2 V2.1.1, Intelligent Transport Systems (ITS); Facilities Layer function; Part 2: Position and Time management (PoTi); Release 2 (2020-03).” 2020.

Navigation of a Differential Drive Mobile Robot Using Nonlinear Model Predictive Control

Welid Benchouche[1], Rabah Mellah[1],and Mohammed Salah Bennouna[2]
[1]*L2CSP Laboratory,Faculty of Electrical and Computing Engineering, University Mouloud Mammri of Tizi-Ouzou, Algeria*
[2]*Mechanical engineering dept, University Kasdi Merbah,Ouargla, Algeria*
welidbenchouche@gmail.com, mellah.rab@gmail.com,bennounams@yahoo.fr

***Abstract*—In this paper, an implementation of a very fast nonlinear model-based predictive controller using a newly developed open-source toolkit (CasADi) was used to attain the two control goals of differential drive mobile robots, point stabilization (regulation) and trajectory following (time-varying reference). The controller's stability was assured by the addition of final state equality constraints, which in general require a long optimization horizon for feasibility. In the work presented here, we performed a full-scale simulation proving the applicability of the terminal stabilization equality constraint have been performed. The obstacle avoidance problem has been solved by adding the obstacle position as a constraint in the main optimal control problem.**

***Index Terms*—Nonholonomic robot, Regulation,Trajectory tracking, Navigation, Nonlinear model predictive**

I. Introduction

The issues of control associated with the class of differential drive mobile robots have attracted the researchers' attention over the last three decennaries. This interest is by cause of theoretical and practical concerns; the nature "non-holonomy" of this category of mobile robot forces limits on velocities acceptable by the system [1]. Notwithstanding, non-holonomy turns out to be valuable because it decreases the control inputs' number, while at the same time, maintaining the system fully controllable in the state space [2]. This benefit, however, introduces a complexity that is related to first control objective: the task cannot be attained with a pure feedback [1]. In the literature, the main control goals considered for this type of systems are point stabilization (regulation) which include forward and parallel parking, and trajectory tracking control. First one aims at driving the robot from one pose to another one. Second one aims to force the robot to follow a provided trajectory changing in time. As it is comparatively simpler, roboticists widely studied the problem of tracking. Researchers in [3] have carried out several tracking techniques, counting feedback linearization, sliding mode, back-stepping and discontinuous methods. In [4], several strategies using Lyapunov control, smooth time-varying control, nonlinear geometric control, piecewise-continuous feedback, and dynamic feedback linearization have been reported. In [2], [5]–[7], Methods fulfilling both control goals were achieved. Among the best cutting-edge control techniques utilized in the industry is model predictive control (MPC); the aim of the latter is to measure a future sequence of control in a given time horizon in order to guide the prediction of the controlled system's output close to the reference value by means of minimizing an objective function over an online optimization phase in relation to future control actions, as a result, a set of command actions and constraints of the states of the system are met [8]. To resolve the two key control goals of nonholonomic differential drives, variations of MPC (linear MPC and nonlinear (NMPC)) have been utilized. Linear version uses a linearized model of the robot dynamic motion equations to allow it to be used exclusively for the problem of trajectory tracking [9], [10]; or its time-non-parameterized case known as path tracking [8], [11]. Nonlinear version includes the nonlinearities of the system and utilizes the motion model of the robot explicitly in the optimization control problem, in [3], [12], researchers have utilized it for tracking; [4], [13] for regulation; and [14] for both. The usage of a predictive control horizon raises a stability problem as mentioned in [4]. It has been shown that stability can be secured by using final-state equality constraints for a finite receding horizon [15], [16]. Further analysis shows that by adding a final-state penalty, the final-state equality limit can be relaxed as a final-state inequality [3], [4]. Another stability criterion was introduced in [14], centered on first-state contractive predictive control. In [3], [4], and [15], it was stated that it is time-consuming and a practically unmanageable task to achieve stability using the terminal equality constraint. None the less, many dynamic optimization packages that implements nonlinear model predictive control have been developed due to developments in hardware and the development of successful numerical algorithms [17], [18]. In comparison with the formerly developed optimization packages, a lately developed package (CasADi) [19], which easily implements NMPC problems, has been shown to be a free software, user-friendly, extensible, and computationally scalable [19]. It has been noted, as per the outlined literature above, that a study using real-time NMPC is needed for the two key control goals of non-holonomic mobile robots, where stabilizing final equality constraints are considered. Navigation is one of the most important problems in the design and development of intelligent mobile robots, it is the ability of a robot to plan and execute collision-free motions within its environment. The sensor data feeds the controller from the environment. This information is considered in the computation of the control law, in which the vicinity to any

obstacle is also penalized [20]. In other words, the obstacle avoidance problem is solved by considering its position as a constraint in the optimal control problem. The problem that is heightened in this paper is that of driving a differential drive to stabilize at a goal position or follow a formerly calculated desired trajectory, avoiding fixed obstacles: A predictive control strategy would seem to be an acceptable approach to the issue, since we know the desired future reference. In this work, our main contribution is to propose a NMPC that utilizes a final state constraint for stability, a norm 2 distance between the robot pose and the obstacle pose constraint for the obstacle avoidance navigation task. A nonlinear model of the robot kinematics is utilized. control variables constraints are also considered and a quadratic objective function is proposed for computing the set of control signals, and the latter is solved using the multi-shooting technique in CasADi toolbox as it reduces the simulation time by 10 to 20 times compared with single shooting technique the solver used for the OCP is the IPOPT.

II. Modelling

In this section, A brief overview of the differential drive kinematics is given along with an example of both control objectives namely regulation and tracking.

A. Robot Kinematics

The derivations of the WMR's kinematics utilized in this paper are based on the assumptions below [3]: Design Assumptions:

- The WMR does not contain flexible parts; it is considered a rigid body robot
- There is no steering link per wheel; wheels can either go forward or backward only

Operational Assumptions:

- The WMR moves on a planar surface.
- The translational friction at the point of contact between a wheel and the surface is large enough so that no translational slip may occur.

The relevant variables for the kinematic model of a typical two-wheel differential mobile robot are its center position coordinates $(x_{rob}; y_{rob})$, its angle of orientation θ_{rob}, along with its linear and angular velocities (v_{rob}, w_{rob}), respectively. To illustrate the position of the robot on the plane, we establish a relationship between the global reference frame on the plane and the local reference frame on the robot. These frames are shown in Fig. 1. Axes X_I and Y_Y define the global reference frame. O is the origin. We choose a point P to represent the position reference point of the robot chassis; the pair $[X_R, Y_R]^T$ represents the robot reference frame point, also referred to as the local frame point, this pair pass-through the point P and defines the WMR's local reference frame. Therefore, the classic prediction model derived from Fig. 1 result in the prediction model described in "(1)".

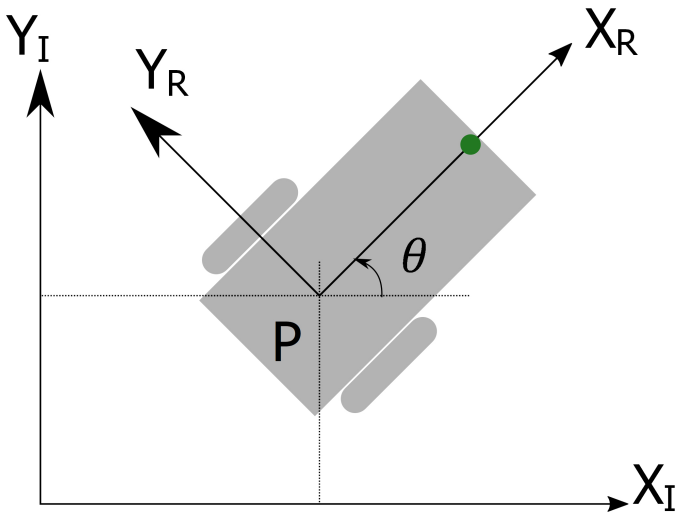


Fig. 1. The global reference frame and the robot local reference frame.

Where, the state and control signal vectors are expressed as $q = (x_{rob}, y_{rob}, \theta_{rob})^T$ and $u = (v_{rob}, w_{rob})^T$.

$$\dot{q} = \begin{bmatrix} \dot{x}_{rob} \\ \dot{y}_{rob} \\ \dot{\theta}_{rob} \end{bmatrix} = \begin{bmatrix} v_{rob} cos(\Theta) \\ v_{rob} sin(\Theta) \\ w_{rob} \end{bmatrix} = \begin{bmatrix} cos(\Theta) & 0 \\ sin(\Theta) & 0 \\ 0 & 1 \end{bmatrix} u \quad (1)$$

Since "(1)" has the form of a driftless system "(2)" and the condition of the accessibility rank is satisfied globally [21], controllability of "(1)" is assured.

$$\dot{q} = \begin{bmatrix} \dot{x}_{rob} \\ \dot{y}_{rob} \\ \dot{\theta}_{rob} \end{bmatrix} = \begin{bmatrix} cos(\Theta) \\ sin(\Theta) \\ 0 \end{bmatrix} v_{rob} + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} w_{rob} \quad (2)$$

B. Point Stabilization and Trajectory Tracking

To describe the two control problems at hand, we define a reference robot according similar to "(1)" and subject to the same constraints, where $q_{ref} = (x_{ref}, y_{ref}, \Theta_{ref})^T$ is the reference state vector, and $u_{ref} = (v_{ref}, w_{ref})^T$ is the input control vector, thus, the reference robot can be described as:

$$\dot{q}_{ref} = \begin{bmatrix} \dot{x}_{ref} \\ \dot{y}_{ref} \\ \dot{\theta}_{ref} \end{bmatrix} = \begin{bmatrix} v_{ref} cos(\Theta_{ref}) \\ v_{ref} sin(\Theta_{ref}) \\ w_{ref} \end{bmatrix} = \begin{bmatrix} cos(\Theta_{ref}) & 0 \\ sin(\Theta_{ref}) & 0 \\ 0 & 1 \end{bmatrix} u_{ref} \quad (3)$$

At this level, if the reference vector q_{ref} has a steady value comparable to the goal position, we are dealing with the point stabilization problem, and the control vector $u_{ref} = (v_{ref}, w_{ref})^{ref} = (0, 0)^T$. On the other hand, according to the chosen reference trajectory, if the vectors q_{ref} and u_{ref} have values changing in time, we are dealing with the trajectory tracking problem. In both cases, controlling "(1)" to track "(3)" is our goal; hence, we define the tracking error model q_e in

the basis of the frame linked to the mobile platform or the local frame as follows:

$$q_e = \begin{bmatrix} x_e \\ y_e \\ \Theta_e \end{bmatrix} = \begin{bmatrix} cos(\Theta) & sin(\Theta) & 0 \\ -sin(\Theta) & cos(\Theta) & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_{ref} - x_{rob} \\ y_{ref} - y_{rob} \\ \Theta_{ref} - \Theta_{rob} \end{bmatrix} \quad (4)$$

It can be easily shown that by forcing the state vector q_e to 0, the two control objectives can be accomplished. We differentiate "(4)" versus time; we get the error dynamics for the tracking problem which is as follows:

$$\begin{aligned} \dot{x}_e &= w_{rob} y_e - v_{rob} + v_{ref} cos(\Theta_e) \\ \dot{y}_e &= -w_{rob} x_e + v_{ref} sin(\Theta_e) \\ \dot{\Theta}_e &= w_{ref} - w_{rob} \end{aligned} \quad (5)$$

Linearizing "(5)", the error model takes the form:

$$\dot{q}_e = \begin{bmatrix} \dot{x}_e \\ \dot{y}_e \\ \dot{\Theta}_e \end{bmatrix} \begin{bmatrix} 0 & w_{ref} & 0 \\ -w_{ref} & 0 & v_{ref} \\ 0 & 0 & 0 \end{bmatrix} q_e + \begin{bmatrix} -1 & 0 \\ 0 & 0 \\ 0 & -1 \end{bmatrix} u_e \quad (6)$$

where u_e is:

$$u_e = \begin{bmatrix} -v_{rob} + v_{ref} cos(\Theta_e) \\ w_{ref} - w_{rob} \end{bmatrix} \quad (7)$$

It can be readily tested that if $[v_{ref}, w_{ref}] = [0, 0]$, the controllability of the model "(6)" is lost, eliminating the ability of applying the point stabilization. Now here, it must be stated that in [4], and [14], a motion model version for "(5)" described in the polar coordinates was also used for the purpose of point stabilization control; however, model "(5)" was only used in the present work to attain the two control problems. Thus, no modification to the controller is needed for our implementation.

III. Design of Model Based Predictive Control

Next, an overview of the nonholonomic mobile robots' scheme of NMPC is provided, outlining the premises that are required for the stability evidence of terminal equality constraints.

A. NMPC Controller Design

Generally, it is possible to express "(1)" in a compact form as follows:

$$\dot{q}(t) = f(q(t), u(t)) \quad (8)$$

Where the state is of n-dimension $q(t) \epsilon R^n$ and the control is of m-dimension $u(t) \epsilon R^m$. The purpose of the control is calculating a permissible command $u(t)$ forcing "(8)" to shift towards the equilibrium defined by ($q_e(t) = 0$ and $u_e(t) = 0$), where $q_e = q - q_{ref}$ and $u_e = u - u_{ref}$. The purpose of the control process is to minimize the cost function given in [3] as follows:

$$J(t, q_e(\tau), u_e(\tau)) = \int_t^{t+T} l(\tau, q_e(\tau), u_e(\tau)) d\tau \quad (9)$$

Where $l(\tau, q_e(\tau), u_e(\tau)) = q_e(\tau)^T Q q_e(\tau) + u_e(\tau)^T R u_e(\tau)$ is called the operating cost, and T is the prediction horizon and matrices Q and R are $(n \times n)$ and $(m \times m)$ respectively, they are symmetric positive definite weight matrices. It has been shown that the stability of predictive regulation is ensured by the imposition of terminal equality constraints [15], [16]. Therefore, at time instant t, the online open-loop optimization problem of our NMPC controller can be illustrated as:

$$\begin{aligned} &\min_u J(t, q_e(\tau), u_e(\tau)) \\ &under\ the\ constraints, \\ &\dot{q}(\tau) = f(x(\tau), u(\tau)) \\ &u(\tau) \epsilon U (\forall \tau \epsilon [t, t+T]) \\ &q_e(t+T) = 0 \end{aligned} \quad (10)$$

Where $0 \epsilon U \epsilon R^m$ is a contract set defining upper and lower bounds of the control effort, and $q_e(t+T) = 0$ describes the equality constraints of the terminal state. Controller stability can be proven, as illustrated in [16], if the following two assumptions are fulfilled.

- The state vector $q_r \epsilon X$ is an equilibrium point where q_r is the reference state vector for the admissible control value $u_r \epsilon U$, and $X \epsilon R^n$is the state space set for the state vector $q(t)$; this means that there is a control value $u_r \epsilon U$ such that $f(q_r, u_r) = q_r$.
- The function of running cost $l : X \times U ß R_0^+$ fulfils $l(q_r, u_r) = 0$ from $u_r \epsilon U$ obtained from the first assumption.

For the first assumption, observing system "(1)" will easily verify these assumptions, and since the operating cost function l has the quadratic form presented in "(9)", the second assumption is also fulfilled.

B. Obstacle Avoidance

To achieve obstacle avoidance, for the Euclidean distance between the prediction of the location of the robot and the location of the obstacle, we must maintain a lower limit. Thus, we ought to enforce the following path restrictions.

$$\sqrt{(x_{rob} - x_{obs})^2 + (y_{rob} - y_{obs})^2} \geq r_{rob} + r_{obs} \quad (11)$$

This leads to the inequality constraint

$$-\sqrt{(x_{rob} - x_{obs})^2 + (y_{rob} - y_{obs})^2} + (r_{rob} + r_{obs}) \leq 0 \quad (12)$$

The OCP becomes

$$\begin{aligned} &\min_u J(t, q_e(\tau), u_e(\tau)) \\ &under\ the\ constraints, \\ &\dot{q}(\tau) = f(x(\tau), u(\tau)) \\ &u(\tau) \epsilon U (\forall \tau \epsilon [t, t+T]) \\ &q_e(t+T) = 0 \\ &-\sqrt{(x_{rob} - x_{obs})^2 + (y_{rob} - y_{obs})^2} + (r_{rob} + r_{obs}) \leq 0 \end{aligned} \quad (13)$$

In the next section, the code that has been created will initialize the NMPC execution routine each time the simulations are analysed.

IV. CasADi Toolkit

In this paper, a toolbox (CasADi) of MATLAB was used to simulate our two discussed control objectives, It is an open-source tool for nonlinear optimization and algorithmic differentiation. It facilitates rapid -yet efficient- implementation of different methods for numerical optimal control, both in an offline context and for nonlinear model predictive control (NMPC). In order to be able to meet the final equality constraints set out in the previous section, it is important to maintain prudently the required number of steps of the prediction horizon to satisfy constraints though sustaining a relatively abrupt update speed for controllers, making the online optimization feasible. The used toolkit allows certain stability requirements to be used, as presented in the next section. The NMPC problem that is solved by (CasADi) is of the general form [19]:

$$\begin{gathered}\min_{q(.),u(.),p} \int_{t_0}^{t_0+T} h(q(t),u(t),p) - \eta(t)^2_Q dt \\ +m(q(t_0+T),p,t_0+T) - \mu_P^2 \\ under\ the\ constraints, \\ q(t_0) = q_0 \\ \forall t\epsilon[t_0,t_0+T] = f(t,q(t),\dot{q}(t),u(t),p) \\ \forall t\epsilon[t_0,t_0+T] \geq s(t,q(t),u(t),p) \\ 0 = r(q(t_0+T),p,t_0+T)\end{gathered} \tag{14}$$

Where $q(.)$ denotes the states, $u(.)$ denotes the manipulated variable, p is a constant parameter of time (optional), T is the prediction horizon, $f(.)$ is the system equation, $s(.)$ the trajectory constraints, and $r(.)$ is the final state constraints. Furthermore, the cost function is stated in the form of a least squares, where η and μ indicate the tracking and final reference. The moving objective function $||h(.)-\eta(t)||^2_Q$ must be stated here exclusively in the work proposed herein. (i.e., $||m(.)-\mu||^2_P = 0$). It is simple to fit the control problem "(14)" written in scalar notation with the control problem stated in "(13)".

V. Simulation Results

This section is devoted for the two control objectives simulation results. Data used here is from the i90 robot from DrRobot company, the latter is a mobile robot platform dedicated to simulation results shown in Fig. 2 and Fig. 3. The robot is a 2 wheeled differential drive mobile robot with an integrated computer, Wi-Fi communications, ultrasonic scanners, IRs, camera, and additional autonomous functions. The robot utilizes a high precision 40 kg.cm 12V DC motor with embedded 800 Count per Cycle Optical Encoder tick encoders for localization purposes. A 2.5 GHz i5 6300 computer with a 8 GB of memory, Windows 10 operating system was utilized to perform the control vector u computation. Full robot specifications can be found in [22].

The online optimisation parameters are selected to achieve the satisfactory controller efficiency including the sampling frequency, the number of prediction horizon steps (N), and the weight matrices Q and R are given in "(9)". In the next, the results of the stabilization point are discussed first, followed by the results of the trajectory.

Fig. 2. The I90 robot from DrRobot company

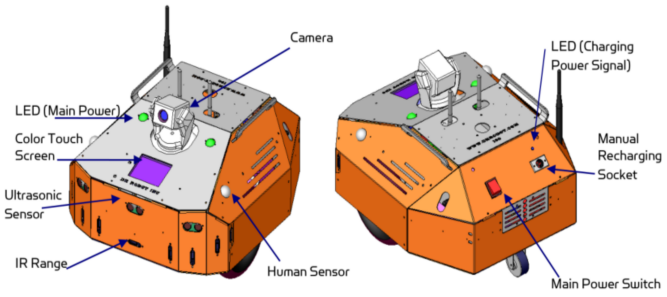


Fig. 3. The I90 robot specifications

A. Point stabilization navigation results

The efficiency of the NMPC controller for point stabilization is seen in this section. The robot begins with the initial pose $q_0 = [000]^T(m,m,rad)$. The robot is commanded to stabilize at the pose $x_r = [8.59.50]^T$. The controller sampling time step is $0.2seconds$ and the number of prediction steps number is $N = 20$, resulting in a prediction horizon time $T = 10seconds$. The weighting matrices Q and R of the objective function "(9)" are diagonal matrices with diagonal elements $(15,10,0.1)$ for Q, and $(0.002,0.002)$ for R. The controller saturation limits for linear velocity v and angular velocity w commands are set to ensure accurate location of the robot and to meet its actuators saturation limits as follows [23]:

$$\begin{bmatrix}-0.75 \\ -753/767\end{bmatrix} \leq \begin{bmatrix}v(ms) \\ w(rads)\end{bmatrix} \leq \begin{bmatrix}0.75 \\ 753/767\end{bmatrix} \tag{15}$$

A summary of the results is in Fig. 4 and Fig. 5. Fig. 4 demonstrates the trajectories performed by the robot (in red).

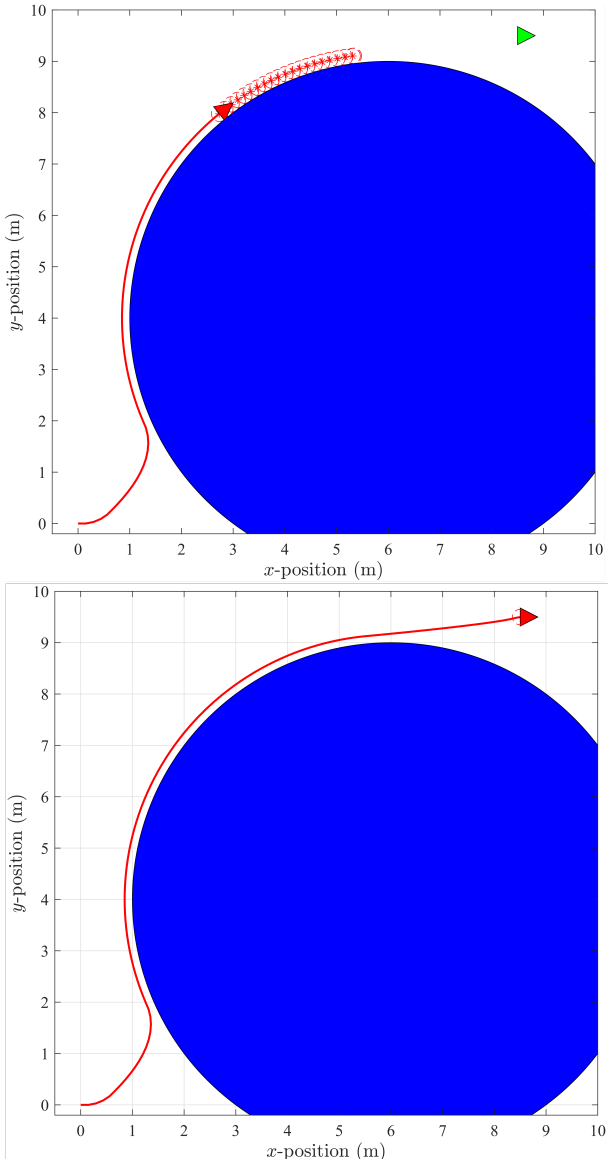


Fig. 4. Point stabilization trajectory results

The red triangle shows the position and orientation of the robot, the circles show the prediction of the state, the obstacle is represented by a blue disk and the reference position by a green triangle. As shown in the Fig. 4, the robot can stabilize the controller perfectly to the required position. The results demonstrate the controller's satisfactory performance in this case. Fig. 5 demonstrates that the robot's actual linear and angular speeds meet the saturation limit specified in "(15)".

B. Trajectory tracking navigation results

For the trajectory tracking problem, the performance of the nonlinear model predictive controller was illustrated by the consideration of two reference paths, a circular and an 8 shape path, namely "(16)", "(17)" and "(18)","(19)". Parameters of the "(16)", "(17)" and "(18)","(19)" trajectories are selected so that v_r and w_r do not violate "(15)", for the circular path,

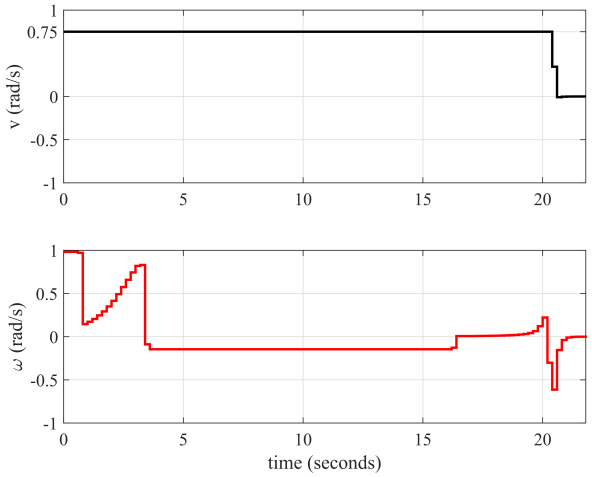


Fig. 5. Point stabilization robot velocities

the initial pose of the robot is $q_0 = [0, 0, 0]^T(m, m, rad)$, and for the eight-shaped path the initial pose is $q_0 = [1, 2, 0]^T(m, m, rad)$

$$x_{ref}(t) = 0.3 + 2sin(0.25t) \tag{16}$$

$$y_{ref}(t) = -2.3 + 2cos(0.25t) \tag{17}$$

$$x_{ref}(t) = 0.3 + 1.5sin(0.3t) \tag{18}$$

$$s_{ref}(t) = 0.3 + 2.5cos(0.15t) \tag{19}$$

The controller sampling time step is $0.2seconds$ with $N = 20$ the prediction steps, resulting in a prediction horizon time $T = 4seconds$. The starting points of the reference trajectories "(16)", "(17)" and "(18)","(19)" have been selected so that an initial error is different than 0. For the circular-shape tracking, the weight matrices Q and R of the objective function "(9)" are diagonal matrices with diagonal elements defined as $(30, 30, 0.2)$ for Q, and as $(50, 50)$ for R.

For the eight-shape tracking, the diagonal elements of Q are $(30, 30, 0.2)$, and the diagonal elements of R are $(9, 5)$. Fig. 6 and Fig. 8 show the actual robot trajectory, the robot trajectory is presented in red, the reference trajetory in dashed blue, the predicted state is shown in red circles and the obstacles in blue disks. Fig. 7 and Fig. 9 show the linear and angular control signals, resulting from following the reference trajectory.

It can be seen from the four figures Fig. 6, Fig. 7, Fig. 8, and Fig. 9 that the errors in the state vector qe are maintained within acceptable limits, whereas the robot speeds are maintained within the limits given in "(15)".

The average computational cost per time step for circular-shape tracking is $(24.2ms)$, the steady-state value of the position error was observed to be within $(\pm 3.5cm)$ and the orientation error was observed to be within $(\pm 0.04rad)$, except when the robot avoids obstacles.

In the 8-shape tracking, the average time computational costs $(23.2ms)$ have been shown to be within $(\pm 4.7cm)$ and orientation errors $(\pm 0.065rad)$, except when the robot is avoiding obstacles.

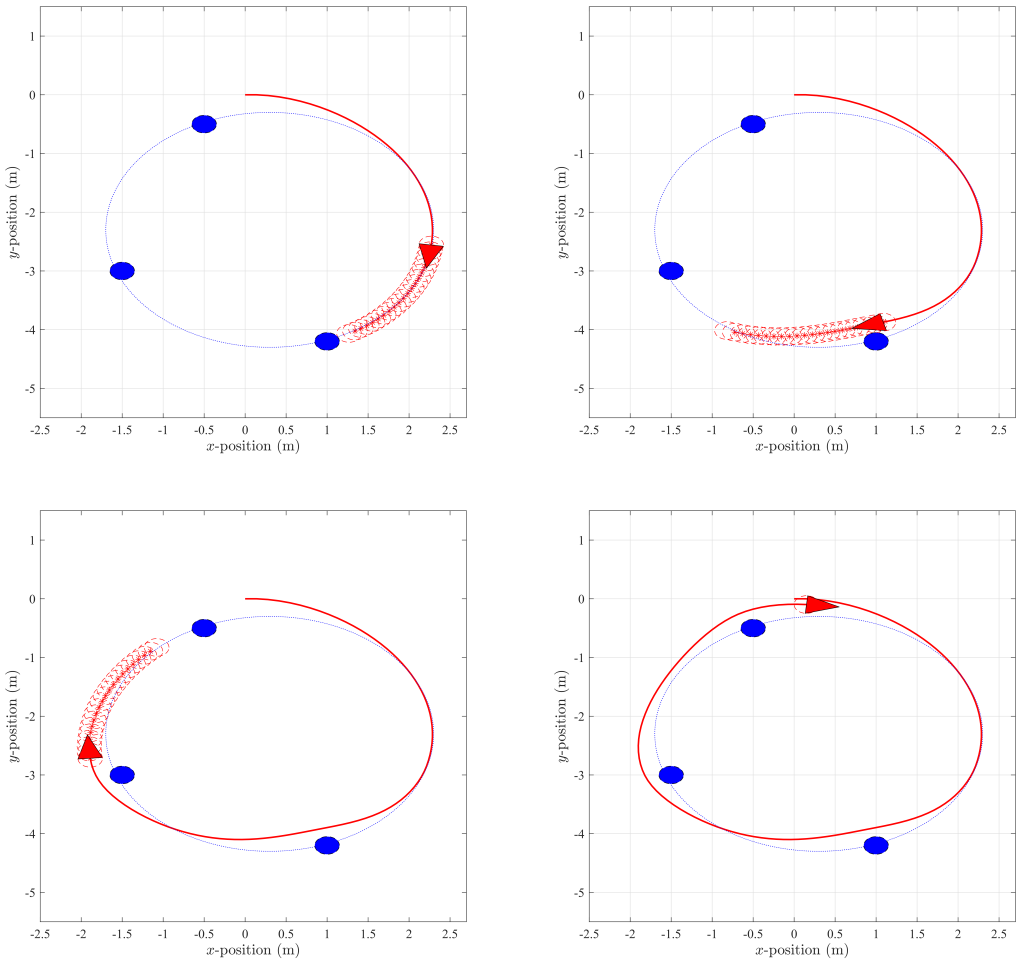


Fig. 6. Circular shape trajectory tracking and navigation results

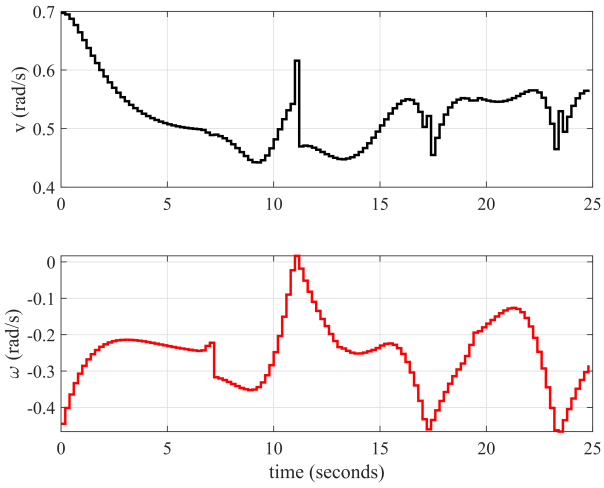


Fig. 7. Circular shape trajectory tracking and navigation velocities results

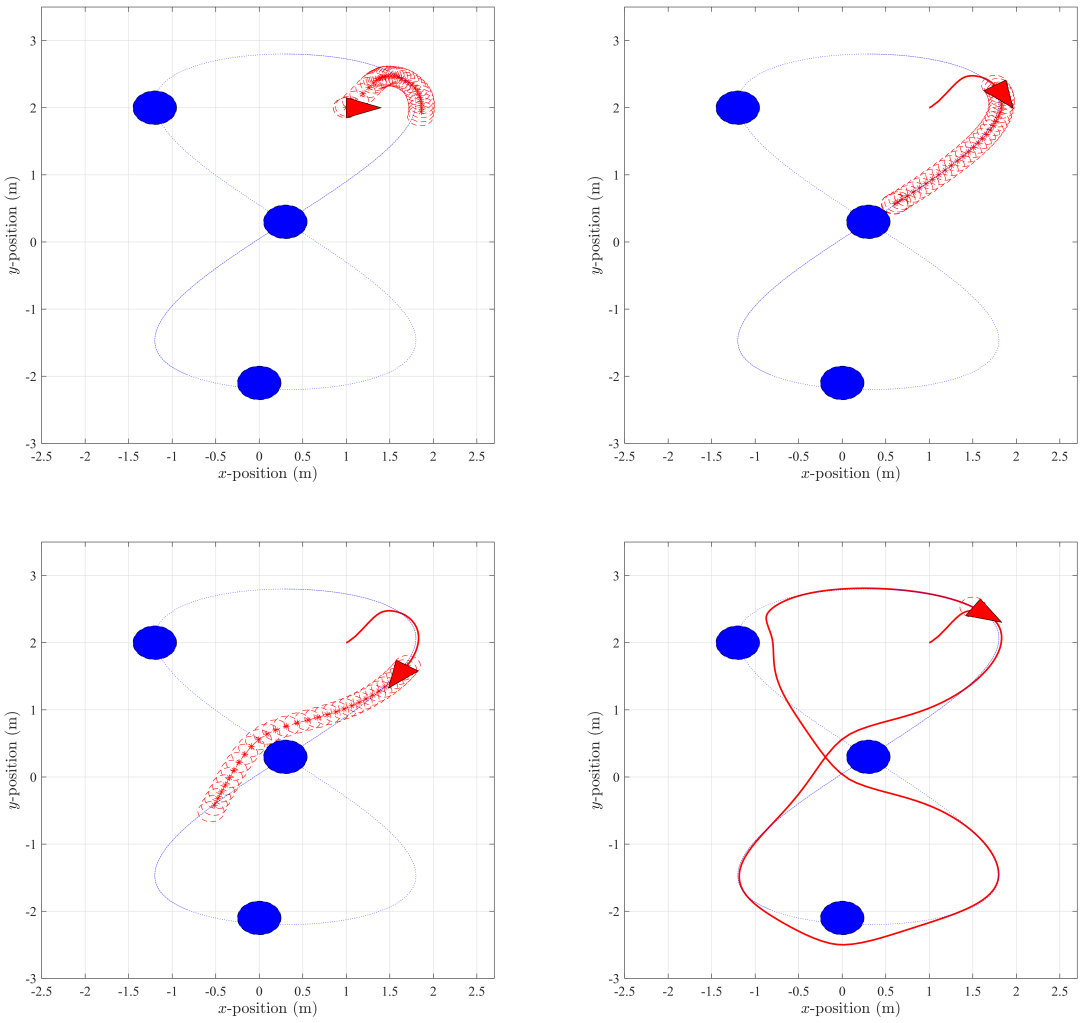


Fig. 8. Lemniscates shape trajectory tracking and navigation results

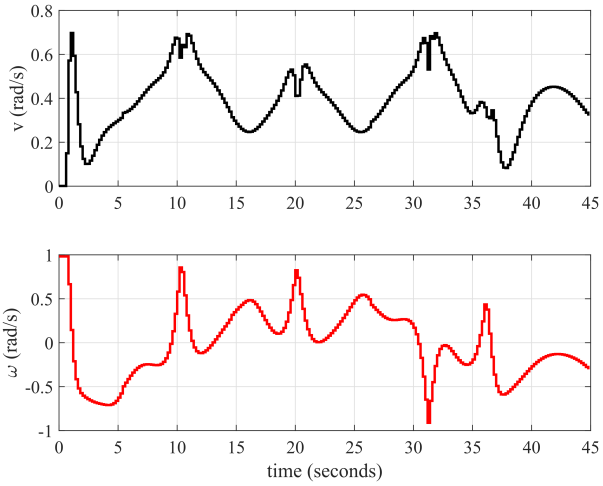


Fig. 9. Lemniscates trajectory tracking and navigation velocities results

VI. Conclusion

In this paper, a stabilizing NMPC controller with a terminal equality constraints has been shown to be applicable, for 2 control objectives namely, point stabilization and trajectory tracking of mobile robots. Usage of a toolkit that implements fast NMPC routines, making tractable the computationally challenging stability requirements. Simulations were conducted using I90 DrRobot research platform specifications. In the point stabilization case, the robot was commanded to perform parallel parking, whereas in the trajectory tracking problem, the robot was commanded to follow circular and eight-shape trajectories. The obtained results showed a satisfactory controller performance in terms of the point stabilization and tracking errors, hence, proving the applicability of the stabilizing NMPC scheme.

References

[1] J.-P. Laumond, S. Sekhavat, and F. Lamiraux, "Guidelines in nonholonomic motion planning for mobile robots," *In Robot motion planning and control*, pp. 1–53, 1998.

[2] M. Michalek and K. Kozlowski, "Vector-field-orientation feedback control method for a differentially driven vehicle," *IEEE Transactions on Control Systems Technology*, vol. 18, no. 1, pp. 45–65, 2009.

[3] D. Gu and H. Hu, "Receding horizon tracking control of wheeled mobile robots," *IEEE Transactions on control systems technology*, vol. 14, no. 4, pp. 743–749, 2006.

[4] D. Gu and H. Hu, "A stabilizing receding horizon regulator for nonholonomic mobile robots," *IEEE Transactions on Robotics*, vol. 21, no. 5, pp. 1022–1028, 2005.

[5] W. E. Dixon, D. M. Dawson, F. Zhang, and E. Zergeroglu, "Global exponential tracking control of a mobile robot system via a pe condition," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 30, no. 1, pp. 129–142, 2000.

[6] G. Oriolo, A. De Luca, and M. Vendittelli, "Wmr control via dynamic feedback linearization: design, implementation, and experimental validation," *IEEE Transactions on control systems technology*, vol. 10, no. 6, pp. 835–852, 2002.

[7] T.-C. Lee, K.-T. Song, C.-H. Lee, and C.-C. Teng, "Tracking control of unicycle-modeled mobile robots using a saturation feedback controller," *IEEE transactions on control systems technology*, vol. 9, no. 2, pp. 305–318, 2001.

[8] G. V. Raffo, G. K. Gomes, J. E. Normey-Rico, C. R. Kelber, and L. B. Becker, "A predictive controller for autonomous vehicle path tracking," *IEEE transactions on intelligent transportation systems*, vol. 10, no. 1, pp. 92–102, 2009.

[9] P. Falcone, M. Tufo, F. Borrelli, J. Asgari, and H. E. Tseng, "A linear time varying model predictive control approach to the integrated vehicle dynamics control problem in autonomous systems," *In 2007 46th IEEE Conference on Decision and Control*, pp. 2980–2985, 2007.

[10] G. Klančar and I. Škrjanc, "Tracking-error model-based predictive control for mobile robots in real time," *Robotics and autonomous systems*, vol. 55, no. 6, pp. 460–469, 2007.

[11] J. Backman, T. Oksanen, and A. Visala, "Navigation system for agricultural machines: Nonlinear model predictive path tracking," *Computers and Electronics in Agriculture*, vol. 82, pp. 32–43, 2012.

[12] H. Lim, Y. Kang, C. Kim, J. Kim, and B.-J. You, "Nonlinear model predictive controller design with obstacle avoidance for a mobile robot," *In 2008 IEEE/ASME International Conference on Mechtronic and Embedded Systems and Applications*, pp. 494–499, 2008.

[13] F. Kuhne, W. F. Lages, and J. G. Da Silva, "Point stabilization of mobile robots with nonlinear model predictive control," *In IEEE International Conference Mechatronics and Automation, 2005*, vol. 3, pp. 1163–1168, 2005.

[14] F. Xie and R. Fierro, "First-state contractive model predictive control of nonholonomic mobile robots," *In 2008 American Control Conference*, pp. 3494–3499, 2008.

[15] J. B. Rawlings and K. R. Muske, "The stability of constrained receding horizon control," *IEEE transactions on automatic control*, vol. 38, no. 10, pp. 1512–1516, 1993.

[16] G. Lars and P. Jürgen, "Nonlinear model predictive control theory and algorithms," 2011.

[17] D. B. Leineweber, I. Bauer, H. G. Bock, and J. P. Schlöder, "An efficient multiple shooting based reduced sqp strategy for large-scale dynamic process optimization. part 1: theoretical aspects," *Computers & Chemical Engineering*, vol. 27, no. 2, pp. 157–166, 2003.

[18] L. L. Simon, Z. K. Nagy, and K. Hungerbuehler, "Swelling constrained control of an industrial batch reactor using a dedicated nmpc environment: Optcon," *In Nonlinear model predictive control*, pp. 531–539, 2009.

[19] B. Houska, H. J. Ferreau, and M. Diehl, "Acado toolkit—an open-source framework for automatic control and dynamic optimization," *Optimal Control Applications and Methods*, vol. 32, no. 3, pp. 298–312, 2011.

[20] D. Feng and B. H. Krogh, "Dynamic steering control of conventionally steered mobile robots," *Journal of robotic systems*, vol. 8, no. 5, pp. 699–721, 1991.

[21] A. Bloch and B. Brogliato, "Nonholonomic mechanics and control," *Appl. Mech. Rev.*, vol. 57, no. 1, pp. B3–B3, 2004.

[22] "I90drrobot," http://drrobot.com/products_item.asp?itemNumber=i90, accessed: 2021-02-30.

[23] M. W. Mehrez, G. K. Mann, and R. G. Gosine, "Stabilizing nmpc of wheeled mobile robots using open-source real-time software," *In 2013 16th International Conference on Advanced Robotics (ICAR)*, pp. 1–6, 2013.

Deep Neural Transformer Model for Mono and Multi Lingual Machine Translation

Mohamed Islam Khaber
Department of computer sciences
University of Ferhat Abbas 1
Setif, Algeria
mohamedislam.khaber@univ-setif.dz

Abdelouahab Moussaoui
Department of computer sciences
University of Ferhat Abbas 1
Setif, Algeria
abdelouahab.moussaoui@univ-setif.dz

Mohamed Saidi
Department of computer sciences
University of Ferhat Abbas 1
Setif, Algeria
mohamed.saidi@univ-setif.dz

Nabila Frahta
Department of technology
University of Ferhat Abbas 1
Setif, Algeria
frahta.nabila@gmail.com

***Abstract*—In recent years, the Transformers have emerged as the most relevant deep architecture, especially machine translation. These models, which are based on attention mechanisms, outperformed previous neural machine translation architectures in several tasks. This paper proposes a new architecture based on the transformer model for the monolingual and multilingual translation system. The tests were carried out on the IWSLT 2015 and 2016 dataset. The Transformers attention mechanism increases the accuracy to more than 92% that we can quantify by more than 4 BLEU points (a performance metric used in machine translation systems).**

Keywords—Neural machine translation (NMT), deep learning, multilingual, transformer, monolingual.

I. INTRODUCTION

Deep learning is a subset of artificial neural network-based machine learning methods [1]. It allows computational models with multiple processing layers to learn different abstraction levels for data representations. These methods have improved the state-of-the-art research in language translation [2].

Neural Machine Translation (NMT) is a deep learning end-to-end machine translation approach that utilizes an extensive artificial neural network to predict a set of words' probabilities. Typically, entire sentences are modelled in a single integrated model. This approach has the advantage of being able to train a single system on both the source and target text and generates high-quality translation results. NMT has recently shown promising results on several language pairs [3],[4].

The end-to-end learning approach of NMT models consists of two essential components, the encoder, and decoder, which are usually built on similar neural networks of different types, such as recurrent neural networks [5], convolution neural networks [6], and more recently on transformer models, which are built entirely with attention layers, without convolution or recurrence [7].

In neural machine translation, multiple model variants and training procedures have been proposed and tested. NMT models were generally used in single language-pair settings, where a parallel corpus from a source language to a target language is required for the training process, and the inference process only involves those two languages in the same direction.

In our approach explained in this paper, we proposed a method deep transformer model for machine translation (DTMMT) with existing transformer architectures for analyses the translation outputs of multiple-languages and single-language models. We utilise the data collected in the IWSLT 2015 and IWSLT 2016 MT evaluation campaign [8]. A multilingual NMT system may be a factor in improving the final system, which improves by over 4 BLEU points over the monolingual NMT system [9].

The paper is organized as follows. In section II, we begin with a brief review of related work interested in the monolingual NMT and multilingual NMT of MT tasks. In Section III, we introduce our monolingual and multilingual NMT approaches to propose a good NMT system. In section IV, describes the transformer architecture. In section V, we describe our experimental set-up and discuss the results of our experiments. Section VI ends the paper with our conclusions.

II. RELATED WORK

In related works, Researchers have tried to build Multilingual NMT systems at Monolingual NMT systems expense in recent approaches. Bahdanau et al. [10] proposed an encoder-decoder architecture based on recurrent neural networks and attention in the Neural Machine Translation field, capable of translating between language pair consider one-to-one translation systems.

In a many-to-many translation system, Firat et al. [11] introduced a way to share the attention mechanism across multiple languages. In particular, multiple languages are applied to both sides. Luong et al. [12] used different encoders and decoders for each source and target language.

Dong et al. [13] proposed a multi-task learning approach for a one-to-many translation system by sharing hidden representations among related tasks to enhance generalization on the target language. They used a single language in the source and separate attention mechanisms and multiple languages on the target side.

Zoph et al. [14] employed a many-to-one translation system that considers multiple languages in the source and one language in the target side. Similarly, Gu et al. [15] propose a

Mixture-of-Language-Experts and a Universal Language Representation layer to improve a many-to-one model from different 5 languages into target English. Malaviya et al. [16] trained a many-to-one system from bible translation and used it to infer typology features for the different languages without evaluating the translation quality. In another related work, Artetxe et al. [17] trained a multilingual NMT model and used the learned representations to perform cross-lingual transfer learning.

Recent works propose different parameter sharing methods between language pairs in a multilingual NMT system. Blackwood et al. [18] propose sharing all parameters and shows improvements in over-sharing all parameters. Sachan et al. [19] explore sharing various components in Transformers models. Platanios et al. [20] propose to share the entire neural network while using a contextual parameter generator that learns to generate the system's parameters given the desired source and target language.

For the Arabic language, Almahairi et al. [21] proposed NMT for Arabic translation in both directions (Arabic-English and English-Arabic) and compared NMT and SMT and showed that NMT better than SMT, which is the first result on Arabic neural machine translation. Preprocessing Arabic texts increase the performance of the system, especially normalization. The morphology of Arabic languages is complex and productive, with a primary word-formation mechanism known as root-and-pattern. For example, from the Arabic word "وسوف يكتبونه "(wasawf yaktwubunahu) and its English translation "and they will write it". A possible analysis of these complex words defines the stem as "aktub" (write), with an inflectional circumfix, "y-uwna", denoting masculine plural, an inflectional suffix, "ha" (it), and two prefixes, "sa" (will) and "wa" (and) [22].

NMT has many challenges, such as; One model trained to translate many languages instead of one model per language [23]. This paper deals with this problem.

III. Deep Transformer Model for Machine Translation (DTMMT)

A. Monolingual NMT System

The proposed approach is performed in two steps. In the first step, a monolingual NMT system which is the simplest and most effective one, trains a single neural network on parallel data, including French-to-English and Arabic-to-English, as shown in Fig 1.

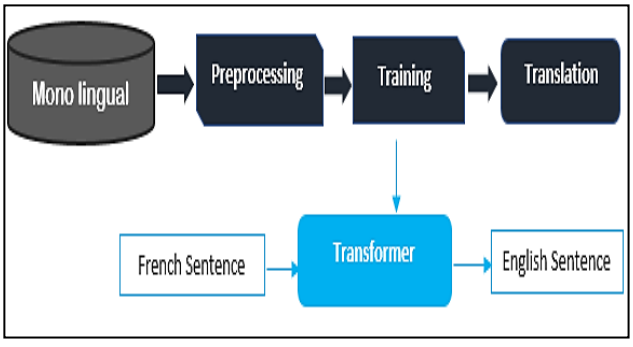


Fig. 1. Generic graph for the monolingual NMT system

B. Multilingual NMT System

In the second step, a multilingual NMT system is trained on the available data from different languages such as French and Arabic after concatenation L1 and L2, as shown in Fig 2.

We follow the method of Zoph et al. [14]. We add a target-language token to each source sentence to enable a many-to-one translation system. This different setup enables us to examine translation quality.

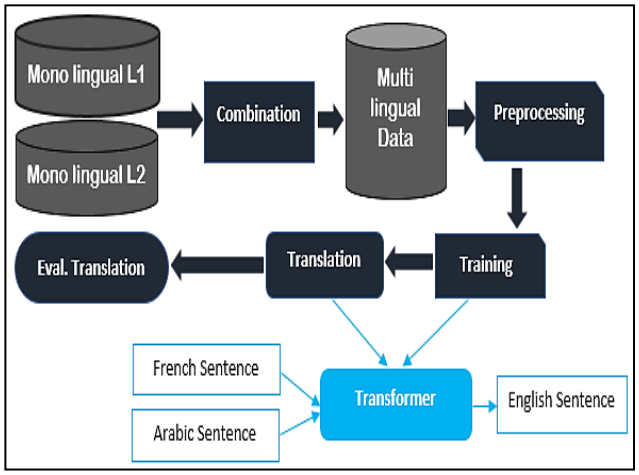


Fig. 2. Generic graph for the multilingual NMT system

We use this approach in our work with the Transformer model, which distinguishes multilingual NMT training and inference from a single language pair NMT to improve translation performance with minimal complexity. In addition to reducing Training of several single language pair systems. Transformer model, Preprocessing and Training, we will describe it in sections IV, V.

IV. The Transformer Model

Transformers are deep learning models introduced in 2017 [7], used for the first time in natural language processing (NLP). The first transduction model relies entirely on a self-attention mechanism to compute representations of its input and output with seq2seq modelling and without using sequence-aligned (RNNs) architecture or convolution architecture (CNN).

A transformer is composed of an encoder and a decoder. The encoder's role is to encode the inputs (i.e. sentence) in a state, which often contains several tensors. Then the state is passed into the decoder to generate the outputs. In machine translation, the encoder transforms a source sentence, e.g., "The Black Cat.", into a state, e.g., a vector, that captures its semantic information. The decoder then uses this state to generate the translated target sentence, e.g., "Le chat noir.". both the encoder and decoder are composed of two main components: Multi-Head Self-Attention and Feed Forward Network.

Attention mechanism (Scaled Dot-Product Attention): The attention mechanism's primary goal is to estimate the relative importance of the keys term in comparison to the query term for the same concept. To that end, the attention mechanism takes query Q that represents a vector word, the keys K which

are all other words in the sentence, and value V represents the vector of the word. the attention mechanism gives us the importance of the word in a specific sentence.

The Transformer model uses the Multi-Head Attention mechanism; it is simply a projection of Q, K and V in h Linear Spaces. Perform the attention function in parallel on each of these projected versions of queries, keys, and values, producing DV-dimensional output values. The final values are calculated by concatenating these and projecting them again.

The Multi-Head Attention mechanism's output, h attention matrix for each word, is then concatenated to create one matrix per word. This Attention architecture enables more complex dependencies between words without adding any training time thanks to the linear projection, which reduces each word vector's size.

Input Embedding aims at creating a vector representation of words. Words with the same meaning will be close in terms of Euclidian distance. The authors decided to use a 512 size embedding for the encoder [7].

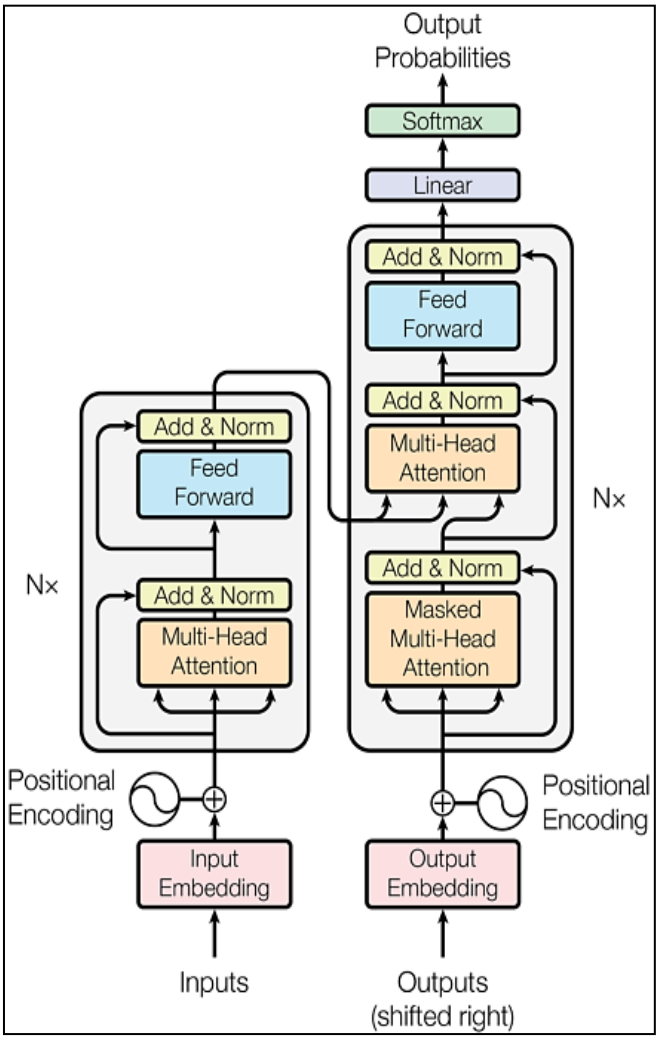


Fig. 3. The Transformer model architecture (from Vaswani et al.)

In the encoder phase, the Transformer first generates initial inputs creating by Input Embedding and Position Encoding for each word in the input sequence. Then, for each word, self-attention aggregates information from all other words in the context of the sentence, thus creating a new representation for each word, which is an attended representation of all other words in the sequence; this is repeated for each word in a sequence, successively building newer representations on top of previous one's multiple times.

The decoder generates one word at a time from left to right. The first word is based on the encoder's final representation (offset by one position). Each word predicted subsequently attends to the decoder's previously generated words at that layer and the final representation of the encoder (Multi-Head Attention) similar to a typical encoder-decoder architecture.

V. Experiment and Results

A. *Dataset and Preprocessing*

We trained and evaluated both monolingual and multilingual NMT systems based on the transformer models, with the relevant training data in the IWSLT 2016[(1)] evaluation campaign [8], which represent transcriptions from TED talks.

The experimental setting comprises two languages: French-to-English and Arabic-to-English; for each language pair, we use the training data of approximately 200,000 parallel sentences. For the models' development and evaluation, we use the corresponding sets from the IWSLT2010, which are composed of 887 sentence pairs. We also use IWSLT2015 and IWSLT2016 datasets as the test set for both language pairs is composed of 1080 and 1133 sentence pairs, respectively. Details about the used data sets are reported in Table I.

TABLE I. The Total Number of Parallel Sentences Used for Training, Development, and Test

Language Pair	Train	Dev10	Test15	Test16
French-to-English	218081	887	1080	1133
Arabic-to-English	211726	887	1080	1133
All-to-English	429807	887	1080	1133

At the preprocessing, we applied word segmentation for each training condition (i.e., monolingual and multilingual) by learning a sub-word dictionary via Byte-Pair Encoding (BPE) [24]. We use byte pair encoding (BPE) to learn a variable-length encoding of the text's vocabulary; unlike the original BPE, it does not compress the plain text. Still, it can reduce the text's vocabulary to a configurable number of symbols,

(1) https://wit3.fbk.eu/

with only a small increase in tokens. BPE is considered the best preprocessing method for Arabic [25]; the number of BPE segmentation rules is set to 6000, following Denkowski et al. [26] for experiments with small training data condition. We removed sentence pairs longer than 100 words.

B. Models and Parameters

The transformer models are trained using the open-source Open-NMT in PyTorch(2) toolkit [27]. The two systems types, monolingual and multilingual, were trained with the same model and parameters.

The hyperparameters for both systems were set as follows: a dropout of 0.1 is used, 4 attention blocks in the encoder and decoder and 8 attention heads were used, and the embedding size was 512, feed-forward dimension 2048. Adam and Noam decay were used for optimization [28].

We trained each of the two monolingual NMT systems separately; for the multilingual NMT system, we combined the two parallel corpora. We stopped training when the validation accuracy became constant or increased very slowly from the previous steps. Training time and training steps are shown in table II.

TABLE II. TRAINING TIME AND TRAINING STEPS FOR DIFFERENT SYSTEMS

Systems	Training time (Hours)	Training steps
French-to-English	3	50000
Arabic-to-English	2.5	45000
All-to- English	6	70000

C. Results

We compare the translation performance of two independently trained single-language models against one multiple-languages model trained on combining the two language pairs. The experiments show that a multilingual NMT system outperforms the monolingual NMT systems. The performance of both types of systems is evaluated on IWSLT2015, IWSLT2016 and reported in Table III.

TABLE III. BLEU RESULTS FOR IWSLT2015 AND IWSLT2016 TEST SETS

Dataset /Systems	**French-to-English**		**Arabic-to-English**	
	IWSLT2015	***IWSLT2016***	***IWSLT2015***	***IWSLT2016***
Monolingual	20.78	19.27	19.03	20.35
Multilingual	**25.31**	**24.65**	**23.06**	**25.88**

The improvements observed in the multilingual NMT system are likely due to increased data, even if it is not from the same source language.

Table IV and V shows some examples of translations with long sentences and short sentences.

TABLE IV. FRENCH/ARABIC TO ENGLISH EXAMPLES FOR IWSLT2016 WITH LONG SENTENCES

French	Rien qu'au cours des dernières années, nous avons beaucoup appris sur la façon dont la Terre s'intègre dans le contexte de notre univers.
Single-Language	In the last few years, we learned a lot about how the Earth is in the context of our universe.
Multi-Language	In the last few years, we have learned a lot about how the Earth fits into the context of our universe.
Arabic	لأكثر من 20 قرناً، كان الأطباء يسردون قصة واحدة عن معنى التوحد وكيف تم إكتشافه، ليتبين فيما بعد أن هذه القصة خاطئة وأن ما نتج عنها ترك أثر مدمر على الصحة العامة.
Single-Language	For more than 20 centuries, doctors telling a single story of a autism and how discovered, only to find out later that this story was wrong and made up of a global impact on the health.
Multi-Language	For more than 20 centuries, doctors have been telling a single story about the meaning of autism and how it was discovered, and it turns out that this story is wrong and that what has resulted has had a devastating impact on public health.

TABLE V. FRENCH/ARABIC TO ENGLISH EXAMPLES FOR IWSLT2016 WITH SHORT SENTENCES

French	Je regarde le comportement des gens et leur réponse au son.
Single-Language	I look at the behavior of people and the answer to sound.
Multi-Language	I look at people's behavior and their response to sound.
Arabic	لقد ولدت صماء، وعلموني أن الصوت ليس جزء من حياتي.
Single-Language	I was born with the audiences, and they that sound is not part of my life.
Multi-Language	I was born deaf, and they taught me that sound is not part of my life.

(2) https://github.com/OpenNMT/OpenNMT-py

Finally, we analysed the results using the IWSLT data, Fig 4 and 5 shows the breakdown of BLEU in the test data, separating the results for French to English and Arabic to English.

When all data are present in training, multilingual NMT system for both dataset 2015 and 2016 has better performance than monolinguals NMT systems. However, we observe test results when training with a single-language pair is low.

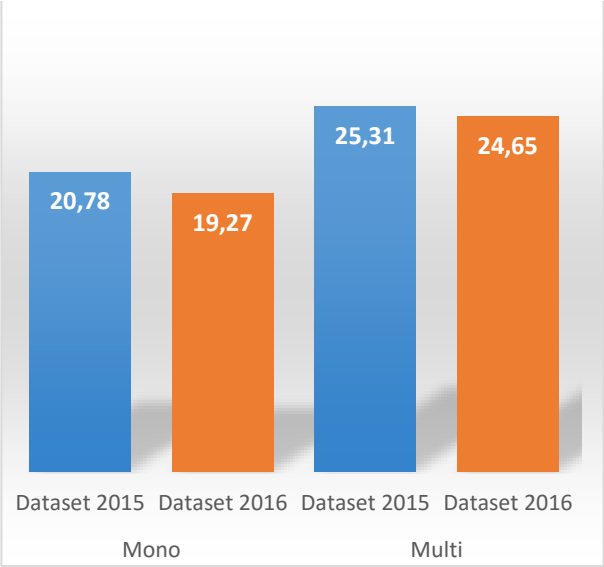


Fig. 4. Detailed comparison of BLEU in IWSLT dataset for French to English

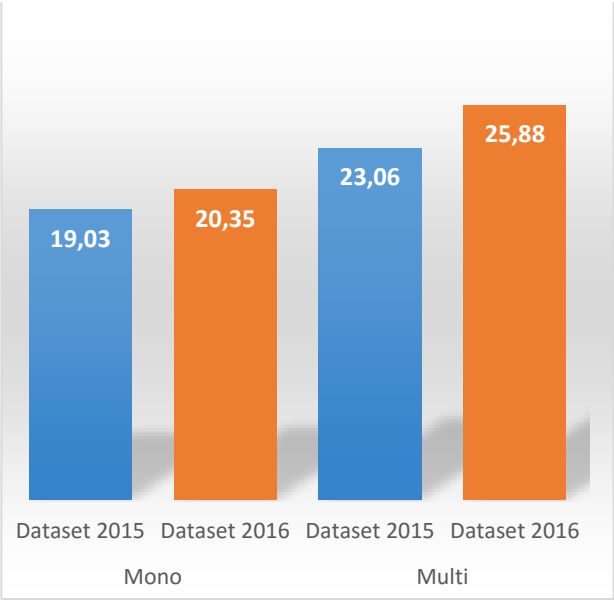


Fig. 5. Detailed comparison of BLEU in IWSLT dataset for Arabic to English

D. Evaluation methods

The accuracy of every translation result was compared based on the BLEU score [9] as implemented in multi-bleu.perl[(3)].

(3) https://github.com/moses-smt/mosesdecoder

VI. CONCLUSIONS

This work showed that a single multiple-languages model outperforms single-languages models applied to the Transformer architecture while avoiding the need for multiple language pairs to be trained. This model shows improvements in the final translation quality with over 4 BLEU points. In future work, we plan to explore our approach across many language varieties using a multilingual model and experiment with different architecture.

It's possible that if we designed a better strategy for multilingual NMT system like add more data or add more languages we may be able to obtain better results.

REFERENCES

[1] A Oppermann, "What is Deep Learning and How does it work?", [Online]. Available: https://towardsdatascience.com/what-is-deep-learning-and-how-does-it-work-2ce44bb692ac ,2019.

[2] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, p. 436, 2015.

[3] Y. Cheng, W. Xu, Z. He, W. He, H. Wu, M. Sun and Y. Liu, "Semi supervised learning for neural machine translation", In Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics , Vol. 1, 2016, pp. 1965–1974.

[4] F. Hieber, T.Domhan, M. Denkowski, D. Vilar, A. Sokolov, A. Clifton, and M. Post, "The SOCKEYE Neural Machine Translation Toolkit at AMTA ", In Proceedings of AMTA, vol. 1, 2018, pp. 200-207.

[5] I. Sutskever, O. Vinyals, and Q. V Le, "Sequence to sequence learning with neural networks", In Advances in neural information processing systems, 2014, pp. 3104–3112.

[6] J. Gehring, M. Auli, D. Grangier, D. Yarats, and Y. Dauphin, "Convolutional sequence to sequence learning", In Proceedings of the 34th International Conference on Machine Learning, 2017, pp. 1243-1252.

[7] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. Gomez, L. Kaiser, and I. Polosukhin, " Attention is all you need", In Advances in Neural Information Processing Systems, 2017, pp. 6000–6010.

[8] M. Cettolo, J. Niehues, S. Stüker, L. Bentivogli, R. Cattoni, and M. Federico, "The IWSLT evaluation campaign", In Proceedings of the International Workshop on Spoken Language Translation (IWSLT), Seattle, WA, 2016.

[9] K. Papineni, S. Roukos, T. Ward, and W. Zhu., "Bleu: a method for automatic evaluation of machine translation", In Proceedings of the 40th annual meeting on association for computational linguistics, 2002, pp. 311–318.

[10] D. Bahdanau, K. Cho, and Y. Bengio, "Neural machine translation by jointly learning to align and translate", In Proceeding of the 3rd International Conference on Learning Representations, ICLR ,USA, May 7-9, 2015.

[11] O. Firat, K. Cho, and Y. Bengio, "Multi-way, multilingual neural machine translation with a shared attention mechanism", In Proceedings of the Conference of the North American Chapter of the Association for Computational Linguistics, 2016, pp. 866–875.

[12] M. Luong, Q. V Le, I. Sutskever, O. Vinyals, and L. Kaiser, "Multi-task sequence to sequence learning", international conference on learning representations, 2016.

[13] D. Dong, H. Wu, W. He, D. Yu, and H. Wang, "Multi-task learning for multiple language translation". In Proceedings of the 53rd Annual Meeting of the Association for Computational Linguistics and the 7th International Joint Conference on Natural Language Processing, vol. 1, 2015, pp. 1723–1732.

[14] B. Zoph and K. Knight, "Multi-source neural translation", In Proceedings of the Conference of the North American Chapter of the Association for Computational Linguistics, 2016, pp. 30–34.

[15] J. Gu, H. Hassan, J. Devlin, and O. K. V. Li, "Universal neural machine translation for extremely low resource languages", In Proceedings of

the Conference of the North American Chapter of the Association for Computational Linguistics, 2018, pp.344–354.

[16] C. Malaviya, G. Neubig, and P. Littell, "Learning language representations for typology prediction", In Proceedings of the Conference on Empirical Methods in Natural Language Processing, 2017.

[17] M. Artetxe and H. Schwenk, "Massively multilingual sentence embeddings for zeroshot cross-lingual transfer and beyond", Transactions of the Association for Computational Linguistics, 2019, pp.597--610.

[18] G. Blackwood, M. Ballesteros, and T. Ward, "Multilingual neural machine translation with task-specific attention", In Proceedings of the 27th International Conference on Computational Linguistics, Santa Fe, New Mexico, USA. Association for Computational Linguistics, 2018, pp.3112–3122.

[19] D. Sachan and G. Neubig, " Parameter sharing methods for multilingual self-attentional translation models", In Proceedings of the Third Conference on Machine Translation, Belgium, Brussels, 2018.

[20] E. A. Platanios, M. Sachan, G. Neubig, and T. Mitchell, "Contextual parameter generation for universal neural machine translation", In Proceedings of the Conference on Empirical Methods in Natural Language Processing, 2018.

[21] A. Almahairi, K. Cho, N. Habash, and A. Courville," First result on Arabic neural machine translation", 2016.

[22] I. Gashaw and H. L. Shashirekha, "AMHARIC-ARABIC NEURAL MACHINE TRANSLATION". Computer Science & Information Technology (CS & IT) Computer Science Conference Proceedings (CSCP), 2019, pp. 55-68.

[23] R. Aharoni, M. Johnson, and O. Firat, " Massively Multilingual Neural Machine Translation". In Proceedings of NAACL-HLT, 2019, pp. 3874–3884.

[24] R.Sennrich, B. Haddow, and A.Birch, "Neural machine translation of rare words with subword units", In Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics, Vol. 1, 2016, pp. 1715–1725.

[25] H. Sajjad, F. Dalvi, N. Durrani, A. Abdelali, Y. Belinkov, S. Vogel, "Challenging Language-Dependent Segmentation for Arabic: An Application to Machine Translation and Part-of-Speech Tagging", In Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics, Vol. 2, 2017, pp. 601–607.

[26] M. Denkowski and G. Neubig, "Stronger baselines for trustable results in neural machine translation", in Proceedings of the First Workshop on Neural Machine Translation, 2017, pp. 18-27.

[27] G. Klein, Y. Kim, Y. Deng, J. Senellart, and A. Rush, "OpenNMT: Open-Source Toolkit for Neural Machine Translation", In Proceedings of association for computational linguistics, 2017, pp. 67–72.

[28] D. P. Kingma, J. Ba, " Adam: A Method for Stochastic Optimization", 3rd International Conference for Learning Representations, San Diego, 2015.

Evaluation and comparison study of video streaming routing protocols in vehicular ad-hoc networks

Sofiane Zaidi[1], Mostafa Ogab[2], Lazhar Khamer[3]
[1]Department of Mathematics and Computer Science, (RELA(CS)2) Laboratory, University of Oum El Bouaghi, Algeria, zaidi.sofiane@univ-oeb.dz, s.zaidi@univ-soukahras.dz
[2]Department of Mathematics and Computer Science, University of Oum El Bouaghi, Algeria, ogabmostafa@hotmail.com
[3]Department of Mathematics and Computer Science, University of Souk Ahras, Algeria, l.khamer@univ-soukahras.dz

***Abstract*—Video streaming is a challenging issue in Vehicular Ad-Hoc Networks (VANETs), due to the strict video streaming Quality of Service (QoS) requirements, such as throughput, delivery ratio, and transmission delay. Moreover, video streaming is influenced by VANET characteristics, such as the high dynamic topology, fluctuation of vehicle density, and environmental obstacles. In VANET, video streaming can be achieved through different VANET communication types, such as Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), and Vehicle to Broadband cloud (V2B). Based on these communications, the vehicles can exchange between them the video stream over single or multi-hop link. When the video content is delivered over a multi-hop link, the vehicles have to use a routing protocol to disseminate the video stream through a path (s) between the sender (s) end the receiver (s) vehicles. In this paper, we have presented an overview of popular existing routing protocols for video streaming in VANET, such as AODV, AOMDV, DSR, and DSDV. Furthermore, we have evaluated and compared these protocols in terms of some QoS evaluation metrics, such as throughput, packet delivery ratio, and end-to-end delay in function with vehicles density in order to judge which one is outperforming for video streaming in VANET. The simulation results show that the reactive routing protocols (AODV, AOMDV, DSR) provide higher throughput and packet delivery ratio than DSDV proactive routing protocol. However, DSDV achieves lower end-to-end delay than AODV, AOMDV, DSR routing protocols.**

***Index Terms*—Vehicular ad-hoc network, video streaming, routing protocol, AODV, AOMDV, DSR, DSDV**

I. Introduction

Vehicular Ad-hoc NETwork (VANET) is a self-organized network that consisted of moving vehicles and fixed Road Side Units (RSUs) [1]. The vehicles exchange the messages between them or with the RSUs in a single or multi-hop communication using wireless communication support [2]. VANET can provide three types of communications: Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), and Vehicle to Broadband cloud (V2B) [3]. VANET aims to reduce the number of road accidents by integrating intelligence techniques into vehicles. The World Health Organization (WHO) estimated that the road traffic deaths number has reached 1.35 million per year [4]. Figure 1 shows the architecture of VANET.

VANET can serve several applications that are classified into three categories: transportation safety, transportation efficiency, and transportation comfort [5]. The first category aims to decrease the road accident number by disseminating the warning messages in the case of accidents. The second one manages and controls the traffic road to avoid the traffic congestion problem. The last one provides comfort and infotainment services to both drivers and passengers.

Video streaming in VANET provides more information than a simple text. However, VANET is characterized by high vehicle mobility, fluctuation of vehicle density, and the presence of environmental obstacles. Therefore, video transmission in VANET faces several challenges, such as packet loss and the high transmission delay due to the rupture of the communication path between the sender and the receiver. Video streaming in VANET is an important topic addressed by current research because many VANET applications focus on video transmission to improve road safety, traffic efficiency, driver assistance, infotainment, and urban sensing.

Routing protocols for video streaming in VANET have to select the appropriate set of relay vehicles between the source (s) and destination (s) to establish a reliable path for video streaming dissemination. In VANET literature, several works use routing protocols for video streaming at the network layer level. However, few of these works propose a comparison between these protocols in VANETs. Our work evaluates and compares AODV, DSDV, DSR, and AMODV routing protocols for video streaming in VANET to choose the most adequate routing protocol for video streaming in VANET. We have used many evaluation metrics in this work, such as throughput, packet delivery ratio, and end-to-end delay.

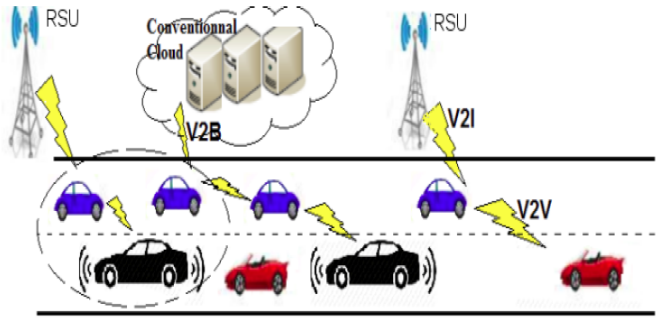


Fig. 1. VANET communication patterns

The rest of the paper is organized as follows. In section

2, we present the related work about the routing protocols for video streaming in VANET. Section 3 presents an overview of some routing protocols that will be compared and evaluated by our network simulation. Section 4 shows and investigates the simulation results. Finally, in section 5 we conclude the paper.

II. Related work

This section presents some recent works that applied and analyzed the different routing protocols for video streaming in VANET.

Honda et al. evaluated in [6] the video transmission in urban VANET using Optimized Link State Routing (OLSR). The proposed work proved that throughput, delay, and jitter of OLSR is influenced by two factors: the video streams number and the environment buildings. This study demonstrate that OLSR outperforms AODV and DSDV protocols. Moreover, this work does not consider the evaluation metrics of video quality like PSNR and SSIM.

Pham et al. proposed in [8] an adaptation of OLSR for video streaming over VANETs named QOV. The proposed routing protocol forwards the video streams through fewer loss paths, in order to improve OLSR in terms of QoE metrics: MOS, USP, MDP, and packets loss rate. QOV has the same limit of OLSR of bandwidth overhead due to the periodic exchange of control messages in VANET, which is characterized by its high dynamic topology.

Rizwan et al. evaluated in [9] AODV and DSR for video streaming in VANET. The proposed work proved that DSR is better than AODV in terms of throughput and transmission delay in a simple scenario with only OBUs, or in a complex scenario that includes both OBUs and RSUs.

Benmir et al. proposed in [10] GeoQoE-Vanet routing protocol for video streaming over VANETs. In this proposed protocol, the selection of relay vehicles is based on a QoE parameters to provide video content with better quality. The selection decision of the next-hop vehicle is based on position, direction, speed, link expiration time, packet loss rate, transmission delay, and jitter. The simulation results showed that GeoQoE-Vanet provides better QoE to the end-user in terms of MOS, PSNR, and SSIM compared to GPSR and GPSR-2P protocols in an urban environment.

Most of these VANET video streaming works focus on video packet routing to guarantee efficient delivery of packets while decreasing packet loss rate and transmission delay. However, due that the data type transmitted between vehicles is the video, this transmission becomes complicated and challenging. The evaluation and comparison between the routing protocols for video streaming in VANET is an important task to choose the adequate routing protocol for this transmission.

III. Routing protocols for video streaming in VANET

The routing is the process that allows the forwarding of messages from one node to another based on some parameters, like the number of hops, the shortest path, and so on. In VANET, the dissemination of data is a challenging task due to the rapid movement of vehicles. Several routing protocols can be used to find optimal paths from the vehicle source to the destination but with some limitations, such as lack of scalability, self-organization, control, and routing complexity.

In this section, we present some routing protocols for video streaming in VANET (AODV, AOMDV, DSR, and DSDV) that will be evaluated and compared through our network simulation. Each routing protocol is designed by a flowchart that explains briefly the different steps of the process followed by this protocol.

A. Ad-hoc On-Demand Distance Vector (AODV)

AODV routing protocol could be classified as a unicast/multicast routing protocol. The process adopted by this routing is that each path is produced only on request. In fact, when a vehicle desires to transmit a packet, via the route discovery mechanism, the used routes are kept [7].

As shown in figure 2, AODV establishes the Route Discovery (RD) by means of Route REQuest (RREQ) and Route REPly (RREP) control messages. In AODV, routes are set up by flooding the network with RREQ packets. When an RREQ traverses a node, it stores the information about the source, the destination, and the node from which they received the RREQ. The later information is used to set up the reverse path back to the source. When the RREQ reaches a node, which knows a route to the destination or it is the destination itself, the node responds to the source with an RREP packet. To avoid overburdening the nodes with information about routes that are no longer used, nodes discard this information after a timeout. When either destination or intermediate node moves, a Route ERRor (RERR) message will be sent to the affected source nodes. When the source node received the RERR, it can re-initiate the RD process if the route is still needed. Neighborhood information is obtained by periodically broadcasting Hello packets [11].

AODV is also known for its capacity to diminish broadcasts, transmission latency, and routing overhead. However, AODV suffers from the high end-to-end delay resulted from the route discovery process before every data transmission. Hence, high E2ED is not suitable for vehicular networks in case of crucial or dangerous information [7].

B. Destination Sequenced Distance Vector (DSDV)

DSDV routing protocol is an adapted version of the conventional Routing Information Protocol (RIP) to the ad-hoc network routing. It adds a new attribute which is the sequence number, to each route table entry of the conventional RIP [12].

DSDV is a proactive table-driven protocol based on the Bellman-Ford routing algorithm to calculate the paths. The cost metric used is counting the number of hops that takes a packet to reach its destination. The changes are propagated through periodic and trigger update mechanisms. Due to these updates, there is a chance of having routing loops within the network. To eliminate routing loops, each update from the node is tagged with a sequence number. The sequence

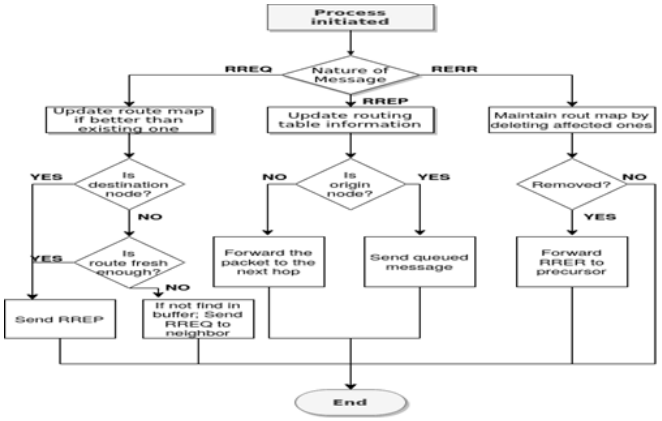


Fig. 2. Flowchart of AODV routing protocol

number from each node is independently chosen but it must be incremented each time a periodic update is made by a node [13]. The update of routing tables of each node is done periodically to make available information about paths to each destination in the network at any time, even if the paths are at this time unused. Despite the benefits of DSDV, such as simplicity, loop-free, and no added transmission delay caused by the discovery of the road technique [6]. Figure 3 depicts the flowchart of DSDV routing protocol.

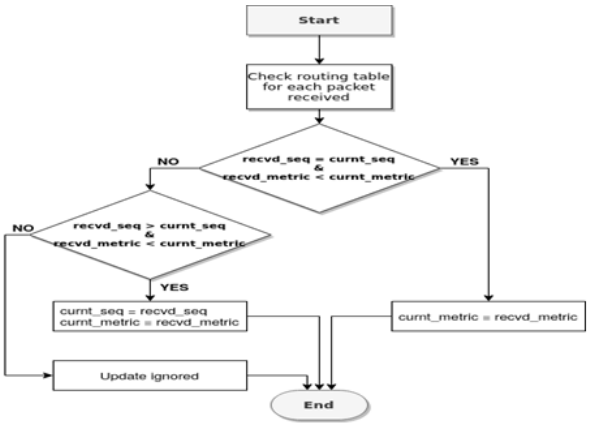


Fig. 3. Flowchart of DSDV routing protocol

C. Ad-hoc On-Demand Multipath Distance Vector (AOMDV)

The basic idea behind multi-path routing is of finding multiple paths between the source and the destination. On-demand routing protocols for wireless Ad-hoc networks discover a route when a source needs to communicate with a destination. The multi-path routing protocol discovers multiple paths during the single route discovery process. These multiple paths can be used for load spreading or as backup routes when the primary route fails [14].

AOMDV is a multi-path extension of AODV. AOMDV is based on the distance vector concept and uses hop by hop routing approach. Moreover, AOMDV also finds routes on demand using an RD procedure. Unlike AODV, AOMDV finds multiple routes in a single route discovery procedure. In AODV all duplicate RREQs are discarded whereas AOMDV looks for an opportunity of getting an alternate route with each duplicate RREQ. In AOMDV, RREQ propagation from the source towards the destination establishes multiple reverse paths both at intermediate nodes as well as the destination. Multiple RREPs traverse these reverse paths back, to form multiple forward paths to the destination at the source and intermediate nodes. AOMDV also provides intermediate nodes with alternate paths as they are found to be useful in reducing route discovery frequency. The core of the AOMDV protocol lies in ensuring that multiple paths discovered are loop-free and disjoint and inefficiently finding such paths using a flood-based route discovery. AOMDV route update rules, applied locally at each node, plays a key role in maintaining loop-freedom and disjoint-ness properties [15]. Figure 4 shows the flowchart of AOMDV routing protocol.

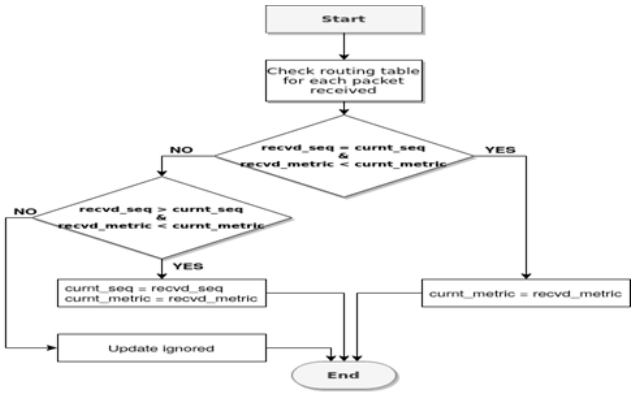


Fig. 4. Flowchart of AOMDV routing protocol

D. Dynamic Source Routing (DSR)

DSR is a reactive protocol for network routing. It is basically made for multi-hop communication. It is a self-organizing and self-configuring protocol that does not require any monitoring. The two main functions of DSR are route discovery and route maintenance [14] as illustrated in figure 5.

1) Route Discovery (RD):: Let a source S wants to send the data to the destination D. S will broadcast an RREQ packet. If the receiver node is not D then it will append its address in the packet and rebroadcast it again. If the node is D then he sends an RREP to S, using the reversed path address that copied from the received packet.

2) Route Maintenance (RM):: During the sending of the data from S to D. If S did not receive an acknowledgment from D for the successful delivery, S will wait for some predefined amount of time and if it does not receives the acknowledgment it will send the RERR packet to all the nodes in the path from which it received the packets. All the nodes which will receive

the packet will update their corresponding route tables for that path and remove the old path. Also, the source S has to initiate the RD to find a valid path again.

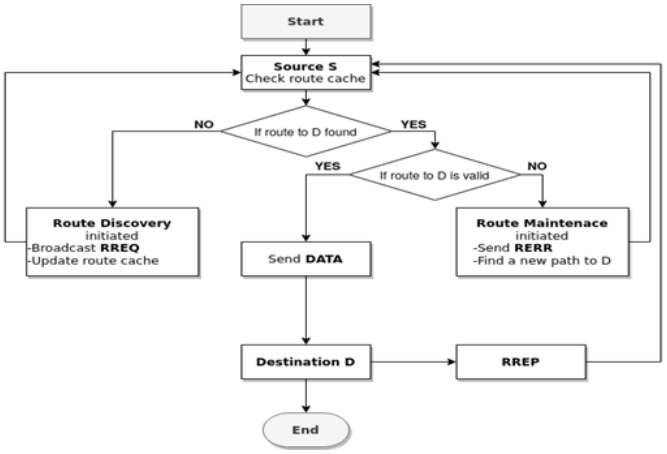


Fig. 5. Flowchart of DSR routing protocol

IV. Simulation

In this section, we have evaluated and compared some routing protocols for video streaming in VANET, such as AODV, AOMDV, DSR, and DSDV in function of vehicle density and in terms of throughput, packet delivery ratio, and end-to-end delay.

we have performed our simulation using network simulator 2 (ns-2) [17]. The network topology is extracted from Oum El Bouaghi city (Algeria) using OpenStreetMap [18], and the traffic mobility is generated using SUMO [16].

A. Simulation setup

We have mainly three parts that cover our simulation procedure for this study. Firstly, road maps are obtained using Open Street Map (OSM), which is a map editor tool that allows the extraction of real-world locations into the OSM file. This is followed by importing the road map into SUMO, a microscopic traffic simulator for generating the required TCL script and mobility trace files. In the last step, NS-2, a network simulator is used to simulate the VANET scenario for analyzing the performance of the aforementioned routing protocols for video streaming in VANET. In order to execute the traffic simulation in this partially used area, three procedures are followed:

1) Studied area: The Oum El Bouaghi city (Algeria) map was extracted from the open-source 'OpenStreetMap' represented as an OSM File. Figure 6 demonstrates the selected city sector that was simulated.

2) Vehicles mobility: The movement of the vehicles within the simulated urban scenario is randomly generated using SUMO to emulate real-world traffic as shown in figure 7. Then, the SUMO mobility traces are adopted for the simulation. The distribution of vehicles on the starting locations (source) in each scenario is made randomly according to the

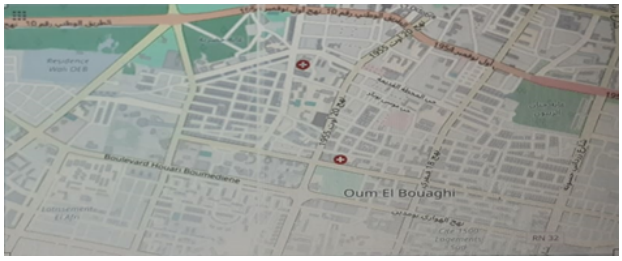


Fig. 6. Studied area of OUM EL BOUAGHI city

binomial distribution. This means each vehicle has a random departure rate (starting time) and a random arrival rate (ending time). The initial placement of vehicles is also randomly assigned by SUMO. It is assumed that each vehicle in the simulation is equipped with an OBU that facilitates onboard computation and communication with other neighboring vehicles based on IEEE 802.11p. As a result, SUMO generates a TCL script for the mobility of vehicles traffic.

Fig. 7. Mobilty simulation of vehicles traffic in OUM EL BOUAGHI city using SUMO tool

3) Network simulation: To simulate our chosen routing protocols and their impact on the video streaming transmission over VANET, we have used a Network Simulator 2 (Version 2.35) integrated with Evalvid (Version 2.7). In our simulation, we have used a video sequence called 'hall-cif' having 300 frames with a frame size 352-288 pixels (YUV format). The frame rate of this sequence is 30 frames/second. We have encoded the video sequences with H.264/ffmpeg standard. During our simulation, the channel bandwidth is fixed at 10 MHz and the vehicle speeds are limited to 20 m/s and 30 m/s.

Figure 8 describes an overview of our simulation process which used the three tools: OpenStreetMap, SUMO, and NS-2. In order to test the effect of the network vehicle density, we test our network sparsity model with several network vehicle density ranging from 50 to 120 vehicles. Table I shows our simulation configuration.

B. Simulation results

The metrics that we have used to evaluate the routing protocols are throughput, End-To-End Delay (E2ED), and Packet Delivery Ratio (PDR).

1) Throughput: Throughput is the rate of successful packet delivery through a network connection per unit of time.

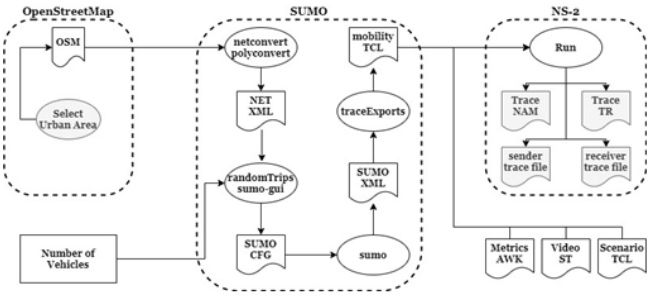


Fig. 8. Workflow of our simulation

TABLE I
SIMULATION PARAMETERS

Parameter	Value
Simulator	NS-2.35
Routing Protocols	AODV, DSDV, AOMDV, DSR
Transport protocol	UDP
Number of vehicles	50, 60, 70, 80, 90, 100, 110, 120
Simulation time	500 s
Simulation area	Oum El Bouaghi city (2492 m X 2381m)
Packet size	1024 Bytes
Channel	Channel/WirelessChannel
Radio propagation	TwoRayGround
Network interface	802.11p

Figure 9 depicts the achieved throughput of different simulated routing protocols for video streaming in VANET in function of the number of vehicles. As shown in this figure, AODV, DSR, and AOMDV provides higher throughput than DSDV routing protocol. The main reason of this result is that contrary to DSDV proactive routing protocol, in the reactive routing protocols (AODV, DSR, and AOMDV), the sender vehicle updates its routing table only when it wants to send the video packets. Therefore, the network overload will be highly reduced which avoids the congestion problem and increases the throughput.

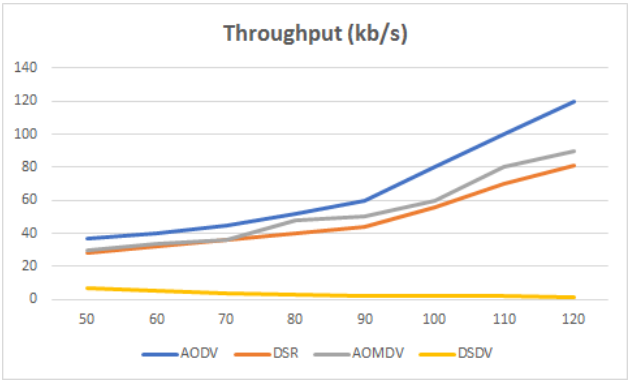


Fig. 9. Throughput of simulated routing protocols for video streaming in VANET

2) End-To-End Delay (E2ED): E2E delay is the average time needed for a packet to reach its destination. Figure 10 shows the E2E delay achieved by the simulated routing protocols for video streaming in VANET in function of the vehicle density. An illustrated in this figure, DSDV provides lower E2E delay than the other routing protocols. This result is due to the periodic updating of DSDV routing tables which allows the vehicles to find quickly the path for the transmission of video packets.

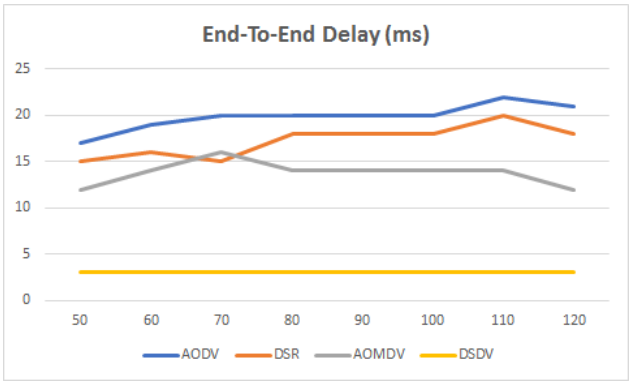


Fig. 10. End-To-End Delay of simulated routing protocols for video streaming in VANET

3) Packet Delivery Ratio (PDR): PDR is the number of packets successfully received divided by the number of sent packets. According to the figure 11, AODV, AOMDV, and DSR have shown a similar result of the Packet Delivery Ratio while the DSDV protocol started with 90% and decreased to 25% of PDR when the number of vehicles reached 120. This result is due to the on demand updating of routing tables of reactive routing protocols (AODV, AOMDV, and DSR) which increases the successful packet delivery, contrary to DSDV proactive routing protocol.

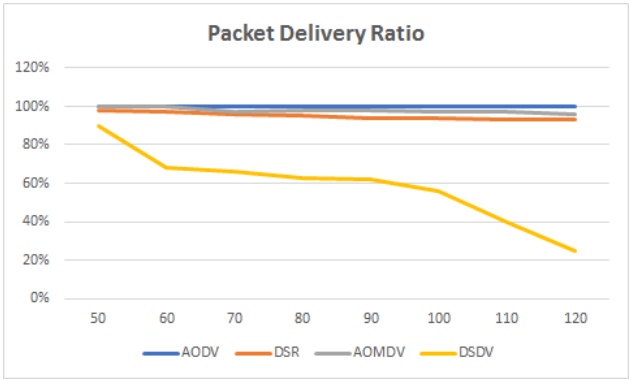


Fig. 11. Packet Delivery Ratio of simulated routing protocols for video streaming in VANET

V. CONCLUSION

In this paper, we have presented our network simulation of four routing protocols for video streaming in VANET (AODV, AOMDV, DSR, and DSDV). Moreover, we have performed an evaluation and comparison of these routing protocols in terms of QoS metrics, such as throughput, E2ED, and PDR. The

experiments were achieved by sending a video file from one source to one destination in an urban area over VANET.

The results generated have showed that the reactive routing protocols (AODV, AOMDV, DSR) provides higher throughput and PDR than DSDV proactive routing protocol. However, DSDV achieves lower E2E delay than AODV, AOMDV, DSR routing protocols.

Our future work is to perform the same study with several routing protocols in VANET as well as apply more QoS parameters to extend the scope of the analysis of the results using different simulation tools, such as NS2, NS3, and so on.

REFERENCES

[1] S. Zaidi, S. Bitam, and A. Mellouk, "Enhanced user datagram protocol for video streaming in VANET," IEEE International Conference on Communications (ICC), pp. 1-6, 2017.

[2] S. Zaidi, S. Bitam, and A. Mellouk, "Hybrid error recovery protocol for video streaming in vehicular ad hoc networks, " Vehicular Communications, vol. 12, pp. 110-126, 2018.

[3] Y. Sahraoui, A. Ghanam, S. Zaidi, et al. "Performance evaluation of TCP and UDP based video streaming in vehicular ad-hoc networks, " International Conference on Smart Communications in Network Technologies (SaCoNeT), pp. 67-72, 2018.

[4] Road traffic injuries 2020, World Health Organization, https://www.who.int/health-topics/road-safety#tab=tab_1, 2020. (Accessed 09 March 2021).

[5] S. Zaidi, S. Bitam, and A. Mellouk, "Enhanced adaptive sub-packet forward error correction mechanism for video streaming in VANET, " IEEE Global Communications Conference (GLOBECOM), pp. 1-6, 2016.

[6] T. Honda, M. Ikeda, E. Spaho, M. Hiyama, and L. Barolli, "Effect of Buildings in VANETs Communication: Performance of OLSR Protocol for Video Streaming Application, " 2013 Eighth International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), pp. 323-327, 2013.

[7] B. MOUSSAOUI, S. DJAHEL, M. SMATI, and J. Murphy, "A cross layer approach for efficient multimedia data dissemination in VANETs, " Vehicular Communications, vol. 9, pp. 127-134, 2017.

[8] T. A. Q. Pham, K. Piamrat, and C. Viho, "QoE-Aware Routing for Video Streaming over VANETs, " 2014 IEEE 80th Vehicular Technology Conference (VTC Fall), pp. 1-5, 2014.

[9] M. R. Ghori, A. S. Sadiq, and A. Ghani, "VANET Routing Protocols: Review, Implementation and Analysis, " International Postgraduate Conference on Applied Science & Physics 2017, IOP Conf, pp. 1-15, 2017.

[10] A. Benmir, A. Korichi, A. Bourouis, M. Alreshoodi, and L. Al-Jobouri, "GeoQoE-Vanet: QoE-Aware Geographic Routing Protocol for Video Streaming over Vehicular Ad-hoc Networks, " Computers 2020.

[11] E. Kulla, S. Morita, K. Katayama, and L. Barolli, "Route Lifetime Prediction Method in VANET by Using AODV Routing Protocol (AODV-LP), " In: CISIS 2018, AISC 772, pp. 311, 2019.

[12] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, " In Proceedings of the ACM Conference on Communications Architectures, Protocols and Applications (SIGCOMM), pp. 234244, 1994.

[13] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing, " In Proceedings - WMCSA99: 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp. 90100, 1999.

[14] V. C. Patil, R. V. Biradar, R. R. Mudholkar, and S. R. Sawant, "On-demand multipath routing protocols for mobile ad hoc networks issues and comparison, " International Journal of Wireless Communication and Simulation, vol. 2, no. 1, pp. 21-38, 2010.

[15] Vivek B. Kute and M. U. Kharat, "Analysis of Quality of Service for the AOMDV Routing Protocol, " ETASR- Engineering, Technology and Applied Science Research, vol. 3, no. 1, pp. 359-362 2013.

[16] "Simulation of Urban Mobility, " [Online]. Available: https://sumo.dlr.de/docs/index.html. (Accessed 09 March 2021).

[17] The Network Simulator 2, Isi. Edu. http://www.isi.edu/nsnam/ns/. (Accessed 09 March 2021).

[18] "OpenStreetMap, " [Online]. Available: http://www.openstreetmap.org/. (Accessed 09 March 2021).

Compressed VGG16 Auto-Encoder for Road Segmentation from Aerial Images with Few Data Training

Abdeldjalil Kebir
LASA Laboratory
Departement of electronics
Badji Mokhtar Annaba University
Annaba, Algeria
kebirabdeldjalil@gmail.com

Mahmoud Taibi
LASA Laboratory
Departement of electronics
Badji Mokhtar Annaba University
Annaba, Algeria
mahmoud.taibi@univ-annaba.org

Francisco Serradilla
Department of Artificial Intelligence
Escuela Técnica Superior
de Ingeniería de Sistemas Informáticos
Universidad Politécnica de Madrid
Madrid, Spain
francisco.serradilla@upm.es

***Abstract*—Deep Learning methods have found many applications such as segmentation, recognition and classification. However, almost all of these methods require large data-set for the training step and a long training time. Indeed, in surveillance video domain, as for many real-world applications, samples are only accessible in limited amounts owing to acquisition and experiments complexity. In this work, we introduce compressed VGG Auto-Encoder system for road image segmentation in high-resolution aerial imagery. The objective of our experiments is to improve the methodology of distinguishing the road network when only few Data is available. We propose an approach based on compressed Auto-encoder; focus on avoiding the over-fitting effect by generating new data augmentation, based on basic filter transformation to increase and enhance the quality of data training, in the aim of learn an appropriate and simplified representation of data from the original data set in order to obtain a deeper insight from large data-set, and to achieve a quick segmentation training time. Our model achieve a good result and is considered as the best network for fast and accurate segmentation of road images, compared to other models. Furthermore, we provide an explanation of these techniques and some recommendation for their use in the field of deep learning.**

***Index Terms*—Auto-Encoder, VGG16, areal images, Road segmentation, Data Augmentation, Feature extraction.**

I. Introduction

The segmentation of foreground regions is the key task in many computer vision systems. While segmentation is considered as an essential pre-processing step, it presents a hindrance for many surveillance applications such as traffic monitoring, people counting, and action recognition [1]–[3].

Automated road segmentation from aerial imagery is a fundamental unit for many applications [4], [5], including geographic information systems, especially for vehicle navigation, traffic management and emergency response [6], [7]. It is also an important component of military topography and cartography. Furthermore, the extraction of roads taken from aerial or satellite imagery offers an effective solution for the rapid development of new cities [8], which requires frequent road updates.

In recent years, Deep Learning approaches have achieved outstanding performance in many computer vision tasks such as image classification, object and anomaly detection and natural language processing [9]–[12]. Indeed, Deep learning is a subset of artificial intelligence. It is distinctive from conventional Machine Learning in how representations are learned from the raw data. Deep learning discovers the hidden structure of complex data using a hierarchical network through multiple layers, where each layer learns representations of data with multiple levels of abstraction. Furthermore, a variety of deep learning methods have been studied and discussed over the past few years [11], [13]. Generally, the Deep learning methods can be divided into four categories: Convolution Neural Networks (CNNs), Restricted Boltzmann Machines, Auto-encoders and Sparse Coding [14].

Nowadays, Deep Learning applications are becoming ubiquitous in the computer vision field, especially for the object segmentation task [15]–[17]. As it has show better performance compared to machine learning methods. Most researchers have worked on developing a robust and sophisticated segmenting objects models based on Deep Learning methods such as in [15], [18], [19]. Authors mainly discussed the accuracy of Deep Learning segmentation methods mainly when large training data are available and a powerful computing unit is used. They rarely explored how to train a model when only small data-sets are available.

Learning developing Deep Learning models trained on small data-set is one of the recent research topics in a variety of fields. However, few works have been conducted to address this problem. In medicine for instance, to make a semantic segmentation of the 3D images in abdominal tomography, the authors in [20] used a cylindrical transformation in a cylindrical coordinate system to increase the limited number of images. The results obtained by these transformations have a higher segmentation performance than the FCNs [21] when a limited number of annotated images is used. In [22] the authors proposed a new approach (SSF-CNNN) based on the

reduction of the learning parameters number by modification of the structure and strength of the filters obtained by CNN to mitigate the lack of the number of training data. The approach has proven to be effective for multiple object classification and a real-world new-born face recognition problem. However, in [23] the authors increased the number of samples in the database by a radial transformation in the polar coordinate system at the pixel level for each image. The proposed technique has improved the generalization performance of the model for several data-sets.

This our paper is part of deep learning models development in the domain of road image segmentation. In deep learning, high-level features extracted from the network layers are learned from data using a basic learning procedure. In addition, to reconstruct the result segmentation mask easily and to achieve good results from these precise features, the presence of large databases is necessary. In fact, in the real world scenario, a large data-set is not always available. Based on the fact that, we will be going over the three models of auto-encoder road segmentation, one based on VGG16 and the others based on compressed VGG. Then, compare the performance of each approach on a adaptive road benchmark dataset called the Teselas dataset [24].

The objective of this paper is to perform feature extraction and high-dimensional data reduction with different filtering strategies in order to create an adaptive learning data set for accurate road segmentation with less computational time.

The rest of the paper is structured as follows: Section II presents the materials and the proposed methods. We describe the models and evaluate the performance of the proposed approaches in Section III. This is followed by a general discussion and Conclusion in Section IV.

II. Methods and Materials

In this section, we describe the method and material used to build a robust road image segmentation system. We provide an overview and a detailed description of each component introduced in the methodology of our work. As well as, the detail of the overall approach and data training process strategies.

A. Auto-Encoder

The Auto-encoder is Deep Neural Network, considered as an unsupervised learning technique. Its main goal is to reproduce its input Data at the output [25], [26] wherein the input and the output layers both have the equal number of neurons. It consists in compressing the data successively until the encoder part obtains a latent form. Then decompress them in the decoder part. It projects the data from a higher to a lower dimension through the use of non-linear transformation and preserve the significant features of the data by deleting the non-essential elements. This lower dimension is used to reconstruct the original data at the output of the network in order to guarantee the accuracy of the input through the usage of non-linear transformation. In fact, there exist four well known Auto-encoders namely; Convolutional auto-encoder, Denoising auto-encoder, Variational auto-encoder and Sparse auto-encoder. Several applications of Auto-encoders can be found in the literature such as Data denoising and Dimensional reduction [27]. The complete network is illustrated in Figure1. The Auto-encoder has three essential blocks:

- **Encoder:** As its name indicates, the encoder attempts to encode all of the useful information about the input into the latent space.
- **Latent space:** The space represented by compressed form of input.
- **Decoder:** In the decoding process the decoder reconstructs the input based only on the information in the latent space.

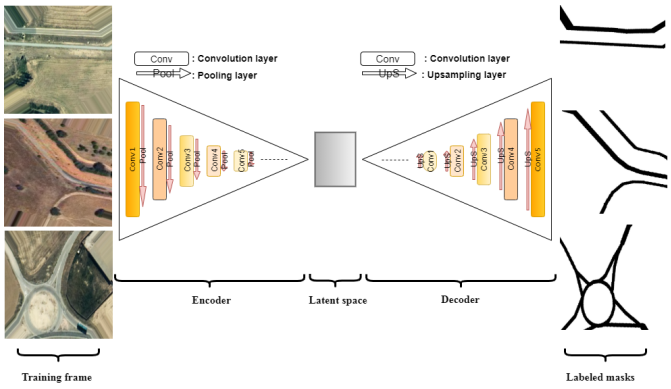


Fig. 1. Architecture of General Auto-encoder approach.

B. Data Augmentation

It is well known that the success of Deep Learning applications is strongly dependent on the amount of data available for its training. To overcome the limitations inherent in small numbers of training samples, we tested data-set augmentation [28]. Image data Augmentation is a regularization process that relies on applying transformations to images for uses both the original image and the transformed images to train model [29], [30]. Therefore, the idea is to use the existing data to create more data, in order to avoid over-fitting, to improve model performance. Some example adjustments include translating, cropping, scaling, rotating, changing brightness and contrast. However, these methods are generally used in all fields of image and video processing such as recognition, detection, segmentation etc.

C. Evaluation protocol

In our experiments we propose approaches based on VGG16 Auto-encoder and Multi-Depth VGG Auto-encoder. In deed, we use the Auto-encoder as supervised learning to perform segmenting the roads for the all approaches.

We construct the VGG16 Auto-Encoder Network with VGG16 model as the encoder part for the first approach by using Pooling and Convolution layers,This process allows to decrease the size of the input data Then, we replaced the fully connected layers as a latent space. For the decoder

part, the transposed architecture of the VGG16 has been used for reconstructing the result mask of input frames. This reconstruction process increases the size of the latent space representation to bring it back to its input dimensions by using Upsampling and Convolution layers which are known as transposed VGG16 architecture.

In the Compressed VGG Auto-Encoder approaches, we stacked Convolution and Pooling layers in the Encoder parts for down-sampling the input images, and in the Decoder part we have placed Convolution and Upsampling layers for up-sampling the images in latent space. In fact, the hidden layers are in multi-depth. In such a way that the number of layers will be reduced, i.e. the VGG16 Auto-Encoder model will be compressed to VGG12 and VGG10.

Finally we train the whole models from scratch with Teselas dataset [24].

General approaches VGG16 Auto-Encoder and Multi-Depth VGG Auto-Encoder architecture can be visualizing in Figure4, Figure5 and Figure6.

D. Data-set and Metric

We trained and tested our model on Teselas Dataset [24] which contains real aerial images of transport routes, collected in Spanish regions and captured in challenging scenarios. The data-set contains 2 categories (category 1—no road, category 2—road exists), around 9000 labelled tiles (png format). Also, we evaluate the models through several metrics recommended in the literature [31] namely: Specificity, Precision, F-Measure.

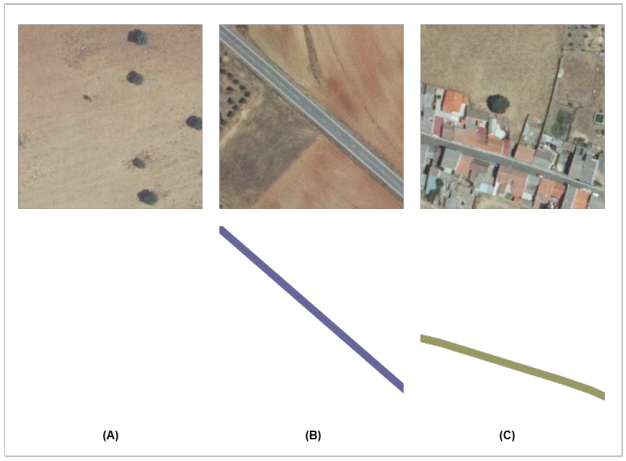


Fig. 2. Examples of labelled aerials images of Teselas Dataset (A) Category 1—no road, (B) and (C)category 2—road exists .

E. Data Training

In this sub-section, we describe the data training process of our data strategies selection, we selected twenty 520 frames for each category. However, the model was fed through various data training strategy namely:

- **Strategy DA:** consists of augmenting data by generating Three classical transformation frames (rotation to cover the essential angles) for each selected training frame.
- **Strategy Filter:** consists in generating four operation filter transformation by (contour detection, Detail enhance, EDGE enhance and FIND edges) for each selected training frame to facilitate data visualization and eliminate non-informative variables.

The table 1 shows the description and the number of samples used for the training of each strategy.

TABLE I
THE DESCRIPTION AND THE NUMBER OF SAMPLES USED FOR THE TRAINING OF EACH STRATEGY.

Strategy	Description	nbr of samples
FEW DATA	520 frames of each category)x2	1040
CLASSIC DATA AUG	Few Data+(3 transformation DA)	4160
FILTER DATA AUG	Few Data+(3 transformation Filter)	4160

The Detailed transformation of different strategies are presented in Figure3.

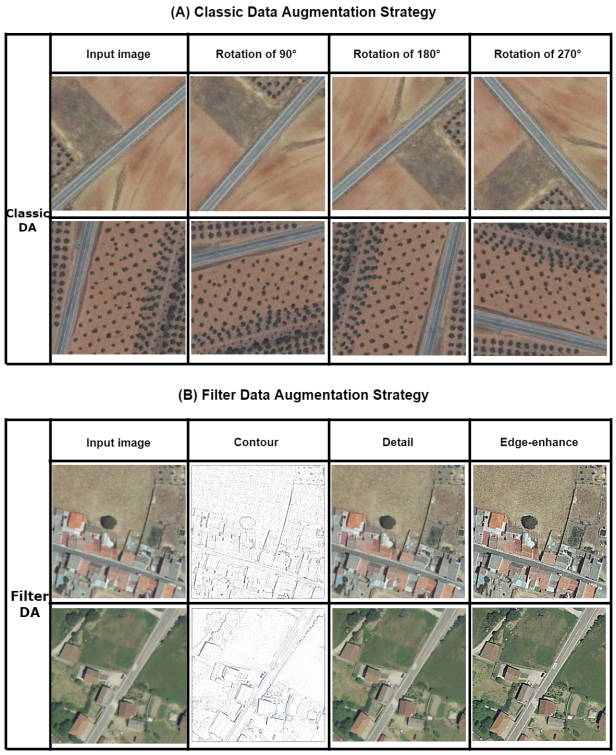


Fig. 3. Detailed transformation of the different Data Augmentation strategies.

The AE was implemented (trained and tested) using Keras library [32] programming in Python and the training process on GPU Nvidia GTX1080TI. The models was trained during 150 epochs. We train the networks with RMSprop optimizer. Loss is computed between the Ground truth label and the predicted result using a binary cross entropy loss function. The entire network was trained with 80% frames from the data training, and 20% frames for validate the training of the networks. We also do the evaluation of the models with 50% of the data-set.

III. Experiments and Results

In this section, we describe how the proposed approaches are implemented as well as the obtained results. Then, we compare the three approaches.

A. Experiments

For the first approach VGG16 Auto-Encoder part. The explanatory diagram is shown in Figure4.

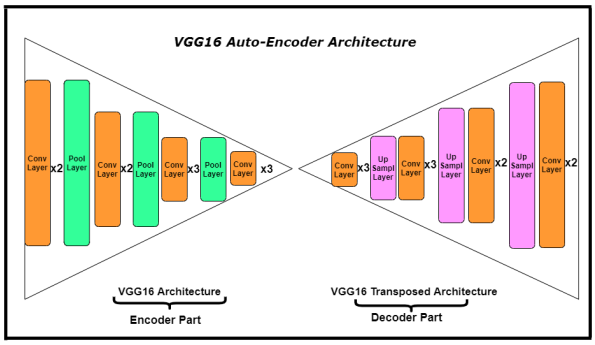


Fig. 4. Structure layers of the approach model based VGG16 Auto-Encoder.

In the two second approach we built models at different depths, we start with 12 hidden layers then gradually decrease to 10 hidden layers.

The detailed information and structure concerning the layers of the approaches models can be found in figure5 and figure6 .

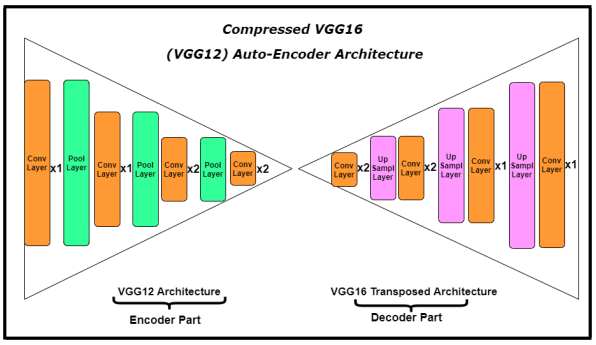


Fig. 5. Structure layers of the approach model based VGG12 Auto-Encoder.

B. Evaluation of the approaches

In this sub-section, we analyze the influence and the result of the training strategies for each approach.

- **Training Time :**

The Training Time of the training strategies results for each approach are shown in Table 2 on second.

The results clearly show that VGG10 AE model trained on New filter data augmentation strategy has less computational time than the other strategies.

To more analyse our models performance we plotting the accuracy and the loss functions between training and validation

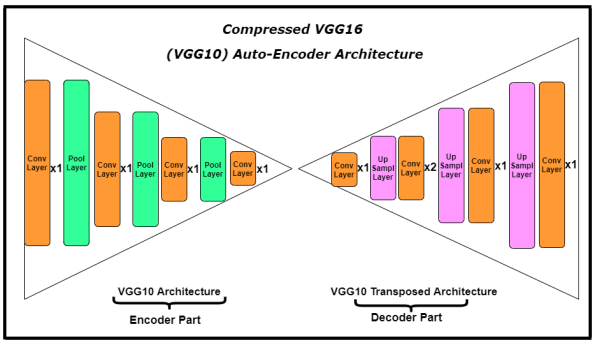


Fig. 6. Structure layers of the approach model based VGG10 Auto-Encoder.

TABLE II
Training Time of the training strategies for each approach

Architecture	Trainable Params	Different training time strategies (S)		
		Small Data	*DA Classic*	*DA Filter*
VGG16 AE	**18087715**	328045	1315534	1312389
VGG12 AE	**9590145**	218174	860137	883612
VGG10 AE	**5460097**	163077	658538	**635932**

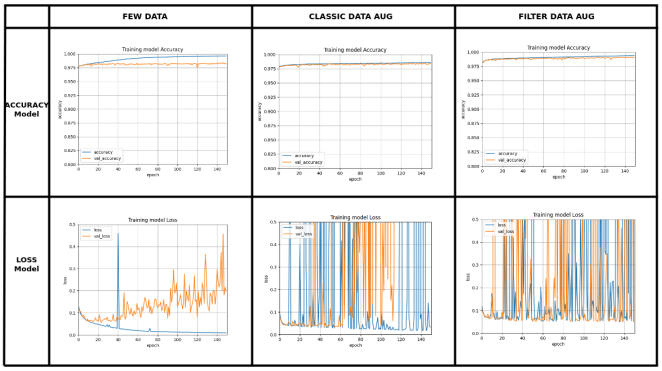


Fig. 7. Training and Validation Accuracy/Loss of the used strategies on VGG16 AE.

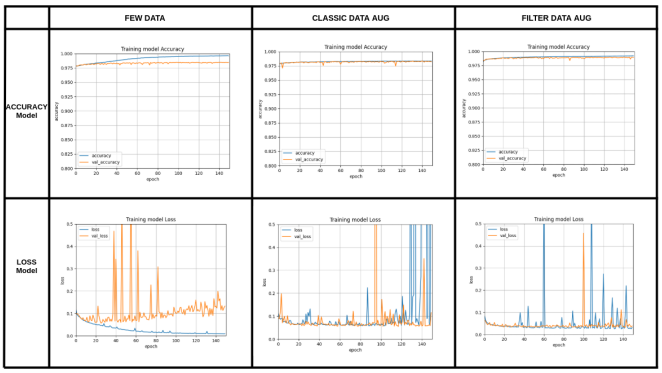


Fig. 8. Training and Validation Accuracy/Loss of the used strategies on VGG12 AE.

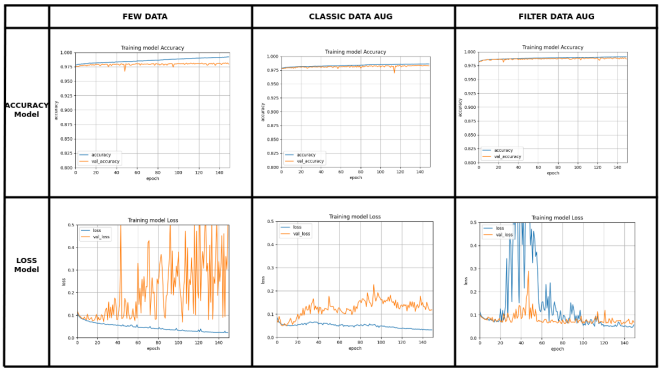


Fig. 9. Training and Validation Accuracy/Loss of the used strategies on VGG10 AE.

data for the all approaches trained on different strategies in Figure7, Figure8 and Figure9.

We can see that for training loss plot of training on data without making any increases for all approaches, the gap between validation and training loss is clear, it shows that the models are over-fitting due to the lack of data training.

From the training loss plot of training on data increased by classical data augmentation of all approaches, we can suggests some intuition that the model is over-fitting, it can clearly be seen starts over-fitting after 50-80 epoch.

From the (VGG10 AE trained on classical data augmentation) training loss plot, there are rarely differences between training and validation loss curves, Therefore, we can see that the effect over-fitting has decreased due to the presence of data augmentation transformation

From the training loss plot of VGG10 AE trained on filter data augmentation strategy, the loss validation and loss training curves are both converging, so the model avoids over-fitting through the new samples added to the training data-set with higher precis features which help and facilitates the system for the learning task, and the number decreased of layer.

For the accuracy curves, observing that with each decrease in the hidden layers of the models the accuracy increases and the both curves converge even more.

We show that the model (VGG10) trained on FILTER data augmentation gives better results compared to others in terms of accuracy and error. When we added more data training through filter transformation in model, we can notice that the validation loss decreased whereas the accuracy validation increased, therefore, we avoided the over-fitting. In this case, the model sounds more robustness.

Our objective is to make a compromise between the four factors (decreasing the number of hidden layers, the error decreasing without presence of over-fitting and the precision increases on less time training possible).

C. Comparison of our results

To make a better visual comparison between our approaches. We present in Figure10, qualitative comparison

TABLE III
A COMPARISON BETWEEN OUR RESULT TEST APPROACH

Method	FM	Pr	Sp
VGG16 AE	0.785	0.863	0.966
VGG12 AE	0.797	0.899	0.971
VGG10 AE	**0.841**	**0.913**	**0.976**

results, we selected as a demonstrative example two frame from the Teselas data-set.

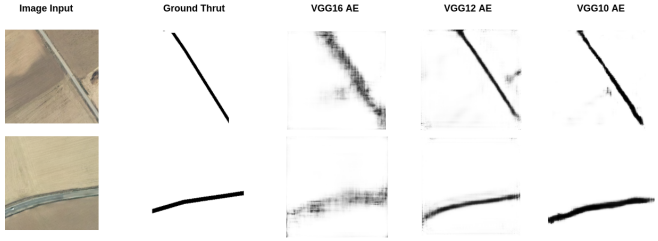


Fig. 10. Visual comparison of foreground masks generated by our selected models.

The first row show input frames, the second row shows the ground truth, the third row present VGG16 AE model, the fourth row show VGG12 AE model and the last row present the results VGG10 AE model. All the models trained on FILTER strategy.

The results from Table 3 and Figure10 shows that VGG10 AE trained on FILTER data augmentation approach has better performance than the other models and shows a very selectivity segmentation.

IV. Discussion and Conclusion

This paper addresses the problem of object segmentation in high-resolution aerial imagery and discusses the application of deep learning techniques to solve a problem related to segmentation and existence of geo-spatial elements (road network) in the available cartographic support. This challenge is addressed by constructing an auto-encoder neural network trained to segment roads in aerial imagery using manually labelled data.

In this study, we use VGG-Auto-Encoder approach with applying data and feature reduction on the data training using an adaptive data augmentation techniques (FILTER transformation) to perform road segmentation from aerial images model with less training time and avoiding the over-fitting effect.

we presented experiments comparing Multi depth VGG Auto-Encoder Deep Learning approaches trained through three strategies of few data. Our techniques for increasing and enhancing sample training are morphological data augmentation and geometric transformation based on filter transformations. The afore-mentioned techniques have been used in order to minimize and reduce the over-fitting effect as well as to generate the features that are necessary for road segmentation and to increase the model performance in the quickest possible time training.

As can be seen from our previous results, the VGG10 AE model trained on FILTER data augmentation strategy significantly improves the performance in terms of all the objective metrics compared to other strategies for the VGG16 AE and VGG12 AE approaches. From the results obtained, we can see that the results of VGG10 AE model achieve improved performance that obtained by other models.

The results indicate that the compressed learning model VGG10 AE trained on FILTER data augmentation can successfully learn road segmentation generalisation in the short possible time with little learning data. In addition, the preservation of the essential information given through the filter-based transformations (contour and edge enhance), has a purpose to increase the size of the data without losing primary information. As well as, to create adapted and necessary information . As a result, new data augmentation strategy were demonstrated based on the preservation of essential and necessary information to adapt the compress Auto-Encoder technique and a new technique to avoid the over-fitting effect.

The main goal is to enhance object segmentation (road network) in high-resolution aerial imagery technique based on supervised deep Auto-Encoder with few data training. However, we can concluded that filter-based transformations for training model, help the model improve the generalization capabilities and build an accurate model with few data training. Moreover, compared to the traditional techniques of data augmentation (flipping, rotation and translation) that relies on the change of location of the coordinates in the same mathematical plane which produce little improvements. Our work shows the importance of augmenting the data training with purpose, as with for creating a new representation of the variables with the results of the operation filters to extract the variables necessary for the segmentation task such as (edge enhance and contour detection) to eliminate the irrelevant variables that could distort the predictions and to achieve a quick segmentation training time.

REFERENCES

[1] W. Ge, Z. Guo, Y. Dong, and Y. Chen, "Dynamic background estimation and complementary learning for pixel-wise foreground/background segmentation," *Pattern Recognition*, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.patcog.2016.01.031

[2] T. Bouwmans, "Traditional and recent approaches in background modeling for foreground detection: An overview," *Computer Science Review*, vol. 11-12, pp. 31–66, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.cosrev.2014.04.001

[3] H. Liu, X. Han, X. Li, Y. Yao, P. Huang, and Z. Tang, "Deep representation learning for road detection using siamese network," *Multimedia Tools and Applications*, vol. 78, no. 17, pp. 24 269–24 283, 2019.

[4] W. Wang, N. Yang, Y. Zhang, F. Wang, T. Cao, and P. Eklund, "A review of road extraction from remote sensing images," *Journal of traffic and transportation engineering (english edition)*, vol. 3, no. 3, pp. 271–282, 2016.

[5] K. K. Eerapu, B. Ashwath, S. Lal, F. Dell'Acqua, and A. N. Dhan, "Dense refinement residual network for road extraction from aerial imagery data," *IEEE Access*, vol. 7, pp. 151 764–151 782, 2019.

[6] Y. Wei, Z. Wang, and M. Xu, "Road structure refined cnn for road extraction in aerial image," *IEEE Geoscience and Remote Sensing Letters*, vol. 14, no. 5, pp. 709–713, 2017.

[7] L. Zhou, C. Zhang, and M. Wu, "D-linknet: Linknet with pretrained encoder and dilated convolution for high resolution satellite imagery road extraction," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2018, pp. 182–186.

[8] J. Wang, Q. Qin, Z. Gao, J. Zhao, and X. Ye, "A new approach to urban road extraction using high-resolution aerial image," *ISPRS International Journal of Geo-Information*, vol. 5, no. 7, p. 114, 2016.

[9] J. Schmidhuber, "Deep Learning in neural networks: An overview," *Neural Networks*, vol. 61, pp. 85–117, 2015.

[10] C. Zhao, X. Li, and H. Zhu, "Hyperspectral anomaly detection based on stacked denoising autoencoders," *Journal of Applied Remote Sensing*, vol. 11, no. 4, p. 042605, 2017.

[11] A. Garcia-garcia, S. Orts-escolano, S. Oprea, V. Villena-martinez, P. Martinez-gonzalez, and J. Garcia-rodriguez, "A survey on deep learning techniques for image and video semantic segmentation," *Applied Soft Computing Journal*, vol. 70, pp. 41–65, 2018. [Online]. Available: https://doi.org/10.1016/j.asoc.2018.05.018

[12] M. G. Narasimhan and S. Kamath, "Dynamic video anomaly detection and localization using sparse denoising autoencoders," *Multimedia Tools and Applications*, vol. 77, no. 11, pp. 13 173–13 195, 2018.

[13] Y. Guo, Y. Liu, A. Oerlemans, S. Lao, S. Wu, and M. S. Lew, "Deep learning for visual understanding: A review," *Neurocomputing*, vol. 187, pp. 27–48, 2016.

[14] W. Liu, Z. Wang, X. Liu, N. Zeng, Y. Liu, and F. E. Alsaadi, "A survey of deep neural network architectures and their applications," *Neurocomputing*, vol. 234, no. December 2016, pp. 11–26, 2017. [Online]. Available: http://dx.doi.org/10.1016/j.neucom.2016.12.038

[15] Y. Wang, Z. Luo, and P. M. Jodoin, "Interactive deep learning method for segmenting moving objects," *Pattern Recognition Letters*, vol. 96, pp. 66–75, 2017. [Online]. Available: http://dx.doi.org/10.1016/j.patrec.2016.09.014

[16] M. Braham and M. Van Droogenbroeck, "Deep background subtraction with scene-specific convolutional neural networks," *International Conference on Systems, Signals, and Image Processing*, vol. 2016-June, 2016.

[17] J. Gracewell and M. John, "Dynamic background modeling using deep learning autoencoder network," *Multimedia Tools and Applications*, pp. 1–21, 2019.

[18] M. Babaee, D. Tung, and G. Rigoll, "A deep convolutional neural network for video sequence background subtraction," *Pattern Recognition*, vol. 76, pp. 635–649, 2018. [Online]. Available: https://doi.org/10.1016/j.patcog.2017.09.040

[19] D. M. Vo and S.-W. Lee, "Semantic image segmentation using fully convolutional neural networks with multi-scale images and multi-scale dilated convolutions," *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 18 689–18 707, 2018.

[20] H. Salehinejad, S. Naqvi, E. Colak, J. Barfett, and S. Valaee, "Cylindrical transform: 3d semantic segmentation of kidneys with limited annotated images," in *2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*. IEEE, 2018, pp. 539–543.

[21] J. Long, E. Shelhamer, and T. Darrell, "Fully convolutional networks for semantic segmentation," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2015, pp. 3431–3440.

[22] R. Keshari, M. Vatsa, R. Singh, and A. Noore, "Learning structure and strength of cnn filters for small sample size training," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2018, pp. 9349–9358.

[23] H. Salehinejad, S. Valaee, T. Dowdell, and J. Barfett, "Image augmentation using radial transform for training deep neural networks," in *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2018, pp. 3016–3020.

[24] C.-I. Cira, R. Alcarria, M.-Á. Manso-Callejo, and F. Serradilla, "A deep convolutional neural network to detect the existence of geospatial elements in high-resolution aerial imagery," in *Multidisciplinary Digital Publishing Institute Proceedings*, vol. 19, no. 1, 2019, p. 17.

[25] K. Lim and C.-s. Kim, "Background Subtraction Using Encoder-Decoder Structured Convolutional Neural Network," *2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, no. August, pp. 1—-6, 2017.

[26] S. Leonov, A. Vasilyev, A. Makovetskii, V. Kuznetsov, and J. Diaz-Escobar, "An algorithm for selecting face features using deep learning techniques based on autoencoders," in *Applications of Digital Image Processing XLI*, vol. 10752. International Society for Optics and Photonics, 2018, p. 107522M.

[27] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016, http://www.deeplearningbook.org.
[28] K. Seddiki, P. Saudemont, F. Precioso, N. Ogrinc, M. Wisztorski, M. Salzet, I. Fournier, and A. Droit, "Towards cnn representations for small mass spectrometry data classification: From transfer learning to cumulative learning," *bioRxiv*, 2020.
[29] A. Garcia-Garcia, S. Orts-Escolano, S. Oprea, V. Villena-Martinez, and J. Garcia-Rodriguez, "A Review on Deep Learning Techniques Applied to Semantic Segmentation," *arXiv preprint arXiv:1704.06857*, pp. 1–23, 2017. [Online]. Available: http://arxiv.org/abs/1704.06857
[30] Y.-D. Zhang, Z. Dong, X. Chen, W. Jia, S. Du, K. Muhammad, and S.-H. Wang, "Image based fruit category classification by 13-layer deep convolutional neural network and data augmentation," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 3613–3632, 2019.
[31] Y. Wang, P. M. Jodoin, F. Porikli, J. Konrad, Y. Benezeth, and P. Ishwar, "CDnet 2014: An expanded change detection benchmark dataset," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pp. 393–400, 2014.
[32] F. Chollet *et al.*, "Keras: The python deep learning library," *Astrophysics Source Code Library*, 2018.

Transfer Learning Using VGG Based on Deep Convolutional Neural Network For Finger-Knuckle-Print Recognition

1st Amira HAMIDI
Laboratoire de Génie Electrique
Université Kasdi Merbah
Ouargla, Algeria
amira.hamidi1963@gmail.com

2nd Salma KHEMGANI
Laboratoire de Génie Electrique
Université Kasdi Merbah
Ouargla, Algeria
salma.khamgani@gmail.com

3rd Khled BENSID
Laboratoire de Génie Electrique
Université Kasdi Merbah
Ouargla, Algeria
bensid.khaled@univ-ouargla.dz

***Abstract*—Transfer learning is an example of Convolutional Neural Network (CNN) method. It based to reusing a pre-trained model knowledge for another task. which used for image classification, feature extraction, and clustering problems. In this paper, we used two types of the pre-trained models VGG–16 and VGG-19 with deep convolutional neural network to extract the features of Finger-Knuckle-Print FKP images in order to develop an efficient multimodal identification system. The results obtained in this work show an excellent performance for unimodal and multimodal identification systems.**

***Index Terms*—Tansfer learning, Convolutional Neural Network (CNN), VGG-16, VGG-19, finger-knuckle-print (FKP).**

I. Introduction

NEW technologies penetrate all life areas and with our world being digitized very quickly, so the confidential information protection has become more and more important to users and organizations. For that, this topic has attracted the attention of researchers today to find a safe and effective way to protect the personal information and improve the privacy.

The automatic computer-based biometric recognition systems have been continuously replacing password-based identification approaches (classic approaches) for the last few years. Token-based methods (ID Card) can be easily stolen or lost, and information or passwords can be guessed or forgotten (pin or ID) [1]. As a result, these approaches are limited in their implementation in academic and commercial settings. In this part, physiological characteristics include biometric features derived from human biological organs such as the iris, retina, ears, and hand features...etc, whereas behavioral characteristics include gait, accent, signature, and gesture. Recently, fingerprints, Finger knuckle print, ears, iris, hand geometry, and many other characteristics have been extensively used as security features in computer laptops, voting systems, visa enrollments, cell phones, e-passports, and e-banking [2].
Finger knuckle print-based recognition systems have many advantages over common hand biometrics such as fingerprint, palm print, hand geometry, or their combinations like low-resolution imaging is possible and provides unlimited access control, insensitive to emotions and other behavioral aspects such as exhaustion, abduction, and sexual assault, ... etc. Furthermore, the finger knuckle print (FKP) is a universal, one-of-a-kind, and permanent biometric pattern used for very precise personal recognition. Contactless/unconstrained acquisition, robust feature extraction, and fusion strategies have been the subject of recent FKP research [3], [4].
A unimodal biometric system is a system that uses a single biometric trait [5] or an information source for verification or identification purposes [6]. Single-mode systems have steadily improved in terms of accuracy and reliability. However, they often suffer from the issues due to non-universal biometric traits, identity theft, and lack of precision due to noisy data. Additionally, single-mode biometric systems achieve less desired performance in real-world applications. Therefore, a method to solve these problems based on the use of multimodal biometric recognition systems [7]. This system can be defined as a system that combines the result obtained from more than one biometric characteristic for identification purposes. Unlike a unimodal biometric system which can result in non-universality, a multimodal system uses several biometric modalities which can result in a highly accurate and secure biometric identification system [8], [9].
Our experience is based on the transfer learning features of convolutional neural network methods called VGG. VGG's have recently shown remarkable success in feature extraction, image recognition, computer vision. VGG transfer learning is one of the deep learning techniques that have recently been used by many companies, such as Adobe, Apple, Facebook, Baidu, Google, IBM, Microsoft, NEC, Netflix, and NVIDIA. This work aims at achieving unimodal and multimodal biometric systems based on multi-sample FKP images using the transfer learning technique. Compared with traditional methods, our proposed VGG could extract more distinctive features and achieve satisfying and best recognition performance. In our experiments, we first evaluate each biometric identification system based on a single finger (unimodal system). Also, the results of two or more unimodal systems are fused at the matching score level to create an efficient and robust multimodal identification system.
The rest of the paper is organized as follows: Section (II) describes the proposed multimodal biometric system in which scores are fused at the matching level. Section (III) briefly describes the transfer learning-based feature extraction method and classification. The fusion rules are illustrated in section

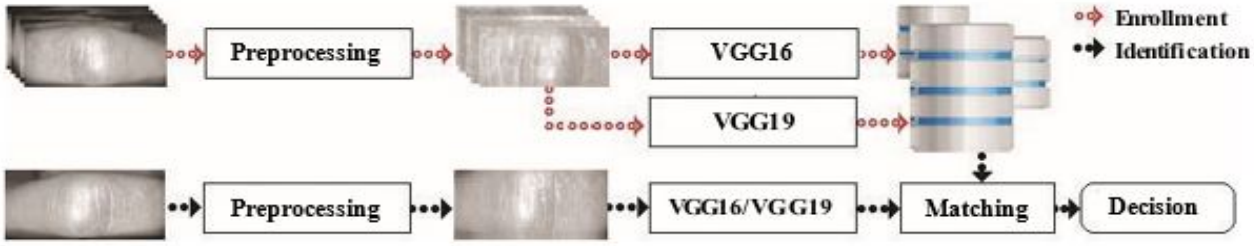


Fig. 1: Multimodal Finger Knuckle Print identification system.

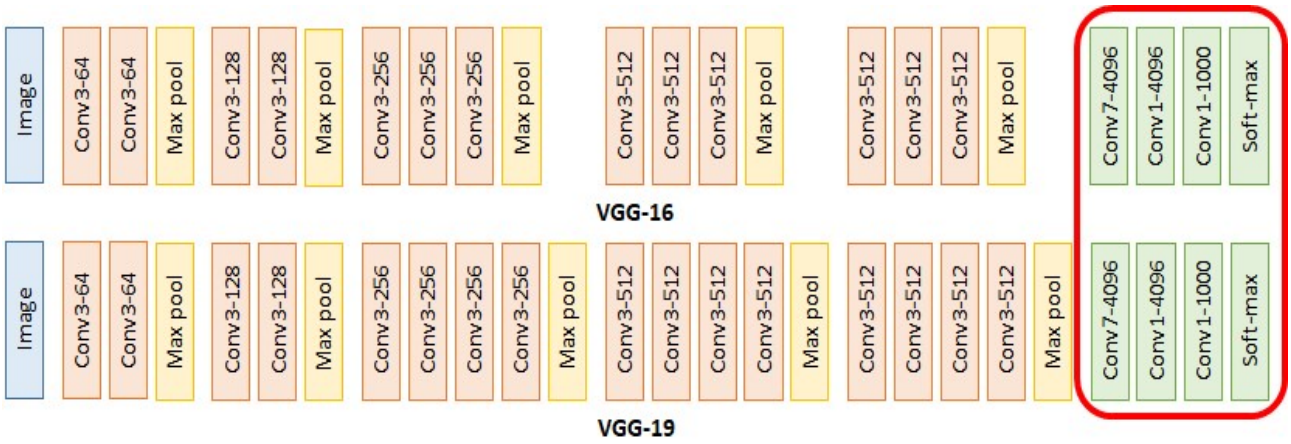


Fig. 2: Architecture of Vgg16 and Vgg19.

(IV). In section (V), the experimental results, obtained using a PolyU database of 165 persons, are presented and discussed. Finally, the last section (VI) includes the conclusion and the intended perspectives.

II. Proposed System

Figure 1 shows the block diagram of a multi-modal biometric recognition system based on the fusion between FKP samples. The region of interest (ROI) [10] is located and cropped from the FKP images in the preprocessing module. The purpose of the feature extraction by VGG 16 and VGG 19 is to represent the feature vector of each ROI image during the enrollment process. At the end, these feature vectors used as a training database used to create a model (matrix) depending on whether each column corresponds to a feature vector. In the second phase, devoted to the identification, the same methods used in the enrolment phase is applied to get extract the feature vector from the test image, and then it uses as an input to the matching module in order to find the decision which owns this finger. In the multimodal biometric identification system, the merger process is done at the score level, which is combining the normalized scores of two or more biometric systems. For each user, the system decision is made as follows:

$$Decision = \begin{cases} Accepted, & \text{if} \quad d_0^i \geq \mathcal{T}_{th} \\ Rejected, & \text{if} \quad d_0^i < \mathcal{T}_{th} \end{cases} \tag{1}$$

where d_0^i indicates the probability for the i^{th} person and (T_0) the system security threshold provided by the system designer (depending on the desired security level). This enhanced scheme takes advantage of each biometric modality and can be used to improve the unimodal biometric system.

III. Feature Extraction and Classification

VggNet is a deep convolutional network [11] for object recognition that was created and educated by Oxford's renowned Visual geometry community (Vgg), and which performed exceptionally well on the ImageNet dataset. Convolutional layers were stacked on top of each other at rising depths to create the Vgg network .
VGG is a further enhancement to AlexNet that makes the network deeper. the structure of VGG is shown in Fig. 2. Because the size of the whole convolution kernel is 3×3, the structure of VGG is neat and its topology is simple, the small size of the convolution kernel also brings advantages such as increasing the number. VGG expands the number of CNN layers to more than 10, improving the expressive capacity of the network and facilitating subsequent changes in the structure of the network [12].

A. VGG16

Unlike AlexNet, VGG16 consists of a replicative structure of convolution, reread, and pooling layers. They increased the number of these network units to design a deeper network.

However, Simonyan et all [13] considered a smaller receive window for each convolutional filter compared to AlexNet. With the preservation of the same nonlinear activation unit of AlexNet.

B. VGG19

In addition, a deeper VGG19 network is offered for the same task (object detection). VGG19 included some additional convolutional rereaders in the middle of the array compared to VGG16. However, this minimal change in architecture turns into an improvement in accuracy for the object recognition task.

IV. Matching, Fusion Scheme and Decision

Matching score is a measure of similarity between the test (input) and train (template) feature vectors. The high match score can be determined by examining the match scores appertaining to all the comparisons and reporting the identity of the template corresponding to the largest similarity score. Recently, several methods have been used in this field, and in our biometric identification system we used three different types (Support Vector Machine (SVM), k-Nearest Neighbor (KNN), and Random Forest (RF)).

A. Support Vector Machine (SVM)

SVM is a kind of machine learning algorithm that can be used to solve problems like classification, regression, and detection. A support vector machine is a technique of discrimination, it is a supervised learning method for classification and regression. It consists in separating two or more sets of points by a hyperplane. Depending on circumstances and configuration points. The original idea of SVM is based on using kernel core functions that allow optimal separation of the points of the plan in different categories. The method uses a set of training data. which enables a hyperplane separating the best points. In this paper we use the multi class SVM [14].

B. K-Nearest Neighbor (KNN)

K-nearest neighbor is the traditional supervised statistical pattern recognition method which classifies an image by comparing the 'K' value of the training data with test data for finding closeness with the testing image or data. The 'K' values are estimated from the feature extraction carried out during the training process. Euclidean equation principle is employed in KNN classifier for identifying the similarity [15].

C. Random Forest (RF)

A random forest is a set of unconditional classifications or regression trees that were constructed using bootstrap samples from training data and random feature selection in tree extrapolation. Forecasting is done by compiling (majority or average vote) the group's forecasts. Two methods for essemble learning a classification tree. The sample subsets creation for a tree is dependent on previous classification results and addition weights are given to the samples that are incorrectly predicted previously [16].

Fusion at the matching score level is the most popular and frequently used method because of its good performance and simplicity. The outputs of the two or more matching modules (LIF, LMF, RIF, RMF) are combined using fusion at the matching-score level.
There are several matching-score fusion rules integrate normalized matching scores of a user to produce the final matching score [17].

1) Simple Sum Rule: The Simple Sum rule takes the sum of the R matching scores of the $(k)_th$ user as the final matching score S_k of this user. S_k is calculated as follows:

$$S = 1/N \sum_{i=1}^{N} S_i \tag{2}$$

2) Product rule: This rule defines the new scores for each matcher, is calculated as follows:

$$S = 1/N \prod_{i=1}^{N} S_i \tag{3}$$

3) Minimum rule: This rule simply sets a new scores as the minimum score of each matcher's scores, is calculated as follows:

$$S = min(S_i) \tag{4}$$

4) Maximum rule: This rule simply sets a new scores as the maximum score of each matcher's scores, is calculated as follows:

$$S = max(S_i) \tag{5}$$

The final result of the fusion is a new matching score, which is the basis for the classification decision of the entire system.

5) Weighted Sum rule: The weighted sum of the R matching scores, which is shown in (6), is considered as the final matching score of the k_{th} user.

$$S = \sum_{i=1}^{N} w_i S_i \tag{6}$$

whereW_i represents the weight of the matching score of the i_{th} biometric trait of the k_{th} user. And

$$w_i = \frac{1/\sum_{i=1}^{N} 1/EER_j}{EER_i} \tag{7}$$

6) Weighted Product rule: Let W_i stand for the weight of the matching score of the i_{th} biometric trait of the k_{th} user. A Weighted Product rule can determine the final matching score of the k_{th} user using

$$S = \prod_{i=1}^{N} w_i S_i \tag{8}$$

The final result of the fusion is a new matching score, which is the basis for the classification decision of the entire system.

TABLE I : Unimodal Identification Test Results Using SVM classifier

Fingers	Open Set		Closed Set	
	T_o	EER(%)	ROR(%)	RPR
VGG 16 Features				
LIF	0.9320	6×10^{-4}	99.79	02
LMF	0.8550	3.7×10^{-3}	99.79	03
RIF	0.6850	0.1016	99.79	41
RMF	0.8460	8×10^{-3}	99.69	05
VGG 19 Features				
LIF	0.8640	3.7×10^{-3}	99.39	03
LMF	0.7120	1.36×10^{-2}	99.79	32
RIF	0.6720	0.1010	99.69	69
RMF	0.8250	3.7×10^{-3}	99.89	04

TABLE II : Unimodal Identification Test Results Using KNN classifier

Fingers	Open Set		Closed Set	
	T_o	EER(%)	ROR(%)	RPR
VGG 16 Features				
LIF	0.090	0.1010	99.39	10
LMF	0.058	0.045	99.19	05
RIF	0.098	0.2020	99.09	32
RMF	0.075	0.1010	99.19	14
VGG 19 Features				
LIF	0.1487	0.2441	98.78	20
LMF	0.126	0.1010	99.69	85
RIF	0.1457	0.3030	98.48	47
RMF	0.1331	0.2020	99.09	20

TABLE III : Unimodal Identification Test Results Using RF classifier

Fingers	Open Set		Closed Set	
	T_o	EER(%)	ROR(%)	RPR
VGG 16 Features				
LIF	0.6200	0.3172	97.07	32
LMF	0.6820	0.1133	98.58	14
RIF	0.6370	0.2772	98.18	33
RMF	0.6180	0.3030	97.47	22
VGG 19 Features				
LIF	0.5650	0.5057	97.27	30
LMF	0.6260	0.2020	98.10	40
RIF	0.5710	0.3030	97.97	43
RMF	0.5350	0.5044	97.97	52

V. Experimental Results and Discussion

A. Experimental datasets

To evaluate the performance of the proposed biometric system and choose their appropriate parameters, a database of FKP images is required. Thus, our experiment tests were performed using the FKP Database from the Poly University (The Hong Kong Polytechnic University 2018) [18]. The database has a total of 7920 images from 660 different fingers obtained by 165 persons. This dataset including 125 males and 40 females. Among them, 143 subjects were 20–30 years old and the others are 30–50 years old. These images are collected in two separate sessions. The average time interval between the first and the second sessions was about 25 days. The maximum and minimum intervals were 96 and 14 days, respectively. In each session, the subject (person) was asked to provide 12 image samples for each of Left Index Fingers *LIF*, Left Middle Fingers *LMF*, Right Index Fingers *RIF* and Right Middle Fingers *RMF*. . Therefore, 48 image samples from 4 finger types were collected from each person.

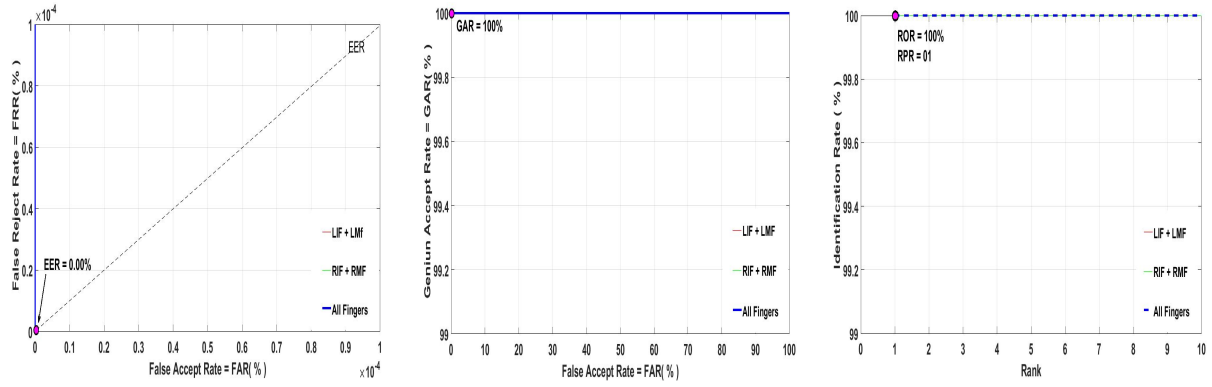
To develop a finger knuckle print recognition system, it is necessary to have two databases: a database to perform training (learning) and other database to test and determine their performance. For the vgg technique, it is best to take more comprehensive training data to avoid overfitting. In our set of tests, we divided the database as follows: The odd images of each person are used for the learning phase, the remaining 6 (even) images of each individual were used for the various

TABLE IV : MULTIMODAL BIOMETRIC IDENTIFICATION SYSTEM TEST RESULTS

Fusion rules	LIF-LMF				RIF-RMF			
	Open Set		Closed Set		Open Set		Closed Set	
	T_o	EER(%)	ROR(%)	RPR	T_o	EER(%)	ROR(%)	RPR
SUM	**0.712**	**0.00**	**100**	**01**	**0.733**	**0.00**	**100**	**01**
WHT SUM	**0.869**	**0.00**	**100**	**01**	0.9090	8.6×10^{-3}	**100**	**01**
PROD	**0.522**	**0.00**	**100**	**01**	**0.642**	**0.00**	**100**	**01**
WHT PROD	**0.837**	**0.00**	**100**	**01**	0.9950	8.52×10^{-3}	**100**	**01**
MIN	**0.666**	**0.00**	**100**	**01**	**0.828**	**0.00**	**100**	**01**
Max	/	/	**100**	**01**	/	/	**100**	**01**

LF-RF All Fingers

Fusion rules	Open Set		Closed Set	
	T_o	EER(%)	ROR(%)	RPR
SUM	**0.718**	**0.00**	**100**	**01**
WHT SUM	**0.845**	**0.00**	**100**	**01**
PROD	**0.174**	**0.00**	**100**	**01**
WHT PROD	**0.800**	**0.00**	**100**	**01**
MIN	**0.606**	**0.00**	**100**	**01**
MAX	/	/	**100**	**01**



(a) (b) (c)

Fig. 3: Multimodal biometric identification system test results. (a) ROC curves (FRR against FAR), (b) ROC curves (GAR against FAR) and (c) CMC curves, identification rate against rank.

tests.

B. Experimental Setup

In this section, the identification tests results are divided into three parts. In the first part, a series of experiments were carried out to use the Vgg transfer learning features to evaluate the performance of the proposed unimodal biometric system using the different FKP finger knuckle print samples. For this, both identification modes (open-set and closed-set modes) are tested. In the last section, the performance of the multimodal biometric system is evaluated. Our biometric system is implemented using MATLAB 2020a in an experimental platform as a workstation (HP Z8 G4), with a 64-bit Microsoft Windows 10 operating system, equipped with an Intel Xeon Silver 4108 processor, a 96 GB of RAM and a graphic processing unit (GeForce RTX 2080 Ti, GeForce RTX 3090).

C. Unimodal biometric System Test Results

The goal of this experiment is to evaluate the system performance when we using information from each modality (each finger). For this, in Open Set identification we found the performance under different modalities (LIF, LMF, RIF, RMF).

Table I, II, III compares the performance of the unimodal system based on VGG feature extraction and different classifier for various fingers. The experimental results indicate that the vgg 16 perform better than the vgg 19 when using all classifier SVM, KNN, and RF. For that, the LIF give the best result compared to all fingers in terms of EER. They give $EER = 6 \times 10^{-4}\%$ in SVM classifier, $4.5 \times 10^{-2}\%$ in KNN classifier respectively. As a result, the SVM classifier is the best compared to all other classifiers.

The tables compare the closed-set identification results. Like the open-set identification biometric system, the closed-set

identification system can achieve high accuracy with the vgg method. In this case, the system generates a Rate-One Recognition (ROR) equal to 97.07% up to 99.89% with a Rank of Perfect Recognition (RPR) equal to 02 up to 85 for all fingers and classifier.

D. Multimodal Biometric System Test Results

Unimodal systems are Faced several problems, such as the possibility of noise in the biometric modality and its non-universality, Intra-class dissimilarity, and inter-class similarity. all this problem increases the system error (EER) and hence the result of identification.

An excellent biometric identification system requires a very low EER value, which can be achieved by the multimodal system. This system combined several features of each modality at different levels, namely the sensor level, the feature level, the matching score level, and the decision level [19].

The goal of the fusion process is to improve the performance by fusing the information from different modalities. We will try to merge the different scores for different fingers to obtain a multimodal system.

In this case, we merge the different samples of some fingers (LIF and LMF, RIF and RMF) and at the end we realize a system based on the fusion between the two fingers (LIF+LMF), (RIF+RMF), and all fingers. For that, we use the results obtained by VGG 16 transfer learning features and SVM classifier.

Table IV and Fig 3 show the performance of the multimodal identification system using different fusion rules, from the results, we note that the all rules give the perfect result with the LIF+LMF, RIF +RMF, and all fingers in combinations, they gives $EER = 0.00\%$ in Open-Set identification.

In Cloused-Set, the system generates a Rate-One Recognition (ROR) equal to 100%. The analysis of the data showed that the results of the multimodal fusion were much better than those of the unimodal biometric systems.

The multimodal system has an $(EER = 0.00\%)$ and an $(ROR = 100\%)$ and an $(RPR = 01)$, thereby obtaining a perfect result. This is ideal precision can be reduced to a large database. The all rules are the best because it gives a perfect result and it is simple to use.

VI. Conclusion and Further Work

This paper produces a multimodal identification system based on finger knuckle print using the merge of different samples (LIF, LMF, RIF, and RMF fingers) at the matching score stage. In this case, we implemented the VGG transfer learning method to extract the FKP features. The experimental results illustrate that the combination of finger modalities images outperforms compared with single finger modality. It produces very low EER 0.00% in open-set identification and a high ROR 100% in closed-set identification.

In conclusion, the fusion schemes with multimodal systems gave significantly better performances than their unimodal systems. Our future work will project to use other modalities like (Palmprint, Face, Voice,...etc) with other transfer learning methods (like AlexNET, ResNet, DenseNet, Inception ResNet v2, Inception v3, Inception v4, and Xception).

References

[1] P. Campisi, *Security and privacy in biometrics*. Springer, 2013, vol. 24.

[2] J. Unar, W. C. Seng, and A. Abbasi, "A review of biometric technology along with trends and prospects," *Pattern recognition*, vol. 47, no. 8, pp. 2673–2688, 2014.

[3] A. Kumar and C. Ravikanth, "Personal authentication using finger knuckle surface," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 1, pp. 98–110, 2009.

[4] K. Usha and M. Ezhilarasan, "Finger knuckle biometrics–a review," *Computers & Electrical Engineering*, vol. 45, pp. 249–259, 2015.

[5] S. Venkatraman and I. Delpachitra, "Biometrics in banking security: a case study," *Information Management & Computer Security*, 2008.

[6] A. Drygajlo, "Multimodal biometrics for identity documents and smart cards: European challenge," in *2007 15th European Signal Processing Conference*. IEEE, 2007, pp. 169–173.

[7] M. El-Abed, R. Giot, B. Hemery, and C. Rosenberger, "A study of users' acceptance and satisfaction of biometric systems," in *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*. IEEE, 2010, pp. 170–178.

[8] M. Mittal and B. Garg, "Secure identity using multimodal biometrics," *Int. J. Inf. Technol. Knowl.*, vol. 7, no. 2, pp. 20–25, 2014.

[9] H. Jaafar and D. A. Ramli, "A review of multibiometric system with fusion strategies and weighting factor," *International Journal of Computer Science Engineering (IJCSE)*, vol. 2, no. 4, pp. 158–165, 2013.

[10] C. Hegde, P. D. Shenoy, K. Venugopal, and L. Patnaik, "Fkp biometrics for human authentication using gabor wavelets," in *TENCON 2011-2011 IEEE Region 10 Conference*. IEEE, 2011, pp. 1149–1153.

[11] H. Jun, L. Shuai, S. Jinming, L. Yue, W. Jingwei, and J. Peng, "Facial expression recognition based on vggnet convolutional neural network," in *2018 Chinese Automation Congress (CAC)*. IEEE, 2018, pp. 4146–4151.

[12] L. Shao, F. Zhu, and X. Li, "Transfer learning for visual categorization: A survey," *IEEE transactions on neural networks and learning systems*, vol. 26, no. 5, pp. 1019–1034, 2014.

[13] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv preprint arXiv:1409.1556*, 2014.

[14] C.-C. Chang and C.-J. Lin, "Libsvm: a library for support vector machines," *ACM transactions on intelligent systems and technology (TIST)*, vol. 2, no. 3, pp. 1–27, 2011.

[15] S. Shakya, "Analysis of artificial intelligence based image classification techniques," *Journal of Innovative Image Processing (JIIP)*, vol. 2, no. 01, pp. 44–54, 2020.

[16] F. Ahmad, K. Roy, B. O'Connor, J. Shelton, G. Dozier, and I. Dworkin, "Fly wing biometrics using modified local binary pattern, svms and random forest," *International Journal of Machine Learning and Computing*, vol. 4, no. 3, p. 279, 2014.

[17] D. Samai, K. Bensid, A. Meraoumia, A. Taleb-Ahmed, and M. Bedda, "2d and 3d palmprint recognition using deep learning method," in *2018 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS)*. IEEE, 2018, pp. 1–6.

[18] R. Chlaoua, A. Meraoumia, K. E. Aiadi, and M. Korichi, "Deep learning for finger-knuckle-print identification system based on pcanet and svm classifier," *Evolving Systems*, vol. 10, no. 2, pp. 261–272, 2019.

[19] A. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern recognition*, vol. 38, no. 12, pp. 2270–2285, 2005.

Lips Recognition for Biometric Identification Systems

1st Boucetta Aldjia
Dept. of computer science
University of Batna2
Batna, Algeria
boucetta_batna@yahoo.fr

2nd Boussaad Leila
Dept. of computer science
University of Batna2
Batna, Algeria
boussaad.mous@gmail.com

***Abstract*—In recent years, researches in biometric methods have gained much attention and they have advanced to a wide scope in security concepts. Therefore, many biometric technologies have been developed and enhanced with many of the most successful security applications. Lately, lip-based biometric identification becomes one of the most relevant emerging tools, which comes from criminal and forensic real-life applications. The main purpose of this paper is to prove the benefit of lips as a biometric modality, by using both handcraft and deep-learning based feature extraction methods. So, we consider three different techniques, Histogram of Oriented Gradients(HOG), Local Binary Pattern(LBP) and pretrained Deep-CNN. All results are confirmed by a ten-fold cross-validation method using two datasets, NITRLipV1 and database1. The mean accuracy is found to be very high in all the experiments carried out. Also the feature extraction using the Inceptionv3 model always achieve highest mean accuracy.**

***Index Terms*—Human identification, Lips recognition, Histogram of Oriented Gradients (HOG), Local Binary Pattern (LBP), Convolutional Neural Network (CNN).**

I. Introduction

Biometric human identification methods have recently gained a lot of attention, since they easily address most traditional identification issues.

In biometric human identification systems, users are recognized by who they are and not by anything to keep in mind or take with them [1]. Several known methods of human identification, like face, iris, retina, etc. are developed and optimized, but there are still need to emerging and innovative solutions [2]. Some of the new biometrics modalities are: heartbeat (ECG) [3], EEG biometrics [4], dental radiograph [5] and finger-nails [6].

Recently, lips recognition [7] has been proposed as a new relevant emerging kind of biometrics, which derived from criminal and forensic real-life applications.

Studies on lip-prints date back to 1950's, where extensive studies on lip-traces have been performed by Japanese researchers, without indicating or proposing a useful application of them. At the beginning of the 1970's, based on the lip prints of 1364 people between the ages of 3 and 60 of both sexes, Yasuo Tsuchihachi and Kazuo Suzuki [8] demonstrated that lip prints are unique and stable for an individual. Further, they suggested the ability to use lip prints in human identification. Also, lip prints are used to gender determination of the examined subject [9].

Lip prints properties have been successfuly applied as a subdiscipline of dactyloscopy, to human identity confirmation by forensic specialists and police. Precisely, when examining the features of the human lips, the anatomical patterns on the lips are often considered. Different classifications have been developed by authors. However, no classification has yet been recognized internationally and each author creates more or less his own by modifying some already existing. For example, Yasuo Tsuchihachi and Kazuo Suzuki identified 6 lip models based on the patterns found, figure 1 and table I present this classification and their description.

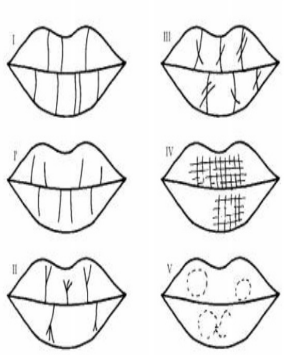


Fig. 1. Yasuo Tsuchihachi and Kazuo Suzuki classification of lip patterns [8].

TABLE I
YASUO TSUCHIHACHI AND KAZUO SUZUKI DESCRIPTION OF LIP PATTERNS [8].

Type of lip pattern	Description
Type I	Complete straight grooves
Type I'	Partial straight grooves
Type II	Branched grooves
Type III	Intersected grooves
Type IV	Reticular grooves
Type V	Other patterns

Unfortunately, in image analysis based recognition system, these features cannot be used because they are difficult to

extract from the acquired images. Therefore, in our approach, we do not use the features of lip prints, but we focus on the features extracted from the lips in a static face image.

Authors in [2] consider that the use of lips as modality for human identification is very interesting, since lips are passive biometrics, in which images can be obtained without the knowledge of the person being examined. Also, lips are usually visible and not hidden or covered with anything. Further lips can be implemented in a hybrid lips-face or lips-voice biometric systems.

In this paper, we study the efficiency of lips based biometrics systems using three feature extraction techniques, i.e., Histogram of Oriented Gradients (HOG), Local Binary Pattern (LBP) and inceptionv3 pre-trained Deep-CNN as automatic feature extractor.

In the recognition step, two classifiers are used for lip recognition, which are K-nearest neighbor (K-nn) and support vector machine (SVM).

The rest of this paper is organized like this: Literature survey is presented in section 2. The proposed lip based biometrics system is presented in section 3. The experimental results and discussion in section 4. Finally, conclusions and future works are drawn in section 5.

II. Literature Survey

Lip biometrics have not been very much studied so far. In this section, we will cite some works that have been realized in this field:

In [10], authors consider both physiological and behavioral information of the lip as biometric. Their results prove that both the static texture feature of lips and the dynamic shape deformation feature can give satisfactory accuracy.

Also, in [2], there have been several investigations to recognize a person directly from the shape and contour of lips, where lip region of interest is determined based on the color distribution around the lip area.

In addition, Choras in his various researches [11] [1] [2], proved that the lip can be used as a strong biometric trait.

Further, Hsu et al. [12] proposed lip recognition method based on active basis model, Particle Swarm Optimization (PSO) algorithm to define the best combination of parameters, and SVM to obtain classified results.

In th same context, Bakshi et al. [13] applied tow techniques to extract the local features from grayscale lip images, viz. SIFT (Scale Invariant Feature Transform) and SURF (Speeded Up Robust Features). The precision turns out to be very high ($> 90\%$) in the two experiments carried out.

In recent work, Bakshi et al. [14] studied the fusion of the shape and texture characteristics of the lip image to verify a person's identity in mobile devices.

Furthermore, Wrobel et al. [15] proposed an efficient lip-based biometric recognition approach using a Probabilistic Neural Network (PNN) for verification purpose. The results obtained by PNN are improved by a Particle Swarm Optimization (PSO) technique.

III. Proposed Lip Biometric approach

In this section, we present the proposed lip biometric system, its overview is illustrated in Fig. 2 and the details of each step are described in the following subsections:

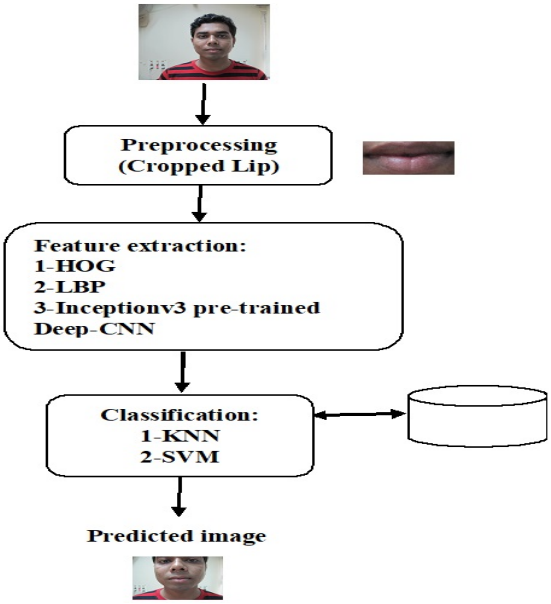


Fig. 2. Basic Design of the Proposed Lip Biometric System.

A. Feature Extraction Phase

In this study, three different feature extraction algorithms are used. The details of these algorithms are given below.

1) Histogram of Oriented Gradients(HOG): HOG is a feature descriptor that focuses on the structure or shape of an object. It is considered as one of the well recognized features due to its superior performance and relatively simple computation [16].
It is initially proposed for the detection of pedestrians [17]. It counts the occurrences of gradient orientation in localized parts of an image. The main steps to calculate HOG features can be summarized as follows [16].
   - Gradient calculation: In this step, the spatial gradients in the vertical and horizontal directions are calculated, then used to calculate the gradient magnitudes and angles.
   - Orientation binning: In this step, the image is divided into small connected regions called cells and according to the gradient angle, the gradient magnitude of each pixel in a cell is voted into different orientation bins.
   - Feature description: In this step, the adjacent cells are grouped into blocks . Each block is normalized by its L2 norm, then to form a descriptor, the normalized block histograms in a detection window are concatenated.

   An example of HOG features over the original image is illustrated in Fig.3.

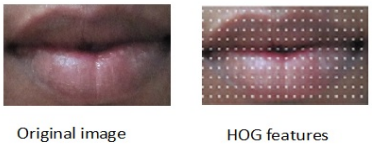


Fig. 3. An Example of HOG Features over the Original Image.

2) Local Binary Pattern(LBP): LBP features are originally proposed for texture analysis, which labels the image pixels by thresholding the neighborhood of each pixel and considers the result as a binary number [18]. The most important properties of LBP features are their tolerance to illumination changes and their ease of calculation. LBP proceeds as illustrated in Fig. 4; each pixel is compared to its eight neighbors in a 3×3 neighborhood by subtracting the value of the central pixel; Strictly negative values are coded with 0 and others with 1; A binary number is obtained by concatenating all these binary codes clockwise from the one at the top left. Derived binary numbers are called Local Binary Patterns or LBP codes [19].

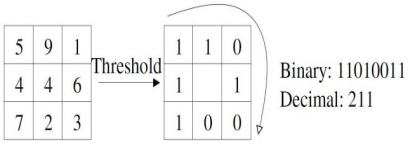


Fig. 4. An Example of the Basic LBP [19].

Initially, the size of the LBP operator was limited to only 3×3 neighborhood, it cannot capture dominant features with large scale structures. To overcome this limitation, the descriptor was generalized to use neighborhoods of different sizes [20].

A local neighborhood is defined as a set of evenly spaced sample points on a circle centered on the pixel to be labeled and the sample points that do not fall in the pixels are interpolated by bilinear interpolation, thus allowing any radius and any number of sampling points in the neighborhood.

Fig.5 illustrates some examples of the extended LBP operators, where (P, R) denotes a neighborhood of P sampling points on a circle with radius R.

The LBP operator used in this paper is the circular (8,1) neighborhood.

3) Pre-trained Inception-v3 Deep CNN model:
Inceptionv3 [21] is a CNN architecture from the Inception family, including three types of Inception modules (Inception A, Inception B and Inception C) as shown in Fig. 6. Each Inception module is composed of several convolutional layers and pooling layers in parallel, which can generate discriminatory features and reduce the number of parameters. In Inception-v3, three Inception A modules, five Inception B modules and two

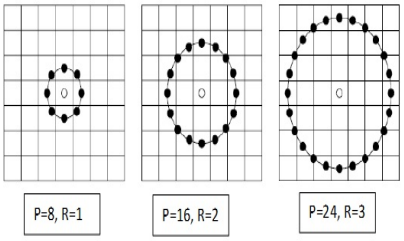


Fig. 5. Three Examples of the extended LBP operator with circular neighborhood [20].

Inception C modules are stacked in series.

In our experiment, feature extraction is computed from the pooling layer 'avg_pool' of the pre-trained DeepCNN InceptionV3 model.

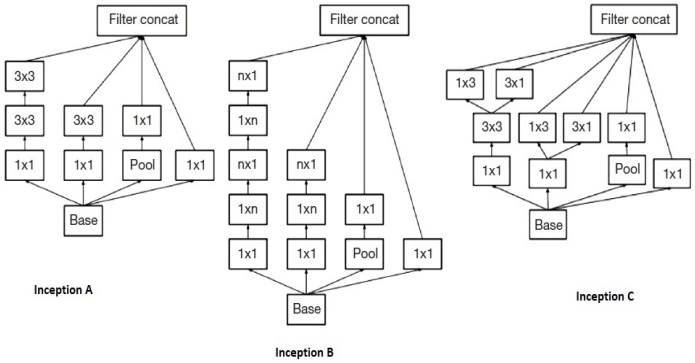


Fig. 6. The Inception Modules of Inception-v3 [21].

A general diagram of the Inception-v3 model is shown in Fig.7.

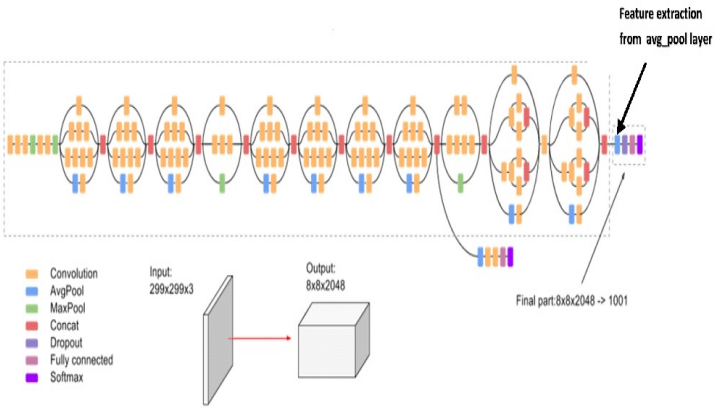


Fig. 7. Inception-v3 model [22].

B. Classification Phase

1) K-Nearest Neighbor (K-nn) classifier:
The KNN classifier is a very simple non-parametric classification method proposed by Cover and Hart in

1968 [23]. Despite the simplicity of the algorithm, it works very well and it is an important reference method. Due to its clear principles and excellent classification performance, it is used in several applications.
The KNN method is based on K which means the number of nearest neighbors. Decision rules can be described as follows [24]:

- If K = 1, the KNN method is called NN (nearest neighbor) method. Firstly, calculate the distances between the test sample x and all training samples by a distance function (Euclidean, Manhattan,...). Secondly, find the nearest neighbor, that is, the nearest training sample to x. Finally, give x the class label identical to nearest neighbors.
- When $K \neq 1$, KNN tries to find the K nearest neighbors of x. Among these K nearest neighbors, if the samples belonging to class i has the largest quantity, the class label of x can be marked with i.

2) Support Vector Machine(SVM) classifier:
SVM is a related supervised learning method used for classification and regression, it was originally proposed by Vapnik [25]. It is the most preferred by many because it can provide significant accuracy with computational efficiency.
The objective of the SVM algorithm is to find the best decision line or boundary (hyperplane) that can separate the n-dimensional space into classes so that we can easily place the new data point in the correct category in the future. Fig. 8 shows an example of the classification process of SVM.

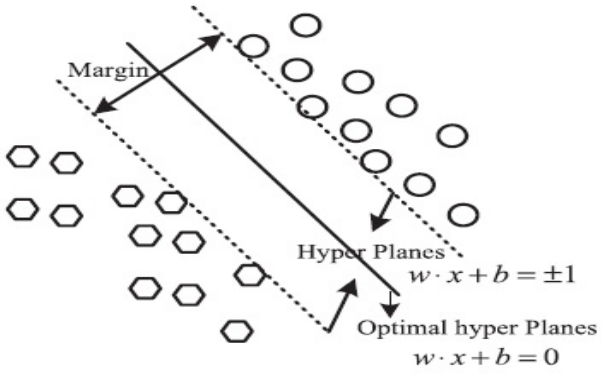


Fig. 8. The SVM Classification Process [26].

In addition, the SVM can efficiently performs nonlinear classification using the kernel function, by mapping its inputs into large feature spaces. The kernel function plays a crucial role in SVM, because it is a kind of measure of similarity between the input object. The proper selection of the kernel function will affect the accuracy of the model. There are four types of kernel function available for SVM which include linear, Radial Basic Function (RBF), polynomial and sigmoid [27]. Among these popular kernel functions, RBF is the most popular choice due to its less numerical difficulties and less hyperparameters than the polynomial kernel.

IV. Experiments and Results

In this section we will discuss the used datasets , and the experimental results that were generated.

A. Description of Databases

The proposed identification system is evaluated on two publicly-available lip databases, namely NITRLipV1 [28] and Database1 [29] databases.

1) NITRLipV1 database captured by Canon PowerShot A1100IS with F2.7 aperture and shutter speed varying from 1/60s to 1/25s. The database images were collected from 15 Indian volunteers, including men and women with age ranged from 20 to 40 years. This database is composed of 109 color images characterized by a variety of illumination conditions saved in JPEG format.
2) The Database1 database contains 23 color and grayscale images of objects, 5 images per object. Images have different sizes from the range 3096×3456 to 4128×4608 pixels and have various illumination and position conditions.

Some examples from the NITRLipV1 and Database1 databases are shown in Fig. 9.

Fig. 9. Examples from the NITRLipV1 and Database1 Databases.

B. Experimental Evaluations

The entire algorithm was evaluated using the Matlab (R2018b) environment. All images in the NITRLipV1 and Database1 databases are used for training and test and the experiments results are reported in terms of average recognition accuracy rates following a 10-fold cross-validation scheme.
The accuracy rate is defined by Eq. 1.

$$\text{Accuracy} = \frac{TPR + TNR}{TPR + TNR + FPR + FNR} \times 100 \quad (1)$$

where TPR (True Positive Rate) is the probability that authorized users are correctly recognized on the total number tested, TNR (True Negative Rate) is the probability of authorized users who are not recognized on the total number tested.

FPR (False Positive Rate) describes the probability of unauthorized users who are recognized over the total number tested.

FNR (False Negative Rate) describes the probability of unauthorized users who are not falsely recognized over the total number tested.

The obtained results from the lip biometric system using the three feature extraction techniques, namely, HOG, LBP and inceptionv3 and two classifiers KNN and SVM are shown in Table II, Fig. 10 for the NITRLipV1 database and Table III, Fig. 11 for the Database1 database.

TABLE II
THE OBTAINED RESULTS FOR THE NITRLIPV1 DATABASE.

Feature Extraction Technique	KNN	SVM
HOG	91.33%	95.20%
LBP	91.76%	94.91%
Inceptionv3	92.42%	97.26 %

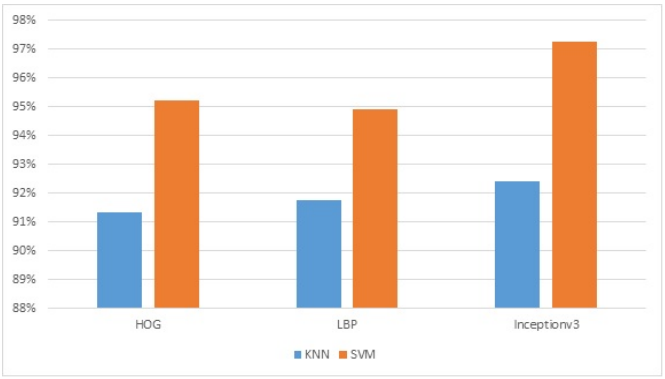


Fig. 10. Recognition Accuracy Rates for the NITRLipV1 Database.

TABLE III
THE OBTAINED RESULTS FOR THE DATABASE1 DATABASE.

Feature Extraction Technique	KNN	SVM
HOG	87.85%	89.14%
LBP	87.96%	88.78%
Inceptionv3	88.31%	90.68 %

From the results reported in TableII, TableIII, Fig. 10 and Fig. 11, we can make the following observations:

1) The accuracy rates provided with the SVM classifier always exceed the results given by the KNN classifier, which clearly proves the powerful of SVM.
2) The pretrained Inceptionv3 CNN model appears to be a great tool for feature extraction, where the highest accuracy rate that is 97.26 % is obtained by SVM classifier for the NITRLipV1 Database.

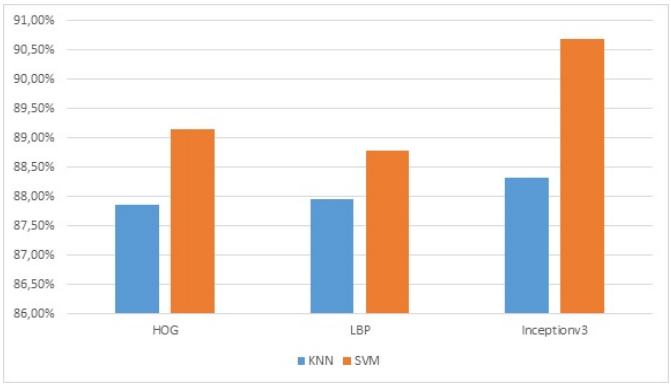


Fig. 11. Recognition Accuracy Rates for the Database1 Database.

3) These results show that lips may be effective biometric modality for identification system.

We are also conducting additional experiments. We use different sizes of training sets to study how the amount of training data affects the accuracy of the test data sets. We randomly choose 20%, 30%, 40%, 50%, 60%, 70%, 80% and 90% images for training. The results are shown in Fig. 12 and Fig.13.

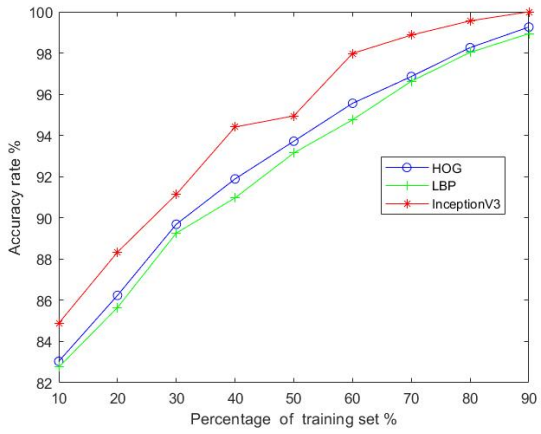


Fig. 12. Accuracy Rate for Different Sizes of Training Set for the NITRLipV1 Database using SVM Classifier.

As shown in Fig. 12 and Fig. 13, the accuracy of all test sets increases as the size of the training set increases and always the results obtained with inceptionv3 are better than HOG and LBP.

V. CONCLUSION AND FUTURE WORKS

In this paper, we have study the efficiency of lips as biometric modality for identification systems using three different techniques for feature extraction, namely, histogram of oriented (HOG), local binary pattern (LBP) and inceptionv3 pre-trained Deep-CNN.

In the recognition step, these feature vectors are used as input data for a K-nearest neighbor (K-nn) or Support Vector Machine (SVM) classifier. From the obtained results, we can

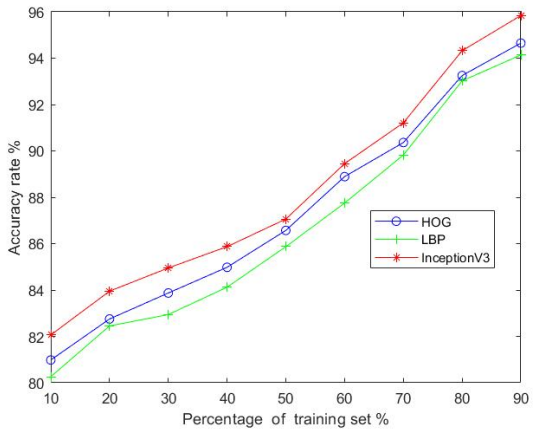


Fig. 13. Accuracy Rate for Different Sizes of Training Set for the Database1 Database using SVM Classifier.

conclude that lip based biometric system offers a promising accuracy rate. This motivates us to investigate in further researches in this field.

In future studies, we aims to expand this research with other lip features and to evaluate the performance of the proposed method using other databases. Also, it is very interesting to implement it in a multimodal biometric system to improve performance of other biometrics.

REFERENCES

[1] M. Choras, "Human lips recognition," in *Computer recognition systems 2*. Springer, 2007, pp. 838–843.

[2] M. Choraś, "The lip as a biometric," *Pattern Analysis and Applications*, vol. 13, no. 1, pp. 105–112, 2010.

[3] M. Ingale, R. Cordeiro, S. Thentu, Y. Park, and N. Karimian, "Ecg biometric authentication: A comparative analysis," *IEEE Access*, vol. 8, pp. 117 853–117 866, 2020.

[4] B. Goudiaby, A. Othmani, and A. Nait-Ali, "Eeg biometrics for person verification," in *Hidden Biometrics*. Springer, 2020, pp. 45–69.

[5] M. Banday and A. H. Mir, "Dental biometric identification system using ar model," in *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)*. IEEE, 2019, pp. 2363–2369.

[6] S. N. G. Dessai and S. Borkar, "Finger nail recognition system using neural network," in *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference on*. IEEE, 2018, pp. 656–659.

[7] S. Das, K. Muhammad, S. Bakshi, I. Mukherjee, P. K. Sa, A. K. Sangaiah, and A. Bruno, "Lip biometric template security framework using spatial steganography," *Pattern Recognition Letters*, vol. 126, pp. 102–110, 2019.

[8] K. Suzuki and Y. Tsuchihashi, "Personal identification by means of lip prints," *J Forensic Med*, vol. 17, no. 2, pp. 52–57, 1970.

[9] S. Vahanwala, C. Nayak, and S. Pagare, "Study of lip prints as aid for sex determination," *Medico-legal update*, vol. 5, no. 3, pp. 93–98, 2005.

[10] S.-L. Wang and A. W.-C. Liew, "Physiological and behavioral lip biometrics: A comprehensive study of their discriminative power," *Pattern Recognition*, vol. 45, no. 9, pp. 3328–3335, 2012.

[11] M. Choraś, "Emerging methods of biometrics human identification," in *Second International Conference on Innovative Computing, Informatio and Control (ICICIC 2007)*. IEEE, 2007, pp. 365–365.

[12] C.-Y. Hsu, C.-H. Yang, Y.-C. Chen, and M.-c. Tsai, "A pso-svm lips recognition method based on active basis model," in *2010 Fourth International Conference on Genetic and Evolutionary Computing*. IEEE, 2010, pp. 743–747.

[13] S. Bakshi, R. Raman, and P. K. Sa, "Lip pattern recognition based on local feature extraction," in *2011 Annual IEEE India Conference*. IEEE, 2011, pp. 1–4.

[14] R. Raman, P. K. Sa, B. Majhi, and S. Bakshi, "Fusion of shape and texture features for lip biometry in mobile devices," *Mobile Biometrics*, vol. 3, p. 155, 2017.

[15] K. Wrobel, R. Doroz, P. Porwik, J. Naruniec, and M. Kowalski, "Using a probabilistic neural network for lip-based biometric verification," *Engineering Applications of Artificial Intelligence*, vol. 64, pp. 112–127, 2017.

[16] W. Zhou, S. Gao, L. Zhang, and X. Lou, "Histogram of oriented gradients feature extraction from raw bayer pattern images," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 5, pp. 946–950, 2020.

[17] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in *2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05)*, vol. 1. Ieee, 2005, pp. 886–893.

[18] H. Wang, J. Hu, and W. Deng, "Face feature extraction: a complete review," *IEEE Access*, vol. 6, pp. 6001–6039, 2017.

[19] D. Huang, C. Shan, M. Ardabilian, Y. Wang, and L. Chen, "Local binary patterns and its application to facial image analysis: a survey," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 41, no. 6, pp. 765–781, 2011.

[20] S. Dey, D. N. Tibarewala, S. P. Maity, and A. Barui, "Automated detection of early oral cancer trends in habitual smokers," in *Soft Computing Based Medical Image Analysis*. Elsevier, 2018, pp. 83–107.

[21] Q. Guan, X. Wan, H. Lu, B. Ping, D. Li, L. Wang, Y. Zhu, Y. Wang, and J. Xiang, "Deep convolutional neural network inception-v3 model for differential diagnosing of lymph node in cytological images: a pilot study," *Annals of translational medicine*, vol. 7, no. 14, 2019.

[22] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 2818–2826.

[23] T. Cover and P. Hart, "Nearest neighbor pattern classification," *IEEE transactions on information theory*, vol. 13, no. 1, pp. 21–27, 1967.

[24] Y. Li and B. Cheng, "An improved k-nearest neighbor algorithm and its application to high resolution remote sensing image classification," in *2009 17th International Conference on Geoinformatics*. Ieee, 2009, pp. 1–4.

[25] C. Cortes and V. Vapnik, "Support-vector networks," *Machine learning*, vol. 20, no. 3, pp. 273–297, 1995.

[26] J. Wei, Z. Jian-Qi, and Z. Xiang, "Face recognition method based on support vector machine and particle swarm optimization," *Expert Systems with Applications*, vol. 38, no. 4, pp. 4390–4393, 2011.

[27] R. Soentpiet, *Advances in kernel methods: support vector learning*. MIT press, 1999.

[28] S. Bakshi, R. Raman, and P. K. Sa, "Nitrlipv1: a constrained lip database captured in visible spectrum," *ACM SIGBioinformatics Record*, vol. 6, no. 1, pp. 1–1, 2016.

[29] "Database1," http://www.biometrics.us.edu.pl/uploads/database1.zip.

An Improved Binary Particle Swarm Optimization of RFM's for ALSAT2 Imagery

O. Mezouar
RCAM Laboratory,Djillali Liabes University
Sidi Bel Abbes, Algeria
ousama31@gmail.com

F. Meskine
RCAM Laboratory,Djillali Liabes University
Sidi Bel Abbes, Algeria
me_fatiha2010@hotmail.fr

I. Boukerch
Space Technology Center
Arzew , Oran, Algeria
issam.boukerch@yahoo.fr

Abstract— **Rational function model (RFM) is commonly used in photogrammetric and remote sensing applications because it does not need sensor parameters. Therefore, the RFM terms or also rational polynomial coefficients (RPCs) have no physical significance but depends on many ground control points (GCPs) that make the model prone to the over parameterization problem. This paper proposes a new binary particle swarm optimization algorithm to surmount the issue of over-parameterization and find the optimum combination of RPCs for the RFM by adding a new transfer function in binary PSO in order to increase the convergence speed and avoid the local minimum phenomenon. The results showed that the proposed method is compatible with different types of RFM, more stable, and gives higher accuracy than the traditional binary PSO.**

Keywords— rational function model, particle swarm optimization, Ortho-rectification, meta-heuristic, high-resolution satellite images

I. INTRODUCTION

One of the most important sources of geographic information systems (GIS) is high-resolution satellite imagery. The high-resolution satellite images are actually used in several contexts at both the industrial and scientific domain [1] but Raw images usually contain some significant geometrical distortions. This distortion depends on the device (airplane or satellite), type of sensor, and the overall field of view, which cannot use the raw images directly in GIS without ortho-rectification in order to correct the geometrical deformations that were introduced during acquisition [2]. Ortho-rectification is the method of transforming an image's central projection into an orthogonal, uniform-scaled view. Thus, the distorting effects of tilt optical projection and terrain relief are removed [3].

The high accuracy potential of ortho-rectification depends on the relationship between images and object spaces [4]. For that, there have been functions and mathematical models developed either through empirical models (such as 2D/3D polynomial or 3D rational functions, RFs) or with rigorous (physical) models [2]. The rigorous models mostly based on the collinear-equation are lack generality because they are complex and its imaging model can differ from one sensor type to another. In addition, parameters such as orbital satellite ephemeris, attitudes, and the physical parameters of the sensor should also be provided for geo-positioning based on a rigorous sensor model; but those parameters may not be accessible because they expose satellite and sensor core technology. Protecting certain key parameters IKONOS, QuickBird and other commercial satellite imagery vendors have adopted empirical models, simpler and more general imaging platform the renowned type and mainly used in empirical models is rational function model (RFM) [3]. There are two methods to solving the RFM named as dependent-terrain and independent-terrain. In the case of the independent terrain, RFM is solved by using the physical sensor model; otherwise in the absence of the sensor parameters, the RFM is solved by using a set of ground control points (GCPs). This solution depending on the number and the distribution of the ground control point on the terrain is known as dependent-terrain method [5].

The independent-terrain approach, RFM necessitates a large number of accurate, well-distributed GCPs which is a time-consuming and costly process. In addition, RFM coefficients or also rational polynomial coefficients (RPC) have no physical significance which makes it difficult to find their best combination [6]. To overcome these problems the binary form of meta-heuristic algorithms can be helpful in optimization and determining the optimum RPCs. Recently, many investigations carried out on the employment of the meta-heuristic approaches for RFM optimizations. Genetic algorithms (GAs) and particle swarm optimization (PSO) are the most useful technique in the literature employed to find the optimum number and combination of RFM parameters.

GA-based approaches for RFM optimization were introduced in [7], [8]. *Zoej et al* in [7] used GA to find an optimum RPC by recommending a three-category division of ground points (GPs): Ground check points (GCPs) are used to estimate RPCs; dependent check points (DCPs) are used to estimate cost functions; and independent check points (ICPs) are used to measure the accuracy of the optimum RFM obtained by the method. In [8] a modified version of GA was employed for RFM optimization. *Jennati* in [8] have suggested using qualified genes in chromosome body to create some genetically modified (transgenic) chromosomes. The conventional PSO and its modified version, known as PSO for rational function optimization (PSORFO), were introduced in [6] and [9] respectively. PSORFO was the first PSO-based approach presented in the RFM literature, that used binary particles to decide whether or not the RPCs where present in the RFM structure and designed to be more likely to omitting coefficients rather than maintaining them. *Yavari* have demonstrates that the binary modified PSO has outperformed GA in terms of computational time and accuracy [6], [9]. Thereafter, PSO's employment has been the subject of several research works as in [10-11].

This paper presents a binary version of PSO (BPSO) to RFM optimization applied for the Algerian satellite (ALSAT2) imagery ortho-rectification. The rest of the paper is organized as follows briefly description of the RFM is presented in section II, the related work presented in section III, implementation and the results are provided in section IV, in section V we described our proposed algorithm, Finally, we give our conclusions in section IV.

II. THEORETICAL BACKGROUND

A. Rational function model RFM

RFM is composed of two mathematical equations which define the spatial relationship between ground space (X,Y,Z) and image space (r,c) using a ratio polynomial [12] as follows :

$$r = \frac{P_1(X,Y,Z)}{P_2(X,Y,Z)} \quad (1)$$

$$c = \frac{P_3(X,Y,Z)}{P_4(X,Y,Z)} \quad (2)$$

Where:

$$P_i = a_{i,0} + a_{i,1}X + a_{i,2}Y + a_{i,3}Z + a_{i,4}XY + a_{i,5}XZ + a_{i,6}YZ + a_{i,7}X^2 + a_{i,8}Y^2 + a_{i,9}Z^2 + a_{i,10}XYZ + a_{i,11}X^3 + a_{i,12}XY^2 + a_{i,13}XZ^2 + a_{i,14}X^2Y + a_{i,15}X^3 + a_{i,16}YZ^2 + a_{i,17}X^2Z + a_{i,18}Y^2Z + a_{i,19}Z^3 \quad (3)$$

Unknown RFCs can be solved with the linearized RFM form [13], [14] as in the following

$$P_1(X,Y,Z) - rP_2(X,Y,Z) = 0 \quad (4)$$

$$P_3(X,Y,Z) - cP_4(X,Y,Z) = 0 \quad (5)$$

The above equations can then be written as follows, by using n GCPs [12]:

$$y = Ax + e \quad (6)$$

Where :
A: design matrix
y: observations vector
e: residuals vector
x: vector of RPCs.

The least-squares (LS) method can be applied to determine RPCs as follows :

$$x = (A^T A)^{-1} A^T y \quad (7)$$

B. Particle Swarm Optimization for RFM optimization

Particle swarm optimization is one of the most common meta-heuristic optimization algorithms inspired by social intelligence and cooperative behavior displayed by various species to fill their needs in the search space. The first version of the particle swarm algorithm developed by James Kennedy and Russell Eberhart in 1995 which works in continuous search space [15], [16].

In RFM optimization, the binary form is applied. The standard binary PSO can be defined by the following equations[15]:

$$v_{ij}(t+1) = w.v_{ij}(t) + c_1 r_1 \left(p_{ij}(t) - x_{ij}(t)\right) + c_2 r_2 \left(p_{gj}(t) - x_{ij}(t)\right) \quad (8)$$

where :
- t is the iteration number.
- v_{ij} is the velocity of the bit j of i^{th} particle bounded within a range of $[v_{min}, v_{max}]$,
- x_{ij} is the position of the bit j of i^{th} particle.
- Pg denotes The best particle of the swarm, that is the particle with the best objective function value, and The best previous position of the i^{th} particle in its own searching trajectory is recorded and represented as P_i.
-W is the inertia weight.

The update function for the position is defined as follows:

$$x_{ij}(t+1) = \begin{cases} 1, & \text{if } r_{ij} < \emptyset(v_{ij}) \\ 0, & \text{otherwise} \end{cases} \quad (9)$$

Each element in the vector velocity is regarded as the input of a normalizing function (transfer function) and usually is a *sigmoid* function [17] which determines the probability in the range of [0,1].

III. THE PROPOSED BINARY PSO FOR RFM OPTIMIZATION (BPSO-RFO)

The algorithm begins with a population of particles which is a set of RFMs structure generated at the first run randomly in a string of the binary values. This implies that each particle is a combination of one and zero, indicating the presence or absence of the corresponding coefficient RPC in the RFM. In this work, the RFM with 78 parameters was used; hence each particle is represented by a string of 78 binary values as indicated in figure bellow.

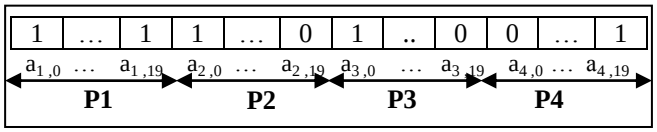


Fig. 1. Particle representation

RFM optimization aims to minimize the number of terms and maintains sufficient accuracies therefore the normalizing function should be structured to be more likely to omit, rather than maintain the terms. Hence in our algorithm called BPSO-RFO the *tanh* function is used as the normalizing function due it deliver successful results as it demonstrated in [9], so the bits updating is performed with eq.9 using the velocity of the bit calculated by eq.8, the normalizing function formula is as follows:

$$\emptyset(v_{ij}) = \begin{cases} \tanh(v_{ij}), & \text{if } v_{ij} > 0 \\ 0, & \text{otherwise} \end{cases} \quad (10)$$

The algorithm is repeatedly updated until a criterion for termination is reached. In this study, we declared the maximum number of iterations (t_{max}) to be termination condition. Fig.2 illustrates the flowchart of our proposed algorithm BPSO-RFO.

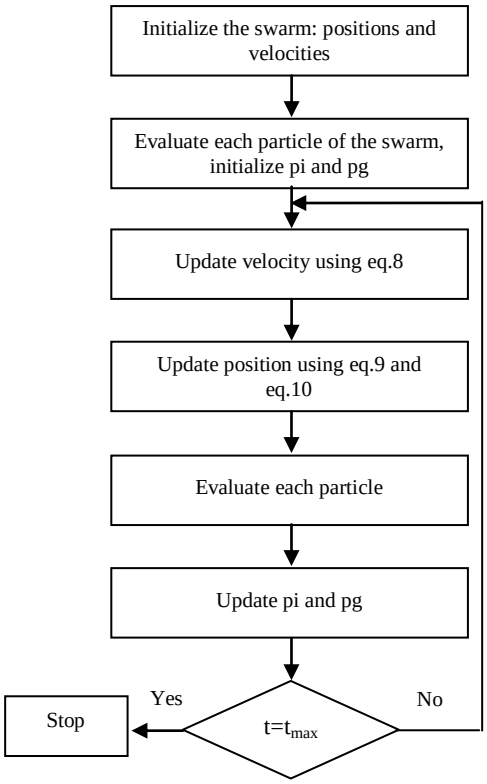


Fig. 2. The flowchart of BPSO-RFO

IV. IMPLEMENTATION AND METHODOLOGY

Two high-resolution images were used for the test, these images acquired by the Algerian satellite ALSAT2 over Winterthur city, Switzerland. The first one "Winterthur_ 1" consists of 18 control points (CPs) and the second "Winterthur_ 2" contain 20 control points (CPs). These CPs detected directly from terrain when the measurements were realized in August 2007 dicted in the repport site of test and validation by [19]. Fig.3 shows Winterthur images of the satellite ALSAT2 within their CPs location.

The RFM optimization process is applied under the CPs in three different parts. First part of these points is employed to estimate the unknown coefficients of the model, which is called Ground Control Points (GCPs). The second part of CPs is used to calculate the fitness value for each particle named Dependent Checkpoints (DCPs). And the last part of these points is used just for accuracy assessment that is addressed as independent check points (ICPs).

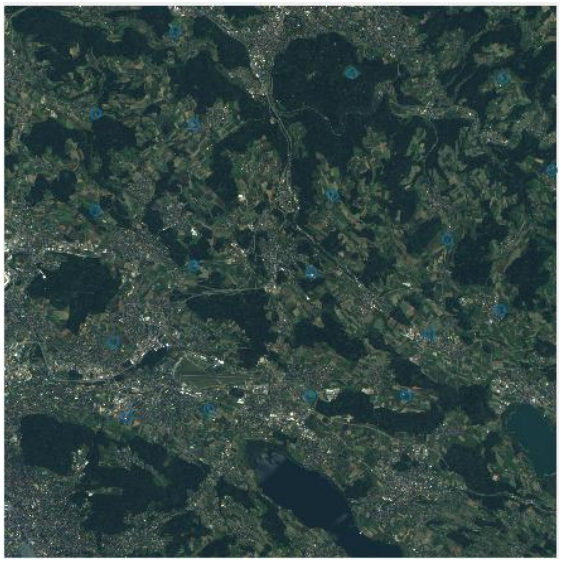
Generally, the most common measure used is Root Mean Square Error (RMSE) given by this equation

$$RMSE = \sqrt{\frac{\sum_{i=1}^{N}(x_i-\hat{x}_i)^2+(y_i-\hat{y}_i)^2}{N}} \quad (11)$$

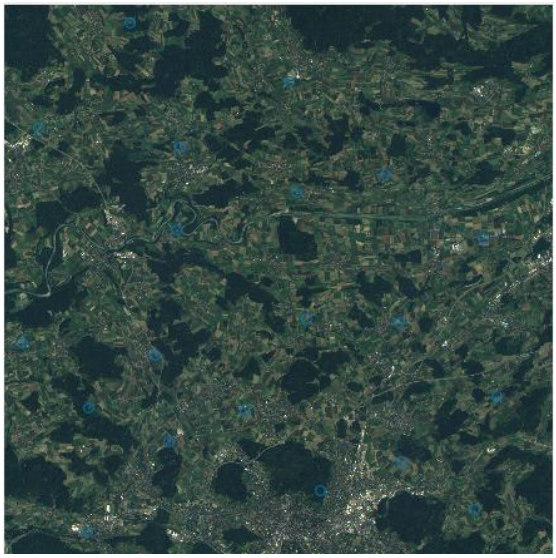
Where:
N is the total number of points, (x_i, y_i) the estimated coordinate (x, y), $(\hat{x}_i, \hat{y}_i)$ denote the actual coordinate (x, y).

We can summarize our methodology of RFM optimization based on the proposed algorithm as follow:

1- Estimation of the RPCs proposed by each particle by using a set of GCPs and the least square method (LS).



(a) Winterthur_1 image



(b) Winterthur_2 image

Fig3. The ALSAT2 test images.

2- Evaluation of each particle by calculating the RMSE over DCPs which is the cost function.

3- Updating the RFM structure according to the BPSO-RFO algorithm. Table I mentions the parameters of the proposing method.

The experiments have been implemented using MATLAB on a personal computer with a 2.40GHz Intel Core i3 CPU and an 8 Gb RAM.

TABLE I
PARAMETERSUSED OF THE BPSO-RFO ALGORITHM

Population size		30
v	v_{max}	+3
	v_{min}	-3
w		0.7
t_{max}		200
C1		1.5
C2		1.5

TABLE II
The accuracy and stability results of different algorithms

Data set	GCP/ICP	RMSE over ICP			STD		
		BPSO-RFO	Conventional PSO	Conventional GA	BPSO-RFO	Conventional PSO	Conventional GA
Winterthur_1	15/3	0.8726	0.9836	**0.8287**	**0.2435**	0.3304	1.6440
	12/6	**0.8839**	1.1383	2.9475	**1.0130**	1.4216	204.4333
	10/8	**1.1363**	4.4652	298.4170	**0.6519**	2.0883e+03	1.0112e+03
	08/10	**1.6471**	205.3063	133.8651	**0.4785**	9.4025	2.7009e+04
	07/11	**1.8783**	175.7524	126.6041	**1.4996e+03**	9.3179e+03	1.7138e+03
Winterthur_2	15/5	**0.8484**	0.8844	0.8781	**0.0822**	0.2578	2.9202
	12/8	**0.8827**	1.4710	0.8976	**1.0938**	2.9363	500.7724
	10/10	**1.2606**	17.0005	15.5123	**2.5304**	421.5296	372.7287
	08/12	**1.6258**	1.0265e+03	742.5804	**231.2884**	2.9080e+03	711.0490
	07/13	**1.9921**	1.0738e+03	780.0430	**126.8536**	2.4229e+03	4.0130e+03

V. Results And Discussion

To evaluate the performance of the proposed algorithm BPSO-RFO, different testing experiments are carried out by selecting different combinations of well distributed GCP/ICP. In all experiments a 20% of the GCPs were selected randomly as DCP to calculate the cost function of each particle. In such issues, the RMSE over DCPs was widely used as a cost function. The accuracy of the obtained results is determined by two measuring criteria: first the RMSE which is calculated over ICPs, second the standard deviation (STD). STD is a proper indicator of stability since it is measured over RMSEs.

Furthermore, a comparison was conducted with the conventional binary PSO and standard GA with the same combinations of GCPs/ICPs. The genetic operators crossover and mutation probabilities used in the experiment are respectively 0.75 and 0.001.

As the meta-heuristic algorithms given a different result in each execution, each algorithm is executed 10 times; the better one with the lowest cost function was selected as the best and mentioned in table II.

The experiments have been divided into two sections: the first is a comparison between our algorithm (BPSO-RFO) to the conventional PSO and GA in terms of accuracy, stability and convergence speed; the second experiment is about the effect of the number of RPCs on the accuracy of our algorithm.

A. The stability and accuracy analysis

As shown in Table II the BPSO-RFO achieve clearly better results than the conventional PSO in all cases and in most cases then the conventional GA in most cases either in term of accuracy or on stability, the value of RMSE over ICP shows the high accuracy of the proposed methods which can optimize the RFMs and obtain a sub-pixel on accuracy just with 12 GCPs. Through table III, we observed that the BPSO-RFO achieved a sub-pixel if the number of GCPs is equal or superior to 12 points and if the number of GCPs is less than 10 the accuracy is degraded in the worst case to 1.99 pixel which is appropriate for photogrammetric and remote sensing applications.

Unlike the conventional PSO and GA which the accuracy value degraded to 1000 pixel this due to the stuck in local minima. In term of stability, our algorithm shows high stability also with 12 and 15 GCPs. In the overall view of the results our method is more stable than both conventional PSO and GA.

When comparing BPSO-RFO to the conventional PSO and GA, it is clear that BPSO-RFO is more accurate and stable, this due to the transfer function eq.10 which is designed to be more omit of the RPC than preserve them, this helped the BPSO-RFO to minimize the number of RPC to the minimum with acceptable accuracy.

B. Convergence speed analysis

To test the convergence speed of the literature methods, the best run among the 10 runs is selected in this section for convergence speed analysis. Fig.4 demonstrates the convergence curve of the literature methods with a different combination of GCPs (15,12,7) for wientherthur1 and wientherthur2 data sets.

As observed in fig.4, the conventional PSO and GA have a slow convergence than BPSO-RFO which is much faster. Our algorithm shows significant performances due to the transfer function that does not just improve the accuracy but also the convergence speed.

C. The effect of RPCs analysis

To validate the effectiveness of the proposed method with different types of RFMs a comparative study is carried out by tested our algorithm for other RFMs with different number of RPC, so we chose the RFM of 18 terms (i.e., $P1$, $P2$, $P3$, and, $P4$: five, four, five, and four terms, respectively) and 42 terms (i.e., $P1$, $P2$, $P3$ and, $P4$: five, four, five, and four terms, respectively), the test is applied to Winterthur1 dataset with a different combination of GCPs (15,12,7). Table III shows the efficiency and compatibility of the proposed method with different types of RFM.

The best result provided with BPSO-RFO is with the RFM of 18 terms because their spaces search range is less than other RFMs (42 terms, 78 terms).

TABLE III
The result of apply BPSO-RFO to different RFM types

GCP/ICP	RMSE over ICP		
	RFM with 18 terms	*RFM with 42 terms*	*RFM with 78 terms*
15/3	**0.8292**	0.8395	0.8726
12/6	**0.6568**	0.7858	0.8839
07/11	1.6922	**1.2126**	1.8783

VI. CONCLUSION

This paper presents a modified binary PSO of RFM optimization for ALSAT2 images ortho-rectification. The proposed binary PSO can achieve a sub-pixel on accuracy with a very limited number of GCPs.

The results obtained demonstrate the performance of our proposed algorithm BPSO-RFO in term of accuracy and stability comparing to the conventional binary PSO and conventional binary GA in the most cases. In term of convergence speed the proposed binary PSO confirm its superiority to other tested method, the BPSO-RFO converges rapidly in most cases less than 60 iteration.

In the last test we apply the BPSO-RFO to different types of RFMs, the results show that the BPSO-RFO is compatible to any RFM types whatever the number of RPC, which make it a good application for RFM optimization.

REFERENCES

[1] O. R. Belfiore and C. Parente, "Comparison of Different Algorithms to Orthorectify WorldView-2 Satellite Imagery," *Algorithms*, vol. 9, no. 4, Art. no. 4, Dec. 2016, doi: 10.3390/a9040067.

[2] T. Toutin, "Review article: Geometric processing of remote sensing images: models, algorithms and methods," *International Journal of Remote Sensing*, vol. 25, no. 10, pp. 1893–1924, May 2004, doi: 10.1080/0143116031000101611.

[3] Z. X. Jeff, "*The Rational Function Model (RFM) in Photogrammetric Mapping: Method and Accuracy*." technical report submitted for the degree of master, May 2004.

[4] Y. Hu, V. Tao, and A. Croitoru, "Understanding the rational function model: Methods and applications," *International Archives of the Photogrammetry, Remote Sensing* , vol. 20, Jul. 2004.

[5] C. V. Tao and Y. Hu, "Use of the Rational Function Model for Image Rectification," *Canadian Journal of Remote Sensing*, vol. 27, no. 6, pp. 593–602, Dec. 2001, doi: 10.1080/07038992.2001.10854900.

[6] S. Yavari, M. J. V. Zoej, M. Mokhtarzade, and A. Mohammadzadeh, "Comparison of Particle Swarm Optimization and Genetic Algorithm in Rational Function Model Optimization," *ISPRS - International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. 39B1, pp. 281–284, Jul. 2012, doi: 10.5194/isprsarchives-XXXIX-B1-281-2012.

[7] M. J. Valadan Zoej, M. Mokhtarzade, A. Mansourian, H. Ebadi, and S. Sadeghian, "Rational function optimization using genetic algorithms," *International Journal of Applied Earth Observation and Geoinformation*, vol. 9, no. 4, pp. 403–413, Dec. 2007, doi: 10.1016/j.jag.2007.02.002.

[8] M. Jannati and M. J. V. Zoej, "Introducing genetic modification concept to optimize rational function models (RFMs) for georeferencing of satellite imagery," *GIScience & Remote Sensing*, vol. 52, no. 4, pp. 510–525, Jul. 2015, doi: 10.1080/15481603.2015.1052634.

[9] S. Yavari, M. J. V. Zoej, A. Mohammadzadeh, and M. Mokhtarzade, "Particle Swarm Optimization of RFM for Georeferencing of Satellite Images," *IEEE Geoscience and Remote Sensing Letters*, vol. 10, no. 1, pp. 135–139, Jan. 2013, doi: 10.1109/LGRS.2012.2195153.

[10] S. H. A. Moghaddam, M. Mokhtarzade, and S. A. A. Moghaddam, "Optimization of RFM's Structure Based on PSO Algorithm and Figure Condition Analysis," *IEEE Geoscience and Remote Sensing Letters*, vol. 15, no. 8, pp. 1179–1183, Aug. 2018, doi: 10.1109/LGRS.2018.2829598.

[11] S. Gholinejad, A. A. Naeini, and A. Amiri-Simkooei, "Robust Particle Swarm Optimization of RFMs for High-Resolution Satellite Images Based on K-Fold Cross-Validation," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 12, no. 8, pp. 2594–2599, Aug. 2019, doi: 10.1109/JSTARS.2018.2881382.

[12] C. V. Tao and Y. Hu, "A comprehensive study of the rational function model for photogrammetric processing," *Photogrammetric engineering and remote sensing*, vol. 67, no. 12, pp. 1347–1358, 2001.

[13] T. Long, W. Jiao, and G. He, "RPC Estimation via L_1-Norm-Regularized Least Squares (L1LS)," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 53, no. 8, pp. 4554–4567, Aug. 2015, doi: 10.1109/TGRS.2015.2401602.

[14] L. Tengfei, W. Jiao and G. He, "Nested Regression Based Optimal Selection (NRBOS) of Rational Polynomial Coefficients," *Photogrammetric Engineering and Remote Sensing*, Mar. 2014.

[15] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proceedings of ICNN'95 - International Conference on Neural Networks*, Nov. 1995, vol. 4, pp. 1942–1948 vol.4, doi: 10.1109/ICNN.1995.488968.

[16] Eberhart and Yuhui Shi, "Particle swarm optimization: developments, applications and resources," in *Proceedings of the 2001 Congress on Evolutionary Computation (IEEE Cat. No.01TH8546)*, May 2001, vol. 1, pp. 81–86 vol. 1, doi: 10.1109/CEC.2001.934374.

[17] J. Kennedy and R. C. Eberhart, "A discrete binary version of the particle swarm algorithm," in *Computational Cybernetics and Simulation 1997 IEEE International Conference on Systems, Man, and Cybernetics*, Oct. 1997, vol. 5, pp. 4104–4108 vol.5, doi: 10.1109/ICSMC.1997.637339.

[18] K. Sastry, D. Goldberg, and G. Kendall, "Genetic Algorithms," in *Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques*, E. K. Burke and G. Kendall, Eds. Boston, MA: Springer US, 2005, pp. 97–125.

[19] A. Gruen and S. Kocaman, "Optical Sensors High Resolution: Geometry Validation Methodology." Technical report submitted to ESA/ESRIN, RFQ/3-11780/06/I-OL, Oct. 2008.

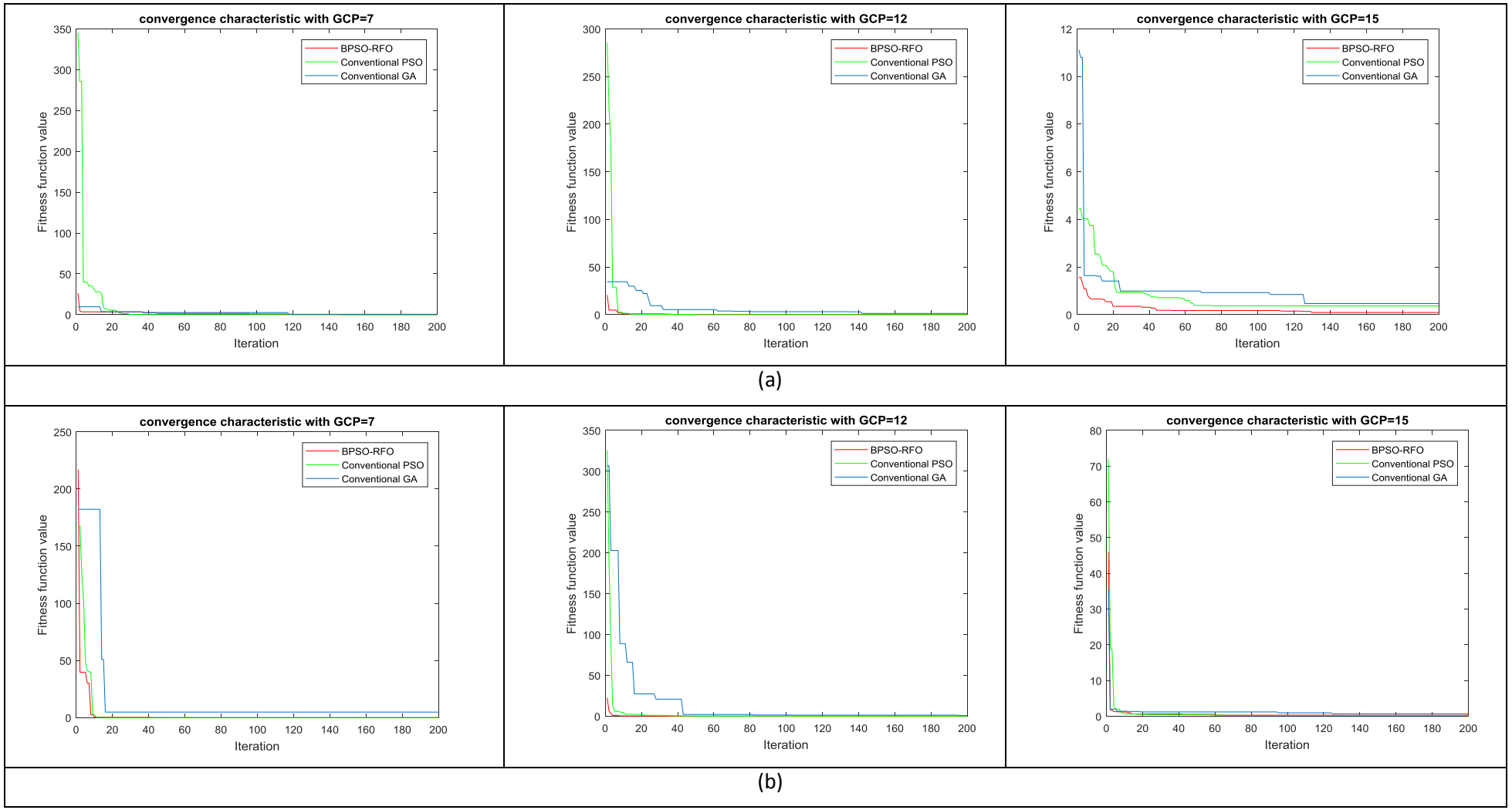


Fig. 4. Convergence characteristic of the tested methods with different number of GCPs and different data set: (a) Winterthur_1 , (b) Winterthur_2

A comparative study of perceptual hashing algorithms: Application on fingerprint images

1st Maamar HAMADOUCHE
University of Science and Technology
Houari-Boumediene, Algiers, Algeria
mhamadouche@usthb.dz

2nd Khalil ZEBBICHE
Military Polytechnic School
Algiers, Algeria
khalil.zebbiche@gmail.com

3rd Mohamed GUERROUMI
University of Science and Technology
Houari-Boumediene, Algiers, Algeria
mguerroumi@usthb.dz

4th Hanane TEBBI
University of Science and Technology
Houari-Boumediene, Algiers, Algeria
htebbi@usthb.dz

5th Youcef ZAFOUNE
University of Science and Technology
Houari-Boumediene, Algiers, Algeria
yzafoune@usthb.dz

***Abstract*—Perceptual image hashing has been broadly used in the literature to authenticate images or to identify similar contents for image copy detection. It can be used to improve the security of fingerprint-based identification systems, especially to guarantee the authenticity of fingerprint images. In this paper, a comparative study of the most used techniques in the field of perceptual hashing is provided, aiming at evaluating their performance when applied to fingerprint images. The study includes five techniques, namely: A-Hash, D-Hash, P-Hash, W-Hash and SVD-Hash. The performance has been assessed in terms of perceptual robustness, discrimination capability and authentication characteristics, through extensive experiments. The obtained results are promising and show that overall both the A-Hash and P-Hash performed well when compared to other evaluated techniques.**

***Index Terms*—perceptual hashing, fingerprint images, robust hashing,**

I. Introduction

With the widespread utilization of fingerprint-based identification systems, establishing the authenticity of fingerprint data itself has emerged as an important research issue. Indeed, it is, in many cases, imperative that the authenticity of the transmitted fingerprint images, for example from intelligence agencies to a central database, must be first verified before it is processed by the identification modules. Recently, perceptual image hashing, which is one of the possible techniques that may be used along with digital watermarking, is becoming one of the most widespread research area and has emerged as an efficient way to check the authenticity of multimedia data (i.e. images and videos) [1].

Perceptual image hashing functions are based on extracting certain robust or invariant features from the image to produce a hash (or a fingerprint) with the property that two completely different images provide uncorrelated hashes while two visually similar images (i.e. perceived as similar by the human eye) generate highly correlated hashes. In this case, an efficient perceptual hashing technique should be able to detect that an image has been derived from another one in a way to remain perceptually similar, even their corresponding files are substantially different [2]. It is meant here by two visually similar images that one image is derived from another via the commonly used content-preserving image manipulations.

In general, an authentication perceptual image hashing system consists of three main phases: the pre-processing stage, the hashing generation stage, and the decision making stage. The main objective of the pre-processing phase is to improve the robustness of features by reducing the effects of possible distortions, by applying image processing operations such as resizing, filtering, color space dimension reduction, etc. In the next phase, the reference hashes are generated and stored in a dataset. In the context of image authentication, the same perceptual hash process is applied to the image to be authenticated to generate a test hash. After that, and at the decision-making phase, the test hash is compared with the reference hashes to check the authenticity of the test image, based on a selected metric such as the Euclidean distance, the Hamming distance, the Normalized Hamming distance, etc. [3].

In the context of authentication applications, the major part of perceptual hashing algorithms can be broadly classified into the following classes : (i) invariant feature transform-based hashing, (ii) local feature points-based hashing, (iii) dimension reduction-based hashing, (iv) statistical features-based hashing, and (v) leaning-based hashing [3]. More details can be found in [4]–[6].

The objective of this paper is to analyze and evaluate the performance of five of the commonly used perceptual hashing techniques when applied to fingerprint images in the context of verifying their authenticity. The evaluated techniques are two spatial domain techniques, namely: the Average hashing (A-Hash) and the Difference hashing (D-Hash), and three frequency domain techniques, including: the DCT-based hashing (P-Hash), the Wavelet-based hashing (W-Hash) and the SVD-based hashing (SVD-Hash). Extensive experiments have been conducted on real fingerprint images, in which we have evaluated the perceptual robustness, the discrimination capability and authentication property of each evaluated technique.

Carrying out this study is motivated by the fact that, and for non expert persons, they perceive fingerprint images as an alternation of curved dark lines, representing the ridges, along with white lines, which represent the valleys and they almost have the same shape. In other word, visually fingerprint images may, in many cases, look the same. Therefore, it is important to analyze how perceptual hashing techniques deal with such kind of images.

The rest of the paper is organized as follows. The evaluated hashing techniques are described in Section II. Evaluation results and analysis are provided in Section III. Conclusions are drawn in Section IV.

II. Perceptual Image Hashing Techniques

In this section, five of the most used perceptual hashing techniques are described. It is worth mentioning that, in this study, we focus on perceptual image hashing algorithms that can produce fast image hashes, while still preserving image identity.

A. A-Hash

The average hashing technique, referred to as A-Hash, is one of the simplest and basic methods used to generate perceptual hashes of images [7]–[9]. This technique produces the hash value of the image based on its low frequencies, which represent the image structure, and eliminates the higher frequencies, corresponding to the image details [10]. For this purpose, the A-Hash uses a number of pre-processing operations including blurring, re-sizing, colors reduction and normalization [8]. It is worth noting that the primary goal of the A-Hash is to find the average color of all the image matrix values by calculating the mean of the matrix. In this study, we followed the same steps cited in [8] to implement this algorithm. These steps are summarized as follows : (i) the input image is resized to a size of 8×8 pixels; (ii) a color space conversion from RGB color space to gray-scale (YCbCr) color space is conducted; (iii) the mean value of all luminance values of the precedent image matrix is calculated; (iv) a comparison of each element of the image matrix and the calculated mean value is done, and a new binary matrix with 64 elements is obtained, where 1 indicates that the intensity of the element is greater than the average and 0 otherwise; (v) construct the vector from the resulting binary matrix, starting from the top left and going to the bottom right, to obtain a 64-bit long hash. The resulting hash can be later compared with other images hashes to retrieve the "similarity score" based on the distance metric between the two hashes.

B. D-Hash

The difference hash technique, also known as D-Hash, is an alternative method and similar to the A-Hash one [11]. Like the A-Hash, D-Hash focuses on the image structure, which is achieved by reducing the image size, i.e. by eliminating the higher frequencies from the image. The main difference between the two techniques is that, the D-Hash generates the hashes by computing the difference hash similarity of the image based on the change of color gradient between adjacent pixels in the image matrix [12], [13]. As for the A-Hash algorithm, we followed the same steps cited in [8] to implement the D-Hash algorithm. These steps are summarized as follows : (i) the image is reduced to a 9×8 block size to produce a total of 72 pixels; (ii) the image is converted to a gray-scale space color; (iii) for each row, we perform a comparison of the difference between each two adjacent pixels, to obtain a total of 8 differences per row; (iv) the 64 differences are computed for each image and then used to build the image hash, so that if the difference value is negative then the hash bit is set to 0, otherwise it is set to 0. At the end, a 64-bit hash is obtained.

C. P-Hash

The perceptive hash, denoted as P-Hash, is a technique that extends the A-Hash method by using the Discrete Cosine Transform (DCT) to obtain the most sensitive information of the human vision system (HVS) [9]. This technique uses the same approach like the A-Hash: finding the mean values and compare [8], but instead of using image intensities to perform the hash generation process, it uses a range of low frequencies obtained after applying the DCT technique [14]. The implementation of P-Hash includes the following steps:(i) the image is resized to a 32×32 pixels matrix; (ii) the obtained image is then converted to the gray-scale space color; (ii) a 32×32 DCT is performed on the gray-scale image to obtain a 32×32 DCT coefficient matrix, where the energy of the image will be gathered into a few low-frequency DCT coefficients; (iv) a vector of length 64 is constructed by concatenating the DCT coefficients from (1,1), corresponding the upper left corner of the 64 size matrix, to the coefficient (8,8), representing the lower right corner; (v) the mean of the resulting coefficients array is computed; (vi) a comparison of the 64 DCT coefficients with the mean value is performed, in a way that the hash bit is set to 1 if the coefficient is greater than the mean value, and 0 otherwise; (vii) finally, a 64 bits binary hash is obtained.

D. W-Hash

The wavelet hash technique, referred to as W-Hash, is a frequency domain hashing technique that uses the Discrete Wavelet Transform (DWT) to generate perceptual hashes. It is based on analyzing the image in the wavelet domain, while retaining temporal information [15]. Note that this transform is often used to remove redundancy in a data with highly correlated neighboring values, such as pixels in images [10]. The original W-Hash was introduced by Venkatesan *et al.* [16], who have described the main steps for implementing this technique as follows: (i) a randomly tilling of each sub-band of the image is calculated in a given number of level wavelet decomposition using the Haar wavelet [17]; (ii) the statistics vector resulting from step 1 is then quantized using a randomized quantizer; (iii) The calculated quantized statistics vector is decoded using a first-order Reed-Muller error-correcting decoder, to produce a binary hash value with a

length n; (iv) finally, the resulting intermediate hash value is passed by another decoding stage of a linear code with random parameters, to transform it into an even shorter hash code.

E. SVD-Hash

The Singular Value Decomposition hash, denoted by SVD-Hash, was first introduced by Kozat *et al.* [18]. The general mechanism of this technique is to derive a secondary image, from the original one using a pseudo-randomly (PR) extracting features that approximately capture semi-global geometric characteristics. Then, the final features are extracted and further suitably quantized to form the final hash value. The SVD-Hash algorithm implementation steps are summarized as follows: (i) from the input image matrix of size $n \times n$, form p possibly overlapping blocks, so that each of them has the size of $m \times m$; (ii) for each resulting block, generate the corresponding feature vector using the SVD transformation ; (iii) generate a secondary image via the PR combination of all intermediate feature vectors; (iv) apply the same steps 1 and 2 to the new resulting image; (v) finally, combine the generated feature vectors from the second image to build the final hash vector.

III. Experimental Results

TABLE I: Content-preserving manipulations and parameters setting

Manipulation	Parameters setting
Gaussian noise (GN)	variance = 0.07
Average filtering (AF)	filter size = 9
Salt & pepper noise (SP)	density = 0.20
Gaussian blurring (GB)	standard deviation = 7
Gamma correction (GC)	gamma = 0.8
Motion blurring (MB)	len = 40, theta = 55
JPEG compression (JC)	quality factor = 40
Median filtering (MF)	filter size = 7
Wiener filtering (WF)	filter size = 7
Image sharpening (SH)	alpha = 0.49
Image scaling (SC)	factor = 0.5

In this section, intensive experiments have been carried out to evaluate the performance of the techniques described in Section II. In all experiments, real fingerprint images from the 'FVC 2000, DB3_a' database [23] have been used. This database contains 800 fingerprint images of size 448×478. Note that these images have been slightly resized to have a size of 448×480 (i.e., having a height and width divisible by 8). Three aspects are considered in our experiments: (i) perceptual robustness, (ii) discrimination capability, and (iii) authentication. Moreover, and in order to make the comparison as fair as possible between the evaluated techniques, the Normalized Hamming distance has been used as a metric to evaluate the similarity between extracted hashes. To perform perceptual robustness and authentication testing, eleven kinds of commonly used content-preserving image manipulations were utilized to produce visually similar images. The details of image manipulations and the corresponding parameter settings are given in Table I.

A. Perceptual Robustness

An efficient perceptual hashing technique should be robust and resist content-preserving manipulations with moderate strength. In other words, for visually similar images, it should produce the same or similar hashes even their digital representations are no longer the same. This characteristic can be measured by evaluating the perceptual robustness. In this work, we conducted a set of experiments to assess the perceptual robustness of the five evaluated techniques. Hence, for every evaluated technique, we extracted the original (reference) hashes from the original 800 fingerprint images and their corresponding manipulated versions under the eleven content-preserving manipulations listed in Table I. Then, the Normalized Hamming distance is calculated between each original hash and its corresponding manipulated hash. The minimum, maximum, and mean values of the resulting distances after each operation are presented in Table II. Note that, to make the comparison as fair as possible, we have normalized the obtained results by mapping them to the same interval.

The obtained results clearly show that, in most cases, the A-Hash technique provides the lowest mean values of the Normalized Hamming distances, computed between reference hashes and their manipulated ones. The P-Hash comes in the second place in most cases. Moreover, the D-Hash shows an acceptable level of robustness against the most manipulations. The least robust technique is the SVD-Hash, where the results clearly show that the applied manipulations affects the Hamming distances significantly. It is worth mentioning that in the absence of manipulations, the Normalized Hamming distances should be equal to 0.

B. Discrimination capability

The discrimination capability of a hashing algorithm, also known as anti-collision capability [21], can be defined as its ability to generate significantly different hashes for visually distinct images. This means that an algorithm with high discrimination capability has a very low probability to generate similar hashes for two perceptually different images [3]. In general, the discrimination capability is evaluated by computing the collision probability of two hashes for two visually distinct images, which is in our case equals to the probability that the Normalized Hamming distance is smaller than the predetermined threshold. According to [20]–[22], the collision probability P_c of the hashes for two visually distinct images is given by

$$\begin{aligned} P_c(T) &= \frac{1}{\sqrt{2}\delta} \int_{-\infty}^{T} exp\left[-\frac{(x-\mu)^2}{2\delta^2}\right] dx \\ &= \frac{1}{2} erfc\left(-\frac{T-\mu}{\sqrt{2}\delta}\right) \end{aligned} \quad (1)$$

where $erfc(.)$ is the complementary error function, T is the predetermined threshold, μ is the mean value, and δ is the standard deviation.

In order to compute P_c, we first need to estimate the parameters μ and δ corresponding to the Normalized Hamming

TABLE II: Normalized Hamming distances under different content-preserving manipulations. Lowest values are in bold.

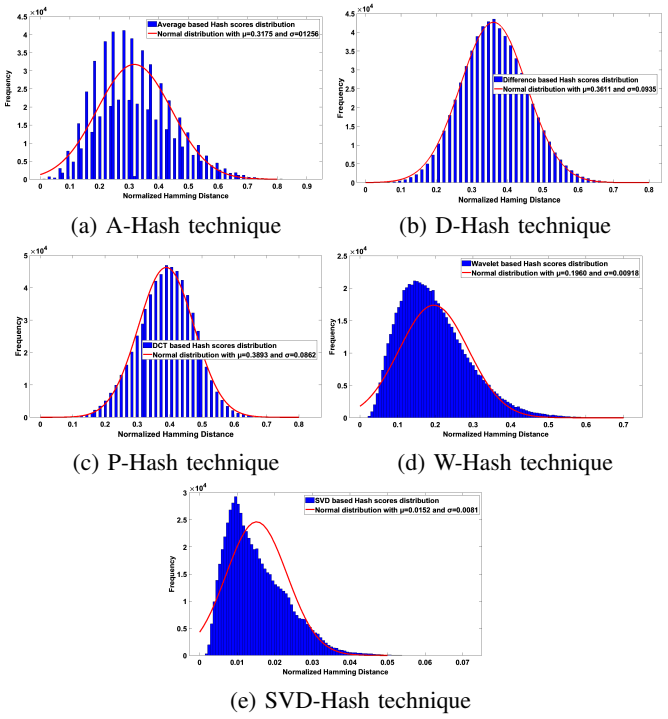
Manipulation	A-Hash			D-Hash			P-Hash			W-Hash			SVD-Hash		
	Min	Max	Mean	Min	Max	Mean	Min	Max	Mean	Min	Max	Mean	Min	Max	Mean
GN	0.000	0.214	**0.035**	0.000	0.375	0.135	0.000	0.273	0.110	0.043	0.385	0.138	0.037	0.567	0.134
AF	0.000	0.156	0.018	0.000	0.119	0.019	0.000	0.097	0.025	0.006	0.035	**0.015**	0.010	0.200	0.058
SP	0.000	0.117	**0.013**	0.000	0.217	0.041	0.000	0.136	0.033	0.022	0.165	0.055	0.021	0.338	0.066
GB	0.000	0.097	**0.008**	0.000	0.127	0.079	0.000	0.097	0.012	0.000	0.029	0.010	0.012	0.214	0.070
GC	0.000	0.097	**0.011**	0.000	0.098	0.016	0.000	0.117	0.020	0.024	0.159	0.071	0.003	0.163	0.032
MB	0.000	0.136	**0.020**	0.000	0.177	0.046	0.000	0.195	0.064	0.000	0.035	0.014	0.014	0.221	0.073
JC	0.000	0.078	**0.001**	0.000	0.039	0.003	0.000	0.039	0.005	0.000	0.010	0.002	0.001	0.012	0.003
MF	0.000	0.253	**0.036**	0.000	0.217	0.048	0.000	0.195	0.055	0.011	0.189	0.043	0.014	0.329	0.066
WF	0.000	0.078	**0.007**	0.000	0.138	0.015	0.000	0.078	0.009	0.000	0.043	0.015	0.009	0.106	0.030
SH	0.000	0.078	0.007	0.000	0.079	0.007	0.000	0.058	**0.003**	0.000	0.030	0.008	0.006	0.083	0.015
SC	0.000	0.078	**0.007**	0.000	0.059	0.010	0.000	0.058	0.008	0.000	0.011	0.001	0.026	0.944	0.235

distance values computed from a large set of visually distinct images. To do so, and for each evaluated technique, we first extracted the reference hashes for all the 800 fingerprint images and then calculated the Normalized Hashing distance for each hash with the other 799 hashes. Consequently, we obtained $800 \times (800-1)/2 = 319600$ Normalized Hashing distances. Then, the values of μ and δ of the obtained Normalized hashing distances are computed by assuming that they all follow a normal distribution. The distribution of these 319 600 distances between hashing pairs, along with the obtained values of μ and δ, for the five evaluated techniques are shown in Fig. 1, where the abscissa is the Normalized Hamming distances and the ordinate represents their frequency. Note that this assumption is widely adopted in the literature [3], [20], [21]. As can be noticed, only the D-Hash and the P-Hash algorithms generate Normalized Hamming distances that follow a normal distribution. The other algorithms are not really approximated by this distribution, and this fact, may lead to a less accurate evaluation of the discrimination capability by the collision probability measure.

After obtaining the parameters μ and δ, we applied Eq. 1 to compute the collision probability P_c for different values of thresholds T. Note that the values of T have been empirically calculated as described in [20]. The obtained results are given in Table III. From these results, one can observe that, the smaller the threshold T is set, the smaller the collision probability is. Furthermore, the collision probability values are close to each other, with a slight superiority of the P-Hash technique.

C. Authentication results

Since perceptual robustness and discrimination are contradictory with each other, we evaluate, in this section, the overall performance of the five evaluated techniques in terms of tampering detection accuracy. This evaluation has been carried out by computing three metrics, namely: the Recall, Precision and F1-measure. The precision expresses the proportion of the images that the hashing algorithm identifies as visually similar and they actually are. Whereas, The Recall is the proportion of similar images that the algorithm identifies as similar. Therefore, Precision measures the accuracy of the algorithm to detect visually similar images, while Recall measures the



(a) A-Hash technique (b) D-Hash technique

(c) P-Hash technique (d) W-Hash technique

(e) SVD-Hash technique

Fig. 1: Distribution of Normalized Hamming distances corresponding to the five tested techniques.

ability of the algorithm to find all the similar images among the dataset [19]. These two metrics are calculated by

$$Precision = \frac{TP}{TP+FP}, Recall = \frac{TP}{TP+FN} \quad (2)$$

where TP is the true positive value which represents the images that have been labeled as similar by the algorithm and they actually are. FP is the false positive value, corresponding to the images that have been labeled as similar by the algorithm, but they are actually not; and FN is the false negative value, representing the images that have been labeled as different by the algorithm, but they are actually similar. The F1-score is the weighted harmonic average of the Precision and the Recall and it can be calculated as follows [19]

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (3)$$

TABLE III: Collision Probability of the five evaluated algorithms with different thresholds T

Technique	Threshold T	Collision probability
A-Hash	0.02	0.89×10^{-2}
	0.04	01.36×10^{-2}
	0.06	02.02×10^{-2}
	0.08	02.93×10^{-2}
	0.10	04.17×10^{-2}
	0.12	05.79×10^{-2}
D-Hash	0.04	0.03×10^{-2}
	0.08	0.13×10^{-2}
	0.12	0.50×10^{-2}
	0.16	01.57×10^{-2}
	0.20	04.24×10^{-2}
	0.24	09.76×10^{-2}
P-Hash	0.04	0.00×10^{-2}
	0.08	0.02×10^{-2}
	0.12	0.09×10^{-2}
	0.16	0.39×10^{-2}
	0.20	01.40×10^{-2}
	0.24	04.16×10^{-2}
W-Hash	0.004	01.82×10^{-2}
	0.008	02.03×10^{-2}
	0.012	02.25×10^{-2}
	0.016	02.50×10^{-2}
	0.020	02.76×10^{-2}
	0.024	03.05×10^{-2}
SVD-Hash	0.0008	03.77×10^{-2}
	0.0010	03.98×10^{-2}
	0.0012	04.20×10^{-2}
	0.0014	04.42×10^{-2}
	0.0016	04.66×10^{-2}
	0.0018	04.90×10^{-2}

Note that higher values indicate better performance for these three metrics.

The same set of tests described in Section III-A has been performed to compute the three aforementioned metrics and the predetermined thresholds are chosen to provide the best results and are set as follows : A-Hash: $T = 0.04$, D-Hash : $T = 0.06$, P-Hash: $T = 0.08$, W-Hash: $T = 0.018$ and SVD-Hash: $T = 0.0018$. The obtained results are given in Table IV. As it can be observed, and by evaluating the performance of each technique against a specific content-preserving operation, the results obtained from Table IV can be described as follows:

- For the Gaussian noise manipulation, the P-Hash is the most powerful technique with a F1-score value of 0.651, whereas the W-Hash and SVD-Hash have not resisted to this attack and were unable to calculate the F1-score with Recall and Precision values of zero.
- For the Average filtering, the three techniques W-Hash, D-Hash and P-Hash performed very well and provide F1-score values of 0.981, 0.941 and 0.935 respectively. The worst technique is the SVD-Hash which generates a poor value of F1-score, equals to 0.191.
- For Salt & pepper noise addition, the P-Hash technique is in the first place with a F1-score value of 0.953, followed by the D-Hash technique with a F1-score value of 0.860, while the the SVD-Hash and W-Hash are the last-rank techniques with F1-score values of 0.253 and 0.015, respectively.
- For the Gaussian blurring, the most powerful techniques are W-Hash, D-Hash and P-Hash with F1-score values of 0.988, 0.941 and 0.939, respectively. The worst technique is SVD-Hash with a F1-score value of 0.093.
- For the Gamma correction manipulation, both D-Hash and P-Hash techniques performed well with F1-score values of 0.946 and 0.934, respectively. The W-Hash technique is the worst one with a F1-score value of 0.007.
- For the Motion blurring operation, the most successful techniques are the W-Hash, the P-Hash and the D-Hash with F1 score values of 0.979, 0.901 and 0.840, respectively. The worst performance is obtained by the SVD-Hash algorithm, which produces a F1-score value of 0.068.
- For the JPEG compression, all techniques performed well and provide good F1-score values, particularly, the W-Hash and the SVD-Hash, which have the highest F1-score values of 0.989 and 0.964, respectively. The A-Hash has generated the lowest F1-score value of 0.640.
- For the Median filtering, the best techniques are the P-Hash and the D-Hash with F1-score values of 0.892 and 0.828, respectively. The worst techniques are the SVD-Hash and the W-Hash with F1-score values of 284 and 0.277, respectively.
- For the Wiener filtering, almost all techniques performed well and the most successful ones are the W-Hash, the D-Hash and the P-Hash with F1-score values of 0.948, 0.944 and 0.937, respectively. The worst technique is the SVD-Hash which generates F1-score value of 0.627.
- For Image sharpening operation, except the A-Hash technique which yields a low F1-score value of 0.638, the other techniques were robust to this operation, and they all produce F1-score values over 0.951.
- For Image scaling operation, almost all techniques have resisted to this operation, except for the SVD-Hash algorithm which performed very poorly and provides a F1-score value of 0.005. The most robust algorithms are the W-Hash, the D-Hash and the P-Hash with F1-score values of 0.989, 0.953 and 0.937, respectively.

Overall, the most successful technique is P-hash, which achieves a F1-score value of 0.905 at a Precision value of 0.890 and a Recall value of 0.933. The second one is the D-hash, which reaches a F1-score value of 0.849 at a Precision value of 0.892 and a Recall value of 0.856. The next successful technique is the W-hash, which yields a F1-score value of 0.651 at a Precision value of 0.815 and a Recall value of 0.640. The forth place was assigned to the A-Hash algorithm, with a F1-score value of 0.614 at a Precision value of 0.461 and a Recall value of 0.915. Finally, the worst performance is obtained by the SVD-hash algorithm, which generates a F1-score value of 0.369 at a Precision value of 0.468 and a Recall value of 0.340.

TABLE IV: Quantitative comparisons using the Recall, Precision and F1-measure metrics. Best results are in bold.

Manipulation	A-Hash			D-Hash			P-Hash			W-Hash			SVD-Hash		
	Prec.	Recall	F1	Prec.	Recall	F1	Prec.	Recall	F1	Prec.	Recall	F1	Prec.	Recall	F1
GN	0.456	0.722	0.559	0.818	0.101	0.180	0.886	0.494	**0.651**	NaN	0.000	NaN	NaN	0.000	NaN
AF	0.461	0.899	0.609	0.912	0.971	0.941	0.878	1.000	0.935	0.984	0.977	**0.981**	0.240	0.159	0.191
SP	0.474	0.947	0.632	0.895	0.827	0.860	0.916	0.994	**0.953**	0.750	0.007	0.015	1.000	0.145	0.253
GB	0.472	0.976	0.636	0.894	0.992	0.941	0.886	1.000	0.939	0.979	0.997	**0.988**	0.087	0.100	0.093
GC	0.477	0.967	0.639	0.911	0.985	**0.946**	0.877	0.999	0.934	0.428	0.004	0.007	0.752	0.589	0.660
MB	0.441	0.889	0.590	0.906	0.784	0.840	0.944	0.862	0.901	0.979	0.979	**0.979**	0.064	0.072	0.068
JC	0.441	0.996	0.640	0.909	1.000	0.952	0.884	1.000	0.938	0.979	1.000	**0.989**	0.930	1.000	0.964
MF	0.427	0.707	0.532	0.901	0.766	0.828	0.872	0.914	**0.892**	0.935	0.162	0.277	0.342	0.242	0.284
WF	0.467	0.986	0.634	0.902	0.991	0.944	0.881	1.000	0.937	0.979	0.920	**0.948**	0.724	0.554	0.627
SH	0.471	0.989	0.638	0.909	0.996	0.950	0.889	1.000	0.941	0.977	0.994	**0.985**	0.956	0.877	0.915
SC	0.482	0.987	0.648	0.911	1.000	0.953	0.882	1.000	0.937	0.978	1.000	**0.989**	0.052	0.002	0.005
Mean	0.461	0.915	0.614	0.897	0.856	0.849	0.890	0.933	**0.905**	0.815	0.640	0.651	0.468	0.340	0.369

IV. Conclusion

In this work, we studied and analyzed the performance of five of the commonly used and fastest perceptual hashing techniques when considering fingerprint images, which visually have almost the same shape (i.e. alternation of ridges and valleys). This study involves the following techniques: the A-Hash, the D-Hash, the P-Hash, the W-Hash and the SVD-Hash. It has been performed through a set of extensive experiments applied to real fingerprint images and has focused on assessing three major aspects, namely: perceptual robustness, discrimination capability and authentication capacity. The obtained results are very interesting. Indeed, for the perceptual robustness property, the A-Hash technique clearly outperforms the other techniques and shows more robustness against the major part of the applied manipulations. For the discrimination capability, the evaluated techniques provide close performance in terms of the probability of collision, with a slight superiority for the P-Hash technique. In regard to the authentication property, which represents the overall performance, the P-Hash has provided the best results, when considering the whole set of applied manipulations.

Although these results are promising, they show that there is no best technique and the choice of a perceptual hashing technique will depend on the context in which it is used. As future works, this study can be extended to include more sophisticated hashing techniques and apply them to other fingerprint databases with different visual aspects, such as the background color, the shapes (flat or rolled), sensor types, etc.

References

[1] F. Khelifi and A. Bouridane, "Perceptual Video Hashing for Content Identification and Authentication", IEEE Trans. Circuits Syst. Video Technol., vol. 29, 2019.

[2] R. Gennaro, D. Hadaller, T. Jafarikhah, Z. Liu, W. E. Skeith and A. Timashova "Publicly Evaluatable Perceptual Hashing" in Applied Cryptography and Network Security, Springer, 2020, pp. 436-455.

[3] L. Du , Z. He, Y. Wang, X. Wang and A. T. S. Ho, "An Image Hashing Algorithm for Authentication with Multi-Attack Reference Generation and Adaptive Thresholding", Algorithms, vol.13, pp.227, 2020.

[4] L. Du, A.T.S. Ho and R. Cong, "Perceptual hashing for image authentication: A survey", Signal Process. Image Commun., vol. 81, 2020.

[5] A. Hadmi, W. Puech, B. A. E. Said and A. A. Ouahman, "Perceptual image hashing", in: Watermarking, Vol. 2, 2012, pp. 17–42.

[6] K. Alice and N. Ramaraj, "Combining hashing techniques in image authentication system:a survey", Int. J. of Scientific Research, Vol. 4, 2015 528– 530.

[7] S. F. C. Haviana and D. Kurniadi, "Average hashing for perceptual image similarity in mobile phone application," J. of Telematics and Informatics, vol. 4, no. 1, pp. 12–18, 2016.

[8] V. Popkov, "Possible application of perceptual image hashing", Master thesis, Tallinn University Of Technology, 2015.

[9] M. Fei, Z. Ju, X. Zhen and J. Li, "Real-time visual tracking based on improved perceptual hashing", Multimed. Tools Appl., 2016.

[10] A. Drmic, M. Silic, G. Delac, K. Vladimir and A. S. Kurdija, "Evaluating robustness of perceptual image hashing algorithms," 40th Int. Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2017, pp. 995-1000.

[11] R. Fitas, B. Rocha, V. Costa and A. Sousa, "Design and Comparison of Image Hashing Methods: A Case Study on Cork Stopper Unique Identification" J. Imaging, vol. 7, no. 3, pp. 48, 2021.

[12] D-Z. Wang and Jun-yan Liang (2019), "Research and Design of Theme Image Crawler Based on Difference Hash Algorithm", IOP Conf. Ser.: Mater. Sci. Eng. 563 042080.

[13] N. Karunanayake, J. Rajasegaran, A. Gunathillake, S. Seneviratne and G. Jourjon (2020), "A Multi-modal Neural Embeddings Approach for Detecting Mobile Counterfeit Apps: A Case Study on Google Play Store," in IEEE Trans. Mob. Comput., doi: 10.1109/TMC.2020.3007260.

[14] F. Vega, J. Medina, D. Mendoza, V. Saquicela and M. Espinoza (2017), "A robust video identification framework using perceptual image hashing," 2017 XLIII Latin American Computer Conference (CLEI), Cordoba, Argentina, 2017, pp. 1-10.

[15] W.-C. Huang, F. Di Troia and M. Stamp, "Robust Hashing for Image-based Malware Classification", the 15th Int. J. Conf. on e-Business and Telecommunications (ICETE 2018) - Volume 1: DCNET, ICE-B, OPTICS, SIGMAP and WINSYS, 2018, pp. 451-459.

[16] R. Venkatesan, S.-M. Koon, M.H. Jakubowski, P. Moulin, "Robust image hashing". IEEE Int. Conf. on Image Processing, Vancouver, Canada, 10–13 September 2000, pp. 664–666.

[17] E. Aboufadel and S. Schlicker, Wavelets Introduction, Encyclopedia of Physical Science and Technology, 3rd ed., 2003.

[18] S.S. Kozat, R. Venkatesan and M. K. Mihcak,, "Robust perceptual image hashing via matrix invariants", IEEE Int. Conf. Image Processing (ICIP 2004), October 24–27, 2004, pp. 3443–3446.

[19] M. Grandini, E. Bagli and G. Visani, "Metrics for multi-class classification: An overview", white paper, arXiv:2008.05756v1 [stat.ML], 13 Aug 2020.

[20] L. Du , Z. Chen and A. T. S. Ho, "Binary multi-view perceptual hashing for image authentication", Multimed. Tools Appl., 2020.

[21] C. Qin, X. Chen, J. Dong and X. Zhang, "Perceptual Image Hashing with Selective Sampling for Salient Structure Features", Displays, vol.45, pp. 26-37, December 2016.

[22] C. Qin, M. Sun, C-C. Chang, "Perceptual hashing for color images based on hybrid extraction of structural features", Signal Processing, vol. 142, pp. 194–205, January 2018.

[23] "Fingerprint verification competition", http://biometrics.cse.msu.edu/fvc00db/index.html.

Robust characteristics for texture classification

AYOUB MAAROUF ABDERRAZAK
l'aboratoire d'Automatique et de Robotique
Département d'Electronique, Université des frères Mentouri Constantine 1 Algerie
ayoub.maarouf@umc.edu.dz

FELLA HACHOUF
l'aboratoire d'Automatique et de Robotique
Département d'Electronique, Université des frères Mentouri Constantine 1 Algerie
hachouf.fella@gmail.com

***Abstract*—In this paper, an exhaustive search for relevant characteristics for automatic texture classification has been carried out. These features have been extracted from different cooperative methods dealing with texture characterization. An optimal features vector has been constructed using genetic algorithms (GA) to avoid characteristics redundancy . Then texture classification has been performed using multi-class SVM, k-nearest neighbors, and random forest classifier algorithms. Obtained results on three texture databases are very satisfying against those produced by existing methods.**

***Index Terms*—texture, classification, genetic algorithms, optimal features, machine learning**

I. Introduction

Texture is one of the most relevant characteristics used to identify objects or regions of interest in an image. Also, texture analysis is one of the central concepts in computer vision [1]. One can identify four major issues on texture analysis: texture synthesis, classification, segmentation, and shape from texture. This work is concentrated on texture classification problems. It consists on the issue of distinguishing objects by there different textures [2, 3]. Thus, the given technique's target is to assign any unknown or test image to at least one of the set of previously known texture classes. Previous works found that the majority of the machine vision-based texture classification techniques have combined texture features with classifiers to supply reasonably good classification accuracy for various images [4, 5]. Texture features provide important information about the primitives that constitute a texture and relationship[6]. Several approaches have been proposed to represent texture. statistical features including co-occurrence matrices [7, 8], Weber Local Descriptor (WLD) [9], Local Binary Pattern (LBP) [10],autocorrelation-based and registration-based features[11]. Structural features include primitive measurements [12], edge measure [13], and morphological operation features. Filter features consist in spatial domain filtering [14], frequency domain analysis [15], and common spatial-frequency methods [16]. Additionally, model-based features include fractal models [17] and auto-regressive models [18].(FIg.1)

In this work, discriminating feature extraction methods have been considered: statistical, structural, model-based, and graph-based approaches. A judicious characteristics vector has been constructed and optimized using genetic algorithms. Because the relevant used features are issued from different methods, their effects cooperate to characterise a texture, yielding to an optimal features vector. Local binary feature Pattern(LBP), histogram of oriented Gradient (HOG), a two random coefficient auto-regressive model(2D-RCA), and the weber descriptor (WLD) have been chosen to construct our characteristics vector because of the different texture information they provide. A multi-class SVM, K-NN and Random Forest algorithms have been used to classify various texture images. Performances of each classifier using the same constructed vector have been estimated and discussed. This study aims to search the utility of mixing various texture features with different kind of information to classify image databases. The remainder of this paper is as follows: Section 2 presents the texture features. Section 3 is dedicated to the different used classifiers. Experimental results carried out on three databases are discussed in section 3. Section 4 concludes the paper and offers future work.

Classes	Methods
Statistical approaches	- Grey level co-occurrence matrix - Grey level run-length matrix - Autocorrelation-based approaches - Histogram of gradient magnitudes - Local mapped patterns-based approaches - Local energy pattern - Variogram - Tamura features - Local binary pattern and variants - Shape index histograms - Weber local descriptor - Deterministic walk
Structural approaches	
Transform-based approaches	- Filter banks: Law's texture features - Fourier transform-based approaches - Gabor decomposition-based approaches - Wavelet-based approaches - Shearlet-based approaches - Contourlet-based approaches - Locally encoded transform feature histogram (LETRIST)
Model-based approaches	- Complex network-based approach - Mosaic models - Random field models - Fractal-based measures - Gravitational models - Wold decomposition
Graph-based approaches	- Local graph structures - Graph of tourist walk approach - Shortest paths in graphs
Learning-based approaches	- Vocabulary learning methods - Extreme learning machine-based methods - Deep learning methods
Entropy-based approaches	- Two-dimensional sample entropy - Two-dimensional distribution entropy - Two-dimensional multiscale entropy

Fig. 1. texture features classes.

II. TEXTURE FEATURES

In this section, A brief description of the used parameters is given.

A. Local binary Pattern (LBP)

Local Binary pattern is a standard feature descriptor used for texture classification[10]. since its presentation by Ojala methods in 1994, LBP have shown a strong ability to describe a region . A 3x3 window is used in opposition to the local pixels to plot an exciting surface and think about a close-by double example (LBP).

The LBP approach uses a binary pattern to represent each image pixel qc. It is dependent on the difference between the pixel qc's grey level value and the radius R of its circular neighborhood centered at qc. As a result, the LBP codes are calculated as follows.

$$LBP_{P,R}\left(q_c\right) = \sum_{p=0}^{P-1} s(x)2^p \tag{1}$$

where x=qp-qc is the difference between the intensity levels of the neighboring pixels (qp) and the central pixel (qc),s(x) is:

$$s(x) = \begin{cases} 1 & x \geq 0 \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

for more detail see [10].

B. 2D RCA PARAMETERS

This calculation's initial step comprises characterizing the texture with the 2D-RCA models presented by equation.3. The 2D-RCA model is an expansion of the 2D-AR model presented to show some non-Gaussian spatial informational collection, for example, image digitization. Its development was enlivened by the renowned 1D-RCA model broadly utilized in econometric displaying and designing applications. A 2D stochastic cycle follows a 2D-RCA model. The 2D-RCA models proposed in [19] have been drawn on a standard network. The more significant part of the image we measure is made of matrices with sporadic pixels. Luckily, In a few circumstances, information with sporadically divided pixels can be supplanted by an ordinary network utilizing image insertion methods and re-testing programs.

$$X(t) = \sum_{\mathbf{s}\in]\mathbf{0};P]} a_{\mathbf{s}}(\mathbf{t})x(\mathbf{t}-s) + e(\mathbf{t}), \mathbf{t} \in Z^2 \tag{3}$$

Under stationary conditions, the estimation of the 2D RCA model given by Equation (3) is achieved by the generalized method of moments (GMM) [20]. Based on the observations the GMM estimator of

$$\theta = (\alpha, \beta, \gamma) \tag{4}$$

is:

$$\hat{\theta}_n = \sum_{i=1}^{n}\sum_{j=1}^{m} \lfloor \underline{x}(i,j)\underline{x}'(i,j) \rfloor^{-1} \times \sum_{i=1}^{n}\sum_{j=1}^{m} \lfloor \underline{x}(i,j)X(i,j) \rfloor \tag{5}$$

Where:

$$\underline{\mathrm{x}} = (X(i,j-1); X(i-1,j); X(i-1,j-1)) \tag{6}$$

for more details see[19]

C. Weber Local Descriptor

Weber's law (a psychological law) is the foundation for the Weber local descriptor (WLD) [9]. There are two sections of this descriptor. As a result, two components of the WLD function are calculated for each pixel of the image under research: differential excitation and gradient orientation.

$$\begin{aligned} \xi\left(I_c\right) &= \arctan\left[\sum_{i=0}^{p-1}\left(\frac{i_i^- l_c}{I_c}\right)\right] \\ \theta\left(I_c\right) &= \operatorname{median}\left\{\frac{I_{R(i+4)}-I_i}{I_{p(i+1)}-I_{p(i+2)}}\right\}; i = 0, 1, \ldots p-1 \end{aligned} \tag{7}$$

Ic is the central pixel of a given neighborhood, and Ii is an Ic's neighbor.

The ratio between the relative intensity differences of a current pixel against its neighbors and the current pixel's intensity determines the differential excitation variable. The gradient orientation of the current pixel is the orientation variable. As a result, the descriptor is influenced by both the local intensity difference and the size of the intensity of the middle pixel. Then, WLD concatenates these two components of all pixels to construct a final histogram.

D. Histogram of oriented Gradient (HOG)

Histogram of oriented Gradient features is one of the most descriptors of images. The hog features consist to describe an image by a set of local histograms. Then, the occurrences of gradient orientation are assembled in a small spatial localized part of the image. The subsequent concatenation of 1-D histograms produces the features vector. Let the image's intensity value be analyzed is L. If the image is divided into N x N cells of size. The orientation θx,y of the gradient in each pixel is calculated using Equation (7).

$$\theta_{x,y} = \tan^{-1}\frac{L(x,y+1) - L(x,y-1)}{L(x+1,y) - L(x-1,y)} \tag{8}$$

The successive orientation θ_i^j, i=1……..N2 belonging to the same cell j is quantized and accumulated into an M-bins histogram. Then, the histograms accumulated into a single HOG histogram.

E. FILTER BANKS: LAW'S TEXTURE FEATURES

The application of basic filters to digital images is used in this feature extraction process. It consists of two stages[21]. To generate twenty-five 3×3 or 5 ×5 masks, multiple 1D arrays are convolved together in a combinatorial way . The texture field is then convolved with the latter to emphasize its micro structure. This yields to an image from which the micro structure's energy (and other statistics) can be calculated. Second, macrostatistic characteristics are derived from data collected over time. Five 1D arrays (size of 5) have been specified by Laws:

- Level L5 D [1 4 6 4 1]

- Edge E5 D [-1 - 2 0 2 1]
- Spot S5 D [-1 0 2 0 - 1]
- Wave W5 D [-1 2 0 - 2 1]
- Ripple R5 D [1 - 4 6 - 4 1].

Steerable filters have also been proposed for directed textures. They are a group of orientation-selective filters created by combining a linear combination of basis filters. Unser and Eden [22] have suggested a nonlinear transformation and an iterative Gaussian smoothing algorithm to create an analogous filter bank. At the performance of this analogous filter bank, the local statistics (texture energy measures) are computed. Mellor et al. [23] suggested a system based on invariant linear filter combinations in 2008. This method consists of two steps: the first is to compute two descriptors for each point in the image. The polar-separable filters form the Hessian matrix, and the eigenvectors (principal directions) and eigenvalues (principal curvatures) of the matrix are then computed. These eigenvectors and eigenvalues are then converted to local phases and energies. Contrast transitions, intensity shifts, rotations, and scaling have little impact on these descriptors locally. They're also resistant to skewing. The texture is then interpreted using these descriptors' first order statistics.

F. LOCAL GRAPH STRUCTURES

The characteristics of local graph structures are derived from the texture. A graph of points is used to represent the image [24]. Local graph systems are involved by a specific function on a pixel's six neighbors. As a threshold, the target pixel I(x; y) is selected. By rotating anti-clockwise at the left region of I(x; y), the neighbors pixels of I(x; y) are "visited" (x; y). If the neighbor pixel has a higher (or equal) grey value than (as) I(x; y), the edge separating the two vertices is given a binary value 1, otherwise a binary value 0 is assigned. When the left region is completed. The same procedure is repeated in an horizontal (clockwise) direction on the graph's right side. The decimal value is then calculated using the generated string. The expanded local graph form was suggested in 2016. In order to collect more spatial detail, the latter takes into account both the vertical and horizontal graphs. As a result, we have two descriptors. For each descriptor, an histogram is generated independently. The attributes of the two histograms are then combined to create a global descriptor.

III. FEATURE SELECTION USING GA

the amount of information carried out by the feature vector is too huge, for large images execution time and required memories space are increased. A solution to resolve this problem is to optimize the number of features.hence irrelevant features are taken of the characteristics vector avoiding data redandinding and time and space consuming.thus GA have been used to optimize this vector.

The next step after extracting features involves the combination of all features extracted to get more accurate results. The dimensions for the fused feature vector are 1×44 for each image. The high dimensional features increase the system execution time and space requirement for processing. For that, the feature selection techniques are used to find a subset of most relevant features from irrelevant data, where not pertinent denotes the redundant features, these fused features are fed to GA for feature optimization[25]. Here a GA approach is utilized for feature selection having cost function mean squared error (MSE). The best-selected features are fed to all classifiers used in the presented method for classification. In the presented work, a feature selection technique is used to improve the classification accuracy's performance to remove the redundancy between features.

The essential components of Genetic algorithms are:

1) Initial population of chromosomes: Let m be the number of features. The size of population is N. To create random population P of N number of chromosomes is given below: P = [C1, C2, ... CN]
2) Fitness function: mean squared error is used to evaluate the fitness of each individual population.
3) Selection: Select two parents from population according to their best fitness, which can generate new offspring. It assures that only the best fittest solutions made to generate offspring.
4) Recombination or Crossover: Recombinant the parents to form new offspring from two parents string, by copying selected bit of each parents.
5) Mutation: after the performance of crossover, mutate the new offspring from single parent. It reduces local optimum.

IV. TEXTURE CLASSIFICATION

The above-presented characteristics have been extracted from textured images. efficiency of each feature has been tested using three machine learning classifiers (multiclass SVM, K-NN, Rf algorithms). Then, the classification has been performed using the concatenation of these features as a data vector for each classifier; the proposed method is presented in fig 2.

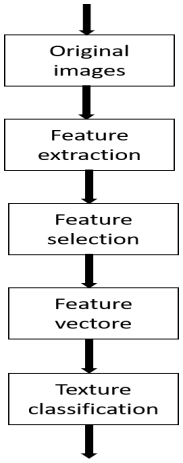


Fig. 2. proposed method.

A. SUPPORT VECTOR MACHINE (SVM)

Support vector machine is a supervised machine learning models. The objective is to find the optimal hyper plane to separate sets of feature vectors into two classes[26]. The SVM training rule devises a model that appends new samples (test data) to one of the two classes. Another significant advantage of exploitation SVM is that it will effectively perform nonlinear classifications by exploiting applicable kernel performance. The rule uses a nonlinear kernel function rather than each real number. The Gaussian radial basis (RBF) is employed because of this paper's kernel function. The radial basis performs on two samples xi, and xj is of the form:

$$K\left(\mathrm{x}_i, \mathrm{x}_j\right) = \exp\left(-\frac{\left\|x_i - x_j\right\|^2}{2\sigma^2}\right) \tag{9}$$

Support Vector Machines designed for binary classification. When it addresses many categories, as in object in image classification, one needs an appropriate multi-class method. Different possibilities include: Modify the design of the SVM, as in, to incorporate the multi-class learning directly in the quadratic solving algorithm. x Combine several binary classifiers: "One-against one" (OAO) applies wise pair comparisons between classes, while "One-against-All" (OAA) compares a given class with all the others put together.

B. K NEAREST Neighbors

A popular non-parametric technique employed for classification and multivariate analysis is the k-Nearest Neighbors (k-NN) algorithm [27]. The k-NN algorithm measures the distance between an objective purpose and a collection of points in the data set. It assigns the target (test) purpose to the most specific category between its k nearest neighbors around it. Discussion associated with neighbors implies that there should be a distance or unsimilarity measurement that may be computed between samples victimization the freelance variables. The instances concerned within the paper consider the only accepted measure of distance, i.e., Euclidean distance. The Euclidean distance between any two points x and y is:

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \tag{10}$$

C. Random Forest

Random Forest (RF) is an ensemble of classification trees.Every tree contributes with one vote for the assignation of the foremost frequent category to the input file [28]. RF uses the most effective split of a random subset of input features or predictive variables within each node's division, rather than mistreatment the most effective split variables, which reduces the generalization error. Besides extending the variety of the trees, RF uses Bagging or bootstrap aggregating to grow from totally different training information subsets. Bagging could be a technique used for training information creation by resampling the first dataset with replacement, i.e., with no deletion of the input sample's information for generating a succeeding subset. Thus, every set selected mistreatment bagging to form every individual three grow containing a precise proportion of the standardization dataset. The samples that do not seem to be a gift within the calibration set are included as a part of another collection referred to as out-of-bag (OOB). Note that a particular OOB set is made for every three of the ensembles, from the bootstrapping method's non-selected parts. The tree will classify these OOB parts that do not seem to be thought-about for the the-tree coaching to evaluate his performance.

V. RESULTS AND DISCUSSION

Various tests have been executed on three databases with several classes, including, Broadatz Database [29], KTH-TIPS [30] and the UIUC [31]. Broadatz Dataset is yhe well-known texture dataset. This dataset is devoted to rotation-invariant texture recognition.It consists of thirteen texture categories from the initial Broadatz album and contains 1248 Pictures of dimensions 128×128 pixels. Textures are given in six different rotation angles (0^o, 30^o, 60^o, 90^o, 120^o, 150^o). The number of samples per category and Orientation is sixteen images.

KTH is the abbreviation for Kungliga Tekniska Högskolan University and TIPS. It stands for textures under Varying illumination, pose and scale. Images have been taken at nine different scales spanning two octaves. At the significant scale, the distance between the camera and the target was 28 cm. In this study, we used nine different types, with 81 images for each class. The considered textures are sandpaper, crumpled aluminum foil, styrofoam, sponge, corduroy, linen, cotton, brown bread, orange peel, and cracker.

UIUC database contains 25 texture classes. Each class contains 40 samples. All images are in greyscale JPG format at 640×480 pixels. Figures 2–4 show samples from each database

To evaluate the performance of the proposed method, a 5-fold cross-validation technique has been computed. The three texture image databases have been used to collect training and test sets. each fold is divided into an 80% train set and a 20 % test set. The training and testing are conducted five times. This process guarantees that each data point ends up in the 20 % test set exactly once. The model has achieved good performance among the five distortions.

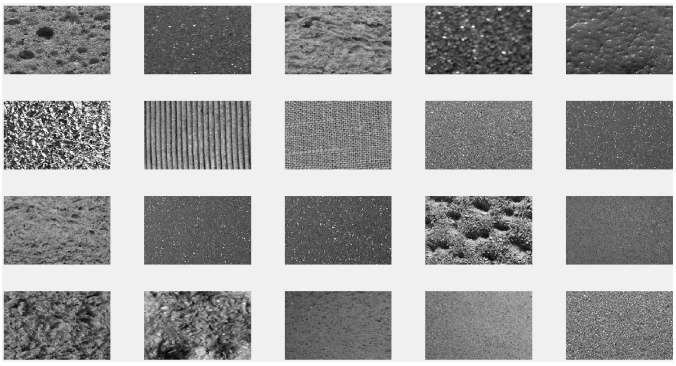


Fig. 3. image database.

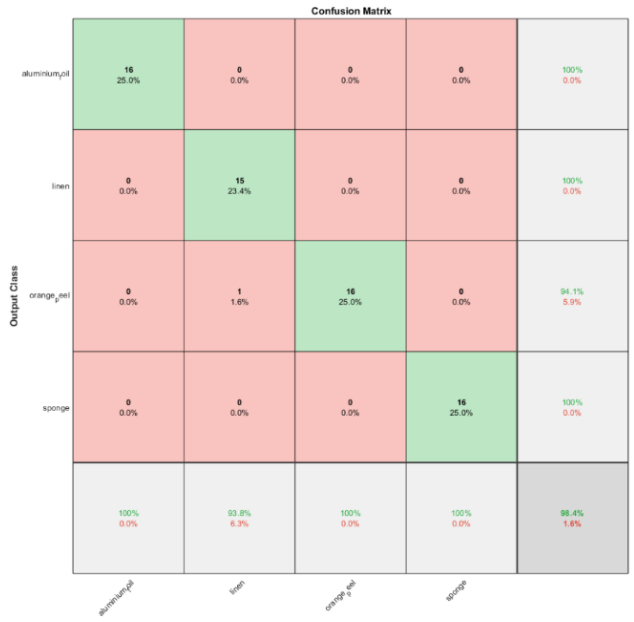


Fig. 4. confusion matrix using four classes with Rf classifiers.

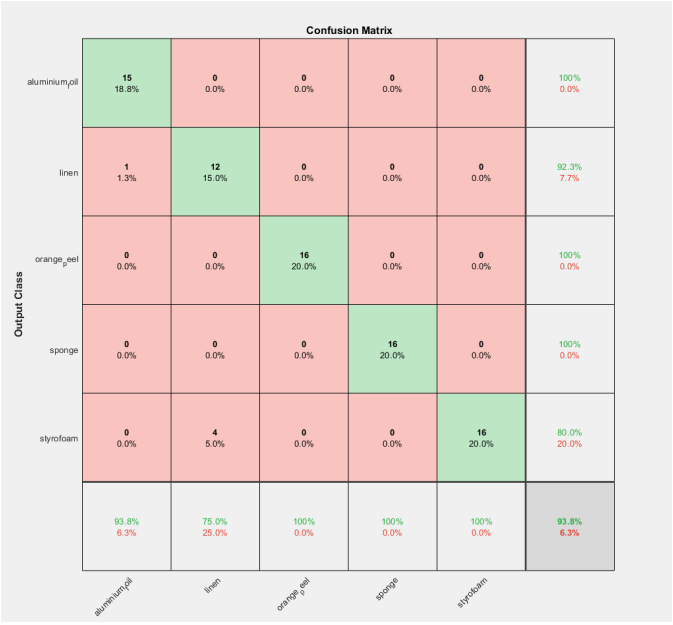


Fig. 5. confusion matrix using five classes with Rf classifiers .

GA is performed to reduce the number of features. The feature set containing six characteristics is used as entries of the three classifiers. A population of 30 chromosomes has been randomly generated. Each chromosome contains 44 genes (One gene for each feature). One-point crossover and mutation genetic operators have been used. The crossover rate has been set to 90%, and the mutation rate to 10%. The Tournoi selection method has been used to select the mating pool.

Classification results are presented in three different steps. In the first step, classification is performed on each feature. Then, in the second step, a fused features vector has been used.

The best features selection method fitted by the GA is performed. Classification results have obtained with 40/50 training and testing sets.

Table 1 presents each feature's performance in each dataset with several classifiers and the fusion of texture features results.It is noticed that combining the four classes of features is the best method among all. It remarkably outperforms all others in all datasets. Then the classification results are calculated for feature selection In the first test, training/ testing part 40/60 has been selected. It achieves a classification accuracy of 98.4 %. It is clear from this table that the proposed selection method gives better results than the first two ones.

Another constructive and useful approach to evaluate the performance of the classifier is the confusion matrix. Such a matrix aims to show the number of class A elements that are assigned to class B. For instance, we chose to show the confusion matrices for the three datasets.

We can observe from table 1 and figure 2 and 3 that the best classification result has been obtained using the random forest classifier to combine the four classes of features. This

TABLE I
TEXTURE CLASSIFICATION ACCURACY

Classification accuracy									
features	Brodatz database			Kh tips			UIUC database		
classifiers	SVM	KNN	RF	SVM	KNN	RF	SVM	KNN	RF
FILTER BANKS	77.652	72.45	77.5	79.123	78.463	79.402	79.8	78.45	79.652
LOCAL GRAPH STRUCTURES	78.45	75.785	78.516	78.45	76.45	77.45	78.45	75.45	79.4
2DRCA parameters	89.45	89.45	88.5	89.45	89.45	89.45	73.8	89.45	87.4
HOG	86.75	84.125	86.45	81.5	80.450	82.45	80.4	79.05	82.2
WDT	85.75	81	85.25	82.67	80.125	83.5	79.45	70.75	82.4
LBP	8.45	89.45	87.5	81.02	75.8	80.3	85.8	84.7	85.8
Combination of for features	92.5	88.3	98.2	90.4	80.1	96.32	88.8	84.3	90.75
Combination of for features using gA	94.5	90	**99**	91.4	80.1	**98.4**	91.8	86.3	**93.75**

is due to:

- It is unexcelled in exactness among current calculations.
- It runs effectively on enormous information bases.
- It can deal with a large number of information factors without variable erasure.
- It is computationally faster than other tree troupe strategies

VI. CONCLUSION

in this paper, an unique combination of features extraction methods for texture classification is proposed .Genetic algorithms have been used to pick the best features from a fused vector which are then fed to three machine learning classifiers for classification: multi-class support vector machine, K-nearest neighbors and random forest. The proposed approach has been validated on three data sets. The proposed technique's classification accuracy is substantially higher than most current approaches, according to the experimental results. As a result of the above discussion, it can be concluded that combining different types of texture features with the best selection algorithm yields better results than using a random combination of features. As a future work, we are planning to extend this work to color images classification.

References

[1] Hsin-Chih Lin, Ling-Ling Wang, and Shi-Nine Yang. "Regular-texture image retrieval based on texture-primitive extraction". In: *Image and Vision Computing* 17.1 (1999). Publisher: Elsevier, pp. 51–63.

[2] Fernando Lopez et al. "A study of registration methods for ceramic tile inspection purposes". In: *Proceedings of the IX Spanish symposium on pattern recognition and image analysis*. Vol. 1. 2001, pp. 145–150.

[3] Jing Yi Tou, Yong Haur Tay, and Phooi Yee Lau. "A comparative study for texture classification techniques on wood species recognition problem". In: *2009 Fifth International Conference on Natural Computation*. Vol. 5. IEEE. 2009, pp. 8–12.

[4] Sourajit Das and Uma Ranjan Jena. "Texture classification using combination of LBP and GLRLM features along with KNN and multiclass SVM classification". In: *2016 2nd International Conference on Communication Control and Intelligent Systems (CCIS)*. IEEE, 2016, pp. 115–119.

[5] Oussama Aiadi and Mohammed Lamine Kherfi. "Image classification using texture features and support vector machine (SVM)". In: (2019).

[6] Anne Humeau-Heurtier. "Texture feature extraction methods: A survey". In: *IEEE Access* 7 (2019), pp. 8975–9000.

[7] Robert M. Haralick. "Statistical and structural approaches to texture". In: *Proceedings of the IEEE* 67.5 (1979). Publisher: IEEE, pp. 786–804.

[8] GN Srinivasan and G Shobha. "Statistical texture analysis". In: *Proceedings of world academy of science, engineering and technology*. Vol. 36. 2008, pp. 1264–1269.

[9] Jie Chen et al. "WLD: A robust local image descriptor". In: *IEEE transactions on pattern analysis and machine intelligence* 32.9 (2009), pp. 1705–1720.

[10] Timo Ojala, Matti Pietikäinen, and David Harwood. "A comparative study of texture measures with classification based on featured distributions". In: *Pattern recognition* 29.1 (1996), pp. 51–59.

[11] Takahiro Toyoda and Osamu Hasegawa. "Texture classification using extended higher order local autocorrelation". In: *International Workshop on Texture Analysis and Synthesis*. Citeseer. 2005, pp. 131–136.

[12] Andrew Mehnert et al. "A structural texture approach for characterising malignancy associated changes in pap smears based on mean-shift and the watershed transform". In: *2014 22nd International Conference on Pattern Recognition*. IEEE. 2014, pp. 1189–1193.

[13] Krystian Mikolajczyk, Andrew Zisserman, and Cordelia Schmid. "Shape recognition with edge-based features". In: *British Machine Vision Conference (BMVC'03)*. Vol. 2. The British Machine Vision Association, 2003, pp. 779–788.

[14] James M Coggins and Anil K Jain. "A spatial filtering approach to texture analysis". In: *Pattern recognition letters* 3.3 (1985), pp. 195–203.

[15] Adolf W Lohmann. "Image rotation, Wigner rotation, and the fractional Fourier transform". In: *JOSA A* 10.10 (1993), pp. 2181–2186.

[16] Thomas P Weldon, William E Higgins, and Dennis F Dunn. "Efficient Gabor filter design for texture segmentation". In: *Pattern recognition* 29.12 (1996), pp. 2005–2015.

[17] George R Cross and Anil K Jain. *Markov random field texture models*. 1983.

[18] Jiřié Anděl. "Autoregressive series with random parameters". In: *Mathematische Operationsforschung und Statistik* 7.5 (1976), pp. 735–741.

[19] Amel Boulemnadjel, Fella Hachouf, and Soumia Kharfouchi. "GMM estimation of 2D-RCA models with applications to texture image classification". In: *IEEE Transactions on Image Processing* 25.2 (2015), pp. 528–539.

[20] Harry H Kelejian and Ingmar R Prucha. *A generalized moments estimator for the autoregressive parameter in a spatial model*. 1999.

[21] R Shenbagavalli and K Ramar. "Classification of soil textures based on laws features extracted from preprocessing images on sequential and random windows". In: *Bonfring International Journal of Advances in Image Processing* 1.Inaugural Special Issue (2011), pp. 15–18.

[22] Michael Unser and Murray Eden. "Multiresolution feature extraction and selection for texture segmentation". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 11.7 (1989), pp. 717–728.

[23] Matthew Mellor, Byung-Woo Hong, and Michael Brady. "Locally rotation, contrast, and scale invariant descriptors for texture analysis". In: *IEEE Transactions on pattern analysis and machine intelligence* 30.1 (2007), pp. 52–61.

[24] Eimad EA Abusham and Housam K Bashir. "Face recognition using local graph structure (LGS)". In: *International Conference on Human-Computer Interaction*. Springer. 2011, pp. 169–175.

[25] David E. Golberg. "Genetic algorithms in search, optimization, and machine learning". In: *Addion wesley* 1989.102 (1989), p. 36.

[26] Johan AK Suykens and Joos Vandewalle. "Least squares support vector machine classifiers". In: *Neural processing letters* 9.3 (1999). Publisher: Springer, pp. 293–300.

[27] Leif E Peterson. "K-nearest neighbor". In: *Scholarpedia* 4.2 (2009), p. 1883.

[28] Leo Breiman. "Random forests". In: *Machine learning* 45.1 (2001). Publisher: Springer, pp. 5–32.

[29] FJ Dıéaz-Pernas et al. "Texture classification of the entire brodatz database through an orientational-invariant neural architecture". In: *International Work-Conference on the Interplay Between Natural and Artificial Computation*. Springer. 2009, pp. 294–303.

[30] Barbara Caputo, Eric Hayman, and P Mallikarjuna. “Class-specific material categorisation”. In: *Tenth IEEE International Conference on Computer Vision (ICCV’05) Volume 1*. Vol. 2. IEEE. 2005, pp. 1597–1604.

[31] Svetlana Lazebnik, Cordelia Schmid, and Jean Ponce. “A sparse texture representation using local affine regions”. In: *IEEE transactions on pattern analysis and machine intelligence* 27.8 (2005), pp. 1265–1278.

Image denoising algorithms using norm minimization techniques

Diffellah Nacira
Dept. of electronics
(Faculty of technology)
ETA Laboratory
University of Bordj Bou Arreridj
Bordj Bou Arreridj 34000, Algeria
diffellahn@gmail.com
ORCID iD is 0000-0003-2474-0700

Bekkouche Tewfik
Dept. of electromechanics
(Faculty of technology)
ETA Laboratory
University of Bordj Bou Arreridj
Bordj Bou Arreridj 34000, Algeria
bekkou66@hotmail.com
ORCID iD is 0000-0002-5405-7382

Hamdini Rabah
Dept. of automatics
(Faculty of technology)
SET Laboratory
univ Saad Dahlab Blida
Blida 09000, Algeria
hamdinirabah@gmail.com
ORCID iD is 0000-0003-3127-1367

***Abstract*—Image denoising is one of the fundamental image processing problems. Noise removal is an important step in the image restoration process. In this paper, firstly we develop and implement two different image denoising algorithms based on norm minimization, namely ℓ_1 and ℓ_2-regularization applied to images contaminated by gaussian noise. Then, after their discretization and implementation, we perform a comparison between the two methods using several test images. Through this study, the algorithm which minimizes ℓ_2-norm of gradient of image has a unique solution and it's easy to implement, but it doesn't accept contour discontinuities, causing the obtained solution to be smooth. The ℓ_2-norm will blur the edges of the image. In order to preserve sharp edges, ℓ_1-norm is introduced. There are different methods to solve the problem of energy minimization. In this work, we have chosen the discretization finite difference method before applying the gradient descent algorithm to optimize the signal (2D grayscale images) denoising functionality.**

Experiments results, show that ℓ_1 regularization encourages image smoothness while allowing for presence of jumps and discontinuities, a key feature for image processing because of the importance of edges in human vision.

***Index Terms*—Denoising, ℓ_1-norm, ℓ_2-norm, Finite difference discretization,**

I. Introduction

In image acquisition systems, acquired digital images always contain noise. There are different kinds of digital image noise which are caused by many factors. In this paper, we focus our research to study, implement and compare two methods based on partial differential equation (PDE) model for removing Gaussian noise. Generally, images are corrupted with additive white Gaussian noise during acquisition e.g. sensor noise caused by poor illumination and/or high temperature, and/or transmission e.g. electronic circuit noise.

In the literature, several methods have been proposed to remove the noise and recover the true image u, such as iterative median filtering [1], Weight Median Filter (WMF) [2], Adaptive Median Filter (AMF) [3] [4], Wavelet Transform (WT) [5], Anisotropic diffusion filtering [6], [7] , Total Variation (TV) filter [8]–[10],...

There are many mathematical models which have been proposed to solve image denoising problems. we consider two types of image denoising problems which are expressed as the following norm minimization problems:

$$\min_{u\in V}\left\{\frac{1}{2}\|u-f\|^2+\lambda\frac{1}{2}\|\nabla u\|_2^2\right\} \tag{1}$$

$$\min_{u\in V}\left\{\frac{1}{2}\|u-f\|^2+\lambda\|\nabla u\|_1\right\} \tag{2}$$

V is the space of images (a space of smooth functions), $u\in\Re^N$ is the real image and $f\in\Re^N$ is the image contaminated by additive noise, $\lambda>0$ is regularization parameter, $\|.\|_2$ and $\|.\|_1$denotes the ℓ_2 and ℓ_1-norm , respectively. The first terms of $J_1(u,f)=\|u-f\|_2^2$ is called the data-fitting (the fidelity) term which forces the final image to be not too far away from the initial image, note that the fidelity term is convex function, and the second terms such as $J_2(u)=\frac{1}{2}\|\nabla u\|_2^2$ and $J_2(u)=\|\nabla u\|_1$ are called the regularization (or penalty) terms, which perform actually the noise reduction and they are also convex . The minimization problem (1) is called the ℓ_2-norm problem (Tikhonov regularization) and (2) is called the ℓ_1-norm regularization problem.

The rest of the paper is organized as follows: The second section presented the noise model. Section III is dedicated to analyze and implement the two different image denoising algorithms based on energy minimization: ℓ_1 and ℓ_2-regularization. In section IV, we provide some numerical experiments. Lastly, section V concludes the paper.

II. Noise model

Probability Density Function (PDF) or Histogram is also used to design and characterize the noise models, in this paper we will discuss only Gaussian noise model in digital images. Gaussian noise is statistical noise having a probability distribution function (PDF) equal to that of the normal distribution, which is also known as the Gaussian distribution. The probability density function of a Gaussian random variable is given by :

$$p_G(z)=\frac{1}{\sigma\sqrt{2\pi}}.e^{-\frac{(z-\mu)^2}{2.\sigma^2}} \tag{3}$$

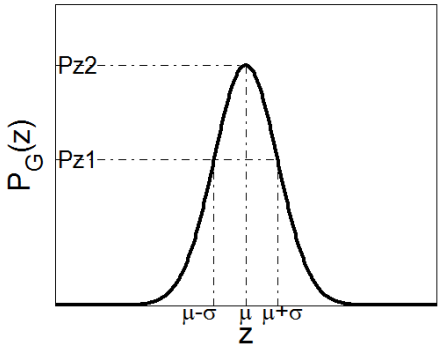


Fig. 1: Probability density function of Gaussian noise

where z represents the grey level, μ the mean value and σ the standard deviation.

The PDF of this noise model Fig. 1 shows that to noisy pixel values of degraded image in between $\mu - \sigma$ and $\mu + \sigma$. (see [11]) where

$$Pz_1 = \frac{0,607}{\sqrt{2\pi\sigma^2}} \tag{4}$$

$$Pz_2 = \frac{1}{\sqrt{2\pi\sigma^2}} \tag{5}$$

III. Methods analysis and implementation

The image denoising problem can be formulated as the following. Given an observed image f, we know f is the addition of the ideal image u and some noise with mean 0 and variance σ^2.

$$f = u + \eta \tag{6}$$

In accordance with Eq. (6), the denoising problem can be considered in the unconstrained form as:

$$J(u) = J_1(u, f) + \lambda J_2(u) \tag{7}$$

Minimization of $J_2(u)$ is equivalent to minimization of the majority of derivative over the dimension of the function. Intuitively, minimization problem (7), simultaneously try to remove the noise from the continuous image u (which is equivalent to minimization of the total first derivative over the domain) and forces the function $J_1(u)$ to be near enough to f. See [8], [12], [13].

A. Removal noise by ℓ_2- norm

The ℓ_2 norm method is a 5 steps process:

- Step 1: Create the energy that describe the quality image u

$$\min_{u\in V} J(u) = \min_{u\in V}\left\{\frac{1}{2}\|u-f\|^2 + \lambda\frac{1}{2}\|\nabla u\|^2\right\} \tag{8}$$

with

$$J_1(u) = \frac{1}{2}\|u-f\|^2 \tag{9}$$

$$J_2(u) = \frac{1}{2}\|\nabla u\|_2^2 \tag{10}$$

- Step 2: Compute the first variation of energy ∇J

$$\nabla J_1(u) = u - f \tag{11}$$

$$\nabla J_2(u) = \Delta u \tag{12}$$

so,

$$\nabla J(u) = u - f + \lambda.\Delta u \tag{13}$$

- Step 3: Setup the PDE describing the steepest descent minimization $\frac{\partial u}{\partial t} = -\nabla J$

$$\frac{\partial u}{\partial t} = -(u - f + \lambda.\Delta u) \tag{14}$$

- Step 4: Discretize the PDE in Eq. (14) by finite difference method

$$\frac{u_{i,j}^{n+1} - u_{i,j}^n}{\tau} = -\left(u_{i,j}^n - f_{i,j}^n + \lambda.D_{\ell_2}{}_{i,j}^n\right) \tag{15}$$

with

$$\Delta u \overset{\text{discretization}}{\rightarrow} D\ell_2{}_{i,j}^n \tag{16}$$

$$D\ell_2{}_{i,j}^n = u_{i-1,j}^n + u_{i+1,j}^n + u_{i,j-1}^n + u_{i,j+1}^n - 4u_{i,j}^n \tag{17}$$

- Step 5: Evolve the PDE towards the minimum of

$$u_{i,j}^{n+1} = u_{i,j}^n - \tau\left(u_{i,j}^n - f_{i,j}^n + \lambda D\ell_2{}_{i,j}^n\right) \tag{18}$$

B. Removal noise by ℓ_1- norm

The ℓ_1 norm method is a 5 steps process:

- Step 1: Create the energy that describe the quality image u

$$\min_{u\in V} J(u) = \min_{u\in V}\left\{\frac{1}{2}\|u-f\|^2 + \lambda\|\nabla u\|_1\right\} \tag{19}$$

with

$$J_1(u) = \frac{1}{2}\|u-f\|^2 \tag{20}$$

$$J_2(u) = \|\nabla u\|_1 \tag{21}$$

- Step 2: Compute the first variation of energy ∇J

$$\nabla J_1(u) = u - f \tag{22}$$

$$\nabla J_2(u) = div\frac{\nabla u}{\|\nabla u\|} \tag{23}$$

so,

$$\nabla J(u) = u - f + \lambda.div\frac{\nabla u}{\|\nabla u\|} \tag{24}$$

- Step 3: Setup the PDE describing the steepest descent minimization $\frac{\partial u}{\partial t} = -\nabla J$

$$\frac{\partial u}{\partial t} = -\left(u - f + \lambda.div\frac{\nabla u}{\|\nabla u\|}\right) \tag{25}$$

- Step 4: Discretize the PDE in Eq. (25) by finite difference method

$$\frac{u_{i,j}^{n+1} - u_{i,j}^n}{\tau} = -\left(u_{i,j}^n - f_{i,j}^n + \lambda.D_{\ell_1}{}_{i,j}^n\right) \tag{26}$$

with

$$div\left(\frac{\nabla u}{\|\nabla u\|}\right) \overset{\text{discretization}}{\rightarrow} D\ell_1{}_{i,j}^n \tag{27}$$

$$D{\ell_1}^n_{i,j} = \frac{1}{h^2}\left[\frac{d^n_{1_{i,j}}}{c^n_{1_{i,j}}} - \frac{d^n_{2_{i,j}}}{c^n_{2_{i,j}}} + \frac{d^n_{3_{i,j}}}{c^n_{3_{i,j}}} - \frac{d^n_{4_{i,j}}}{c^n_{4_{i,j}}}\right] \quad (28)$$

$$c^n_{1_{i,j}} = \sqrt{\varepsilon^2 + \left(\frac{d^n_{1_{i,j}}}{h^2}\right)^2 + \left(\frac{u_{i,j+1} - u_{i,j-1}}{2h}\right)^2} \quad (29)$$

$$c^n_{2_{i,j}} = \sqrt{\left(\frac{d^n_{2_{i,j}}}{h^2}\right)^2 + \left(\frac{u_{i-1,j+1} - u_{i-1,j-1}}{2h}\right)^2} \quad (30)$$

$$c^n_{3_{i,j}} = \sqrt{\left(\frac{u_{i+1,j} - u_{i-1,j}}{2h}\right)^2 + \left(\frac{d^n_{3_{i,j}}}{h^2}\right)^2} \quad (31)$$

$$c^n_{4_{i,j}} = \sqrt{\left(\frac{u_{i+1,j-1} - u_{i-1,j-1}}{2h}\right)^2 + \left(\frac{d^n_{4_{i,j}}}{h^2}\right)^2} \quad (32)$$

$$d^n_{1_{i,j}} = u^n_{i+1,j} - u^n_{i,j} \quad (33)$$

$$d^n_{2_{i,j}} = u^n_{i,j} - u^n_{i-1,j} \quad (34)$$

$$d^n_{3_{i,j}} = u^n_{i,j+1} - u^n_{i,j} \quad (35)$$

$$d^n_{4_{i,j}} = u^n_{i,j} - u^n_{i,j-1} \quad (36)$$

- Step 5: Evolve the PDE towards the minimum of

$$u^{n+1}_{i,j} = u^n_{i,j} - \tau\left(u^n_{i,j} - f^n_{i,j} + \lambda D{\ell_1}^n_{i,j}\right) \quad (37)$$

IV. Numerical results

In this section, we will compare and discuss the results of the different algorithms. Our implementation of the two algorithms has been tested against the set of images: cameraman of size 256×256 pixels, Einstein 1064×948 pixels, Tower 474×422 pixels and Lena 512×512 pixels shown in Fig. 2a , Fig. 3a, Fig. 4a and Fig. 5a respectively.

As a measure of quality, we use three metrics, namely , Signal Noise to Ratio $SNR\,[dB]$, Peak Signal-to-Noise Ratio (PSNR) and Structural SIMilarity index (SSIM) [14].

- The Signal Noise to Ratio $SNR\,[dB]$ is defined as:

$$SNR = \frac{S_A - S_B}{\partial_0} \quad (38)$$

S_A is the original image and S_B is the restored noisy image, σ_0 is standard deviation of the image.
This measure of SNR is useful in giving an indication of the noise in an image, but the exact visual effect of such noise is highly image dependent.

- The PSNR metric is defined as:

$$PSNR\,(u, \hat{u}) = 10 \log \frac{{L_d}^2}{MSE} \quad (39)$$

where L_d is the dynamic range of the pixel-values. If the input image has an 8-bit unsigned integer data type, $L_d = 255$.
Equation 40 give the expression of the quality measures Mean Squared Error (MSE):

$$MSE\,(u, \hat{u}) = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(u\,(i,j) - \hat{u}\,(i,j)\right)^2. \quad (40)$$

$u\,(i,j)$ denote the original image and $\hat{u}\,(i,j)$ its reconstructed image, respectively. M and N are the image size. PSNR determines the degradation in the embedded image with respect to the original image. PSNR is more consistent in the presence of noise compared to SNR. The main advantages of PSNR are that it is very fast and easy to implement. The value of PSNR is larger, indicating that denoising effect is better.

- The mathematical representation of the SSIM is as follows:

$$SSIM\,(u, \hat{u}) = \frac{(2\mu_u\mu_{\hat{u}} + C_1)\,(2\sigma_{u\hat{u}} + C_2)}{(\mu_u^2 + \mu_{\hat{u}}^2 + C_1)\,(\sigma_u^2 + \sigma_{\hat{u}}^2 + C_2)} \quad (41)$$

where

$$\mu_u = \frac{1}{N}\sum_{i=1}^{N} u_i \quad (42)$$

$$\mu_{\hat{u}} = \frac{1}{N}\sum_{i=1}^{N} \hat{u}_i \quad (43)$$

$$\sigma_u = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}\left(u_i - \mu_u\right)^2} \quad (44)$$

$$\sigma_{\hat{u}} = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}\left(\hat{u}_i - \mu_{\hat{u}}\right)^2} \quad (45)$$

$$\sigma_{u\hat{u}} = \frac{1}{N-1}\sum_{i=1}^{N}\left(u_i - \mu_u\right)\left(\hat{u}_i - \mu_{\hat{u}}\right) \quad (46)$$

μ_u and $\mu_{\hat{u}}$ are the means and variances of u and $\hat{u}$ respectively.
σ_u^2 and $\sigma_{\hat{u}}^2$ are variances of u and $\hat{u}$ respectively.
$\sigma_{u\hat{u}}$ is the standard deviation between u and $\hat{u}$.
C_1 and C_2 are constants which are used to avoid instability when $\mu_u^2 + \mu_{\hat{u}}^2$ and $\sigma_u^2 + \sigma_{\hat{u}}^2$ are very close to zero.

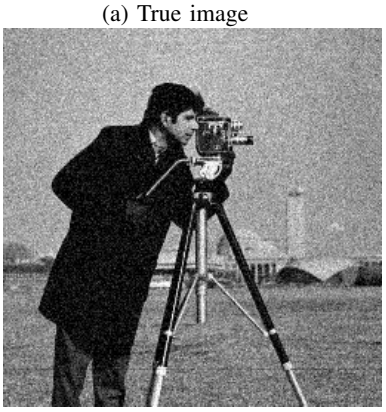
$$C_1 = \left(K_1 L_d\right)^2 \quad (47)$$

$$C_2 = \left(K_2 L_d\right)^2 \quad (48)$$

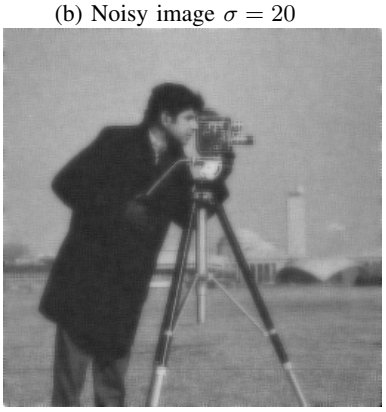
K_1 and K_2 are two scalar constants given by; $K_1 = 0.01$ and $K_2 = 0.03$.
$SSIM$ satisfies the following conditions:

- $SSIM\,(u, \hat{u}) = SSIM\,(\hat{u}, u)$
- $SSIM\,(u, \hat{u}) \leq 1$
- $SSIM\,(u, \hat{u}) = 1\ si\ \hat{u} = u$

(a) True image



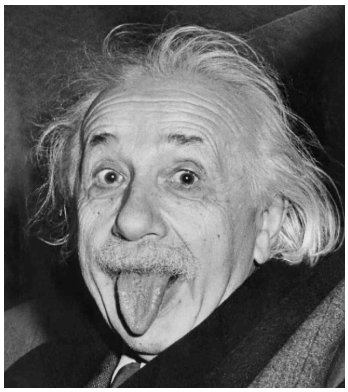
(b) Noisy image $\sigma = 20$



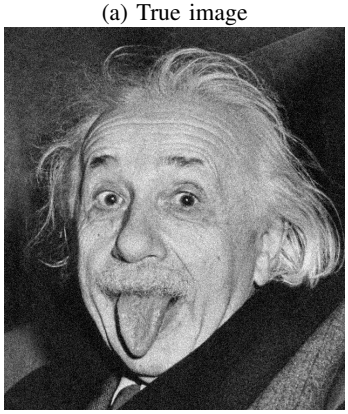
(c) ℓ_2-norm

(d) ℓ_1-norm

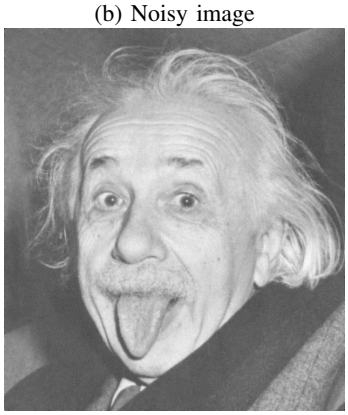
Fig. 2: Removal noise applied to 'Cameraman'



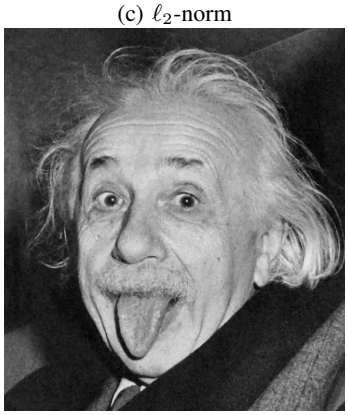
(a) True image



(b) Noisy image

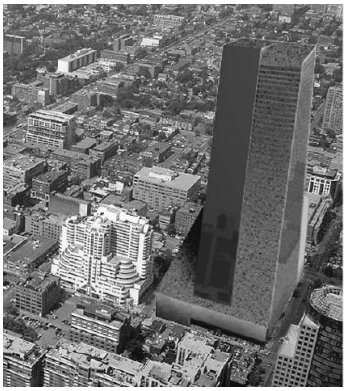


(c) ℓ_2-norm

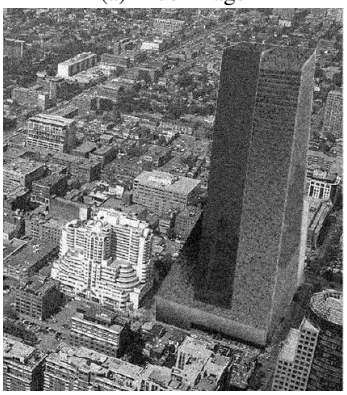


(d) ℓ_1-norm

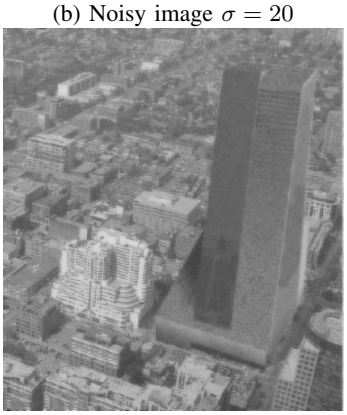
Fig. 3: Removal noise applied to 'Eistein'



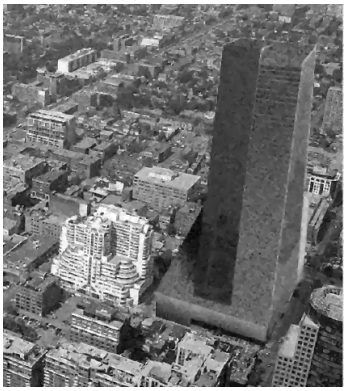
(a) True image



(b) Noisy image $\sigma = 20$



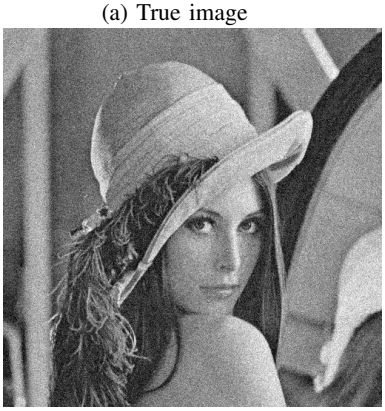
(c) ℓ_2-norm



(d) ℓ_1-norm

Fig. 4: Removal noise applied to 'Tower'

(a) True image



(b) Noisy image $\sigma = 20$

(c) ℓ_2-norm

(d) ℓ_1-norm

Fig. 5: Removal noise applied to 'lena'

SSIM compares two images using information about luminous, contrast and structure, it's decimal value is between $[-1, 1]$.

Images corrupted by Gaussian noise are shown in Fig. 2b, Fig. 3b, Fig. 4b and Fig. 5b. The results using ℓ_1-norm regularization and images denoised with ℓ_2-norm regularization are shown in Fig. 2d, Fig. 3d, Fig. 4d, Fig. 5d and Fig. 2c, Fig. 3c, Fig. 4c and Fig. 5c.

Obtained results of SNR, PSNR and SSIM for the two proposed algorithms are summarized in Tables I, II and III, respectively.

TABLE I: Comparison of the denoising SNR results

Image	ℓ	σ					
		10	20	30	50	70	100
Camera-man	ℓ_1	16.91	15.55	12.83	7.36	3.33	-0.73
	ℓ_2	15.86	11, 60	6.31	1.92	-0.99	-4.09
Einstein	ℓ_1	21.82	19.54	14.83	8.05	3.82	-0.42
	ℓ_2	16.15	11, 19	6.61	2.17	-0.74	-3.84
Tower	ℓ_1	9.93	9, 33	8.02	4.56	1.22	-2.60
	ℓ_2	13.93	4, 92	4.34	-0.05	-2.99	-6.09
Lena	ℓ_1	18.48	16.08	11.83	5.39	1.23	-2.98
	ℓ_2	13.61	10, 36	4.07	-0.37	-3.30	-6.41

TABLE II: Comparison of the denoising $PSNR$ results

Image	ℓ	σ					
		10	20	30	50	70	100
Cameraman	ℓ_1	29.14	27.82	25.06	19.60	15.57	11.50
	ℓ_2	28.10	22.11	18.55	14.16	11.23	8.14
Einstein	ℓ_1	33.82	31.53	26.83	20.05	15.81	11.57
	ℓ_2	28.12	22.11	18.58	14.14	11.22	8.12
Tower	ℓ_1	23.85	23.27	21.94	18.48	15.14	11.31
	ℓ_2	28.14	22.08	18.56	14.16	11.22	8.12
Lena	ℓ_1	33.01	30.59	26.36	19.92	15.76	11.54
	ℓ_2	28.14	22.11	18.60	14.15	11.22	8.12

TABLE III: Comparison of the denoising $SSIM$ results

Image	ℓ	σ					
		10	20	30	50	70	100
Cameraman	ℓ_1	0.85	0.78	0.57	0.30	0.19	0.11
	ℓ_2	0.63	0.39	0.28	0.17	0.12	0.07
Einstein	ℓ_1	0.96	0.92	0.83	0.64	0.50	0.36
	ℓ_2	0.96	0.88	0.78	0.61	0.48	0.35
Tower	ℓ_1	0.90	0.88	0.81	0.68	0.54	0.39
	ℓ_2	0.95	0.86	0.76	0.59	0.46	0.33
Lena	ℓ_1	0.94	0.88	0.71	0.46	0.32	0.20
	ℓ_2	0.87	0.67	0.53	0.35	0.25	0.16

The ℓ_1 method has significantly better reconstruction results, both in terms of SNR, $PSNR$, $SSIM$ and visual quality than the ℓ_2 method.

V. Conclsuion

To denoise image corrupted with Gaussian noise, we have studied and implemented two algorithms regularization schemes ℓ_1 and ℓ_2. The ℓ_2 regularization scheme does not have edge preserving properties, but is capable of removing almost all the noise from the image, but the ℓ_1 regularization scheme is capable of removing noise and also preserving edges to a large extent.

Finally, we confirm through experimental results that the ℓ_1 regularization problem involved by Eq. (2) restore the true image better than ℓ_2 regularization problem expressed by Eq. (1).

For future works, there are many aspects need to be investigated. For example, minimizing the energy function using a variational method and deep learning-based methods.

Acknowledgements

The authors would like to thank the organizers of the conference ICCSA'2021 and the anonymous reviewers for their valuable comments and suggestions which greatly improved the quality of the paper. Authors would like to thank too the General Directorate for Scientific Research and Technological Development of the Algerian Republic in general and the ETA research laboratory of Bordj Bou Arreridj University in particular, for all material and financial support to accomplish this work.

References

[1] J. Nichol and V.Vohra, "Noise over water surfaces in landsat tm images," *International Journal of Remote Sensing*, vol. 25, no. 11, pp. 2087–2093, 2004.

[2] F. N. Hasson, "Weight median filter using neural network for reducing impulse noise," Ph.D. dissertation, Department Computer Sciences, University of Putra,Putra, Malaysia, 2004.

[3] D. Dhanasekaran, A. Krishnamurthy, and J. Ramkumar, "High speed pipeline architecture for adaptive median filter," *Journal of Scientific Research*, vol. .29, no. 4, pp. 454–460, 2009.

[4] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 4th ed., Pearson, Ed., 2018.

[5] M. Longkumer and H. Gupta, "Image denoising using wavelet transform,median filter and soft threshoding," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 7, pp. 729–732, 2018.

[6] N. K. Gill and A. Sharma, "Noise models and de-noising techniques in digital image processing," *International Journal of Computer & Mathematical Sciences IJCMS*, vol. 5, pp. 21–25, 2016.

[7] W. S. abd Min Han, "Adaptive search based non-local means image denoising," *2nd International Congress on Image and Signal Processing CISP*, vol. 9, pp. 1–4, 2009.

[8] L. I.Rudin, S. Osher, and E. Fatemi, "Nonlinear total variation based noise removal algorithms," *Physica D: Nonlinear Phenomena*, vol. 60, pp. 259–268, 1992.

[9] A. Chambolle, "An algorithm for total variation minimization and applications," *Journal of Mathematical Imaging and Vision*, vol. 20, pp. 89–97, 2004.

[10] D. N. H. Thanh, L. T. Thanh, N. N. Hien, and S. Prasath, "Adaptative tototal variation l1 regularization for salt and pepper image denoising," *Optik*, vol. 208, no. 208, 2020.

[11] W. Bryc, *The Normal Distribution Characterizations with Applications*. Springer-Verlag New York, 1995, no. 1.

[12] F. Alter, V. Caselles, and A. Chambolle, "Evolution of characteristic functions of convex sets in the plane by the minimizing total variation flow," *Interfaces and Free Boundaries*, vol. 7, no. 1, pp. 29–53, 2005.

[13] A. Chambolle and T. Pock, "A first-order primal-dual algorithm for convex problems with applications to imaging," *Journal of Mathematical Imaging and Vision*, vol. 40, pp. 120–145, 2011.

[14] Z. Wang, A. Bovik, H. Sheikh, and E. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600 – 612, 2004.

Towards emotion recognition in immersive virtual environments: A method for Facial emotion recognition

Kahina Amara
Centre of developpement of advanced technologies
Algiers, Algeria
kahina.amara88@gmail.com

Naeem Ramzan
School of Engineering and Computing, University of the West of Scotland
Paisley, Scotland

Nadia Zenati
Centre of developpement of advanced technologies
Algiers, Algeria

Oualid Djekoune
Centre of developpement of advanced technologies
Algiers, Algeria

Cherif Larbes
ENP Ecole Nationale politechnique
Hassen Badi Avenue, Algiers, Algeria

Mohamed Amine Guerroudji
Centre of developpement of advanced technologies
Algiers, Algeria

Djamel Aouam
Centre of developpement of advanced technologies
Algiers, Algeria

***Abstract*—Virtual Reality (VR) is, thus, proposed as a powerful tool to simulate complex, real situations and environments, offering researchers unprecedented opportunities to investigate human behaviour in closely controlled designs in controlled laboratory conditions. Facial emotion recognition has attracted a great deal of interest for interaction in virtual reality, healthcare system: therapeutic applications, surveillance video application etc. In this paper, we propose a method for facial emotion recognition for immersive virtual environment based on 2D and 3D geometrical features. We used our collected dataset of 17 subjects' performance of six basic facial emotions (anger, fear, happiness, surprise, sadness, and neutral) using three devices: Kinect (v1), Kinect (v2), and RGB HD camera. In addition, we present the performance results of the RGB data for facial emotion recognition using Bagged Trees algorithm. To assess the performance of the proposed system, we used leave-one-out-subject cross-validation. We compared the 2D and 3D data performance for facial expression recognition. The obtained results show the superior performance of the RGB-D features provided by Kinect (v2). Our findings highlight that the 2D images are not robust enough for facial emotion recognition. The built facial emotion models will animate virtual characters that can express emotions via facial expressions. This could be deployed for Chatting, Learning and Therapeutic Intervention.**

***Index Terms*—Virtual Reality, Facial emotion recognition, Immersive Environment, Avatar animation, Interaction, RGB, RGB-D, Machine Learning, Geometrical features.**

I. Introduction

Emotions have a critical impact in our daily lives, so the understanding and recognition of emotional responses is crucial for human behaviour understanding. Emotion recognition research has mostly used non-immersive two-dimensional (2D) images or videos to elicit emotional states. However, immersive virtual reality, which allows researchers to simulate environments in controlled laboratory conditions with high levels of sense of presence, immersion, and interactivity, is becoming more popular in emotion research. Moreover, its synergy with implicit measurements and machine-learning techniques has the potential to impact transversely in many research areas, opening new opportunities for the scientific community.

Healthcare, education and training are examples of application area where VR has been much applied (figure 1. The studies showed that VR can offer great educational advantages. It can solve time-travel problems, for example, students can experience different historical periods. VR can address physical inaccessibility, for example, students can explore the solar system in the first person. It can circumnavigate ethical problems, for example, students can "perform" serious surgery. Surgical training is now one of the most analysed research topics. On the other side, several researchers have also showed the effectiveness of VR in therapeutic applications. To overcome certain inconveniences such us the lack of the dynamism that is inherent to facial expressiveness with some patients, over the last years different authors have proposed the use of virtual avatars. The main goal is to make use of virtual environments and avatars to provide new objective methods for assessing patients' interpersonal behaviour characteristics [1]. VR offers some distinct advantages over standard therapies,

Fig. 1. Virtual reality application: Healthcare, Movie industry

including precise control over the degree of exposure to the therapeutic scenario, the possibility of tailoring scenarios to individual patients' needs and even the capacity to provide therapies that might otherwise be impossible. Taking some examples, studies using VR have analysed the improvement in the training in social skills for persons with mental and behavioural disorders, such as phobias, schizophrenia (SZ) [2], [3] and autism [4]. Moreover, it has been proposed as a key tool for the diagnosis of neuro-developmental disorders [5]. In [2], the authors present a VR-based system that incorporates implicit cues from peripheral physiological signals and eye tracking for the under-standing of facial emotional expression. They compare how a SZ group and a matched group of healthy non-psychiatric adults performed emotion recognition tasks when presented in the form of static slides and when presented in a VR environment with the avatars expressing emotions dynamically. Virtual reality (VR) has been observed to improve both assessment and training of emotional recognition skills of people with Severe mental illness [3]. In [7], a method EEG-based feature extraction technique is presented for emotion recognition using higher order crossings (HOC).

Virtual reality has proven its potential in the movie industry. Reproducing facial and bodily emotions in a completely immersive virtual environment (VE) in a faithful manner is of paramount importance for real virtual rendering (figure 2). Facial emotion expressions are nonverbal way of expressing feeling. Many studies addressed the facial expression [6]–[8].

Recent approaches use 3D facial points, such techniques have gained more attention lately due to the proliferation of affordable commodity depth sensing devices, such as the Kinect. According to the data used in this work, different approaches have been proposed for feature extraction. Positional and temporal features have been investigated in [9] using the facial data collected by Kinect. They defined a feature vector composed of the coordinates of tracked points and Euclidean distance between the tracked points and the angle between those points for the positional features.

Many studies are based on 2D images for facial emotion recognition. In [6], the authors proposed a software for the analysis of facial behaviour. Furthermore, several approaches have demonstrated state-of-the-art performance on RGBD input, or only depth input. We can cite the work presented in [8], [10]. In [10], the authors proposed the skeleton based approach to extract facial features for facial emotion recognition by using a depth camera. Billy et al. [11] used Kinect sensor to recognise emotions under different conditions. The authors used a publicly available database which contains facial images (RGB-D) captured by Kine ct sensor with different poses, expressions, illumination and disguise. Their results demonstrated that using RGB-D information could improve the performance of facial emotion recognition compared with the methods using 2D information. The conventional approaches for facial emotion recognition still suffer from some constraints and limitations which directly affect the system performance [12]. We can cite among these problems, the lack of publicly available database, the environmental changes including illumination changes, the different personnel style for emotion expression.

The existing approaches for facial expression recognition suffer from some constraints and limitations. Firstly, the lack of publicly available database. Furthermore, the selection of non-significant features for depicting different expressions can cause model failure. To deal with these problems, we propose in this work a system for mono-modal facial expression recognition based on facial movements.

In this paper, we present a proposal for facial emotion classification for interaction in immersive virtual environment. The facial emotion recognition is based on 3D angle and 3D Euclidean distance features for the RGB-D data, provided by kinect sensors, and 2D angle and Euclidean 2D distance for the RGB data provided by HD RGB camera. This paper consists of four sections. In the second section, we describe the proposed approach, the feature extraction will be presented in detail. In the third section, we discuss the experimental results. The conclusions and future works will be drawn in the last section.

II. Our proposal

Emotion can be expressed in different ways and plays important role in daily life. The facial expression is a common, nonverbal and effective way of expressing emotion. The presented work is included in this area; the process for facial expression recognition is depicted in figure **??**, we aim to distinguish the expressions as accurate as possible by establishing computational models. We carried out experiments on synthetic RGB-D sequences captured by Kinect (v1) and Kinect (v2) sensors and RGB sequences recorded using RGB HD camera. In this work, we target six basic emotions (anger, fear, happiness, surprise, sadness, and neutral).

We collected our own database including the performance of 17 students (9 male and 8 female) recruited from the School of computing and engineering at the University of West of Scotland. The participants are from different cultures with different skin colour. In order to obtain actual facial expression data, we conducted an emotion priming experiment using different emotional videos. The subjects were first asked to perform emotional states depicted on projected images on screen. In the second part of the experiment, we used 20 emotional videos used in [13] collected from Youtube. We used many types of emotional videos including neutral, happy, surprise, anger, fear and sad video which could induce corresponding emotional state. The participants were asked to perform their feeling according to their personal style. They have to repeat the performance for three times. The face-recorded videos were segmented and stored in a database. The collected dataset contains 1581 RGB videos recorded by RGB HD camera and more than 3000 synthetic RGBD sequences captured by Kinect (v1) and Kinect (v2). Figure displays the participants' facial expression.

In this work, the facial expressions were tracked using the face and skeleton tracking API available in the Microsoft Kinect Software Development Toolkit. The synthetic RGB-D sequences captured by Kinect sensors provided 3D facial

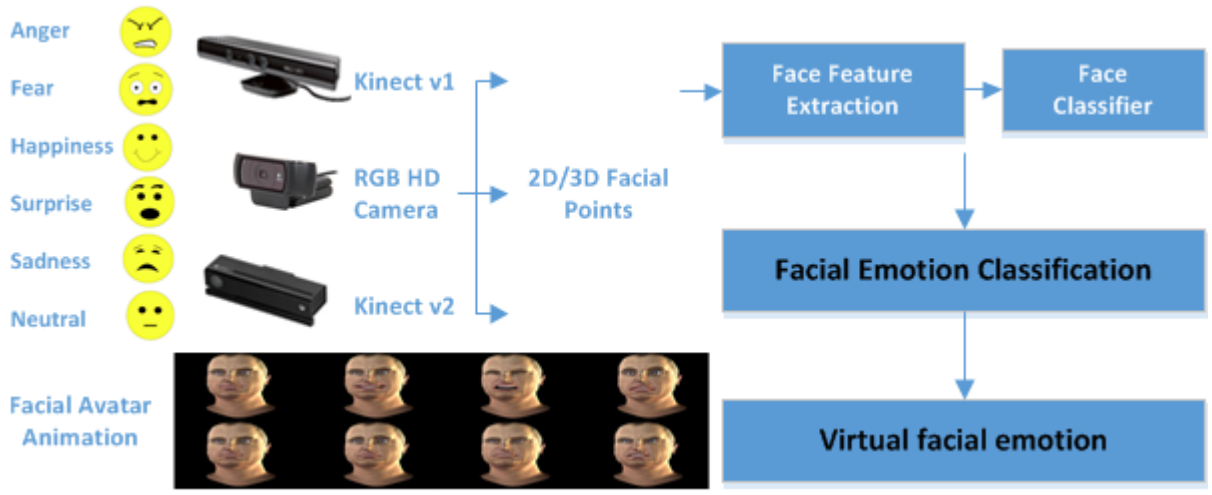


Fig. 2. The proposed framework for virtual facial expression recognition.

points. We choose representative points, which represent significant movement in order to describe the subtle changes of facial expression. The face tracking Kinect toolkit provides 121 facial points for Kinect 1 and 1347 facial points for Kinect 2. However, not all of these points are significant to facial expressions. In [17], the authors proposed that the main areas englobing the eyes, eyebrows, and the mouth are involved in facial expression displays. Out of the available points, facial points around eyebrows, eyes, mouth, nose, chin and cheeks were tracked and some other key positions were finally selected to improve the recognition accuracy. For the RGB video recorded by RGB HD camera, we used the open source tool OpenFace [6]. It provides facial landmark using the Conditional Local Neural Fields (CLNF) [15] (see figure 3). The CLNF performs the detection of 68 facial landmark. The CLNF is an instance of a Constrained Local Model (CLM) [16]. The CLM is composed of two main components: Point Distribution Model (PDM) which captures landmark shape variations; patch experts, which capture local appearance variations of each facial landmark [6]. Finally, we choose 26 facial points. The new face feature vector (FV_{Face} is defined using geometric features: distance and angle with the horizontal axis and the coordinates of tracked points from one frame.

Given two facial points $P_n^{face}(t)$ and $P_{n-1}^{face}(t)$ with coordinates $(x_n(t), y_n(t), z_n(t))$ and $(x_{n-1}(t), y_{n-1}(t), z_{n-1}(t))$ respectively at frame t,

$$D_n^{face}(P_{n-1}^{face}(t), P_n^{face}(t) = \begin{cases} (x_{n-1}(t) - x_n(t)) \\ (y_{n-1}(t) - y_n(t)) \\ (z_{n-1}(t) - z_n(t)) \end{cases} \quad (1)$$

$$\theta_n^{face}(P_{n-1}^{face}(t), P_n^{face}(t)) = \begin{cases} \theta(x_{n-1}(t), x_n(t)) \\ \theta(y_{n-1}(t), y_n(t)) \\ \theta(z_{n-1}(t), z_n(t)) \end{cases} \quad (2)$$

$$FV_{Face} = \begin{cases} D_1^{face}(P_0^{face}(t), P_1^{face}(t)), ..., D_n^{face}(P_{n-1}^{face}(t), \\ P_n^{face}(t)), \theta_1^{face}(P_0^{face}(t), P_1^{face}(t)), \\ ..., \theta_n^{face}(P_{n-1}^{face}(t), P_n^{face}(t)) \end{cases} \quad (3)$$

Fig. 3. The facial key points generated bu OpenFace [23]

The feature vector is based on position of the tracked points from one frame. The face feature vector is defined as follows (equation 3). It is a set of distance difference $D(t)$ and $\theta(t)$ which is the angle between each selected facial points which are depicted in equation 1 and equation 2. We calculated 36 distance and 36 angle between each tracked points. We selected key facial points representing significant changes based on psychological studies [17].

Experiments in this study were conducted on a computer with an Intel® Xeon ® CPU E3-1245 v3 3.40 Ghz and 8 GB RAM. All the experiments have been run in Matlab 2016b environment, using Matlab's own implementation of classification algorithms (Bagged Trees, k-NN, Linear SVM). Support vector machine [18] proposed by Vapnik and Chervonenk is a powerful statistical learning method, it models the situation by creating a feature space. The goal is to train

a model that assigns new unseen objects into a particular category. Linear SVM is one method used in statistics and machine learning to find a linear combination of features which characterize or separate two or more classes or events. Since emotion recognition may not be linearly separable, we also considered non-linear classification algorithms. Bagging is a method for improving results of machine learning classification algorithms. This method was formulated by Leo Breiman and its name was deduced from the phrase "bootstrap aggregating" [14]. Bagged Trees can be used to reduce the variance associated with prediction and improve the prediction process. Many bagging samples are drawn from the available data, some prediction method is applied to each bagging sample, and then the results are combined, by simple voting process for classification, to obtain the overall prediction, with the variance being reduced due to the averaging. The bagging method generates additional data for training from the original dataset using combinations with repetitions to produce multi-sets of the same cardinality/size as the original data. By increasing the size of the training set, it can not improve the model predictive force, but just decrease the variance, narrowly tuning the prediction to expected outcome.

The k-NN algorithm as non-parametric lazy learning algorithm is one of the simplest classification algorithm [19]. This is pretty useful , as in the real world , most of the practical data does not obey the typical theoretical assumptions made (gaussian mixtures, linearly separable etc). It is also a lazy algorithm which means is that k-NN does not use the training data points to do any generalization. There is no explicit training phase or it is very minimal and fast . All the training data is needed during the testing phase, the k-NN algorithm keeps all the training data. This is in contrast to other techniques like SVM where it is possible to discard all non support vectors without any problem. Most of the lazy algorithms – especially k-NN – makes decision based on the entire training data set. Predictions are made for a new instance by searching through the entire training set for the k most similar instances (the neighbors) and summarizing the output variable for those k instances. To determine which of the K instances in the training dataset are most similar to a new input a distance measure is used. For real-valued input variables, the most popular distance measure is Euclidean distance [20] which is calculated as the square root of the sum of the squared differences between a new point and an existing point.

III. Results and discussion

To solve our multi-classification problem, we defined six models to distinguish the six target emotional states (anger, fear, happiness, sadness, surprise, and neutral). As different classifiers may yield to different classification performance for the same dataset, we used for the training linear and non-linear classifiers including Bagged Trees, Fine k-NN and Linear SVM.

one-subject-out validation. We left the performance of one participant for testing, and the data of 16 participants were used for training and. Comparing the results of different

TABLE I
THE OBTAINED FACIAL EMOTION RECOGNITION RESULTS USING k-NN.

Devices	Accuracy%	Recall%	F1-score%	Precision%
Kinect 1	97.09	91.94	91.74	91.67
Kinect 2	97.40	92.86	92.65	92.49

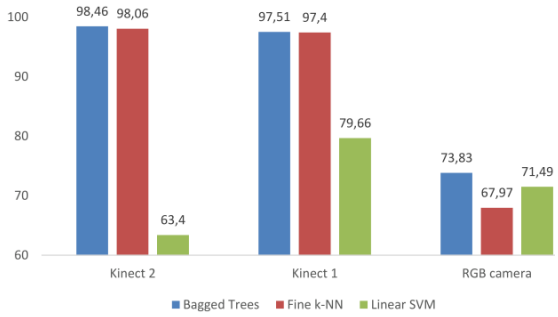


Fig. 4. The classifiers accuracy performance.

training algorithms, we notice that Bagged Trees algorithm outperforms the remaining classifiers with accuracy rate of 98.46%, 97.51%, and 73.83% for Kinect (v2), Kinect (v1) and HD RGB camera respectively. Comparing the devices used to collect the data, the Kinect captors achieved better results than OpenFace, which gives the lowest performance with 73.83%, 67.97%, and 71.49% of accuracy for Bagged Trees, Fine k-NN and Linear SVM respectively. The obtained results showed that Kinect (v2) performs better than Kinect (v1). The figure 4 showcases the obtained results using the three devices. The histogram presents the accuracy rates obtained by each classifier. Based on our experiment, the data collected by the HD RGB camera showed the lowest performance, which can be explained by the sensitivity to the surroundings, especially to illumination conditions [21]. The RGB-D images can capture essential geometrical features, and enable higher precision and preservation of facial details insensitive to different conditions. Table III shows the performance comparison between the proposed work in this paper and state-of-the-art works.

For performance comparison, we choose the accuracy, recall, precision, F1-score metrics that can be estimated by describing random errors (TP: True positive; TN: True negative; FP: False positive; FN: False negative), a measure of statistical changes (equation 4, equation 5,equation 7, equation 6). The obtained results are depicted on table II and table III.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{4}$$

$$Recall = \frac{TP}{TP + FN} \tag{5}$$

$$Precision = \frac{TP}{TP + FP} \tag{6}$$

$$F1 - score = 2 * \frac{Precision * Recall}{Precision + Recall} \tag{7}$$

Fig. 5. Future work

For the RGB data collected using RG HD camera, we use the open source OpenFace [23]. The results are depicted in table II.

TABLE II
RGB DATA PERFORMANCE: ACCURACY RATES FOR EACH CLASS USING BAGGED TREES.

Device	Accuracy (%)	anger	fear	happiness	sadness	surprise	neutral
RGB HD camera	72.39	67.62	77.31	64.73	86.92	75	71.39

TABLE III
ACCURACY PERFORMANCE COMPARISON WITH STATE OF THE ART WORKS. $^{*}Kinect1$, ** KINECT 2, ^{1} K-NN, ^{2} BAGGED-TREES.

Works	**Number of classes**	**Accuracy %**
[12] ^{**1}	6	89.44
	8	90.33
[22] *	6	80.75
	7	80.57
[8] ^{**1}	6	96.74
	8	96.92
Proposed approach ^{**2}	6	**98.46**
Proposed approach ^{*2}	6	**97.51**

To the best of our knowledge and based on the comparison depicted on table III, we believe that the proposed approach for emotion recognition outperform the state-of-the-art works.

At this point, we want to reproduce the emotions detected from the facial expressions in a virtual environment. This is by exploiting the models of the six basic emotions already built during the classification phase using machine learning (figure 4). We want the avatar in the virtual environment faithfully reproduce the facial emotions expressed by a user present in a real scene (figure 5). This proposal could be used in healthcare application (Patients with Schizophrenia therapies), serious game, human-computer interaction, etc.

IV. CONCLUSION

The paper proposes a concept for virtual avatar animation. This could be used for therapeutic intervention, chatting: social media interaction, and maybe for learning activities. We presented results of machine learning classification of facial emotion expression. The recognition was mainly based on a combination of 2D, 3D angle and Euclidean distance between facial key points as features carefully selected. We provided a comparison between RGB and RGB-D data performance for facial emotion recognition. Our findings deduced that the non-linear algorithms presented the best performance due the data nature. The Bagged Trees and k-NN consistently outperformed all the tested classification algorithms on our collected dataset. We observed that the 2D data are not robust enough for facial emotion recognition, which are 3D changes of facial expression. The RGB-D data can capture essential geometrical features, and enable higher precision and preservation of facial emotion critical details. The RGB-D data are more insensitive to different conditions compared to RGB data. Future works will concentrate on building real time system for facial virtual avatar animation in an immersive virtual environment.

REFERENCES

[1] Marcos-Pablos, Samuel González Pablos, Emilio Martín-Lorenzo, Carlos Flores Pérez, Luis Gómez-García-Bermejo, Jaime Zalama, Eduardo. 2016. Virtual Avatar for Emotion Recognition in Patients with Schizophrenia: A Pilot Study. Frontiers in Human Neuroscience. 10. 10.3389/fnhum.2016.00421.

[2] Bekele, Esube Bian, Dayi Zheng, Zhi Peterman, Joel Park, Sohee Sarkar, Nilanjan. 2014. Responses during Facial Emotional Expression Recognition Tasks Using Virtual Reality and Static IAPS Pictures for Adults with Schizophrenia. Human-Computer Interaction. 8526. 10.1007/978-3-319-07464-1-21.

[3] Souto, Teresa Silva, Hugo Leite, Ângela Baptista, Alexandre Queirós, Cristina Marques, António. 2019. Facial Emotion Recognition: Virtual Reality Program for Facial Emotion Recognition—A Trial Program Targeted at Individuals With Schizophrenia. Rehabilitation Counseling Bulletin. 63. 003435521984728. 10.1177/0034355219847284.

[4] Nyaz Didehbani, Tandra Allen, Michelle Kandalaft, Daniel Krawczyk, Sandra Chapman, Virtual Reality Social Cognition Training for children with high functioning autism, Computers in Human Behavior, Volume 62, 2016, Pages 703-711, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2016.04.033.

[5] Alcañiz Raya, Mariano Olmos, Elena Abad, Luis. 2019. Use of virtual reality for neurodevelopmental disorders. A review of the state of the art and future agenda. Medicina. 79. 77-81.

[6] T. Baltrušaitis, P. Robinson and L. P. Morency, "OpenFace: An open source facial behavior analysis toolkit", 2016 IEEE Winter Conference on Applications of Computer Vision (WACV), Lake Placid, NY, 2016, pp. 1-10. doi: 10.1109/WACV.2016.7477553

[7] P. C. Petrantonakis and L. J. Hadjileontiadis, "Emotion Recognition From EEG Using Higher Order Crossings", in IEEE Transactions on Information Technology in Biomedicine, vol. 14, no. 2, pp. 186-197, March 2010. doi: 10.1109/TITB.2009.2034649

[8] N. Chanthaphan, K. Uchimura, T. Satonaka and T. Makioka, "Facial Emotion Recognition Based on Facial Motion Stream Generated by Kinect," 2015 11th International Conference on Signal-Image Technology and Internet-Based Systems (SITIS), Bangkok, 2015, pp. 117-124. doi: 10.1109/SITIS.2015.31

[9] Z. Zhang, L. Cui, X. Liu and T. Zhu, "Emotion Detection Using Kinect 3D Facial Points," 2016 IEEE/WIC/ACM International Conference on Web Intelligence (WI), Omaha, NE, 2016, pp. 407-410.doi: 10.1109/WI.2016.0063

[10] X. Zhao, J. Zou, H. Li, E. Dellandréa, I. A. Kakadiaris and L. Chen, "Automatic 2.5-D Facial Landmarking and Emotion Annotation for Social Interaction Assistance," in IEEE Transactions on Cybernetics, vol. 46, no. 9, pp. 2042-2055, Sept. 2016. doi: 10.1109/TCYB.2015.2461131

[11] B. Y. L. Li, A. S. Mian, W. Liu and A. Krishna, "Using Kinect for face recognition under varying poses, expressions, illumination and disguise," 2013 IEEE Workshop on Applications of Computer Vision (WACV), Tampa, FL, 2013, pp. 186-192. doi: 10.1109/WACV.2013.6475017

[12] N. Chanthaphan, K. Uchimura, T. Satonaka, T. Makioka, "Novel facial feature extraction technique for facial emotion recognition system by using depth sensor", 2016, International Journal of Innovative Computing, Information and Control ,12 2067–2087.

[13] C . A. Gabert-Quillen, E. E. Bartolini, B. T. Abravanel, C. A. Sanislow, Ratings for emotion film clips, Behavior Research Methods 47, 2015, 773–787.

[14] Breiman, L. Machine Learning (1996) 24: 123. https://doi.org/10.1023/A:1018054314350.

[15] T. Baltrusaitis, P. Robinson and L. P. Morency, "Constrained Local Neural Fields for Robust Facial Landmark Detection in the Wild," 2013 IEEE International Conference on Computer Vision Workshops, Sydney, NSW, 2013, pp. 354-361. doi: 10.1109/ICCVW.2013.54

[16] Cristinacce D, Cootes TF. Feature detection and tracking with constrained local models. British Machine Vision Conference. 2006:929–938.

[17] B. Fasel, J. Luettin, Automatic Facial Expression Analysis: A Survey, 2003,Idiap-RR Idiap-RR-19-1999, IDIAP, 1999. Published in Pattern Recognition, 36(1):259-275.

[18] Cortes, C. and Vapnik, V. Machine Learning ,1995, 20: 273. https://doi.org/10.1023/A:1022627411411.

[19] S. Zhang, X. Li, M. Zong, X. Zhu and R. Wang, "Efficient kNN Classification With Different Numbers of Nearest Neighbors," in IEEE Transactions on Neural Networks and Learning Systems, vol. PP, no. 99, pp. 1-12. doi: 10.1109/TNNLS.2017.2673241.

[20] Hui Wang, "Nearest neighbors by neighborhood counting," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, no. 6, pp. 942-953, June 2006.doi: 10.1109/TPAMI.2006.126

[21] S. M. Lajevardi and H. R. Wu, "Facial Expression Recognition in Perceptual Color Space," in IEEE Transactions on Image Processing, vol. 21, no. 8, pp. 3721-3733, Aug. 2012. doi: 10.1109/TIP.2012.2197628

[22] Mao, Qi-rong,Pan, Xin-yu, Zhan, Yong-zhao, and Shen, Xiang-jun,"Using Kinect for real-time emotion recognition via facial expressions", Frontiers of Information Technology & Electronic Engineering,2015,vol.16, no.4, pp.272-282,issn="2095-9230".

[23] B. Amos, B. Ludwiczuk, M. Satyanarayanan, "Openface: A general-purpose face recognition library with mobile applications," CMU-CS-16-118, CMU School of Computer Science, Tech. Rep., 2016.

An extended artificial bee colony with skyline operator for solving the QoS uncertainty-aware web service composition under interval QoS properties

1st Fateh Seghir
Laboratoire des Systèmes Intelligents (LSI), Université Sétif 1
Sétif, Algérie
fateh.seghir@univ-setif.dz

2nd Ghizlane Khababa
Département d'Informatique, Université Sétif 1
Sétif, Algérie
ghizlane.khababa@yahoo.com

***Abstract*—In this paper, we provide an extended artificial bee colony (EABC) algorithm with skyline operator for solving the QoS uncertainty-aware web service composition (IQSC) problem, where the uncertain QoS properties have been expressed as intervals numbers. At first, we formulate the addressed problem as an interval constrained single-objective optimization model. Then we employ the skyline operator to reduce the search space of IQSC. Whereas, the EABC algorithm has been performed to solve IQSC in a reduced search space more effectively and efficiently. To validate the performance and efficiency of the proposed approach, we present the experimental comparisons to an existing skyline-based PSO algorithm on an interval extended version of the public QWS dataset.**

***Index Terms*—Web service composition, Quality of Service (QoS), Interval number, Skyline operator, Artificial bee colony**

I. Introduction

As far as the Service Oriented Architecture (SOA) is concerned, any hardware or software resource can be easily provided as a web service to the end-users. However, with the increasing number of the web services, it offers the same functionalities but with different values in their nonfunctional properties, known by the Quality of Service (QoS) parameters such as response time, price, availability, ..., etc. Therefore, selecting the best web services from their sets of functionally equivalent ones to build the best Composite Service (CS), which should satisfy the end-users' local and global QoS requirements, becomes a challenging problem for both industrial and academic researchers [1], [2]. This problem, known by the QoS-aware web service composition (QSC), is an NP-hard optimization one, where many optimization methods including exact, heuristic and meta-heuristic web service composition approaches have been provided to solve it [3].

From the systematic literature review of [3], most of the existing exact web services selection algorithms modeled the QSC problem as an integer/mixed-integer linear programming model [2], [4], where solvers like LpSolve[1] and CPLEX[2] have been performed to solve the modeled QSC. These solvers can get the optimal solutions of QSC, but they need the linearization of the QSC's objective functions and constraints. Moreover, as the QSC scale increases, the efficiency of the exact web services selection algorithms decreases. Therefore, those based on the evolutionary and bio-inspired algorithms like Genetic Algorithm (GA) [5], Particle Swarm Optimization (PSO) [6], Artificial Bee Colony (ABC) [7], [8], and so on, have drawn the attention of the QSC researchers. These algorithms can get optimal/near-optimal solutions within reasonable processing times and without any objective functions and constraints linearization.

All the above QSC studies consider the advertised QoS values as non-ambiguous, but in real-world environments and due to some unconditional factors of the SOAs such as the network topologies changes and economic policies. Therefore, the QoS values of web services are uncertain in nature [9]. For this reason, some recent QoS-aware web service composition approaches have been proposed to solve the QSC problem under uncertain QoS parameters that have been modeled as intervals numbers [10], [11], probabilistic variables [12] or fuzzy numbers [13]. In the web services selection process of these approaches, all the provided web services are considered as potential candidates to construct the final CS. However, some of them are not possible candidates to build this final solution. Therefore, some existing studies [14]–[16] have used the Skyline operator [17] to reduce the search space of QSC by pruning the web services that cannot be part of the final solutions, since they are dominated by some of their functionally equivalent web services partners. However, in all the aforesaid Skyline-based QSC studies, the QoS parameters are considered with precise and exact values. Hence, our motivation in this work is to provide an efficient approach for solving the QoS uncertainty-aware service composition in a reduced search space.

In this paper, we first propose an interval constrained single-objective optimization model to the QoS uncertainty-aware web service composition (IQSC) problem, where its QoS parameters are expressed as intervals numbers. Then, and to address the formulated IQSC, we propose an approach including two components. **(1)** The first one (Skyline operator) is used to reduce the search space of IQSC, and thus its best CS

[1]http://lpsolve.sourceforge.net/5.5/
[2]https://www.ibm.com/analytics/cplex-optimizer

can be found very quickly with high solution quality. **(2)** The second component is an extended version of the basic ABC algorithm, named EABC, which is performed to solve the formulated IQSC in a reduced search space more effectively and efficiently. Finally, to demonstrate the performance and efficiency of the proposed approach, we have compared it to the one of reference [15], where the comparison experiments are performed on a new interval extended version of the public QWS [18] dataset.

The remainder part of this paper is organized as follows. In Section II, we review and summarize some relevant and notable works to ours. In Section III, we give some preliminaries on intervals numbers to be used throughout the rest of this study. In Section IV, we mathematically formulate the QoS uncertainty-aware web service composition under interval QoS properties, denoted by IQSC, as an interval constrained single-objective optimization model. To address the formulated IQSC, our proposed approach, which includes two components Skyline operator and EABC, is described with details in Section V. Section VI is devoted to discuss the comparison results of our experiments. Finally, our conclusion and future work are given in Section VII.

II. Related work

From the literature, the QSC has been addressed by two main categories of web service selection approaches, including **(1)** Exact and **(2)** Meta-heuristic (i.e., evolutionary and bio-inspired) optimization methods [3]. Moreover, to improve the efficiency of the QSC approaches, the Skyline operator [17] has been used by some researchers to reduce the time of web services selection [14]–[16]. In addition, due to some unconditional factors of the SOA environments, such as the network topologies changes and economic policies [9], some QSC studies have considered the QoS parameters with ambiguous values [11], [13]. Here in this section, we have only reviewed and discussed some relevant and notable works to ours.

The exact optimization methods have modeled the QSC problem as an Integer Linear Programming (ILP) model [1] or a Mixed ILP (MILP) one [2], [4] and have solved it using existing ILP/MILP solvers such as LpSolve and CPLEX. For the QSC problem instances with small search spaces, these methods yield good performance in terms of running time and solution quality of the obtained final CSs solutions. However, the computation time of these methods increases exponentially with the increasing number of the provided functionally identical web services. Moreover, the exact optimization approaches require the linearization of the QSC objective functions and the users' global QoS constraints. Therefore, those based on evolutionary and bio-inspired optimization algorithms like GA [5], PSO [6], ABC [7], [8], and so on, have drawn the attention of the QSC researchers. Compared to the exact optimization methods that can obtain optimal CSs solutions, the meta-heuristic algorithms can get near-optimal ones, but with reasonable processing times and without any linearization of the objective functions and the users' global QoS constraints of the QSC problem.

To improve the efficiency of the QSC optimization approaches, a representative mechanism: Skyline operator [17] has been employed to reduce the search space of the QSC problem. Hence, the computation time cost of these approaches is shortened. For instance, authors of [14] were the firsts who have used the Skyline operator to reduce the QSC search space where a new service dominance based on the QoS attributes of web services has been performed, among web services, to prune the dominated ones. In this study, the QSC problem was formulated as an ILP model and solved more efficiently using the existing LpSolve solver in a reduced search space. In [15], the corresponding authors proposed a fast cloud-based web service composition approach, which prunes the redundant and dominated candidate web services by an adopted Skyline operator and performs the PSO algorithm to find out a more powerful final CS solution. In [16], the authors have used the mathematical programming language (AMPL) [19] to formulate the QSC problem as a nonlinear integer programming model, which has been solved by the existing Bonmin[3] solver. In this study, and similar to the ones of [14] and [15], the Skyline operator has been employed to reduce the search space of the QSC problem.

However, all the above studies consider the advertised QoS values as non-ambiguous ones, which is unreal for dynamic SOA environments since some unconditional factors, like network topologies and economic policies, render the QoS values uncertain in nature. Therefore, some researchers have formulated the QSC problem as a non-deterministic optimization model using interval-numbers [10], [11], fuzzy numbers [13], or probabilistic models [12].

Here, by representing the QoS uncertainty with the interval number model, we formulated the QSC problem as an interval constrained single-objective optimization one. The latter is solved by an extended artificial bee colony algorithm, while an interval-based version of the Skyline operator is employed to reduce the search space of IQSC that will improve the efficiency of the provided algorithm.

III. Preliminaries on intervals numbers

Here in this section, we have introduced the following definitions related to the intervals numbers that have been employed throughout the remainder part of this article.

***Definition** 1:* (*Interval Number* [20]) Given any two real numbers a^l and a^u with $a^l \leq a^u$. The set $A = \{x : x \in \mathbb{R}$ and $a^l \leq x \leq a^u\}$ denoted by $A = [a^l, a^u]$ is named an interval number, where a^l and a^u are called its lower and upper limits, respectively.

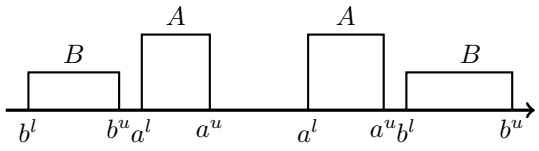
***Definition** 2:* (*Arithmetic operations on intervals numbers* [21]) Let $A = [a^l, a^u]$ and $B = [b^l, b^u]$ be any two intervals numbers, then the arithmetic operations on A and B are defined as follows:

- **Addition $\oplus$:** $A \oplus B = [a^l, a^u] \oplus [b^l, b^u] = [a^l + b^l, a^u + b^u]$

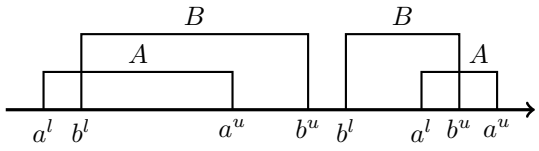
[3]https://github.com/coin-or/Bonmin

- **Subtraction** $\ominus$**:** $A \ominus B = [a^l, a^u] \ominus [b^l, b^u] = [a^l - b^u, a^u - b^l]$
- **Multiplication** $\otimes$**:** $A \otimes B = [a^l, a^u] \otimes [b^l, b^u] = [m^l, m^u]$ with $m^l = \min(a^l b^l, a^l b^u, a^u b^l, a^u b^u)$ and $m^u = \max(a^l b^l, a^l b^u, a^u b^l, a^u b^u)$
- **Scalar multiplication:** $\forall \lambda \in \mathbb{R}$, $\lambda \otimes A = \lambda \otimes [a^l, a^u] = \begin{cases} [\lambda * a^l, \lambda * a^u] \text{ if } \lambda >= 0 \\ [\lambda * a^u, \lambda * a^l] \text{ if } \lambda < 0 \end{cases}$

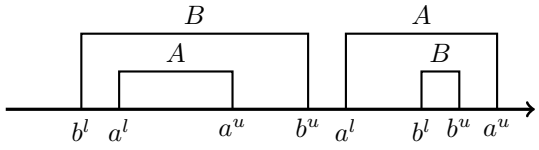
Moreover, let $A = [a^l, a^u]$ and $B = [b^l, b^u]$ be any two intervals numbers, the three possible types of overlapping between A and B as shown in Fig. 1 [22] are used in the following definitions for ranking intervals numbers of the maximization (minimization) optimization problems with objective functions modeled as intervals numbers.



(a) **Type I:** Non-overlapping between intervals numbers



(b) **Type II:** Partial overlapping between intervals numbers



(c) **Type III:** Full overlapping between intervals numbers

Fig. 1. Types of overlapping between intervals numbers

***Definition** 3: (Interval greater ranking operator for maximization optimization problems:* $>_{\max}$ [11]) For any two intervals numbers $A = [a^l, a^u]$ and $B = [b^l, b^u]$, the interval greater ranking operator $>_{\max}$ between A and B is defined as follows:

1) For intervals numbers of Type I or Type II, $A >_{\max} B$ if $(a^l > b^l)$ and $(a^u > b^u)$;
2) For intervals numbers of Type III, $A >_{\max} B$ if:
   a) $(a^l - b^l) > (b^u - a^u)$;
   b) or $\big((a^l - b^l) = (b^u - a^u)\big)$ and $(a^u < b^u)$

***Definition** 4: (Interval smaller ranking operator for minimization optimization problems:* $<_{\min}$) [11]) For any two intervals numbers $A = [a^l, a^u]$ and $B = [b^l, b^u]$, the interval smaller ranking operator $<_{\min}$ between A and B is defined as follows:

1) For intervals numbers of Type I or Type II, $A <_{\min} B$ if $(a^l < b^l)$ and $(a^u < b^u)$;
2) For intervals numbers of Type III, $A <_{\min} B$ if:
   a) $(a^l - b^l) < (b^u - a^u)$;
   b) or $\big((a^l - b^l) = (b^u - a^u)\big)$ and $(a^u < b^u)$

***Definition** 5: (Interval equal ranking operator*: $=$) For any two intervals numbers $A = [a^l, a^u]$ and $B = [b^l, b^u]$, if $a^l = b^l$ and $a^u = b^u$ then A and B are equal intervals numbers represented as $A = B$.

***Definition** 6:* For any two intervals numbers A and B, the interval greater or equal ($\geq_{\max}$) and the interval smaller or equal ($\leq_{\min}$) ranking operators for the maximization and the minimization optimization problems, respectively, are defined as follows:

- $A \geq_{\max} B \Leftrightarrow (A >_{\max})$ or $(A = B)$
- $A \leq_{\min} B \Leftrightarrow (A <_{\min})$ or $(A = B)$

***Theorem** 1:* Given any three intervals numbers A, B and C, the following mathematical order relations are provided:

($\mathcal{O}1$) $A \leq_{\min} (\geq_{\max}) A$, which is named reflexivity.
($\mathcal{O}2$) If $A \leq_{\min} (\geq_{\max}) B$ and $B \leq_{\min} (\geq_{\max}) A$ then $A = B$, which is named anti-symmetry.
($\mathcal{O}3$) If $A \leq_{\min} (\geq_{\max}) B$ and $B \leq_{\min} (\geq_{\max}) C$ then $A \leq_{\min} (\geq_{\max}) C$, which is named transitivity.

***Proof** of **Theorem** 1 :* Since the pages number of this paper is limited; the mathematical order relations proofs of $\mathcal{O}1$, $\mathcal{O}2$ and $\mathcal{O}3$ are omitted. We have easily proofed them using Definitions 3, 4, 5 and 6.

***Definition** 7: (The interval minimum* (Min) *and the interval maximum* (Max) *operators*) let $\{A_j, j = 1, 2, \ldots, m\}$ be a set of m intervals numbers, then the minimum and the maximum intervals numbers of $\{A_j, j = 1, 2, \ldots, m\}$ for the minimization and the maximization optimization problems, respectively, are defined as follows:

- If $A_q \leq_{\min} A_j$ for all $j = 1, 2, \ldots, m$ with $j \neq q$ then $A_q = \text{Min}_{j=1}^{m}\{A_j\}$ is the minimum interval number of $\{A_j, j = 1, 2, \ldots, m\}$.
- If $A_p \geq_{\max} A_j$ for all $j = 1, 2, \ldots, m$ with $j \neq p$ then $A_p = \text{Max}_{j=1}^{m}\{A_j\}$ is the maximum interval number of $\{A_j, j = 1, 2, \ldots, m\}$.

IV. Interval model of the QoS uncertainty-aware web service composition problem

Let given a very large set of atomic web services, where each web service, denoted by ws, is characterized by two types of properties, functional and nonfunctional ones. The functional parameters (i.e., input and output attributes) of a ws represent its supported functionality. Whereas, the non-functional properties (QoS) of a ws, such as response time, availability, reputation, price, ..., etc, represent its parameters quality. Each QoS attribute, denoted by q_t with $t = 1, 2, \ldots, r$ and r is the size of the whole considered QoS parameters, can be either positive or negative parameter, where a ws with larger (lower) values in its positive q_ts, the better (worse) is, whereas a ws with lower (larger) values in its negative q_ts, the better (worse) is. Here in this study, the positive list of q_ts is denoted by QoS^+ and the negative list of q_ts is indicated by QoS^-. For example, the reputation and availability attributes belong to the QoS^+ list, whereas the price and response time parameters belong to the QoS^- list. Furthermore, a web

services class, denoted by $S = \{ws_1, ws_2, \ldots, ws_m\}$, is a set of m atomic web services that have similar functionalities but with different values in their q_ts.

As seen in Fig. 2, which represents the graphic depiction of the QSC problem. For a given abstract composite service, denoted by $ACS = \{S_1, S_2, \ldots, S_n\}$, which represents the n needed web services classes to reply a complex user request, and a list of k user's global QoS requirements, denoted by Cst_{q_k}s with $k \leq r$. A concert composite service, indicated by CCS, represents the user request's response, which is built by selecting from each web services class $S_i = \{ws_i^1, ws_i^2, \ldots, ws_i^{m_i}\}$ a unique web service ws_i^j with $j \leq m_i$, where the global QoS values of CCS that have been evaluated by aggregating the QoS values of their atomic wss should meet the considered Cst_{q_k}s. In this study, as shown in Fig 3, four basic connection structures (i.e., sequential, parallel, branch and loop) have been considered to compose the atomic wss of CCSs. Furthermore, due to some unconditional factors of the SOAs like network architectures changes and economic policies, the wss' QoS values are uncertain in nature [9]. Therefore, motivated by the fact that the interval number is efficient, general and easy representation model to express perfectly the uncertain QoS values [11], and by considering the four mostly used QoS parameters in solving the QSC problem [2] including two positive QoS attributes: *availability* (q_1) and *throughput* (q_2), and two negative ones: *response time* (q_3) and *price* (q_4). Hence, the interval constrained single-objective optimization model of QSC, denoted by IQSC, can be stated as follows:

Determine the best CCS solution among all the possible ones[4], which maximize

$$\text{Maximize } IU(CCS) = \textstyle\sum_{t=1}^{r} w_{q_t} \otimes \overline{CCS_{q_t}} \tag{1}$$

Subject to k user's global QoS constraints

$$\forall t = 1 \ldots k \begin{cases} CCS_{q_t} \leq_{\min} Cst_{q_t}, \text{ if } q_t \in QoS^- \\ CCS_{q_t} \geq_{\max} Cst_{q_t}, \text{ if } q_t \in QoS^+ \end{cases} \tag{2}$$

Where CCS_{q_t} is the global interval QoS value of the CCS solution in the q_t attribute that can be evaluated as seen in Table I using the interval arithmetic operations given in Definition 2 and the four basic connection structures as depicted in Fig. 3 for the interval values $ws_{i,q_t} = \left[ws_{i,q_t}^l, ws_{i,q_t}^u\right]$ of each atomic web service ws_i of CCS. $IU(CCS)$ is the interval utility function of CCS that maps the CCS_{q_t}s values into a single interval value. This function adopts the well-known *Simple Additive Weighting* (SAW) method [23] through scaling the interval values CCS_{q_t}s into their normalized interval ones $\overline{CCS_{q_t}}$s. Then afterwards, these normalized values are aggregated using the weights w_{q_t}s with $w_{q_t} \in [0, 1]$ and $\sum_{t=1}^{r} w_{q_t} = 1$, which represent the importance and priority of each q_t by the user. The normalized interval value $\overline{CCS_{q_t}}$ of its related original one $CCS_{q_t} = \left[CCS_{q_t}^l, CCS_{q_t}^u\right]$ is calculated as given in the following interval positive and negative normalization Equations 3 and 4, respectively.

[4]For an ACS of n web services classes, where each one has m candidate web services, then m^n different CCSs can be obtained

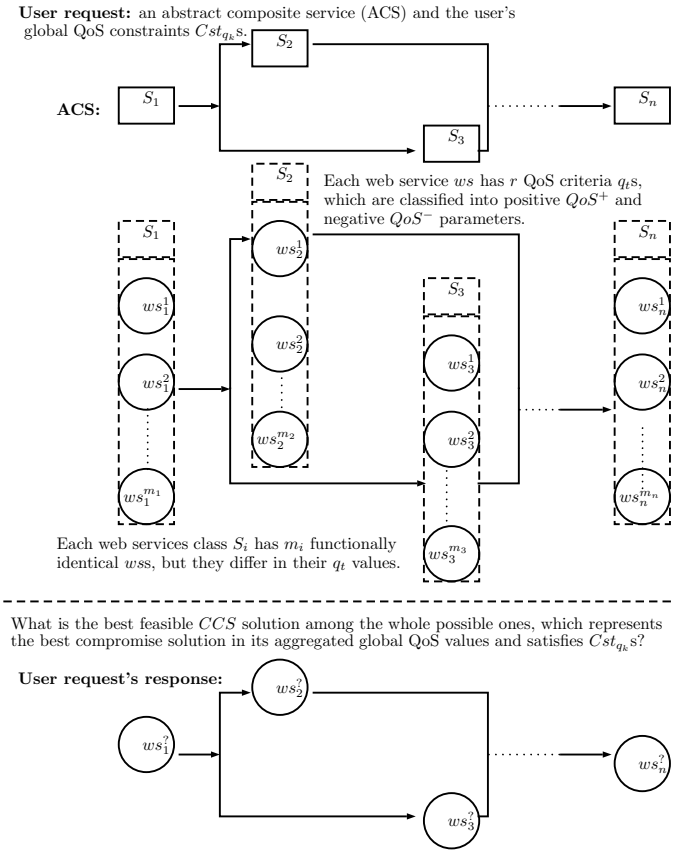


Fig. 2. Graphic depiction of the QoS-aware web service composition problem

- Interval positive normalization

$$\forall q_t \in QoS^+, \overline{CCS_{q_t}} = \begin{cases} \left[\frac{CCS_{q_t}^l - min_{q_t}^l}{max_{q_t}^u - min_{q_t}^l}, \frac{CCS_{q_t}^u - min_{q_t}^l}{max_{q_t}^u - min_{q_t}^l}\right] & \text{if } max_{q_t}^u \neq min_{q_t}^l \\ [1, 1] & \text{if } max_{q_t}^u = min_{q_t}^l \end{cases} \tag{3}$$

- Interval negative normalization

$$\forall q_t \in QoS^-, \overline{CCS_{q_t}} = \begin{cases} \left[\frac{max_{q_t}^u - CCS_{q_t}^u}{max_{q_t}^u - min_{q_t}^l}, \frac{max_{q_t}^u - CCS_{q_t}^l}{max_{q_t}^u - min_{q_t}^l}\right] & \text{if } max_{q_t}^u \neq min_{q_t}^l \\ [1, 1] & \text{if } max_{q_t}^u = min_{q_t}^l \end{cases} \tag{4}$$

Where the real limit values $min_{q_t}^l$ and $max_{q_t}^u$ for an $ACS = (S_1, S_2, \ldots, S_n)$ with $\forall i \in \{1, 2 \ldots, n\}$, $S_i = \{ws_i^1, ws_i^2, \ldots, ws_i^{mi}\}$ and $\forall j \in \{1, 2 \ldots, m_i\}$, $ws_{i,q_t}^j = \left[ws_{i,q_t}^{j,l}, ws_{i,q_t}^{j,u}\right]$ are evaluated as follows

$$max_{q_t}^u = Agg_{q_t}{}_{i=1}^{n} \left(\text{Max}_{j=1}^{m_i} \left\{ws_{i,q_t}^{j,u}\right\}\right) \tag{5}$$

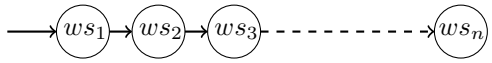
$$min_{q_t}^l = Agg_{q_t}{}_{i=1}^{n} \left(\text{Min}_{j=1}^{m_i} \left\{ws_{i,q_t}^{j,l}\right\}\right) \tag{6}$$

Where $Agg_{q_t}{}_{i=1}^{n}$ denotes the related crisp QoS aggregation formula (i.e., $\sum$, $\prod$, Min and Max) of the q_t attribute as defined in Table I that has been employed to aggregate the n

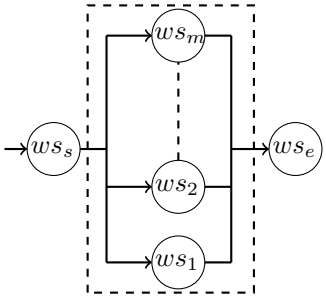
TABLE I
INTERVAL QOS AGGREGATION FORMULAS FOR EVALUATING THE GLOBAL QOS VALUES OF CONCRETE COMPOSITES SERVICES CCSs

QoS parameter	n **sequential web services** ws_i	m **parallel web services** ws_i	**branch**[a] **of** m **web services** ws_i **with their** pr_i**s probabilities**	**call a web service** ws **with** p **times**
Availability (q_1)	$\prod_{i=1}^{n}\left[ws_{i,q_1}^{l}, ws_{i,q_1}^{u}\right]$	$\prod_{i=1}^{m}\left[ws_{i,q_1}^{l}, ws_{i,q_1}^{u}\right]$	$\mathrm{Min}_{i=1}^{m}\left\{\left[ws_{i,q_1}^{l}, ws_{i,q_1}^{u}\right]\right\}$	$\prod_{i=p}^{n}\left[ws_{i,q_1}^{l}, ws_{i,q_1}^{u}\right]$
Throughput(q_2)	$\mathrm{Min}_{i=1}^{n}\left\{\left[ws_{i,q_2}^{l}, ws_{i,q_2}^{u}\right]\right\}$	$\mathrm{Min}_{i=1}^{m}\left\{\left[ws_{i,q_2}^{l}, ws_{i,q_2}^{u}\right]\right\}$	$\mathrm{Min}_{i=1}^{m}\left\{\left[ws_{i,q_2}^{l}, ws_{i,q_2}^{u}\right]\right\}$	$\left[ws_{i,q_2}^{l}, ws_{i,q_2}^{u}\right]$
Response time (q_3)	$\sum_{i=1}^{n}\left[ws_{i,q_3}^{l}, ws_{i,q_3}^{u}\right]$	$\mathrm{Max}_{i=1}^{m}\left\{\left[ws_{i,q_3}^{l}, ws_{i,q_3}^{u}\right]\right\}$	$\mathrm{Max}_{i=1}^{m}\left\{\left[ws_{i,q_3}^{l}, ws_{i,q_3}^{u}\right]\right\}$	$p * \left[ws_{i,q_3}^{l}, ws_{i,q_3}^{u}\right]$
Price (q_4)	$\sum_{i=1}^{n}\left[ws_{i,q_4}^{l}, ws_{i,q_4}^{u}\right]$	$\sum_{i=1}^{m}\left[ws_{i,q_4}^{l}, ws_{i,q_4}^{u}\right]$	$\mathrm{Max}_{i=1}^{m}\left\{\left[ws_{i,q_4}^{l}, ws_{i,q_4}^{u}\right]\right\}$	$p * \left[ws_{i,q_4}^{l}, ws_{i,q_4}^{u}\right]$

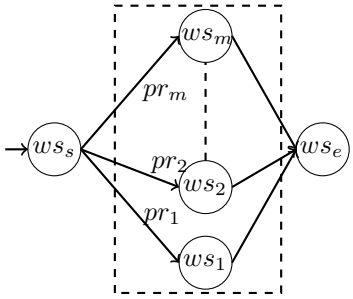
[a]In the branch connection structure, according to the pr_is of ws_i, only one web service among them is executed.



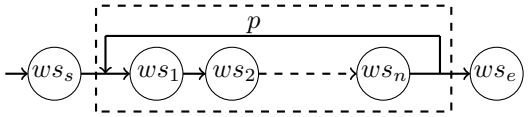
(a) Sequential connection of n wss



(b) Parallel connection of m wss



(c) Branch connection of m wss with their pr_is probabilities, $\forall i = 1, 2, \ldots, m$: $pr_i \in$ [0,1] and $\sum_{i=1}^{m} pr_i = 1$



(d) Loop conncetion structure of n wss with p calls

Fig. 3. Connection structures between atomic web services

obtained real values $\mathrm{Max}\left\{ws_{i,q_t}^{j,u}\right\}/\mathrm{Min}\left\{ws_{i,q_t}^{j,l}\right\}$ from each web services class S_i with $j = 1, 2, \ldots, m_i$.

V. PROPOSED APPROACH

To solve the IQSC problem, we propose an approach including two components. The first one, which uses the Skyline operator [17], is employed to reduce the search space of IQSC by pruning the dominated candidate web services. The second component is to quickly find out the optimal/near-optimal solution of IQSC by performing an interval extended version of the basic ABC algorithm, named EABC.

A. Skyline service

Our main goal in this study is to find an optimal/near-optimal CCS solution for IQSC that maximize the interval utility value as defined in Equation 1 and satisfies the user's overall QoS constraints as given in Equation 2. This optimal/near-optimal solution contains a set of atomic wss, where each one is selected from its related web services class. However, not all wss of each web services class are potential candidates to construct the final optimal/near-optimal solution. Hence, some existing studies [14]–[16] have used the Skyline operator [17] to reduce the search space of QSC by pruning the wss that cannot be part of the final solutions, since they are dominated by some of their functionally identical wss partners. However, in the whole aforesaid skyline-based studies, the QoS parameters are considered with precise and exact values. Therefore, extended definitions of *Service Dominance* and *Skyline Service* [15] that consider QoS properties as intervals numbers have been introduced in this paper.

***Definition** 8:* (*Service Dominance*) Let's consider a web services class S and two web services $ws_1, ws_2 \in S$, where each one has a set of QoS parameters q_ts . We say ws_1 dominates ws_2, denoted as $ws_1 \prec ws_2$, if and only if: **(1)** $\forall q_t \in QoS^+$: $ws_{1,q_t} \geq_{\max} ws_{2,q_t}$ and $\exists q_t \in QoS^+, ws_{1,q_t} >_{\max} ws_{2,q_t}$, and **(2)** $\forall q_t \in QoS^-$: $ws_{1,q_t} \leq_{\min} ws_{2,q_t}$ and $\exists q_t \in QoS^-, ws_{1,q_t} <_{\min} ws_{2,q_t}$.

***Definition** 9:* (*Skyline Service*) For a given web services class $S = \{ws_1, ws_2, \ldots, ws_m\}$ of m functionally identical wss. The skyline service of S, denoted by SkS, contains the candidate wss in S that cannot be dominated by any other ws of S. i.e, $SkS = \{ws_i \in S \mid \nexists ws_j \in S : ws_j \prec ws_i\}$.

To define the skyline service SkS of each web services class S, the skyline computation process performs pair-wise comparisons between the ws_{q_t}s interval values of the compared wss of S. This calculation process can be expensive in terms of evaluation time, especially, if S has numerous wss. However, for the IQSC problem, the skylines services are independent of any online user request [14]. Therefore, the skyline computation can be performed offline by any of the exiting efficient skyline algorithms [17].

B. Extended Artificial Bee Colony: EABC

The ABC algorithm is a well-known bio-inspired optimization algorithm that mimics the smart work of honey bees to find out the optimal/near-optimal solution of an optimization problem [24]. It has been widely applied to solve the QSC problem for several service-based environments like service-oriented applications [8] and cloud computing [7]. Similar to the canonical ABC algorithm, in order to find out the optimal/near-optimal solution of IQSC, EABC performs repetitively and successively three types of bees (Employees, Onlookers and Scouts) on each explored food sources area src_g to find a new better one src_{g+1} with $g = 0, 1, 2, \ldots, MITR$ and $MITR$ is a maximum iteration number of the EABC algorithm. The initial food sources area of Z solutions (food sources positions) $src_0 = \{CCS_1^0, CCS_2^0, \ldots, CCS_Z^0\}$ is generated randomly, where the dimensional values (i.e., web services) of each food source position CCS_z^0 with $z = 1, 2, \ldots, Z$ are defined according to the encoding schema given in the next Section and its nectar amount (i.e. fitness value) is evaluated through using the interval utility function, i.e., $IU(CCS_z^0)$, as defined in Equation 1. Moreover, for each generated food source position CCS_z^0, an integer variable $trial_z$, which is initialized to zero, is assigned to it. In the following subsections, we describe the encoding schema of CCSs, generation of the initial food sources area src_0, the works of the three types of bees for searching good food sources areas, which are *Employees work*, *Onlookers work* and *Scouts work*, as well as the ending criterion of EABC.

1) Encoding schema of food sources positions CCSs and generation of the initial food sources area src_0: Here, in this study, an n-dimensional array of integers is used to represent each food source position CCS_z^g of the g^{th} food sources area src_g, where $z = 1, 2, \ldots, Z$ and Z is the number of food sources positions (i.e., population size of EABC). The CCS_z^g position denoted as $CCS_z^g = (CCS_{z,1}^g, CCS_{z,2}^g, \ldots, CCS_{z,n}^g)$ has n integer elements indicating the selected atomic wss from their skylines services SkS_i, $i = 1, 2, \ldots, n$. For the initial food sources area src_0, each integer element of each food source position $CCS_z^0 = (CCS_{z,1}^0, CCS_{z,2}^0, \ldots, CCS_{z,n}^0)$ was randomly generated as follows

$$\begin{gathered} \forall : i = 1, 2, \ldots, n \\ CCS_{z,i}^0 = 1 + \lceil rand(0,1) * (m_r - 1) \rceil \end{gathered} \tag{7}$$

Where $CCS_{z,i}^0$ is an integer number representing the i^{th} selected ws from the i^{th} skyline service SkS_i that has m_i functionally identical wss, $rand(0,1)$ is a real number, which was randomly generated from the range $[0, 1]$, and $\lceil\ \rceil$ is the rounding up integer function.

2) Employees work: The employees bees explore each current food sources area src_g to find a new better one src_g^{Emp}, where similar to the ABC's conventional updating positions of food sources [24], only one dimension (i.e., a unique web service) of each food source position $CCS_z^g = (CCS_{z,1}^g, CCS_{z,2}^g, \ldots, CCS_{z,j}^g, \ldots, CCS_{z,n}^g)$ with n atomic web services is considered to update the CCS_z^g position. Hence, the new food source position $CCS_z^{Emp} = (CCS_{z,1}^g, CCS_{z,2}^g, \ldots, CCS_{z,j}^{Emp}, \ldots, CCS_{z,n}^g)$ has the same atomic web services as its old one CCS_z^g, except for the j^{th} web service (i.e., the $CCS_{z,j}^{Emp}$ value), which is defined using the following Equation.

$$CCS_{z,j}^{Emp} = \lceil CCS_{z,j}^g + \phi_j * (CCS_{z,j}^g - CCS_{l,j}^g) \rceil \tag{8}$$

Where for each explored CCS_z^g, j is a randomly-selected dimension (i.e., the j^{th} skyline service SkS_j) from the range $[1, n]$, CCS_l^g with $l \neq z$ represents a randomly-selected food source position from src_g, ϕ_j is a random generated real value within the range $[-1, 1]$ for every selected skyline service SkS_j and $\lceil\ \rceil$ is the rounding up integer function.

After defining the new food sources positions CCS_z^{Emp}s with $z = 1, 2, \ldots, Z$, their interval utility values, i.e., $IU(CCS_z^{Emp})$, are calculated using Equation 1. And finally, in order to update each old food source position CCS_z^g by its new defined one CCS_z^{Emp}, the greedy selection mechanism of ABC [24] is adapted through using the following steps of the Deb's selection procedure [25].

- If CCS_z^{Emp} and CCS_z^g are feasible food sources positions and $IU(CCS_z^{Emp}) >_{\max} IU(CCS_z^g)$ then CCS_z^{Emp} is maintained and its $trial_z$ is reset to zero.
- If CCS_z^{Emp} is a feasible food source position and CCS_z^g is an infeasible one then CCS_z^{Emp} is maintained and its $trial_z$ is reset to zero.
- If CCS_z^{Emp} is an infeasible food source position and CCS_z^g is a feasible one then CCS_z^{Emp} is replaced by its old one CCS_z^g and its $trial_z$ is incremented by one.
- If CCS_z^{Emp} and CCS_z^g are infeasible food sources positions then:
  - If the lower global constraint violation of CCS_z^{Emp}, as will be given in the next paragraph, is lower than the one of CCS_z^g then CCS_z^{Emp} is maintained and its $trial_z$ is reset to zero; otherwise, CCS_z^{Emp} is changed by its old one CCS_z^g and its $trial_z$ is augmented by one.

Global constraint violation of an infeasible food source position: Given any infeasible food source position, denoted by $ICCS$, the constraint violation amounts of its violated user's overall QoS requirements, denoted by $ICCS_{q_k}^{cst}$s, are evaluated as follows.

$$\begin{aligned} \forall q_k \in QoS^+ :\ & \text{if } Cst_{q_k} >_{\max} ICCS_{q_k} \text{ then} \\ & ICCS_{q_k}^{cst} = Cst_{q_k} \ominus ICCS_{q_k} \end{aligned} \tag{9}$$

$$\begin{aligned} \forall q_k \in QoS^- :\ & \text{if } Cst_{q_k} <_{\min} ICCS_{q_k} \text{ then} \\ & ICCS_{q_k}^{cst} = ICCS_{q_k} \ominus Cst_{q_k} \end{aligned} \tag{10}$$

By adapting the SAW method [23] to support the interval numbers calculations, the $ICCS_{q_k}^{cst}$s intervals values are aggregated into a single interval value $ICCS_{cst}$ through using the following equation.

$$ICCS_{cst} = \frac{1}{V} \otimes \sum_{t=1}^{k} \overline{ICCS_{q_t}^{cst}} \tag{11}$$

Where V is the total number of the violated overall QoS constraints by $ICCS$, $\overline{ICCS_{q_k}^{cst}}$ is the normalized interval value of its associated original one $ICCS_{q_k}^{cst} = \left[ICCS_{q_k}^{l,cst}, ICCS_{q_k}^{u,cst}\right]$ for the kth user's global QoS constraint $Cst_{q_k} = \left[Cst_{q_k}^{l}, Cst_{q_k}^{u}\right]$. Since the lower $ICCS_{q_k}^{cst}$ is, the lower its global constraint violation amount is (i.e., in other words, the higher its aggregated normalized interval value of its violated constraint $ICCS_{cst}$ is). Therefore, the interval values $\overline{ICCS_{q_k}^{cst}}$s are calculated using the interval negative normalization process as given in the following Equations.

$$\forall q_k \in QoS^{-}, \overline{ICCS_{q_k}^{cst}} = \begin{cases} \left[\frac{max_{q_k}^{u} - Cst_{q_k}^{l} - ICCS_{q_k}^{u,cst}}{\left(max_{q_k}^{u} - Cst_{q_k}^{l}\right) - \left(min_{q_k}^{l} - Cst_{q_k}^{u}\right)}, \frac{max_{q_k}^{u} - Cst_{q_k}^{l} - ICCS_{q_k}^{l,cst}}{\left(max_{q_k}^{u} - Cst_{q_k}^{l}\right) - \left(min_{q_k}^{l} - Cst_{q_k}^{u}\right)}\right] & \text{if } \left(max_{q_k}^{u} - Cst_{q_k}^{l}\right) \neq \left(min_{q_k}^{l} - Cst_{q_k}^{u}\right) \\ [1,1] & \text{if } \left(max_{q_k}^{u} - Cst_{q_k}^{l}\right) = \left(min_{q_k}^{l} - Cst_{q_k}^{u}\right) \end{cases} \quad (12)$$

$$\forall q_k \in QoS^{+}, \overline{ICCS_{q_k}^{cst}} = \begin{cases} \left[\frac{max_{q_k}^{u} - Cst_{q_k}^{l} + ICCS_{q_k}^{l,cst}}{\left(max_{q_k}^{u} - Cst_{q_k}^{l}\right) - \left(min_{q_k}^{l} - Cst_{q_k}^{u}\right)}, \frac{max_{q_k}^{u} - Cst_{q_k}^{l} + ICCS_{q_k}^{u,cst}}{\left(max_{q_k}^{u} - Cst_{q_k}^{l}\right) - \left(min_{q_k}^{l} - Cst_{q_k}^{u}\right)}\right] & \text{if } \left(max_{q_k}^{u} - Cst_{q_k}^{l}\right) \neq \left(min_{q_k}^{l} - Cst_{q_k}^{u}\right) \\ [1,1] & \text{if } \left(max_{q_k}^{u} - Cst_{q_k}^{l}\right) = \left(min_{q_k}^{l} - Cst_{q_k}^{u}\right) \end{cases} \quad (13)$$

Where $max_{q_k}^{u}$ and $min_{q_k}^{l}$ have been previously defined in Equations 5 and 6, respectively.

3) Onlookers work: The onlooker bees select Z food sources positions from the discovered src_g^{Emp} by the employees bees to be explored again. In the basic ABC algorithm, the selection criterion of the Z food sources positions is based on the roulette wheel selection [24]. However, the latter has the local optima stagnation problem [26]. Therefore, in our study, the binary tournament selection method [27] is employed to create the new selected food sources area, denoted by src_g^{Sel}. The same Deb's selection procedure as given in the above subsection is used to create src_g^{Sel} by repeating this selection procedure Z times for each two randomly-selected solutions from the discovered food sources area src_g^{Emp}.

Again, a new food sources area src_g^{Onl} is explored from the selected one src_g^{Sel} through using the same updating food sources positions given in Equation 8, where the aforesaid steps of the Deb's selection procedure given in the *Employees work* subsection are used to update src_g^{Sel} by src_g^{Onl}.

4) Scouts work: Like the scouts work of the original ABC algorithm, here, the scouts bees of EABC are used to update one randomly-selected food source position from the generated ones by the onlookers bees (i.e., src_g^{Onl}) that have not updated theirs positions after $limit$ iterations, where the $limit$ parameter of EABC indicates the criterion to identify an abandoned food source position. The latter is updated using Equation 7 and its $trial$ value is reinitialized to zero. As result, a new food sources area src_{g+1} is obtained.

5) Ending criterion of EABC: The aforesaid works of employees, onlookers and scouts bees are repeated for each new generated food sources area src_{g+1} until the stopping criterion of the EABC algorithm is satisfied (i.e., the maximum iteration number $MITR$ is reached). The best feasible food source position among the ones of the last discovered src_{g+1} that has the highest interval utility value is the final optimal/near-optimal CSS solution in solving IQSC by EABC.

VI. Experiments

In order to validate the effectiveness of our proposed approach, we have used two comparison metrics: **(a) Running time** and **(b) Optimality**. The first one indicates the needed computation time by each performed algorithm to find out its optimal/near-optimal solutions in solving IQSC. Whereas, the second one shows the quality of these obtained solutions in terms of their interval utility values as defined in Equation 1.

A. Interval version of the public QWS dataset

In the comparison experiments, as the public QWS dataset [18] was published with 2507 atomic web services, where each web service has 09 non-ambiguous QoS values for 09 QoS properties including (1) Response Time, (2) Availability, (3) Throughput, (4) Successability, (5) Reliability, (6) Compliance, (7) Best Practices, (8) Latency and (9) Documentation. Therefore, an interval version of QWS, denoted by IQWS, is provided to be used in our experiments, where the QoS intervals numbers of IQWS are generated via multiplying the precise QoS values of each considered QoS parameter of QWS by the random interval number $[r_1, r_2]$ with $r_1 = 0.9 + 0.1 * rand(0,1)$, $r_2 = 1.0 + 0.1 * rand(0,1)$, and $rand(0,1)$ is a uniformly distributed random real number in the range $[0,1]$. Since the QWS dataset dos not contain the price parameter, and as we said previously, only the availability (q_1), throughput (q_2), response time (q_3) and price (q_4) attributes are considered to generate the IQWS dataset. Hence, the interval numbers of the price attribute have been randomly generated by $r3 \otimes [r_1, r_2]$ with $r3$ is a random generated real number from the range $[2,5]$\$. Moreover, the importance and priorities of the four considered QoS attributes were set to the same value (i.e, $\forall t \in \{1,2,3,4\}, w_{q_t} = \frac{1}{4}$) and each considered user's global QoS requirement Cst_{q_t} for the

q_t attribute was set as given in the following Equation.

$$Cst_{q_t} = \left[\max\left(r_1 * SU_{q_t}, min^l_{q_t}\right), \min\left(r_2 * SU_{q_t}, max^u_{q_t}\right)\right]$$

With

$$SU_{q_t} = \begin{cases} \mu_{q_t} * (max^u_{q_t} - min^l_{q_t}) + min^l_{q_t} & \text{if } q_t \in QoS^+ \\ max^u_{q_t} - \mu_{q_t} * (max^u_{q_t} - min^l_{q_t}) & \text{if } q_t \in QoS^- \end{cases} \quad (14)$$

Where $\mu_{q_t} \in [0, 1]$ is a severity factor, which is used to adjust the considered user's global QoS constraint Cst_{q_t}, and $max^u_{q_t}$ and $min^l_{q_t}$ are calculated as given by Equations 5 and 6, respectively.

Here, only two global QoS constraints Cst_{q_3} and Cst_{q_4} of the response time and price attributes are considered in solving IQSC by setting their severity factors μ_{q_3} and μ_{q_4} to 0.3 and 0.2, respectively, whereas, μ_{q_1} and μ_{q_2} of the availability and throughput properties are set to the zero values.

B. Parameters setting of the compared algorithms

To investigate the performance and the efficiency of our proposed EABC, we have compared it to that obtained using the PSO algorithm with skyline operator [15]. The latter was proposed to solve the QSC problem with non-ambiguous QoS parameters. Hence, we have adapted it to support interval utility calculations of solutions as defined in Equation 1. For simplicity, the extended version of the proposed PSO-based approach in [15] is named EPSO. For the parameters setting of the two compared approaches, EABC and EPSO share the same population size ($Z = 40$) and the same stopping criterion, which is the number of solutions evaluations that was set to 50000. However, for their appropriate parameters, the inertia weight (w) and the two accelerating coefficients (c_1 and c_2) of EPSO are set to $w = 0.8$ and $c_1 = c_2 = 2.0$, as they were recommended in their related reference [15]. Whereas, the $limit$ parameter of EABC was set to the value of 80.

EABC and EPSO are performed to solve five abstract composite services ACS^m_ns, with $(n, m) \in \{(5, 501), (10, 250), (15, 167), (20, 125), (25, 100)\}$, where each ACS^m_n consists of solving IQSC with n web services classes per m functionally identical web services that have been randomly selected from the 2507 ones of IQWS. The compared algorithms are implemented with Matlab R2016b and performed on the same personnel computer, which runs Windows 7 and has an Intel(R) Core(TM) i5-4570, CPU 3.20 GHz and 4 Go of memory as a hardware configuration. For each ACS^m_n, the compared EABC and EPSO algorithms are carried out 30 independent times to define the best, worst and average optimality values, and average running times of their obtained optimal/near-optimal solutions.

C. Comparison results discussion

For each solved ACS^m_n, the best, worst and average interval utility values of the obtained optimal/near-optimal solutions by EABC and EPSO have been written down in Table II, and the average running times to get these optimal solutions over 30 independent executions have been plotted in Fig. 4. As we can show from the results of solving the five ACS^m_ns listed in Table II, that our proposed EABC reach very higher interval optimality values compared to the ones of EPSO. Furthermore, as seen in Fig. 4, when the number of web services classes n was set with small values, i.e., $n \leq 10$, the average running times of EPSO are better than the ones of EABC. However, when n was set with large values, $n \geq 15$, our proposed EABC algorithm obtain optimal/near-optimal solutions with less average running times compared to ones of EPSO.

From this discussion, our EABC outperforms the compared EPSO, especially for solving users requests that need the composition of an important number of atomic web services.

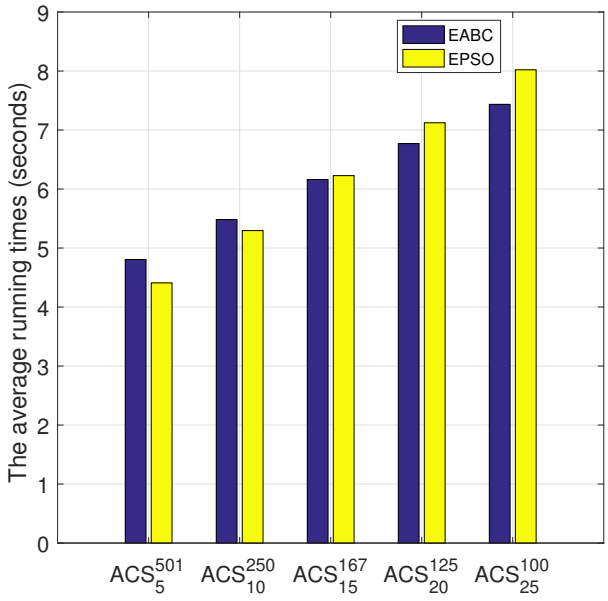


Fig. 4. The average running times of EABC and EPSO in solving ACS^m_ns of n web services classes per m functionally equivalent web services.

VII. Conclusion and Future Work

In this study, the interval number, which is a simple and general uncertain model, is used to represent the ambiguity of the QoS values in solving the QoS uncertainty-aware web service composition problem. The latter is modeled as an interval constrained single-objective optimization (IQSC) model, while a new approach that combines two components: skyline operator and interval extended version of the basic artificial bee colony (EABC) algorithm, is introduced to address the formulated IQSC. The first component (skyline operator) is used to reduce the search space of IQSC by pruning the redundant and dominated web services from their sets of functionally equivalent ones. Whereas, the second component (EABC) is performed to obtain the optimal/near-optimal composite service of IQSC in a reduced search space. The experimental results of comparing our proposed approach to an existing skyline-based PSO method, which have been performed on an interval extended version of the public QWS dataset, demonstrate and validate the performance of the introduced approach. As a future work, we are planning

TABLE II

COMPARISON RESULTS OF THE BEST, WORST AND AVERAGE INTERVAL UTILITY VALUES OF THE OBTAINED OPTIMAL/NEAR-OPTIMAL SOLUTIONS BY THE COMPARED APPROACHES IN SOLVING EACH ACS_n^m OF IQSC WITH n WEB SERVICES CLASSES PER m FUNCTIONALLY EQUIVALENT WEB SERVICES

ACS_n^m	EABC			EPSO		
	Best	***Worst***	***Average***	***Best***	***Worst***	***Average***
ACS_5^{501}	**[0.7075,0.8234]**	**[0.7043,0.7777]**	**[0.7023,0.8048]**	[0.6830,0.7962]	[0.6463,0.7486]	[0.6716,0.7697]
ACS_{10}^{250}	**[0.5891,0.7418]**	**[0.5795,0.7244]**	**[0.5887,0.7279]**	[0.5773,0.6802]	[0.5287,0.6336]	[0.5571,0.6614]
ACS_{15}^{167}	**[0.5529,0.7144]**	**[0.5437,0.6987]**	**[0.5515,0.7016]**	[0.5055,0.5985]	[0.4708,0.5555]	[0.4915,0.5701]
ACS_{20}^{125}	**[0.5274,0.6761]**	**[0.5212,0.6342]**	**[0.5195,0.6547]**	[0.4874,0.5421]	[0.4557,0.4932]	[0.4571,0.5243]
ACS_{25}^{100}	**[0.5161,0.6059]**	**[0.4993,0.5703]**	**[0.5169,0.5773]**	[0.4792,0.5260]	[0.4387,0.4767]	[0.4640,0.4949]

The best interval utility values are in boldface.

to solve the QoS uncertainty-aware web service composition problem for the Internet of Things (IoT) and Cloud computing environments that consider more specialized QoS parameters.

REFERENCES

[1] L. Zeng, B. Benatallah, A. H. Ngu, M. Dumas, J. Kalagnanam, and H. Chang, "Qos-aware middleware for web services composition," *IEEE Transactions on software engineering*, vol. 30, no. 5, pp. 311–327, 2004.

[2] M. Alrifai, T. Risse, and W. Nejdl, "A hybrid approach for efficient web service composition with end-to-end qos constraints," *ACM Transactions on the Web (TWEB)*, vol. 6, no. 2, p. 7, 2012.

[3] C. Jatoth, G. R. Gangadharan, and R. Buyya, "Computational intelligence based qos-aware web service composition: A systematic literature review," *IEEE Transactions on Services Computing*, vol. 10, no. 3, pp. 475–492, 2017.

[4] D. Ardagna and B. Pernici, "Adaptive service composition in flexible processes," *IEEE Transactions on software engineering*, vol. 33, no. 6, pp. 369–384, 2007.

[5] G. Canfora, M. Di Penta, R. Esposito, and M. L. Villani, "An approach for qos-aware service composition based on genetic algorithms," in *Proceedings of the 7th annual conference on Genetic and evolutionary computation*. ACM, 2005, pp. 1069–1075.

[6] J. Liao, Y. Liu, X. Zhu, and J. Wang, "Accurate sub-swarms particle swarm optimization algorithm for service composition," *Journal of Systems and Software*, vol. 90, pp. 191–203, 2014.

[7] Y. Huo, Y. Zhuang, J. Gu, S. Ni, and Y. Xue, "Discrete gbest-guided artificial bee colony algorithm for cloud service composition," *Applied Intelligence*, vol. 42, no. 4, pp. 661–678, 2015.

[8] x. wang, X. Xu, Q. Z. Sheng, Z. Wang, and L. Yao, "Novel artificial bee colony algorithms for qos-aware service selection," *IEEE Transactions on Services Computing*, vol. 12, no. 2, pp. 247–261, 2019.

[9] M. Razian, M. Fathian, and R. Buyya, "Arc: Anomaly-aware robust cloud-integrated iot service composition based on uncertainty in advertised quality of service values," *Journal of Systems and Software*, vol. 164, p. 110557, 2020.

[10] X. Jian, Q. Zhu, and Y. Xia, "An interval-based fuzzy ranking approach for qos uncertainty-aware service composition," *Optik-International Journal for Light and Electron Optics*, vol. 127, no. 4, pp. 2102–2110, 2016.

[11] F. Seghir, A. Khababa, and F. Semchedine, "An interval-based multi-objective artificial bee colony algorithm for solving the web service composition under uncertain qos," *The Journal of Supercomputing*, 2019.

[12] H. Zheng, J. Yang, and W. Zhao, "Probabilistic qos aggregations for service composition," *ACM Transactions on the Web (TWEB)*, vol. 10, no. 2, p. 12, 2016.

[13] J. Xu, L. Guo, R. Zhang, H. Hu, F. Wang, and Z. Pei, "Qos-aware service composition using fuzzy set theory and genetic algorithm," *Wireless Personal Communications*, vol. 102, no. 2, pp. 1009–1028, 2018.

[14] M. Alrifai, D. Skoutas, and T. Risse, "Selecting skyline services for qos-based web service composition," in *Proceedings of the 19th international conference on World wide web*, 2010, pp. 11–20.

[15] S. Wang, Q. Sun, H. Zou, and F. Yang, "Particle swarm optimization with skyline operator for fast cloud-based web service composition," *Mobile Networks and Applications*, vol. 18, no. 1, pp. 116–121, 2013.

[16] H. Ying and Z. Jiande, "A nonlinear service composition method based on the skyline operator," *Journal of Systems Engineering and Electronics*, vol. 31, no. 4, pp. 743–750, 2020.

[17] S. Borzsony, D. Kossmann, and K. Stocker, "The skyline operator," in *Proceedings 17th international conference on data engineering*. IEEE, 2001, pp. 421–430.

[18] E. Al-Masri and Q. H. Mahmoud, "Investigating web services on the world wide web," in *Proceedings of the 17th international conference on World Wide Web*. ACM, 2008, pp. 795–804.

[19] D. M. Gay, "The ampl modeling language: An aid to formulating and solving optimization problems," in *Numerical analysis and optimization*. Springer, 2015, pp. 95–116.

[20] A. K. Bhunia and S. S. Samanta, "A study of interval metric and its application in multi-objective optimization with interval objectives," *Computers & Industrial Engineering*, vol. 74, pp. 169–178, 2014.

[21] S. Mahato and A. Bhunia, "Interval-arithmetic-oriented interval computing technique for global optimization," *Applied Mathematics Research Express*, vol. 2006, 2006.

[22] S. Karmakar and A. K. Bhunia, "A comparative study of different order relations of intervals." *Reliable Computing*, vol. 16, no. 2, pp. 38–72, 2012.

[23] R. V. Rao, "Introduction to multiple attribute decision-making (madm) methods," *Decision Making in the Manufacturing Environment: Using Graph Theory and Fuzzy Multiple Attribute Decision Making Methods*, pp. 27–41, 2007.

[24] D. Karaboga and B. Basturk, "A powerful and efficient algorithm for numerical function optimization: artificial bee colony (abc) algorithm," *Journal of global optimization*, vol. 39, no. 3, pp. 459–471, 2007.

[25] K. Deb, "An efficient constraint handling method for genetic algorithms," *Computer methods in applied mechanics and engineering*, vol. 186, no. 2-4, pp. 311–338, 2000.

[26] W.-L. Xiang and M.-Q. An, "An efficient and robust artificial bee colony algorithm for numerical optimization," *Computers & Operations Research*, vol. 40, no. 5, pp. 1256–1265, 2013.

[27] B. L. Miller, D. E. Goldberg *et al.*, "Genetic algorithms, tournament selection, and the effects of noise," *Complex systems*, vol. 9, no. 3, pp. 193–212, 1995.

NECS-based Cache Management in the Named Data Networking

N. FETHELLAH, H.BOUZIANE, A.CHOUARFIA

Département Informatique

Université des Sciences et de la Technologie d'Oran- Mohamed Boudiaf

Oran, Algérie

Email :{ nourelhouda.fethellah, hafida.bouziane, abdallah.chouarfia}@univ-usto.dz

***Abstract*—the Information-Centric Networking ICN architectures proposed to overcome the problems of the actual internet architecture. One of the main straight points of the ICN architectures is in-network caching. The effectiveness of the adopted caching strategy, which manages and decides where to store them, influences the performance of the ICN. However, the major issue that faces the caching strategies in the ICN architectures is the strategic selection of the cache routers to store the data through its delivery path. This will reduce congestion, optimize the distance between the consumers and the required data furthermore improve latency and alleviate the viral load on the servers. In this paper, we propose a new efficient caching strategy for the Named Data Networking architecture NDN named NECS, which is the most promising architecture between all the ICN architectures. The proposed strategy reduces the traffic redundancy, eliminates the useless replication of contents, and improves the replay time for users due to the strategic position of cache routers. Besides, we evaluate the performance of this proposed strategy and compare it with three other NDN caching strategies, using the simulator network environment NdnSIM. Based on the simulations carried out, we obtained interesting and convincing results.**

Keywords—ICN, NDN, caching strategy, future internet architecture, in-network caching, cache management policies

I. INTRODUCTION

The explosion of Internet usage in everyday life has created a set of new challenges. Each minute, more volume of information is broadcasted over the Internet People around the world increasingly move to the network for their daily activities such as work, education, research, shopping, and entertainment. Millions of people are online at the same time, which leads to a massive size of digital activities at the same time and saturates the network. Internet changes the world in completely unexpected ways and the emerging trends demonstrate the inefficiency of the current Internet architecture, showing the need for the new Internet architecture. It proves that the world has already started a new era, where content and technology play a critical role.

According to the Domo[1] website annual statistics for the year 2020 regarding Internet traffic for one minute, the internet users are more than 4.5 billion users. They send 41,666,667 What Sapp messages. They made 1,388,889 video and voice calls. The Zoom application records 208,333 participants attending an online meeting. On LinkedIn, 69,444 people apply for jobs. On the Amazon website, 6,659 Amazon packages shipped. On YouTube, 500hrs video viewed.

By 2023, Internet users will be nearly two-thirds of the global population. It is expected that Internet users will be about 5.3 billion, which means 66% of the global population with 3.9 billion additional users compared to 2018[2].

As mentioned earlier, the massive broadcast on the Internet while the architecture is unresponsive. This challenge has motivated many research initiatives to adapt the actual Internet architecture to the current requirements. Despite the significant research efforts in this context, there are still many open issues.

The key issue remains the explosive growth of content demand and the dominance of bandwidth-intensive applications, which increases the content size as well as the Internet traffic. Thus, content/information is a core Internet architecture. Among the adopted techniques, the Information-Centric Networking (ICN) architectures try to overcome such constraints by in-network caching. It allows cache routers to store the disseminated content across the network, eliminating redundant requests and decreasing the network traffic[1].

The Named Data Networking (NDN) is the most prominent architecture among the ICN architectures, proposed as a future Internet architecture [4]. It has as perspectives using names to retrieve contents, securing contents instead of securing channels, adopting caching contents, caching mechanism, and NDN transfer to IP transfer.

The NDN default caching mechanism consists of leaving a copy of the required content on each NDN cache router located in the delivery path, which alleviates the burden on the original content provider. The intermediates NDN cache routers provide content to consumers. The requested contents provided from a near NDN cache router improve the response time.

However, the NDN default caching mechanism sufferers from inefficient use of cache router storage, high cache redundancy, and high replacement overhead, which makes the NDN system inefficient. The NDN architecture would be more efficient and robust by suggesting an appropriate content caching mechanism, which takes into consideration to determine the important cache routers to allow them to store the disseminated content across the network.

In previously published work, we investigated these requirements and the trade-off for making this decision and we present the main idea of a suggested caching strategy. The proposed approach contains two main parts, which are clustering the network and caching routers selection. The improved K-medoid algorithm does the clustering. In each

resulting cluster, the three most important cache routers are selected based on three pertinent criteria using relevant Multi-Attribute Decision-Making (MADM) methods. The three criteria are the distance between a router and its cluster centroid (dis), the number of neighbors (nbrn), and congestion level (cl)).

In the present paper, we prove the efficiency of the proposed caching strategy for the NDN architecture, which we give as a name NECS, which means New Efficient Caching Strategy. The contributions of this paper are presented as follows:

- Presenting the cache management process of the NECS caching strategy.
- An extensive simulation analysis has been conducted to prove NECS approach superiority as in-network caching for the NDN architecture compared to the default NDN caching strategy (LCE) and the two other selected caching strategies (Random and Prob(p)).

The NECS caching strategy enables fetching content from near cache routers by minimizing latency and minimizing traffic overhead leading to a higher cache-hit ratio and shorter potential stretches (hops). It is a well-suited alternative to the actual default caching strategy of the NDN architecture since it improves network performance and resilience.

Section II discusses the related work. Section III presents NECS caching strategy concept. Section IV reports the simulation parameters and discusses the obtained results. Finally, section V concludes the paper and gives some perspectives about future work.

II. RELATED WORK

The NDN architecture is the most prominent architecture among all the proposed ICN approaches as future Internet architecture. It enhances the Quality of Service in different terms such as bandwidth, delay, use of resources, congestion, and load server.

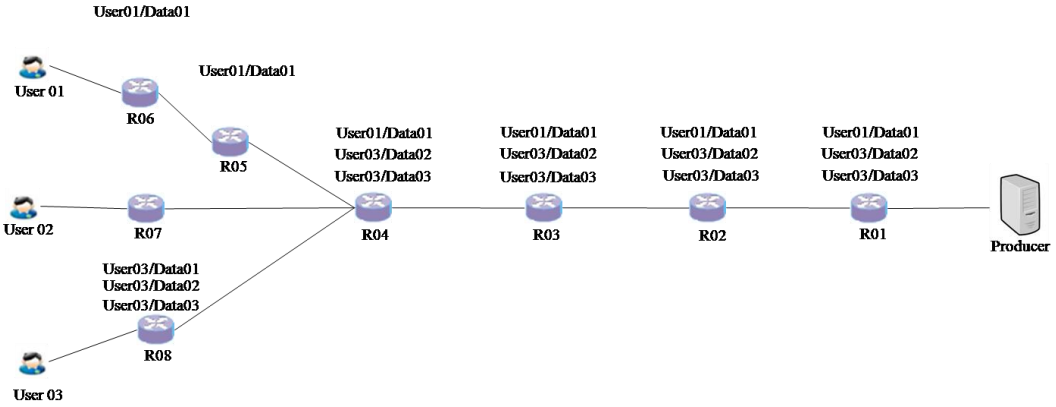


Fig. 1 Illustrative example of LCE caching strategy

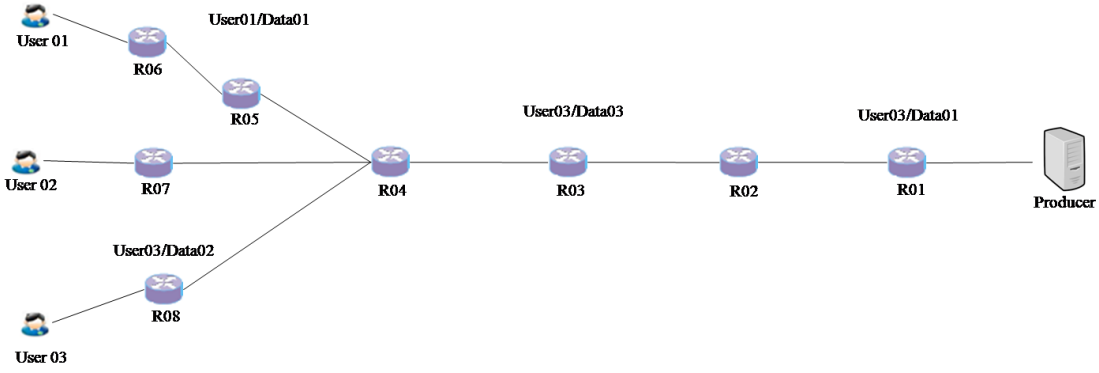


Fig. 2 Illustrative example of Radom caching strategy

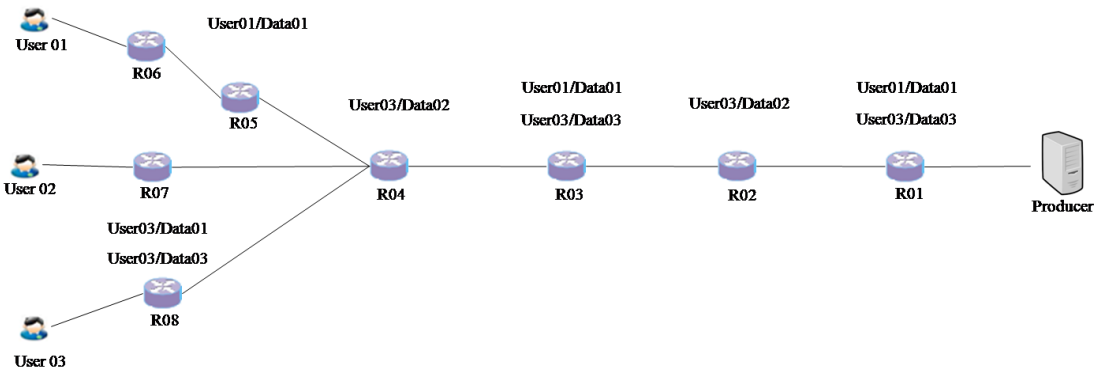


Fig. 3 Illustrative example of Prob(p) caching strategy with p=0.5

To get the benefits of NDN architecture, efficient cache management is required. Several recent studies have focused specifically on finding optimal caching schemes to enhance the overall network performance. However, the investigations in this context are still at an early stage. An efficient caching requires the election of the most advantageous locations on the delivery path to store disseminated content [4]. In this section, we present some important contributions proposed in the literature.

Leave a copy everywhere: LCE[2], [3] is the default caching strategy for the NDN architecture. The LCE stores a copy of the requested data packet on each NDN cache router along the delivery path. It aims to reduce the upstream demand. Fig. 1 presents an illustrative example of the LCE strategy. There are three users User01, User02, User03, and one Producer. The User01 requests the Data01.This data replicated on all cache routers located between the Producer and the User01 (R01, R02, R03, R04, R05, R06). User02 does not request any data. The User03 requests Data01, Data02, and Data03 respectively. Data01 fetched from the cache router R04 and duplicated on all the cache routers located along the delivery path. Data02 and Data03 are obtained from the Producer and duplicated on the same delivery path. When the User03 requests once more Data01, Data02, or Data03, it is satisfied from the cache router R08. The copies on the cache routers R01, R02, and R03 are unnecessary. They only consume the network resources. The LCE eases access to content and reduces response time. However, duplicating content on all NDN cache routers along the delivery path wastes network resources. Sometimes popular content replaced with less popular content due to the limited cache router size.

Leave a Copy Down LCD[4] is a cache management policy. The LCD strategy consists of leaving a copy of the requested data packet at the NDN cache router one level down toward the consumer after each demand. It aims to reduce the cache redundancy in the network. However, it wastes the network resources such as the bandwidth, the NDN cache routers storages on the delivery path, and a long time to place content near to the user.

Move a Copy Down MCD[5] same as the LCD strategy, it moves the content from the actual cache router to the next cache router on the delivery path. This allows freeing more space on the caching router and reducing the content redundancy. However, it increases the content request delay by removing the requested content from the previous NDN cache router and duplicating the requested content on the next router[6]. The repetitive requests for the same content consume the network resources.

Most Popular Content: MPC[7] designed to store only popular content. Each NDN cache router computes the number of demands (popularity count) for each request (content name). It saves the request names and their size in the popularity table (PT). Requested content is considered popular when its request number is equal to or greater than the popularity threshold. The NDN cache router stores the popular content. It sends a Suggestion message to its neighbors to save the popular content. The neighbors accept or not to cache the popular content. It depends on their local policies. It reaches a high cache-hit ratio and reduces the stretch ratio. However, it records high redundancy and low diversity. The content popularity calculation increases the response delay.

The random strategy is a cache management policy[8]. It places only one copy of the requested data packet on a single NDN cache router located on the delivery path. The NDN cache router is randomly selected. Fig. 2 presents an illustrative example of the Random strategy. We take the same scenario as the LCE strategy. The User01 requests the Data01. The Producer satisfies it, a copy of the Data01 is stored on the router R05. The User03 requests the Data01. The NDN cache router R05 does not serve the request. It is not located on the same common part of the delivery path. Data01 is retrieved from the Producer and a copy is stored on the router R01. The User03 requests the Data02. It is satisfied by the Producer and a copy is stored on the router R03. The User03 requests the Data03. It is fetched from the Producer and a copy is saved on the router R08. The Random strategy is an autonomous randomly cache content policy. It reduces content duplication and increases content diversity. It achieves a high cache hit, reduces the delay, and reaches low overhead. However, the arbitrary location of a copy decreases the NDN architecture effectiveness. It has an unpredictable nature[9].

The Prob(p) strategy is a non-cooperative policy. It aims to store the data packet copies on NDN cache routers located on the delivery path with a defined probability p and does not cache the data packet with probability (1−p). When the NDN cache router receives the data packet, it generates a random number from zero to one. If the generated number is small than the p-value then the NDN cache router duplicates the requested data packet. Otherwise, the NDN cache router disseminates the requested data packet without storing it. The Prob(p) is employed to improve the cache efficiency and to minimize caching redundancy[6]. Fig. 3 presents an illustrative example of the Prob(p) strategy with a p-value equal to 0.5. We reserved the same scenario as the LCE strategy. The User01 requests the Data01. This one is duplicated on the routers with a p-value less than 0.5. Data01 is stored on the routers R01, R03, and R05. The User03 requests the Data01. It is retrieved from the router R03 and duplicated on each router with a p-value small than 0.5 on the delivery path. The User03 requests the Data02, then the Data03. They are fetched from the Producer and duplicated on each router whose generated p-value is less than the defined p-value. Respectively, the Data02 on the routers R02 and R04, and Data03 on R01, R03, and R08. The Prob(p) strategy stores diverse data packets at each cache router on the delivery path. It enhances the cache efficiency, converges to save popular content, and enhances the cache-hit ratio. However, its performance relies on the defined probability p-value. The Prob(p) behaves as the LCE policy when the probability p-value is equal to one[10].

Probcache[11] is a probabilistic caching policy. The Probcache strategy computes the content caching probability by multiplying the time-in by the cache weight based on the TSI and the TSB values. It includes a Time-Since-Inception (TSI) field in the interest packet header and a Time-Since-Birth (TSB) field in the data packet header. The TSI value is set to zero when the user sends an interest packet. At every hop, the TSI value is incremented by one. The content producer sets the TSB value to zero. The data packet is sent to the data requester across the delivery path. The TSB value is also incremented by one for each NDN cache router reached. The Probcache strategy aims to store content near to the user to guarantee resource allocation fairness, reduce content redundancy, and save popular content. However, the

computation requires the knowledge of the remaining cache size for each cache router on the delivery path. The computations on each NDN cache router consume the NDN cache router resources and increase the response time. The fixed value of the meantime gives unreal evaluation. Probcache+[12] is an enhanced version of the Probcache. It has a slight difference. The cache weight increases by the TSB value. However, the Procache+ still suffers from the same drawbacks as the Probcache.

Intra-AS Cache Cooperation[13] is an intra-domain cache cooperation policy that adds to each NDN cache router two tables: Local Cache Summary Table (LCST) and Exchange Cache Summary Table (ECST). Periodically, the NDN cache routers announce their LCST to their direct neighbors. The policy reduces cache redundancy. However, the regular exchange of lists wastes the network resources and slows down the network. Some records in the ECST table are obsolete.

In-Network Caching for Information-Centric Networking with Partitioning and Hash-Routing: CPHR[14] is a collaborative in-network caching strategy with content space partitioning and hash-routing information-centric networking. The CPHR modifies the NDN cache router FIB structure by adding two new fields (Cache router name, Egress content router) to allow mapping content via the hash function. The CPHR reduces the cache redundancy on the network. However, the hash mechanism demands centralized control. It incurs high overhead.

Cluster-based in-networking caching for content-centric networking[15] is a cluster base caching strategy with a virtual distributed hash function to manage the cluster resources. The cluster cache routers utilize the same hash function to compute the cache router location. It improves cache diversity, enhances the hits ratio, and reduces cache redundancy. The cluster construction is very interesting. It replaces the Euclidean distance in the k-medoid clustering algorithm with a new distance to reflect the real relationship between the NDN cache routers in the network. However, the stretch ratio increases, due to the hash function utilization to manage the stored content at the cluster cache routers. It has limited scalability and no-cache router location consideration. The hash routing schema incurs a high link load. The hash function increases the stretch ratio.

Caching strategy based on the hierarchical cluster for named data networking[16] is a two-layer hierarchical cluster-based caching strategy. The Core Layer contains the NDN cache routers that focus only on content routing. The Edge Layer contains the NDN cache routers that store contents near to users. It takes into consideration the cache router placement and cache popularity. It reduces the cache redundancy. However, the cluster heads have numerous computations that slow down the network. In case of failure, the network is paralyzed. The frequent exchange messages introduce extra overhead and flood the network. The arbitrary selection of some parameter values and the static update period incurred inefficient performance. The search for stored contents in the cluster increases the response time. Only the number of shortest paths passing by the caching router defines the cache router's importance. It would be interesting to add other parameters for a more relevant evaluation.

To overcome the shortcomings discussed above, we propose NECS as a new efficient caching strategy for NDN architecture. The main idea of this work based on clustering was published in a previous article [17]. Pertinent criteria selected three cache routers (the main, the first, and the second) for each cluster. The clustering offers the NDN architecture high scalability and efficiency. The cache routers selection allows the NDN architecture to minimize the content redundancy, increase the cache-hit ratio, increase the content diversity, remove redundant traffic and, optimize network resources.

III. THE PROPOSED APPROACH

In this section, we present only the main idea of the NECS caching strategy because we are limited with the allowed number of pages. However, we explain in detail the suggested approach in two previously published works [17], [18]. The NECS caching strategy contains two main parts, which are clustering the network and selecting the three most important cache routers in each resulting cluster.

Clustering

The network is divided into several clusters using the clustering mechanism, which is the improved k-medoid clustering algorithm [15] with appropriate parameters: delay, bandwidth, cache size, and the number of hops. These parameters give more realistic and efficient cluster construction. This clustering algorithm has input the graph of the network and the number of the desired clusters. It has as output the resulting clusters. Each resulting cluster contains at least one border node considered as an NDN cache router. It has a direct link with an NDN cache router that belongs to another cluster. Its basic process is as follows:

- deleting all the routers with only one link,
- Set the K routers with the most number of links as initial centroids of K clusters,
- For each router, compute its distance to each centroid of the K clusters,
- Assign the router into the cluster with the smallest distance value,
- For every single cluster, compute the distance between every two routers.
- Set the router with the smallest distance value as the new centroids of its cluster,
- Repeat all the steps except the two first steps until the centroid is unchanged.

Cache routers selection

We present the main idea of the NECS for the cached routers selection. However, we explain in detail the caching router selection mechanism in two previously published works [17], [18]. In each resulting cluster, the three most efficient cache routers are selected based on three pertinent criteria: congestion level, number of connections, and distance to the centroid cluster.

We utilize two Multi-Attribute Decision-Making methods (MADM), which are the Technique for Order of Preference by Similarity to Ideal Solution method (TOPSIS) combined with the Analytic Hierarchy Process (AHP). The

TOPSIS method allows ranking all the cluster cache routers by descending order from the best to the worst, based on the selected criteria. The AHP method is utilized to evaluates the assigned weights of the selected criteria in the TOPSIS method. For assuring the optimal caching routers selection with the three chosen criteria, we utilize two MADM approaches. The two MADM approaches are the Technique for Order of Preference by Similarity to Ideal Solution method (TOPSIS) combined with the Analytic Hierarchy Process (AHP). The criteria become the distance between a node and its cluster centroid (dis), the number of neighbors (nbrn), and the congestion level (cl). Fig.4. illustrates the process of the cache routers selection.

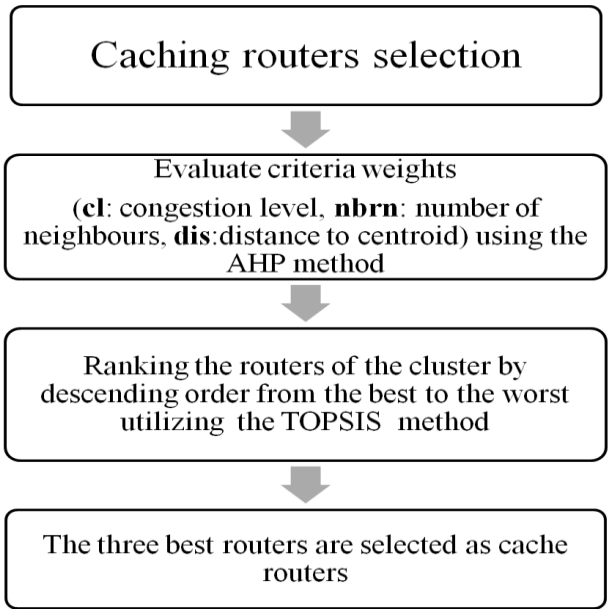


Fig.4 The process of cache router selection

Cache management in the network

For cluster management, we proceed as follows: when the cluster's user sends an interest packet or the cluster's border router cache receives an interest packet, they send the interest packet to the main router cache via the shortest path.

The main router cache checks its storage; if the requested content is found then it returned it to the cluster's user else it is redirected to a border router cache via the shortest path. The border router cache redirects the interest packet to the next cluster via its cluster's border router cache.

When a data packet reaches the cluster's border router cache, it is redirected to the cluster's main router, which stores a copy and sends the packet to the requester user. If the data packet arrives in the main cache router with a full cache, the policy Least Frequently Used (LFU) is applied rather than Least Recently Used policy (LRU), which is the default replacement policy of the NDN architecture. The main cache router of the cluster is the only router that has permission to store incoming contents into the cluster. Inside each cluster, the contents of the secondary router cache and those of the tertiary router cache are using as a backup to replace the primary router cache in the event of a failure. No cache routers except the main cache router store any content.

The above-proposed mechanism reduces cache redundancy in-network, eliminates unnecessary traffic, improves response time, increases contents diversity, optimizes resource use, minimizes bandwidth consumption, and releases overload on the servers. It has low complexity with high performance.

IV. PERFORMANCE EVALUATION

In this section, we describe the experimental setup. We present simulation results and compare the performance of the proposed approach with other content caching strategies, namely, the Leave a Copy Everywhere (LCE), Random, and Prob(p) with two values of the probability parameter p=0.1 and p=0.5 respectively, store size 10% and 50% of the requested contents. The performance is rated in terms of cache-hit ratio.

Simulation setup

The proposed caching strategy is implemented and simulated under the NdnSIM simulator[19], [20]. The NdnSIM relies on the Network Simulator NS3. We compared the obtained results of the proposed caching strategy to the results of three in-network caching strategies performed using the same simulator, the same topology, and the same parameters. Table I shows the simulation parameters.

TABLE I. SIMULATION PARAMETERS

The α parameter of the Zipf distribution	α= {0.5, 0.75, 1, 1.25, 1.5, 1.75, 2, 2.25, 2.5, 2.75, 3}
The required contents (catalog size)	10^3, 10^4, 10^5, 10^6, 10^7
Content store size	200 GB
Bandwidth	100 Mbps
Topology size	21
Consumer and producer	(08,01)
Simulator	NdnSIM

The network topology contains 21 NDN cache routers (nodes). The cache memory is configured at 200GB. The network topology contains 08 data requesters and one data provider. The bandwidth link is configured at 100 Mbps. The requesters send 100 interest packets per second.

The performances of LCE, Prob(0.1), Prob(0.5), and Random strategies compared to the NECS performances. NECS performance analysis takes on different content sizes and popularities (represented by α parameter of the Zipf distribution).

The Internet content traffic is classified into four types of content categories: Web content, User Generated Content (UGC), File sharing, and Video on Demand VoD [21]. The popularity of Internet content traffic categories is modeled by Zipf distribution[22]. The content popularity demonstrated that it generally follows Zipf distribution[23], [24]. The α parameter value of the Zipf law is related to the behavior of user requests, where slightly high values indicate that requests are more concentrated on some contents namely, how often each particular content is required. Different scenarios and applications may require different values of the α parameter. In the literature, α parameter Zipf varies largely from 0.5 to 3.5. For instance, the α parameter value varies between 0.8 and 1.2 in [25]. The α parameter value ranges

from 0.65 to 2.5 in [26]. The Daily motion catalog is determined with α equal to 0.88 and the PirateBay catalog is determined with α equal to 0.75[27]. The α parameter value ranges between 0.65 and 1.0 according to Video on Demand china statistic[28].

In simulations, the Zipf probability distribution is used as a popularity model with different α parameter values between 0.5 and 3to compare extensively the behavior of the NECS to the selected caching strategies.

For robust analysis, the present study utilizes a reasonable interval for the α parameter value of the Zip distribution to simulate popular and unpopular Internet contents. The selected α parameter values are as follows: 0.5, 0.75, 1, 1.25, 1.5, 1.75, 2, 2.25, 2.5, 2.75, and 3.

For a relevant evaluation, we study the impact of different requested content sizes on the performance of the NECS proposed approach. We selected different requested content sizes to range from a small size to a large size. The requested content amounts are as follows: 10^3, 10^4, 10^5, 10^6, and 10^7.

The cache-hit ratio metric is used to evaluate the NECS performances and against the selected cache strategies (LCE, Random, Prob(0.1), and Prob(0.5)).

The cache-hit ratio metric is an essential parameter to measure the efficiency and performance of any caching strategy in the NDN architecture. A high cache-hit ratio means more requests are satisfied from network cache routers. The cache-hit ratio is the most commonly used metric for evaluating network performances.

The cache-hit ratio represents the average number of found content hits to satisfy interest packets from a caching router. (1) expressed the cache-hit ratio.

$$CacheHitRatio = \frac{\sum_{i=1}^{n} Hit_i}{\sum_{i=1}^{n} Hit_i + \sum_{i=1}^{n} Miss_i} \qquad (1)$$

Where

- n represents the total number of the network cache routers,
- $\sum_{i=1}^{n} Hit_i$ represents the contents sum satisfied from the network cache routers,
- $\sum_{i=1}^{n} Miss_i$ represents the contents sum dissatisfied with the network cache routers.

Simulation Results

In this subsection, we study the impact of different α Zipf parameter values on the performances of NECS's proposed caching strategy against the selected caching strategies. We also study the impact of different requested content sizes on the NECS proposed caching strategy performances against the selected caching strategies.

The performance evaluation of the NECS strategy against the selected cache strategies relies on the cache-hit ratiometric.

Fig. 5, Fig. 6, Fig. 7, Fig. 8, and Fig. 9 present the simulation performance results of the four caching strategies (NECS, LCE, Prob(0.1), Prob(0.5), and Random) with different requested cache sizes over the α Zipf parameter values ranging from 0.5 to 3.

Each Figure represents a graph that reflects the simulation results for the four approaches with the same values of α parameter for a single requested content amount. Each curve represents a single cache strategy. The horizontal axis represents the different values of the α parameter and the vertical axis, the cache-hit ratio according to a specific requested content amount.

From the results obtained by the conducted simulations, we observe that the requested content amount has no significant impact on the cache-hit ratio as α Zipf distribution parameter. It presents the content Internet traffic model.

We notice in Fig. 5, Fig. 6, Fig. 7, Fig. 8, and Fig. 9 that the cache-hit ratio increases for all the caching strategies as α Zipf parameter value increases. The increased α Zipf parameter value means that only a small set of contents is more frequently requested. It favors retrieving the required contents from NDN cache routers rather than retrieving the required contents from the data provider.

Case requested contents size and α parameter

- Requested contents size$\leq 10^3$ and $0.5 \leq \alpha \leq 0.8$: The Random cache strategy is the best among the four caching approaches because this cache strategy records the highest cache-hit rate compared to other caching strategies. The Prob(0.5) at the second place strategy. The NECS caching strategy and the LCE caching strategy are found in third place. The Prob(0.1) cache strategy was found at the last place with the lowest recorded cache-hit values (see Fig. 5).
- Requested contents size $\leq 10^3$ and $0.8 < \alpha \leq 3$: The NECS is the best caching strategy. It records the highest cache-hit ratio values compared to the other caching strategies. The LCE cache strategy and the Random cache strategy rank second. The Prob(0.5) cache strategy rank third. The Prob(0.1) cache strategy ranks last with the lowest cache-hit rate ratio values (see Fig. 5).
- Requested contents size = 10^4 and $0.5 \leq \alpha \leq 1.1$: The LCE cache strategy is the best caching strategy. It records the highest cache-hit ratio compared to the other selected caching strategies. The NECS strategy rank second. The Random caching strategy ranks third. The Prob(0.5) caching strategy ranks fourth. The Prob(0.1) strategy ranks fifth (see Fig. 6).
- Requested contents size = 10^4 and $1.1 < \alpha \leq 3$: The NECS strategy is the best compared to the remaining caching strategies. It records the highest cache-hit ratio values. The LCE and the Random caching strategies rank second. The Prob(0.5) cache strategy ranks third. The Prob(0.1) cache strategy ranks last (see Fig. 6).
- Requested contents size = 10^5 and $0.5 \leq \alpha \leq 3$: The NECS strategy is the best caching strategy. It records

the highest cache-hit ratio compared to the remaining selected caching strategies. We notice a clear performance advantage over the other selected caching strategies. The LCE caching strategy ranks second with the Random caching strategy. The Prob(0.5) caching strategy ranks third. The Prob(0.1) caching strategy ranks fourth with the lowest cache-hit ratio values (see Fig. 7, Fig. 8, and Fig. 9).

The NECS caching strategy is the adequate caching strategy for the Internet. It shows efficient performance at the large scale of requested contents. It is the Internet case.

When the α Zipf parameter value increases more popular contents are stored at strategic main cache routers and records a high cache-hit ratio.

The NECS adequate for a large requested content size with the different values for α parameter (popular and unpopular contents). The NECS is also adequate for small and medium requested contents size with somewhat high values of α parameter.

Simulations show that the default caching strategy of the NDN architecture is not a suitable caching mechanism for the NDN architecture. It does not achieve a high cache-hit rate. Likewise, the Random caching approach and the Prob(p) caching strategy does not achieve a high cache-hit rate. Their performance relies a lot on the p probability parameter as shown by the results above.

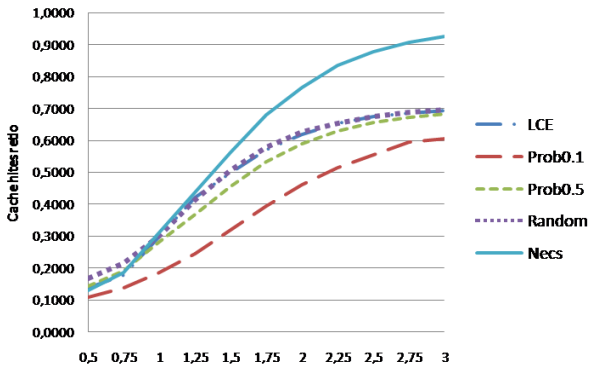


Fig. 5 Required contents size 10^3

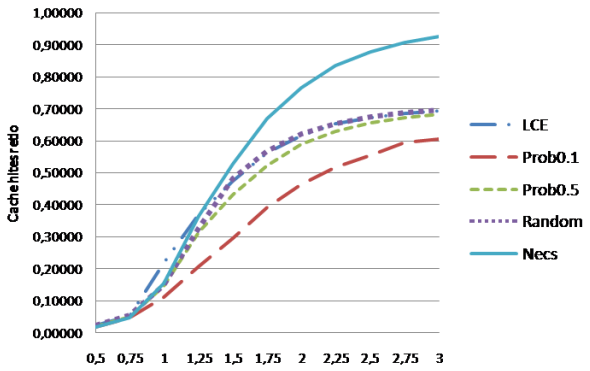


Fig. 6 Required contents size 10^4

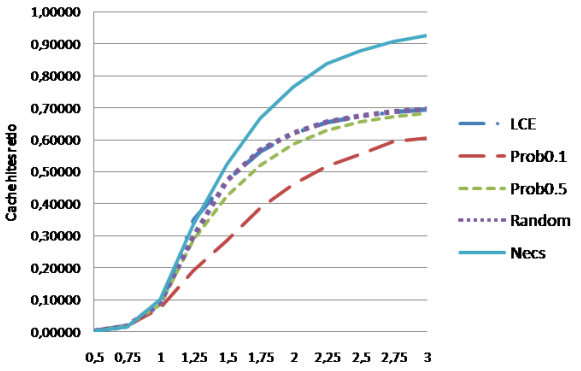


Fig. 7 Required contents size 10^5

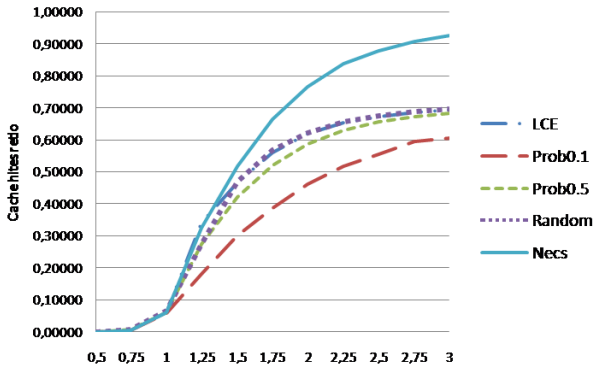


Fig. 8 Required contents size 10^6

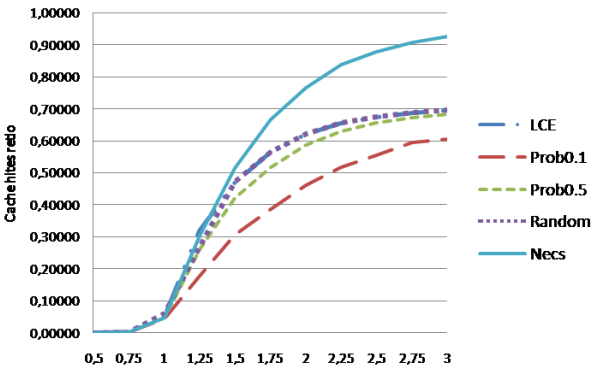


Fig. 9 Required contents size 10^7

The NECS caching approach greatly improves the cache-hit rate for the NDN architecture. The content is retrieved from the selected cache router according to relevant criteria. The NECS reduces retrieving contents from the content provider.

Simulation results show the important impact of the cache router's selection to store contents in strategic locations to satisfy future requests. They also show the impact on improving the caching strategy performance and effectiveness thus, the NDN architecture efficiency. The cache router's choice to store copies of the requested data is a critical task.

The NECS caching strategy gives satisfactory and encouraging results. The appropriate selection of cache routers to store the requested content gives the NECS cache strategy high performance. It saves the network bandwidth, optimizes the network resources, eliminates unnecessary network traffic, reduces cache redundancy, and increases content diversity.

V. CONCLUSION

In this paper, we present the main concept NECS caching strategy. It is based on the clustering mechanism and caching router's selection to store contents. We also present the results obtained by the conducted simulation study for the NECS caching strategy and compare its performances against three selected caching strategies, namely, the Leave a Copy Everywhere (LCE), Random, and Prob(p).

The evaluation results clearly show significant benefits of the NECS based on cache-hit ratio and its superiority over LCE for large requested contents size. The LCE strategy is the default caching strategy of the NDN architecture.

We believe that the NECS caching mechanism will play a key role in NDN architecture. It can easily retrieve content from the nearest main cache router, eliminate redundant traffic, improve content diversity, minimize content redundancy, optimize the network resources utilization, and alleviate the burden on the content provider. The NECS strategy presents a promising caching solution for the NDN architecture.

The cache-ratio implies, at least, an improvement in the delivery time. In future work, we plan to choose as metric an objective function (cache-hit ratio, delay, and congestion), compare the NECS caching strategy to other NDN caching mechanisms, and assess the performance under other network topologies.

REFERENCES

[1] Y. Yamamoto, J. Takemasa, Y. Koizumi, and T. Hasegawa, "Analysis on caching large content for information-centric networking," in *Proceedings of the 5th ACM Conference on Information-Centric Networking*, New York, NY, USA, Sep. 2018, pp. 24–30, DOI: 10.1145/3267955.3267957.

[2] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking Named Content," in *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies*, New York, NY, USA, 2009, pp. 1–12, DOI: 10.1145/1658939.1658941.

[3] L. Zhang *et al.*, "Named data networking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, p. 8, 2014.

[4] D. Rossi and G. Rossini, "Caching performance of content-centric networks under multi-path routing (and more)," p. 9, 2011.

[5] N. Laoutaris, H. Che, and I. Stavrakakis, "The LCD interconnection of LRU caches and its analysis," *Perform. Eval.*, vol. 63, no. 7, pp. 609–634, Jul. 2006, doi: 10.1016/j.peva.2005.05.003.

[6] H. Jin, D. Xu, C. Zhao, and D. Liang, "Information-centric mobile caching network frameworks and caching optimization: a survey," *EURASIP J. Wirel. Commun. Netw.*, vol. 2017, no. 1, p. 33, Feb. 2017, DOI: 10.1186/s13638-017-0806-6.

[7] C. Bernardini, T. Silverston, and O. Festor, "MPC: Popularity-based caching strategy for content-centric networks," in *2013 IEEE International Conference on Communications (ICC)*, Budapest, Hungary, Jun. 2013, pp. 3619–3623, DOI: 10.1109/ICC.2013.6655114.

[8] K. Cho, M. Lee, K. Park, T. T. Kwon, Y. Choi, and Sangheon Pack, "WAVE: Popularity-based and collaborative in-network caching for content-oriented networks," in *2012 Proceedings IEEE INFOCOM Workshops*, Mar. 2012, pp. 316–321, DOI: 10.1109/INFCOMW.2012.6193512.

[9] "Performances of Probabilistic Caching Strategies in Content-Centric Networking - IEEE Journals & Magazine." https://ieeexplore.ieee.org/document/8478220 (accessed Dec. 20, 2019).

[10] M. Zhang, H. Luo, and H. Zhang, "A Survey of Caching Mechanisms in Information-Centric Networking," *IEEE Commun. Surv. Tutor.*, vol. 17, no. 3, pp. 1473–1499, 2015, DOI: 10.1109/COMST.2015.2420097.

[11] I. Psaras, W. K. Chai, and G. Pavlou, "Probabilistic in-network caching for information-centric networks," 2012, p. 55, DOI: 10.1145/2342488.2342501.

[12] I. Psaras, W. K. Chai, and G. Pavlou, "In-Network Cache Management and Resource Allocation for Information-Centric Networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 11, pp. 2920–2931, Nov. 2014, DOI: 10.1109/TPDS.2013.304.

[13] J. M. Wang, J. Zhang, and B. Bensaou, "Intra-AS cooperative caching for content-centric networks," 2013, p. 61, DOI: 10.1145/2491224.2491234.

[14] S. Wang, J. Bi, J. Wu, and A. V. Vasilakos, "CPHR: In-Network Caching for Information-Centric Networking With Partitioning and Hash-Routing," *IEEE ACM Trans. Netw.*, vol. 24, no. 5, pp. 2742–2755, Oct. 2016, DOI: 10.1109/TNET.2015.2480093.

[15] C. Li and K. Okamura, "Cluster-based In-networking Caching for Content-Centric Networking," p. 9, 2014.

[16] H. Yan, D. Gao, W. Su, C. H. Foh, H. Zhang, and A. V. Vasilakos, "Caching Strategy Based on Hierarchical Cluster for Named Data Networking," *IEEE Access*, vol. 5, pp. 8433–8443, 2017, DOI: 10.1109/ACCESS.2017.2694045.

[17] N. E. H. Fethellah, H. Bouziane, and A. Chouarfia, "New Efficient Caching Strategy Based on Clustering in Named Data Networking," *Int. J. Interact. Mob. Technol. IJIM*, vol. 13, no. 12, pp. 104–119, Dec. 2019.

[18] N. E. H. Fethellah, H. Bouziane, and A. Chouarfia, "New efficient Caching strategy based on clustering in Named Data Networking," in *1 st International Conference on Networking Telecommunications, Biomedical Engineering and Applications (ICNTBA'19)*, Boumerdes, Algeria, Nov. 2019, vol. 1, p. P. 26-32.

[19] S. Mastorakis, A. Afanasyev, I. Moiseenko, and L. Zhang, "ndnSIM 2: An updated NDN simulator for NS-3," p. 8, 2016.

[20] S. Mastorakis, A. Afanasyev, and L. Zhang, "On the Evolution of ndnSIM: an Open-Source Simulator for NDN Experimentation," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 47, no. 3, pp. 19–33, Sep. 2017, DOI: 10.1145/3138808.3138812.

[21] A. Lareida, R. Pernischova, B. B. Rodrigues, and B. Stiller, "Abstracting .torrent content consumption into two-mode graphs and their projection to content networks (ConNet)," in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, May 2017, pp. 151–159, DOI: 10.23919/INM.2017.7987275.

[22] G. Hasslinger, K. Ntougias, and F. Hasslinger, "Performance and Precision of Web Caching Simulations Including a Random Generator for Zipf Request Pattern," in *Measurement, Modelling and Evaluation of Dependable Computer and Communication Systems*, Cham, 2016, pp. 60–76, DOI: 10.1007/978-3-319-31559-1_7.

[23] L. Breslau, Pei Cao, Li Fan, G. Phillips, and S. Shenker, "Web caching and Zipf-like distributions: evidence and implications," in *IEEE INFOCOM '99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No.99CH36320)*, Mar. 1999, vol. 1, pp. 126–134 vol.1, DOI: 10.1109/INFCOM.1999.749260.

[24] M. Cha, H. Kwak, P. Rodriguez, Y.-Y. Ahn, and S. Moon, "I tube, you tube, everybody tubes: analyzing the world's largest user-generated content video system," in *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, New York, NY, USA, Oct. 2007, pp. 1–14, DOI: 10.1145/1298306.1298309.

[25] C. Fricker, P. Robert, J. Roberts, and N. Sbihi, "Impact of traffic mix on caching performance in a content-centric network," Mar. 2012, pp. 310–315, DOI: 10.1109/INFCOMW.2012.6193511.

[26] G. Rossini and D. Rossi, "A dive into the caching performance of Content-Centric Networking," Sep. 2012, pp. 105–109, DOI: 10.1109/CAMAD.2012.6335307.

[27] M. Mangili, F. Martignon, and A. Capone, "A comparative study of Content-Centric and Content-Distribution Networks: Performance and bounds," Dec. 2013, pp. 1403–1409, DOI: 10.1109/GLOCOM.2013.6831270.

[28] H. Yu, D. Zheng, B. Y. Zhao, and W. Zheng, "Understanding user behavior in large-scale video-on-demand systems," *ACM SIGOPS Oper. Syst. Rev.*, vol. 40, no. 4, pp. 333–344, Apr. 2006, DOI: 10.1145/1218063.1217968.

ISBN 978-9931-9788-0-0