REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE LARBI BEN M'HIDI -OUM EL BOUAGHI

FACULTE DES SCIENCES EXACTES ET DES SCIENCES DE LA NATURE ET DE LA VIE

DEPARTEMENT DE MATHEMATIQUES ET INFORMATIQUE

MEMOIRE DE FIN D'ETUDE EN VU DE L'OBTENTION DU DIPLOME DE

MASTER EN INFORMATIQUE

OPTION VISION ARTIFICIELLE

Thème

RECONNAISSANCE BIOMETRIQUE MULTIMODALE BASEE SUR LA DIMENSION FRACTALE

PRESENTE PAR :

- **BENDAOUD Mohamed Saïd Ramzi**
- **SOLTANI Sofiane**

Soutenu publiquement le : 13 / 06 / 2018

Devant le jury composé de :

Mme. ZERTAL	**Présidente**	**univ OEB**
Mr. TAOUCHE	**Encadreur**	**univ OEB**
Mr. KOUADRIA	**Examinateur**	**univ OEB**

Année Universitaire : 2017 / 2018

Remerciement

En préambule à ce mémoire nous remerciant ALLAH qui nous aide et nous donne la patience et le courage durant ces longues années d'étude.

Nous souhaitons adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de ces formidables années universitaires.

Ces remerciements vont tout d'abord au corps professoral et administratif, pour la richesse et la qualité de leur enseignement et qui déploient de grands efforts pour assurer à leurs étudiants une formation actualisée.

Nous tenant à remercier sincèrement ***Monsieur TAOUCHE.C****, qui, en tant qu'encadreur de ce mémoire, ainsi que tous les professeurs, qui se sont toujours montrés à l'écoute et très disponibles tout au long de la réalisation de ce mémoire, ainsi pour l'inspiration, l'aide et le temps qu'ils ont bien voulu nous consacrer et sans qui ce mémoire n'aurait jamais vu le jour.*

On n'oublie pas nos parents pour leur contribution, leur soutien et leur patience.

Enfin, nous adressons nos plus sincères remerciements à tous nos proches et amis, qui nous ont toujours encouragées au cours de la réalisation de ce mémoire.

Merci à tous et à toutes.

Dédicace

Je dédie ce mémoire:

À mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

À mes chers amis, pour leur appui et leur encouragement,

À toute ma famille pour leur soutien tout au long de mon parcours universitaire,

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fruit de votre soutien infaillible,

Merci d'être toujours là pour moi.

Sommaire

Titre	Page
Remerciement……	i
Dédicace……	ii
Table des figures……	iii
Table des tableaux……	v
Résumé……	vi
Introduction générale……	vii
Chapitre 1 : La Biométrie	
Introduction ……	1
1. La biométrie……	1
1.2 Définition de la biométrie……	1
1.3 les caractéristiques biométriques ……	1
1.4 Les modèles biométriques……	3
1.5 Les modalités biométriques……	4
1.6 Utilisation de la biométrie……	7
1.7 La biométrie et les méthodes d'authentification traditionnelle……	8
1.8 Les applications de la biométrie……	9
2. Systèmes biométriques……	9
2.1 Modes de fonctionnement……	10
2.2 Architecture d'un système biométrique……	11
2.3 Les types de systèmes biométriques……	13
2.3.1 Les systèmes multimodaux……	13
2.3.2 L'architecture des systèmes multimodaux……	15
2.4 Les niveaux de fusion……	17
2.4.1 La fusion pré-classification……	18
2.4.2 La fusion post-classification……	19
2.5 Principe de fonctionnement d'un système biométrique……	20
2.6 Performance d'un système biométrique……	21
3. Les avantages et les limites de la biométrie……	22
3.1 Les avantages de la biométrie……	22
3.2 Les limites de la biométrie……	23
Conclusion……	25

Chapitre 2 : La reconnaissance faciale & d'empreinte palmaire avec les fractales

Introduction …….……....	**26**
A. La reconnaissance du visage……..……....	**26**
1. Définition de la reconnaissance du visage……..……....	**26**
2. Processus d'un système de reconnaissance du visage……..……	**27**
2.1 Le monde physique……..……	**28**
2.2 L'acquisition de l'image……..…….	**28**
2.3 Les prétraitements……..……..……	**28**
2.4 l'extraction de paramètres……..……..……	**28**
2.5 La classification (Modélisation)…….……..……...	**28**
2.6 L'apprentissage……..……..……...	**28**
2.7 La décision……..……..……...	**29**
3. Les méthodes utilisées pour la reconnaissance de visage……..……...	**29**
3.1 Les méthodes globales……..……...	**29**
3.1.1 L'analyse en composante principale (ACP)…….……..……...	**29**
3.1.2 L'algorithme LDA (Linear Discriminant Analysis)…….……..……...	**29**
3.1.3 Les réseaux de neurones……..……..……	**29**
3.1.4 SVM (Machine à Vecteurs de support)……..……..……...	**30**
3.2 Les méthodes locales (Géométrique)……..……..……..	**30**
3.2.2 EBGM (Elastic Bunch Graph Matching)…….……..……...	**30**
3.2.3 EingenFace modulaire……..……..……	**30**
3.2.4 Méthode de Markov cache……..……..……...	**30**
3.3 Les approches hybrides……..……..……	**30**
4. Performances d'un système de reconnaissances de visage……..……..……...	**31**
5. Difficultés de la reconnaissance de visages……..……..……...	**32**
5.1 Changement d'illumination……..……	**32**
5.2 Variation de pose……..……	**32**
5.3 Les expressions faciales……..……	**33**
5.4 Présence ou absence des composants structurels……..…….	**33**
5.5 Les vrais jumeaux……..……..…….	**34**
B. La reconnaissance de l'empreinte palmaire……..…….	**34**
1. Définition de l'empreinte palmaire……..……..……	**34**
2. Caractéristiques du système de reconnaissance de l'empreinte palmaire……..……	**35**
3. Le processus de la reconnaissance d'empreinte palmaire……..……	**38**
C. La reconnaissance biométrique avec la dimension fractale…….……..……	**40**
1. Les fractales……..……..……	**40**
2. Définition d'un objet fractale……..……..……...	**41**
3. Caractéristiques d'un objet fractale……..……..……	**41**
4. Classification des objets fractals……..…….	**42**
4.1. Fractales déterministes……..……..……	**42**

4.2. Fractales non déterministes……..……...	**45**
5. La dimension fractale…..……..……	**47**
6. Méthodes de calcul de dimension fractale……..……..	**48**
6.1 Méthodes de comptage de boites……..……..	**48**
6.2 Méthodes de mesure d'air……..……..……	**51**
Conclusion…...……..……..……	**52**
Chapitre 3 : Conception	
Introduction……..	**53**
1. Le sous-système de reconnaissance faciale……	**53**
1.2 Méthode de Box Counting (Comptage des boites) …….	**53**
1.3 Procédure et implémentation de la méthode……	**53**
2. Le sous-système de reconnaissance de l'empreinte palmaire……	**55**
2.1 Traitement de l'empreinte palmaire ……	**55**
2.2 La classification……	**57**
3. La reconnaissance multimodale basée sur la fusion d'empreinte palmaire et du visage…...	**57**
Conclusion……	**60**
Chapitre 4 : Implémentation	
Introduction……...	**61**
1. Les bases de données……..	**61**
1.1 Base de données unimodale…….	**61**
1.2 Base de données multimodale……..	**63**
1.2.1 Définition la base virtuelle……	**63**
2. Séparation de la base de données……...	**64**
2.1 Visage……...	**64**
2.2 Empreinte palmaire……..	**65**
3. Environnement du travail……...	**65**
3.1 Outils de développement …….....	**65**
3.2 Environnement matériel……...	**66**
4. Développement de l'application……	**66**
4.1 Interface principale……...	**67**
4.2 Interface du visage……...	**68**
4.3 Interface empreinte palmaire……	**69**
4.4 Interface multimodale……..	**70**
4.5 Interface statistique……..	**71**
5. Résultats expérimentaux……	**71**
5.1 Système uni-modal……...	**71**
5.2 Système multimodale……...	**72**
6. Expérimentation et discussion……	**73**
Conclusion……	**74**
Conclusion générale……...……..	

LISTE DES FIGURES

	Titre	Page
Chapitre 1 : *La Biométrie*		
Figure.1	Quelques modalités biométriques.	**3**
Figure.2	Quelques exemples de modèles biométriques. De gauche à droite, de haut en bas : minuties extraites d'une empreinte, Iris code, graphe d'un visage utilisant les points d'intérêt, signal vocal et signal de dynamique de frappe au clavier.	**4**
Figure.3	Images de l'empreinte digitale	**5**
Figure.4	Géométrie de la main	**5**
Figure.5	L'iris	**6**
Figure.6	La rétine	**6**
Figure.7	La voix	**6**
Figure.8	Visage	**7**
Figure.9	Parts de marché des techniques biométriques en 2009	**8**
Figure.10	Enrôlement d'une personne dans un système biométrique	**10**
Figure.11	Authentification d'un individu dans un système biométrique.	**11**
Figure.12	Identification d'un individu dans un système biométrique	**11**
Figure.13	Architecture générique d'un système biométrique (extrait de l'Organisation Internationale de Normalisation ISO/IEC 19795-1 [5]).	**12**
Figure.14	Systèmes multi algorithmes	**14**
Figure.15	Systèmes multi échantillons	**14**
Figure.16	Systèmes multi capteurs	**14**
Figure.17	Systèmes multi instances	**15**
Figure.18	Systèmes multi caractères	**15**
Figure.19	Architecture de fusion en parallèle	**16**
Figure.20	Architecture de fusion en série (incrémentale ou séquentielle)	**17**
Figure.21	Les différents niveaux de fusion	**17**
Figure.22	Schéma de fusion au niveau du capteur	**18**
Figure.23	Schéma de fusion au niveau du l'extraction des caractéristiques	**19**
Figure.24	Schéma de fusion au niveau de la décision	**20**
Figure.25	Schéma de fusion au niveau de scores	**20**
Figure.26	Illustration du FRR et du FAR	**22**

Chapitre 2 : La reconnaissance faciale et d'emprinte palmaire avec les fractales		
Figure.1	Scores de compatibilité pour différentes technologies biométriques dans un système MRTD	**27**
Figure.2	Processus d'un système de reconnaissance	**27**
Figure.3	une classification des algorithmes principaux utilisés en reconnaissance faciale	**31**
Figure.4	Exemple de variation d'éclairage	**32**
Figure.5	Exemples de variation de poses	**33**
Figure.6	Exemples de variation d'expressions	**33**
Figure.7	Paume de la main	**34**
Figure.8	Régions de la paume de la main	**35**
Figure.9	Lignes principales de la paume de la main	**36**
Figure.10	Régions d'une empreinte palmaire	**36**
Figure.11	Caractéristiques géométriques et points delta d'une empreinte palmaire	**37**
Figure.12	Image hors ligne et en ligne de palmprint	**38**
Figure.13	Dispositif de capture de palmprints en ligne	**39**
Figure.14	Régions d'intérêts extraits d'une image palmprint	**39**
Figure.15	Quelques schémas fractals	**40**
Figure.16	image de synthèse représentant l'irrégularité d'un objet fractal	**41**
Figure.17	objet fractal représentant l'auto similitude a différents échelles	**42**
Figure.18	Ensemble de Cantor	**43**
Figure.19	Courbe de Von Koch	**43**
Figure.20	Flocon de Von Koch	**44**
Figure.21	Triangle de Sierpinskien	**44**
Figure.22	la fougère	**45**
Figure.23	la fougère après grossissement	**46**
Figure.24	réseau sanguin	**46**
Figure.25	réseau sanguin après grossissement	**47**
Figure.26	mesure de la dimension fractale d'une courbe par la méthode des boites	**49**
Figure.27	méthode comptage différentiel de boites	**50**
Figure.28	méthode des prismes triangulaires	**51**
Chapitre3 : La conception		
Figure.1	Image du visage à traiter	**54**
Figure.2	Image du visage après filtrage gaussien	**54**
Figure.3	Image d'une empreinte capturée	**55**
Figure.4	Région d'intérêt extraite d'une empreinte palmaire	**56**
Figure.5	Contour de la région d'intérêt	**56**
Figure.6	Schéma de la fusion de scores	**57**

Figure.7	Fusion au niveau score dans notre système biométrique multimodal	**58**
Figure.8	Architecture de système multimodale au niveau des scores	**59**
Figure.9	Architecture de système multimodale au des caracteristiques	**59**
Chapitre 4 : Implémentation		
Figure.1	Extrait de la base AT&T	**62**
Figure.2	la base CASIA-MS-PalmprintV1	**63**
Figure.3	La création d'une base multimodale	**64**
Figure.4	Caractéristiques de l'ordinateur	**66**
Figure.5	Interface principale du système	**66**
Figure.6	Interface visage	**67**
Figure.7	Interface visage (2)	**68**
Figure.8	Interface Empreinte palmaire	**68**
Figure.9	Interface Empreinte palmaire(2)	**69**
Figure.10	Interface multimodale	**69**
Figure.11	Interface multimodale(2)	**70**
Figure.12	Interface statistique	**71**

Liste des Tableaux

	TITRE	**page**
Chapitre 1 : *La Biométrie*		
TAB 1	Comparaison entre les techniques biométriques	3
TAB 2	Comparaison entre l'authentification biométrique et par mot de passe/clé.	9
Chapitre 4 : Implémentation		
TAB 1	Taux de reconnaissance unimodale.	71
TAB 2	Taux de reconnaissance multimodale.	72

Résumé

La biométrie, appliquée dans un contexte de traitement automatisé des données et de reconnaissance des identités, fait partie de ces technologies nouvelles dont la complexité d'utilisation fait émerger de nouveaux enjeux et où ses effets à long terme sont incalculables. L'envergure des risques suscite des questionnements dont il est essentiel de trouver les réponses. On justifie le recours à cette technologie dans le but d'apporter plus de sécurité, mais, vient-elle vraiment apporter plus de protection dans le contexte actuel?

Les technologies biométriques sont flexibles en ce sens qu'elles permettent de saisir une multitude de caractéristiques biométriques et offrent aux utilisateurs plusieurs modalités de fonctionnement. Par exemple, on peut l'utiliser pour l'identification tout comme pour l'authentification. Bien que la différence entre les deux concepts puisse être difficile à saisir, nous verrons qu'ils auront des répercussions différentes sur nos droits et ne comporteront pas les mêmes risques.

Par ailleurs, le droit fondamental qui sera le plus touché par l'utilisation de la biométrie sera évidemment le droit à la vie privée. Encore non bien compris, le droit à la vie privée est complexe et son application est difficile dans le contexte des nouvelles technologies.

La circulation des données biométriques, la surveillance accrue, le détournement d'usage et l'usurpation d'identité figurent au tableau des risques connus de la biométrie. De plus, nous verrons que son utilisation pourra avoir des conséquences sur d'autres droits fondamentaux, selon la manière dont le système est employé.

Les tests de nécessité du projet et de proportionnalité de l'atteinte à nos droits seront les éléments clés pour évaluer la conformité d'un système biométrique. Ensuite, le succède la technologie dépendra des mesures de sécurité mises en place pour assurer la protection des données biométriques, leur intégrité et leur accès, une fois la légitimité du système établie.

Mots-clés : Biométrie, donnée biométrique, Biométrie multimodale, sécurité, nouvelles technologies, vie privée, visage, empreinte palmaire, reconnaissance biométrique.

Introduction Générale

La biométrie est un terme dont on entend de plus en plus parler dans la vie de tous les jours. Si de nombreuses applications utilisent aujourd'hui la biométrie, celle qui correspond au plus grand déploiement est la mise en place, prévue pour 2009 des passeports biométriques utilisant le visage et l'empreinte palmaire digitale pour la délivrance et le contrôle de l'identité. Cependant, la biométrie n'est pas vraiment récente. Son apparition remonte au 19ème siècle, avec les premières études alors appelées anthropométrie. Les empreintes digitales ont ensuite été utilisées pour l'identification des personnes par la police. Cette utilisation policière n'a d'ailleurs jamais été abandonnée, et les empreintes palmaires sont toujours utilisées (aujourd'hui de manière automatique avec les traitements informatiques) pour l'identification criminelle. La biométrie soufre d'ailleurs un peu de cette image policière et a du mal à se faire accepter par le grand public pour d'autres types d'applications. Cela dit, aujourd'hui la biométrie n'est plus limitée aux empreintes digitales et à l'identification criminelle. De nombreuses modalités sont aujourd'hui utilisées pour des applications de contrôle d'accès à des locaux ou à des objets personnels. On peut citer le visage, la voix, la signature, l'iris ou la forme de la main, et d'autres encore sont à l'étude comme la démarche, la forme de l'oreille ou la dynamique de frappe au clavier.

L'objectif de notre projet de fin d'étude est l'étude de deux systèmes de reconnaissances empreinte palmaire et faciale.

Les objectifs de notre travail s'inscrivent dans le cadre de :

- L'étude de la biométrie multimodale.
- L'étude de système la reconnaissance d'empreinte palmaire et ces différents méthodes et étapes.
- L'étude de la reconnaissance faciale avec ces méthodes et approches.
- La technique de fusion et ces différents niveaux.
- La conception d'un système d'empreinte palmaire et faciale par la méthode des dimensions fractales.
- L'implémentation et la réalisation du système de la biométrie multimodale.

Ce mémoire se décompose en quatre chapitres :

Le premier chapitre intitulé «Biométrie & systèmes biométriques» définit la biométrie et le système biométrique et leur principe de fonctionnement.

Dans le deuxième chapitre intitulé «La reconnaissance faciale & d'empreinte palmaire avec les fractales » nous définissons les caractéristiques des empreintes palmaires et le visage Par la suite nous présentons les divers méthodes de la reconnaissance faciale. Enfin une présentation détaillé sur les la nouvelle approche des fractales, Nous y détaillons le principe de fonctionnement de la dimension fractale.

Le troisième chapitre intitulé « la conception « en premier lieu nous présentons la conception de notre système de reconnaissance d'empreinte palmaire avec tout les algorithmes de cette étape, et aussi une description de la méthode fractale utilisé pour la reconnaissance et même chose pour les palmprints.

Le quatrième chapitre intitulé « Implémentation » nous présentons le système de reconnaissance de deux modalités qu'on a choisi .par la suite, nous présentons le langage de programmation et l'environnement de développement utilises lors de l'implémentation de notre application .enfin nous exposons quelque résultats expérimentaux obtenus en utilisant des captures de l'application.

Nous finalisons ce mémoire par une conclusion générale.

Chapitre 1

Biométrie & systèmes biométriques

Introduction

Un système biométrique est essentiellement un système de reconnaissance de formes qui utilise les données biométriques d'un individu. Les systèmes biométriques sont de plus en plus utilisés depuis quelques années. L'apparition de l'ordinateur et sa capacité à traiter et à stocker les données ont permis la création des systèmes biométriques informatisés.

Nous introduirons dans ce chapitre quelques notions et définitions de base liées à la biométrie. Nous donnerons le principe de fonctionnement des systèmes biométriques ainsi que les outils utilisés pour mesurer leurs performances. Nous insisterons surtout sur la place de la reconnaissance faciale parmi les autres techniques biométriques, car elle constitue l'objectif de ce thème.

1. La biométrie

1.2 Définition de la biométrie

Il existe trois façons génériques pour vérifier ou déterminer l'identité d'un individu :

i) ce que l'on sait (code PIN, mot de passe, etc.)
ii) ce que l'on possède (badge, carte à puce, etc.)
iii) ce que l'on est ou ce que l'on sait faire (empreinte digitale, dynamique de frappe au clavier, etc.)

Ce dernier point fait référence à la biométrie.

La biométrie consiste à vérifier ou déterminer l'identité d'un individu à partir de ses caractéristiques biologiques (comme l'ADN), comportementales (comme la voix) ou morphologiques (comme l'empreinte digitale).

1.3 Les caractéristiques biométriques

Les caractéristiques biométriques par lesquelles il est possible de vérifier l'identité d'un individu sont appelées modalités biométriques. La figure 1 illustre un exemple de quelques modalités biométriques. Ces modalités sont basées sur l'analyse des données liées à l'individu et sont généralement classées en trois catégories : biométrie biologique, comportementale et morphologique. La biométrie biologique se base sur l'analyse des données biologiques liées à l'individu (salive, ADN, etc.). La biométrie comportementale se base sur l'analyse de comportements d'un individu (manière de marcher, dynamique de frappe au clavier, etc.). La biométrie morphologique se base sur les traits physiques particuliers qui, pour toutes personnes, sont permanents et uniques (empreinte digitale, visage, etc.). Pratiquement, n'importe quelle caractéristique morphologique ou comportementale peut être considérée comme une caractéristique biométrique, dans la mesure où elle satisfait les propriétés suivantes [1]

– **Universalité** : toutes les personnes à identifier doivent la posséder ;

– **Unicité** : l'information doit être aussi dissimilaire que possible entre les différentes personnes.

– **Permanence** : l'information collectée doit ˆêtre présente pendant toute la vie d'un individu.

– **Collectabilité** : l'information doit être collectable et mesurable afin d'être utilisée pour les comparaisons.

– **Acceptabilité** : le système doit respecter certains critères (facilite d'acquisition, rapidité, etc.) afin d'être employé.

Les caractéristiques biométriques ne possèdent pas toutes ces propriétés, ou les possèdent mais à des degrés différents. Le tableau 1, extrait de [2], compare les principales modalités biométriques selon les propriétés suivantes : universalité, unicité, permanence, Collectabilité, acceptabilité et performance. Ce tableau montre qu'aucune caractéristique n'est donc idéale et qu'elles peuvent être plus ou moins adaptées à des applications particulières. Par exemple, l'analyse basée sur l'ADN est une des techniques les plus efficaces pour vérifier l'identité d'un individu ou l'identifier [3].

Néanmoins, elle ne peut pas être utilisée pour le contrôle d'accès logique ou physique pour des raisons de temps de calcul, mais aussi, parce que personne ne serait prêt à donner un peu de sang pour faire la vérification. Le choix de la modalité est ainsi effectue selon un compromis entre la présence ou l'absence de certaines de ces propriétés selon les besoins de chaque application. A noter que le choix de la modalité biométrique peut aussi dépendre de la culture locale des usagers. En Asie, les méthodes nécessitant un contact physique comme les empreintes digitales sont rejetées pour des raisons d'hygiène alors que les méthodes sans contact sont plus répandues et acceptées.

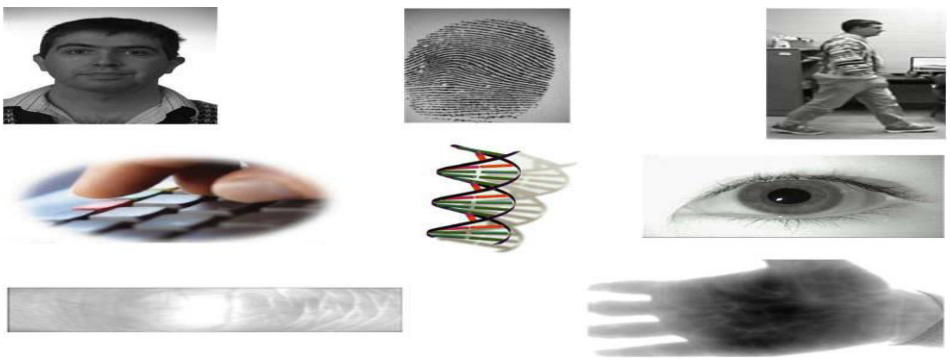

Figure1 : Quelques modalités biométriques.

Biométrie	Universalité	Unicité	Permanence	Mesurabilité	Performance	Acceptabilité	Circonvention
DNA	Haute	Haute	Haute	Faible	Haute	Faible	Faible
Oreille	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Haute	Moyenne
Visage	Haute	Faible	Moyenne	Haute	Faible	Haute	Haute
Thermo Visage	Haute	Haute	Faible	Haute	Moyenne	Haute	Haute
Empreinte	Moyenne	Haute	Haute	Moyenne	Haute	Moyenne	Moyenne
Démarche	Moyenne	Faible	Faible	Haute	Faible	Haute	Moyenne
Géométrie Main	Moyenne	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Moyenne
Veines Main	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Faible
Iris	Haute	Haute	Haute	Moyenne	Haute	Faible	Faible
Frappe Clavier	Faible	Faible	Faible	Moyenne	Faible	Moyenne	Moyenne
Odeur	Haute	Haute	Haute	Faible	Faible	Moyenne	Faible
Rétine	Haute	Haute	Moyenne	Faible	Haute	Faible	Faible
Signature	Faible	Faible	Faible	Haute	Faible	Haute	Haute
Voix	Moyenne	Faible	Faible	Moyenne	Faible	Haute	Haute

TAB. 1: Comparaison entre les techniques biométriques [2].

1.4 Les modèles biométriques

Un modèle biométrique (appelé aussi gabarit ou Template) est l'ensemble des données utilisées pour représenter un utilisateur. Les caractéristiques biométriques acquises ne sont pas enregistrées et utilisées telles quelles. Une phase de traitement est effectuée pour réduire les données biométriques brutes et produire ainsi le modèle biométrique. La figure 2 illustre quelques exemples de modèles biométriques. Pour le stockage de ces modèles, il existe quatre emplacements principaux que sont le l'EUSB, la base centralisée, la machine individuelle de travail et le capteur biométrique. Chacun de ces emplacements présente des avantages et faiblesses en termes de temps de traitement, confidentialité et respect de la vie privée. En France, l'utilisation de la base centralisée est proscrite pour un nombre d'individus élevé par la Commission Nationale Informatique et Libertés (CNIL).

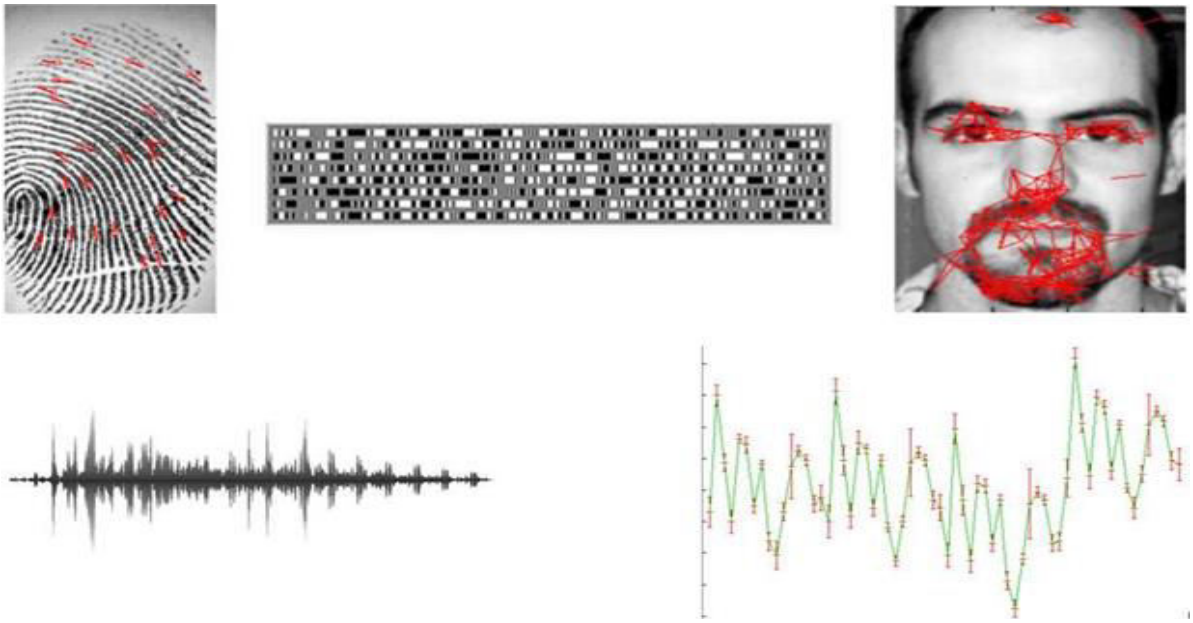

Figure 2 : Quelques exemples de modèles biométriques. De gauche à droite, de haut en bas : minuties extraites d'une empreinte, Iris code, graphe d'un visage utilisant les points d'intérêt, signal vocal et signal de dynamique de frappe au clavier.

1.5 Les modalités biométriques

La multitude des caractères biométriques de l'être humain a donné naissance à plusieurs systèmes d'authentification, chacun repose sur un caractère morphologique ou comportemental, parmi ces systèmes il y a ceux qui ont prouvé leur fiabilité et leurs cours d'évolution.

- **Les systèmes morphologiques :** Ce type de systèmes est basé sur l'identification de traits physiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe la reconnaissance des empreintes digitales, de la forme de la main, de la forme du visage, de la rétine, de l'ADN et de l'iris de l'Sil.

    1) **Les Empreintes digitales :** Il s'agit d'une des premières biométries utilisées dans des machines d'authentification, La formation des empreintes dépend des conditions initiales développement embryogénique, ce qui les rend uniques à chaque personne et même à chaque doigt.

Figure 3 : Images de l'empreinte digitale

2) **Géométrie de la main :** Il consiste à mesurer plusieurs caractéristiques de la main (jusqu'à 90) telle que la forme de la main, longueur et largeur des doigts, formes des articulations, longueurs inter articulations, &etc. La technologie associée à cela est principalement de l'imagerie infrarouge**.**

Figure 4 : Géométrie de la main

3) **L'iris :** est la membrane colorée de l'Sil. Une caméra proche des infrarouges photographie une tranche de l'iris, elle relève les caractéristiques particulières du relief.

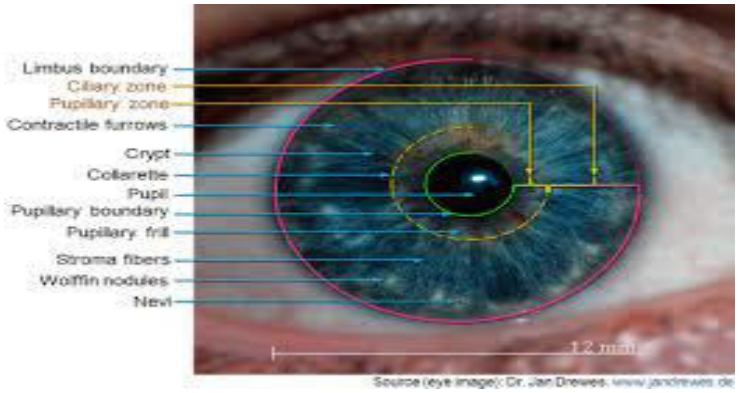

Figure 5 : L'iris

4) **La rétine :** Il a été montré que chaque Sil possède en sa rétine un vaisseau sanguin. La technique basée sur la rétine utilise la texture de ces vaisseaux. L'identification consiste à éclairer le fond de l'Sil par un faisceau lumineux de faible intensité.

Figure 6 : La rétine

5) **La voix :** La reconnaissance par voix utilise les caractéristiques vocales pour identifier les personnes en utilisant des phrases mot de passe. Un téléphone ou un microphone peut être utilisé comme dispositif d'acquisition ce qui rend cette technologie relativement économique et facilement réalisable, cependant elle peut être perturbée par des facteurs extérieurs comme le bruit de fond ou la maladie ou l'état émotionnel de la personne.

Figure 7 : La voix

6) **Le visage :** Il s'agit de capter la forme du visage d'un individu et d'en extraire certaines informations jugées évidentes pour l'authentification. Selon le système utilisé, l'individu doit être positionné devant l'appareil où peut-être en mouvement à une certaine distance. Les données biométriques qui sont obtenues sont par la suite comparées au fichier référence. Au début des années 1970, la reconnaissance par le visage était principalement basée sur des attributs faciaux mesurables comme l'écartement des yeux, des sourcils, des lèvres, la position du menton, la forme,& etc. Depuis les années 1990, les différentes technologies

utilisées exploitent toutes les découvertes effectuées dans le domaine du traitement d'image et de l'analyse de données.

Figure 8 : Visage

- **Les systèmes comportementaux :** Ce type de systèmes se base sur l'analyse de certains comportements d'une personne comme le tracé de sa signature, sa démarche et sa façon de taper sur un clavier.
- **Les modalités biologiques :** Elle est basée sur l'identification de traits biologique particuliers.
  - ADN
  - Odeur
  - Salive
  - Urine
  - Cheveux
  - Veines de la main

1.6 Utilisation de la biométrie

Le champ d'application de la biométrie est t'es vaste. En effet, tous les domaines qui nécessitent de vérifier ou d´déterminer l'identité de personnes sont concernés. On retrouve ainsi des applications de la biométrie pour gérer l'accès à des ressources physiques (comme l'accès à des lieux sécurisés) et logiques (comme le commerce elle-tronique). La biométrie intéresse aussi plusieurs pays (l'Europe, les Etats-Unis, etc.) afin de produire des titres d'identité plus sûres, telle que la carte nationale d'identité ou le passeport biométrique. A noter qu'en France, le passeport biométrique est désormais d´employé. Il intègre une puce RFID qui contient au moins deux informations biométriques : une empreinte digitale et une image du visage numérisée. Enfin, la biométrie n'a pas que des applications à vocation sécuritaire, mais également des applications qui facilitent le quotidien des usagers. Ainsi, la biométrie est utilisée dans certains aéroports permettant aux clients réguliers de ne pas perdre

de temps lors de l'embarquement. La figure 9, réalisée d'après les chiffres d'International Biométrique Group [4], montre les parts de marché des principales méthodes biométriques en 2009. Les empreintes digitales sont toujours les plus utilisées, suivies par la reconnaissance faciale. Ces deux modalités représentent les trois quarts du marché de la biométrie.

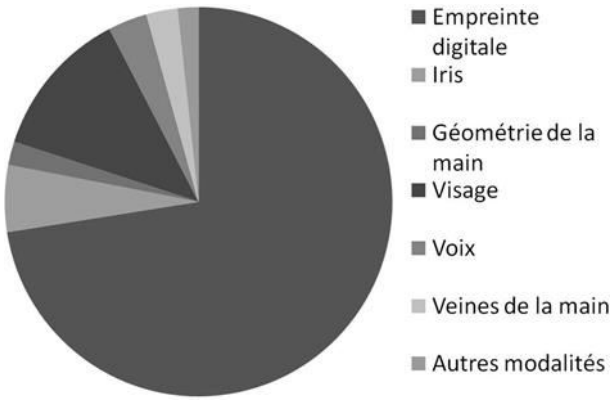

Figure 9 : Parts de marché des techniques biométriques en 2009 [4]

1.6 La biométrie et les méthodes d'authentification traditionnelles

Puisque la biométrie fait appel à ce que l'on est, elle comporte un avantage primordial sur les méthodes traditionnelles, dans le sens où elle évite l'usage d'un grand nombre de mots de passe complexes, de badges, etc. Le tableau 2 présente un parallèle entre la biométrie et les méthodes d'authentification traditionnelles. Ce tableau montre que les systèmes biométriques facilitent le processus d'authentification et résiste aux différentes attaques existantes sur les systèmes basés sur un secret ou une possession. Cependant, ces systèmes présentent plusieurs inconvénients concernant le respect de la vie privée et l'incertitude de l'information biométrique. Une comparaison de ces techniques est détaillée par O'Gorman. [5]

Authentification biométrique	Authentification par mot de passe / clé
-Basée sur des mesures morphologiques, comportementales ou biologiques	-Basée sur l'on sait où que l'on possède
-Utilisation facile (Pas de secret à retenir)	-Pouvant être plus compliquée (mot de passe complexe)
-Authentifie l'individu	-Il peut être perdu, volé ou oublié
-L'information est en relation étroite à l'utilisateur de façon permanente	-exacte : utilise une comparaison
-Probabiliste : Utilise une comparaison	-L'information ne varie pas, elle est sûre
-L'information biométrique peut être modifié	-Moindre impact sur la vie privée
-Problème de respect de la vie privée	-Changement aisé
-Difficile à révoquer l'information	-Authentifie l'individu

TAB 2 : Comparaison entre l'authentification biométrique et par mot de passe/clé. [5]

1.7 Les applications de la biométrie

Trois secteurs sont particulièrement concernés par l'utilisation de la biométrie

- **Application judiciaires :**

C'est certainement le premier secteur ou l'identification biométrique a été appliquée : Identification de criminels, de terroristes, de cadavres, enfants disparus, etc…

- **Application gouvernementales :**

La biométrie peut éviter un usage frauduleux de documents (ex : passeport, permis de conduire, etc…).

- **Contrôle d'accès physique et logique :**

- Le contrôle d'accès logique (contrôle d'accès à un ordinateur, login d'ouverture de session réseaux, accès distants connexions VPN,…).
- Le contrôle d'accès physique à des locaux (salle informatique, service de recherche, site sensible,…), serrures électroniques,…

2. Systèmes biométriques

Un système biométrique est essentiellement un système de reconnaissance de formes qui utilise les données biométriques d'un individu. Les systèmes biométriques sont de plus

en plus utilisés depuis quelques années. L'apparition de l'ordinateur et sa capacité à traiter et à stocker les données ont permis la création des systèmes biométriques informatisés.

2.1 Modes de fonctionnement

Les systèmes biométriques fonctionnent selon trois modes que sont l'enrôlement, la vérification d'identité et l'identification :

- **Enrôlement**

L'enrôlement est la première phase de tout système biom´etrique. Il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois. Elle est commune à la vérification et l'identification. Pendant l'enrôlement, la caractéristique biom´etrique est mesurée en utilisant un capteur biom´etrique afin d'extraire une représentation numérique. Cette représentation est ensuite réduite, en utilisant un algorithme d'extraction bien d´fini, afin de réduire la quantité de données `à stocker pour ainsi faciliter la vérification et l'identification. Dépendant de l'application et du niveau de sécurité souhaité, le modèle biométrique retenu, est stocke soit dans une base de données centrale soit sur un élément personnel propre à chaque personne.

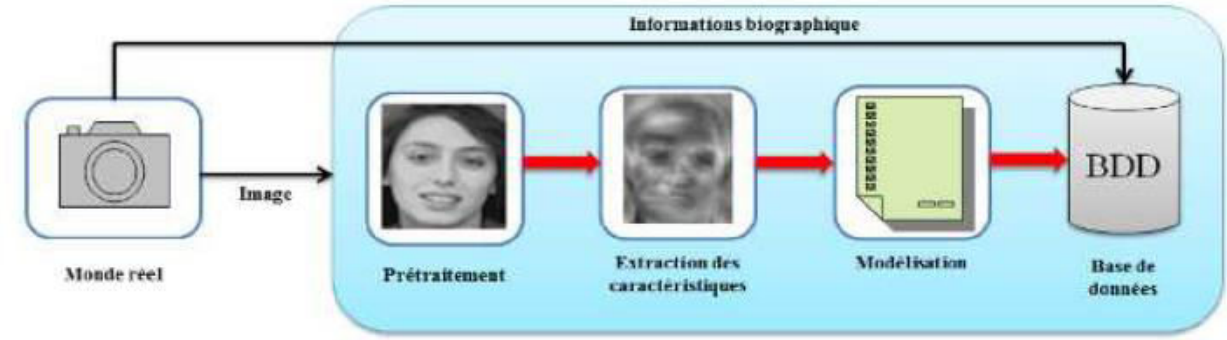

Figure 10 : Enrôlement d'une personne dans un système biométrique.

- **Vérification (Authentification)**

C'est la comparaison 1-à-1, entre les données biométriques capturées (model test) et les données stockée dans sa propre base (les modèles d'apprentissage). Dans un tel système, un individu qui désire être identifié réclame une identité, habituellement par l'intermédiaire d'un PIN (numéro d'identification personnelle), d'un nom d'utilisateur, d'une carte d'identité, etc.
Le système doit alors répondre à la question suivante "Suis-je réellement la personne que suis-je entrain de proclamer?" [6].

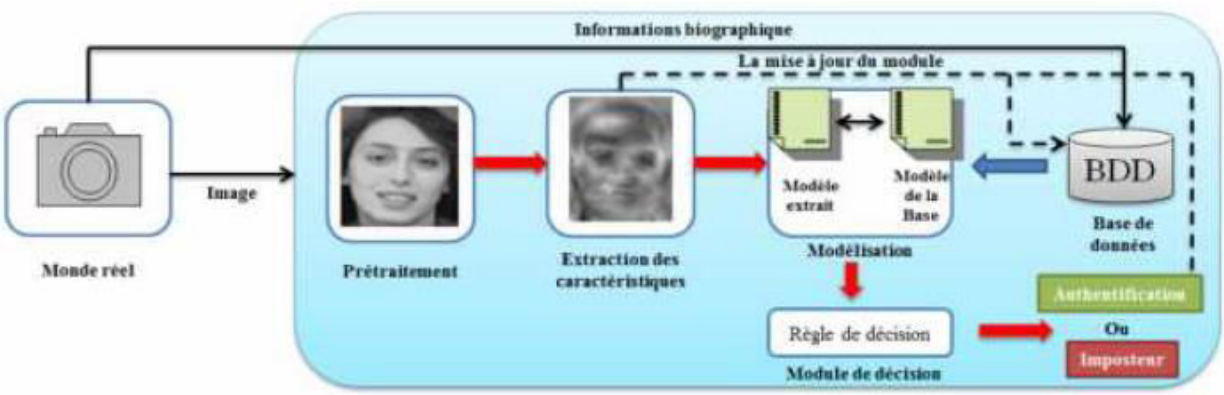

Figure 11 : Authentification d'un individu dans un système biométrique.

- **Identification**

Le système identifie un individu en cherchant les signatures (Template) de tous les utilisateurs dans la base de données. Par conséquent, le système conduit plusieurs comparaisons 1-à-N pour établir l'identité d'un individu [7]. En résumé, un système biométrique opérant en mode identification répond à la question "Suis-je bien connu du système ?".

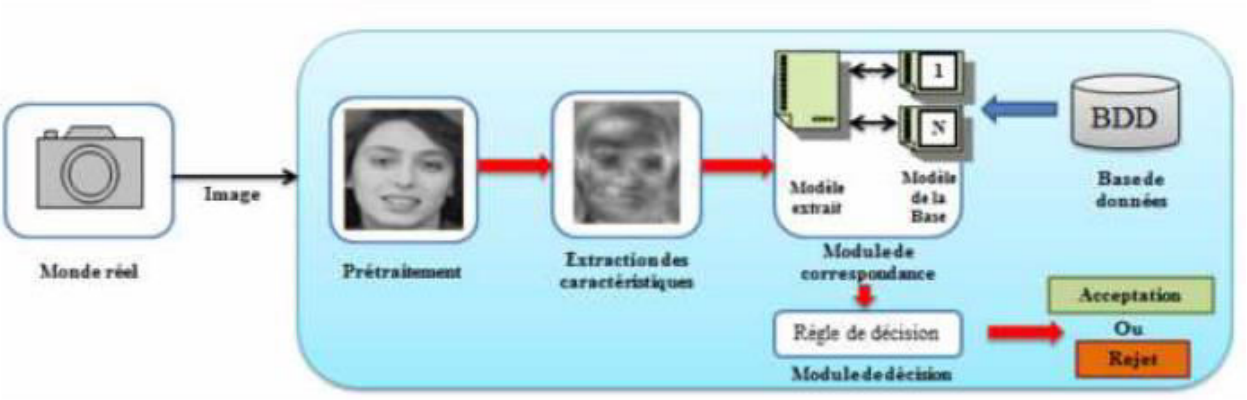

Figure 12 : Identification d'un individu dans un système biométrique.

2.2 Architecture d'un système biométrique

L'architecture d'un système biométrique contient 5 modules comme le montre la figure 13:

- **Le module de capture** qui consiste à` acquérir les données biométriques afin d'extraire une représentation numérique. Cette représentation est ensuite utilisée pour l'enrôlement, la vérification ou l'identification. Il s'agit d'un capteur biométrique qui peut être de type sans ou avec contact. [8]

- **Le module de traitement du signal** qui permet de réduire la représentation numérique extraite afin d'optimiser la quantité de données a` stocker lors de la phase d'enrôlement, ou pour faciliter le temps de traitement pendant la phase de vérification et l'identification. Ce module peut avoir un test de qualité pour contrôler les données biométriques acquises.
- **Le module du stockage** qui contient les modèles biométriques des utilisateurs enrôlés du système.
- **Le module de similarité** qui compare les données biométriques extraites par le module d'extraction de caractéristiques à un ou plusieurs modèles probablement enregistrés. Ce module détermine ainsi le degré de similarité (ou de divergence) entre deux vecteurs biométriques.
- **Le module de décision** qui d´détermine si l'indice de similarité retourné est suffisant pour d´déterminer l'identité d'un individu.

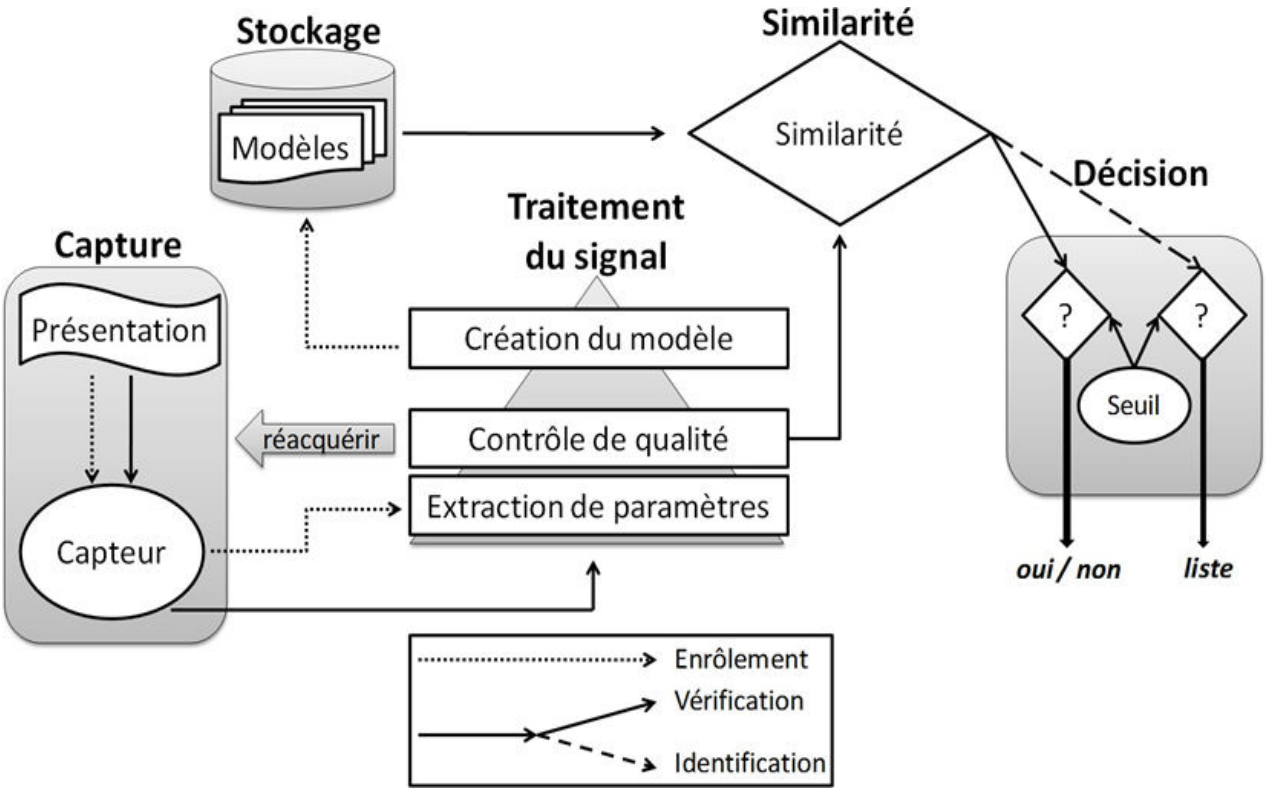

Figure 13 : Architecture générique d'un système biométrique (extrait de l'Organisation Internationale de Normalisation ISO/IEC 19795-1 [6]).

2.3 Les types de systèmes biométriques

La multitude des caractères biométriques de l'être humain a donné naissance à plusieurs systèmes d'authentification, chacun repose sur un caractère morphologique ou comportemental, parmi ces systèmes il y a ceux qui ont prouvé leur fiabilité et leurs cours d'évolution.

- **Monomodalité**

La biométrie monomodale est une technologie d'authentification de personne en se basant sur une seule modalité biométrique. Avant de procéder à proposer un système biométrique, il est nécessaire de choisir la modalité la plus appropriée à l'application.

- **Multimodalité**

Elle peut se définir comme l'association de différentes technologies biométriques en vue d'améliorer la précision ou les résultats du système (elle est également appelée «biométrie
multi niveaux»). Les systèmes biométriques utilisent au moins deux traits/modalités biométriques de la même personne lors du processus d'établissement de correspondances. Ces systèmes peuvent travailler de différentes manières, soit en collectant différentes données biométriques avec différents capteurs soit en collectant plusieurs unités des mêmes données biométriques. Certaines études englobent également dans cette catégorie les systèmes qui procèdent à plusieurs lectures des mêmes données biométriques et les systèmes qui utilisent plusieurs algorithmes pour l'extraction de traits du même échantillon biométrique. Parmi les systèmes biométriques multimodaux, on retrouve le passeport électronique au niveau de l'UE ainsi que le système d'identification biométrique US-VISIT aux États-Unis.

2.3.1 Les systèmes multimodaux

Peuvent se référer à de nombreux systèmes différents :

- **Systèmes multi algorithmes:** C'est le type de système le plus classique implicitement utilisé par de nombreuses approches. Les caractéristiques sont extraites via différents algorithmes puis fusionnées. La fusion de caractéristiques extraites via un algorithme analysant les textures et un autre la forme d'un caractère biométrique entre dans ce cadre.

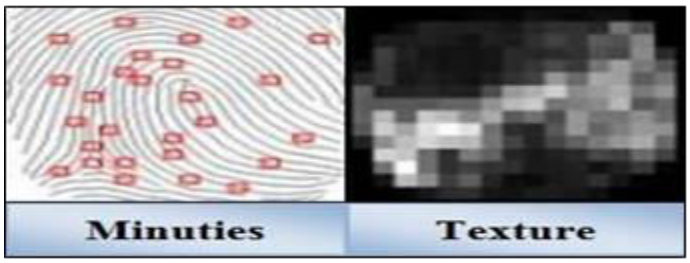

Figure 14 : Systèmes multi algorithmes

- **Systèmes multi échantillons:** Un capteur unique peut capturer plusieurs instances du même caractère biométrique dans le but de rendre plus robuste l'extraction des caractéristiques ou d'enrichir le modèle biométrique d'une personne. C'est le cas, par exemple, de plusieurs captures de visage d'une personne sous différents angles. L'utilisation de vidéos entre également dans ce cadre.

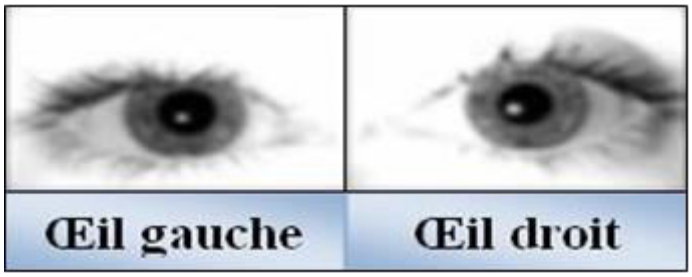

Figure 15 : Systèmes multi échantillons

- **Systèmes multi capteurs:** Plusieurs capteurs permettent de capturer le même caractère biométrique sous différents angles. Ainsi la capture d'un visage à l'aide d'une caméra classique et d'une caméra infrarouge entre dans ce scénario. Ce type de système permet notamment la fusion au niveau capteur, ce que ne permettent pas d'autres systèmes comme les systèmes multi caractères.

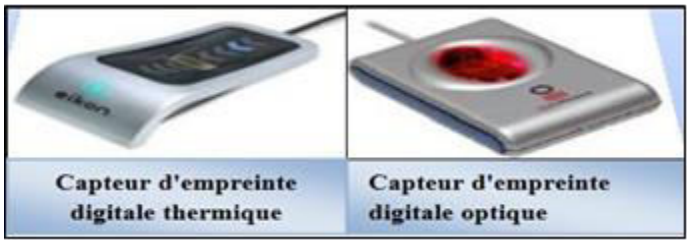

Figure 16 : Systèmes multi capteurs

- **Systèmes multi instances:** Ce type de système permet de capturer plusieurs instances du même caractère biométrique. L'acquisition de plusieurs empreintes digitales via le même capteur est l'exemple typique de ce type de système. Ces systèmes n'entraînent

pas de surcoût de capteurs, ni le développement de nouveaux algorithmes. À ne pas confondre avec les systèmes multi échantillons.

Figure 17 : Systèmes multi instances

- **Systèmes multi caractères:** Ce type de système combine différents traits biométriques d'un individu. Les fusions visage iris, ou visage empreinte digitale font partie de ce type d'approche. Ces systèmes nécessitent différents capteurs ainsi que des algorithmes dédiés à chaque caractère biométrique. Ce type de système a comme principale caractéristique que les caractères biométriques considérés peuvent être plus décorrélées que pour les systèmes multi capteurs.

Figure 18 : Systèmes multi caractères

La fusion de données issues de visages capturés via une caméra en lumière visible et une autre en lumière infrarouge entre dans le cadre des systèmes multi capteurs, où il est considéré que les deux captures sont issues de modalités différentes. Même si les deux captures sont sensiblement décorrélées (la chaleur émise par un visage n'est pas visible en lumière visible), la fermeture des yeux d'un individu est visible sur les deux modalités. À noter la présence de systèmes hybrides combinant plusieurs scénarios. Une revue de nombreux systèmes biométriques multimodaux développés peut être trouvée dans [9].

2.3.2 L'architecture des systèmes multimodaux

Les systèmes multimodaux associent plusieurs systèmes biométriques et nécessitent donc l'acquisition et le traitement de plusieurs données. L'acquisition et le traitement peuvent se faire successivement, on parle alors d'architecture en série, ou simultanément, on parle

alors d'architecture en parallèle. L'architecture est en réalité surtout liée au traitement. En effet, l'acquisition des données biométriques est en général séquentielle pour des raisons pratiques. Il est difficile d'acquérir en même temps une empreinte digitale et une image d'iris dans de bonnes conditions. Il existe cependant certains cas où les acquisitions peuvent être faites simultanément lorsque les différentes données utilisent le même capteur par exemple les capteurs d'empreintes multi-doigts qui permettent d'acquérir plusieurs doigts simultanément ou même les empreintes palmaires. L'architecture est donc en général liée au traitement et en particulier à la décision. En effet la différence entre un système multimodal en série et un système multimodal en parallèle réside dans le fait d'obtenir un score de similarité à l'issue de chaque acquisition (fusion en série) ou de procéder à l'ensemble des acquisitions avant de prendre une décision (fusion en parallèle). L'architecture en parallèle (figure 4.3) est la plus utilisée car elle permet d'utiliser toutes les informations disponibles et donc d'améliorer les performances du système. En revanche, l'acquisition et le traitement d'un grand nombre de données biométriques est coûteux en temps et en matériel, et réduit le confort d'utilisation. C'est pour cela que l'architecture en série (figure 19) peut être privilégiée dans certaines applications ; par exemple si la Multimodalité est utilisée pour donner une alternative pour les personnes ne pouvant pas utiliser l'empreinte digitale. Pour la majorité des individus seule l'empreinte est acquise et traitée mais pour ceux qui ne peuvent pas être ainsi authentifiés on utilise un système à base d'iris alternativement.

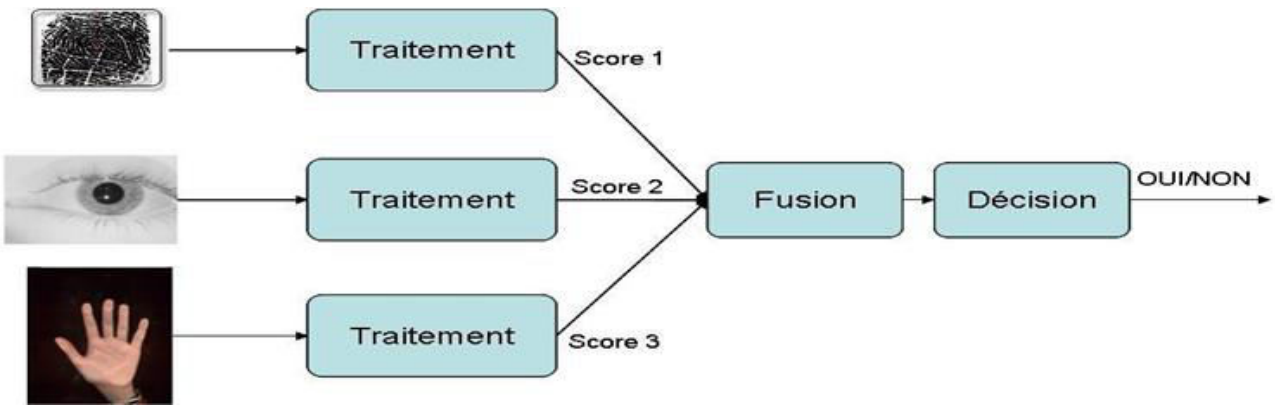

Figure 19 : Architecture de fusion en parallèle

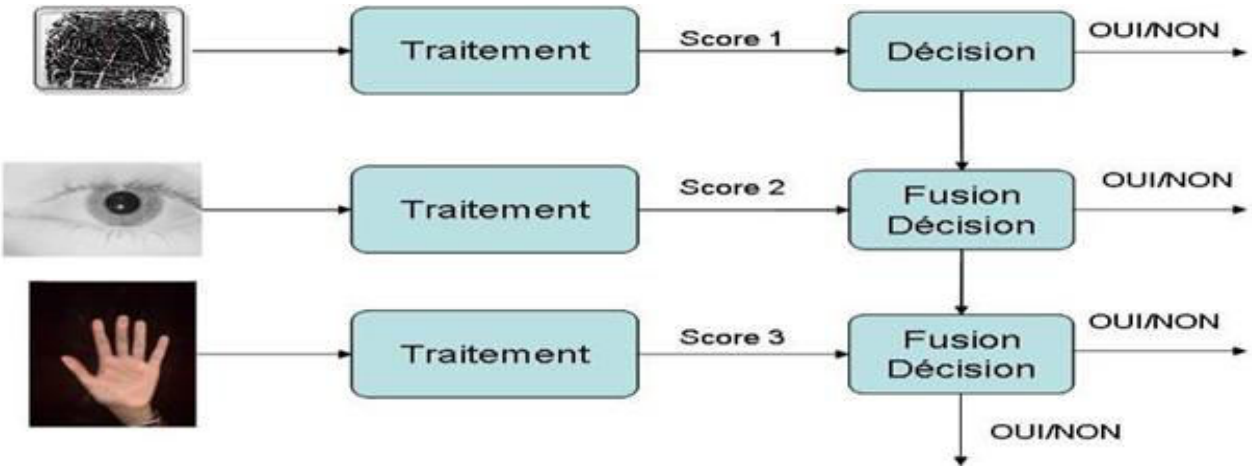

Figure 20 : Architecture de fusion en série (incrémentale ou séquentielle)

2.4 Les niveaux de fusion

La combinaison de plusieurs systèmes biométriques peut se faire à quatre niveaux différents: au niveau des données, au niveau des caractéristiques extraites, au niveau des scores issus du module de comparaison ou au niveau des décisions du module de décision (figure 4.4).

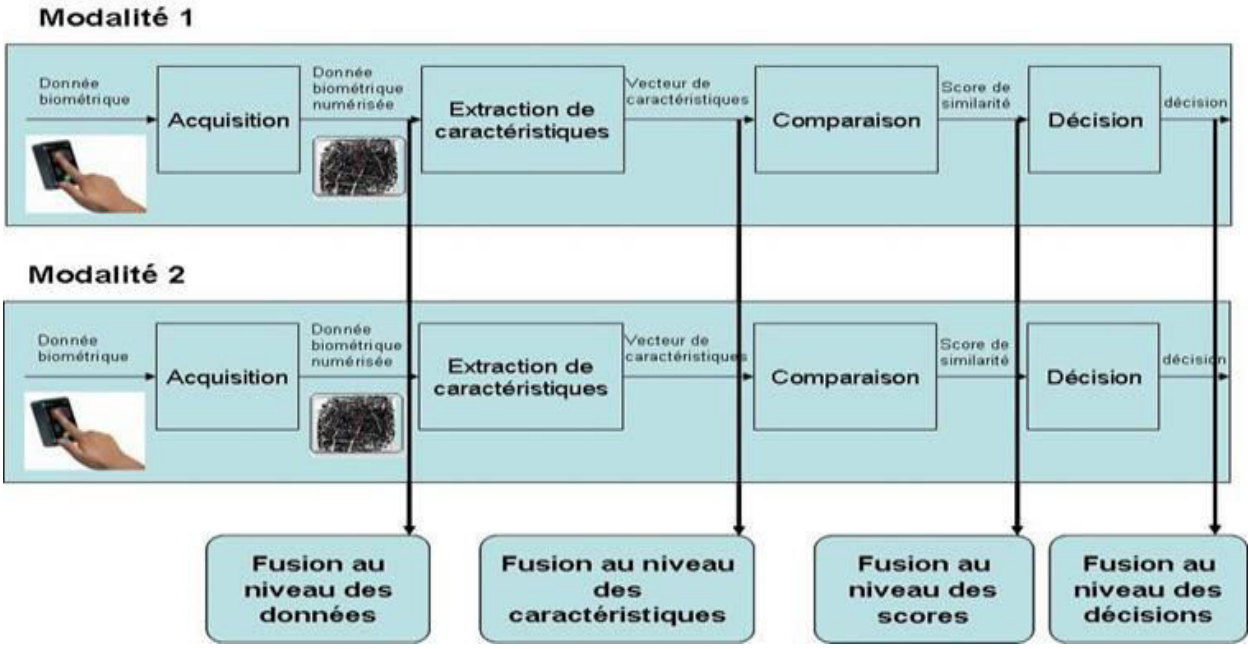

Figure 21 : Les différents niveaux de fusion

Ces quatre niveaux de fusion peuvent être classés en deux sous-ensembles :

- la fusion pré-classification (avant comparaison),
- la fusion post-classification (après la comparaison).

2.4.1 La fusion pré-classification

La fusion pré-classification correspond à la fusion des informations issues de plusieurs données biométriques au niveau du capteur (images brutes) ou au niveau des caractéristiques extraites par le module d'extraction de caractéristiques.

1) Niveau du capteur (Sensor Level)

La fusion au niveau capteur est relativement peu utilisée car se faire uniquement si les diverses captures sont des instances du même trait biométrique obtenu à partir de plusieurs capteurs compatibles entre eux ou plusieurs instances du même trait biométrique obtenu à partir d'un seul capteur. De plus, les captures doivent être compatibles entre elles et la correspondance entre les points dans les données brutes doit être connue par avance. Par exemple, les images de visage obtenues à partir de plusieurs caméras peuvent être combinées pour former un modèle 3D du visage. Un autre exemple de fusion au niveau capteur consiste à mettre en mosaïque plusieurs images d'empreintes digitales afin de former une image d'empreinte digitale finale plus complexe. La fusion au niveau capteur n'est généralement pas possible si les instances des données sont incompatibles (par exemple, il est peut être difficile de fusionner des images de visages provenant de caméras ayant des résolutions différentes).

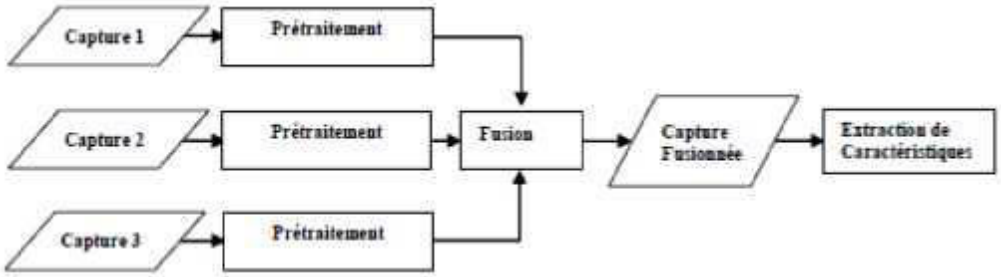

Figure 22 : Schéma de fusion au niveau du capteur.

2) Niveau Caractéristiques (Feature Level)

La fusion au niveau des caractéristiques est moins limitée par la nature des données biométriques. Cependant une certaine homogénéité est nécessaire pour la plupart des méthodes de fusion au niveau des caractéristiques comme par exemple la moyenne de plusieurs "templates" d'empreintes ou de visage. Un exemple de fusion au niveau des caractéristiques qui ne nécessitent pas vraiment d'homogénéité est la concaténation de plusieurs vecteurs de caractéristiques avant le traitement par l'algorithme de comparaison. Par exemple, dans [292], Jing et al proposent une méthode de fusion de caractéristiques pour de la fusion de visage et d'empreinte palmaire. La fusion est effectuée par concaténation d'images obtenues par transformée de Gabor sur les images de visage et d'empreinte de la main. Mais la

concaténation pose le problème de la dimension de l'espace de classification qui lorsqu'il augmente, rend plus difficile la tâche de classification.

Les méthodes de fusion pré-classification sont assez peu utilisées car elles posent un certain nombre de contraintes qui ne peuvent être remplies que dans certaines applications très spécifiques. En revanche, la fusion post-classification est très étudiée par les chercheurs.

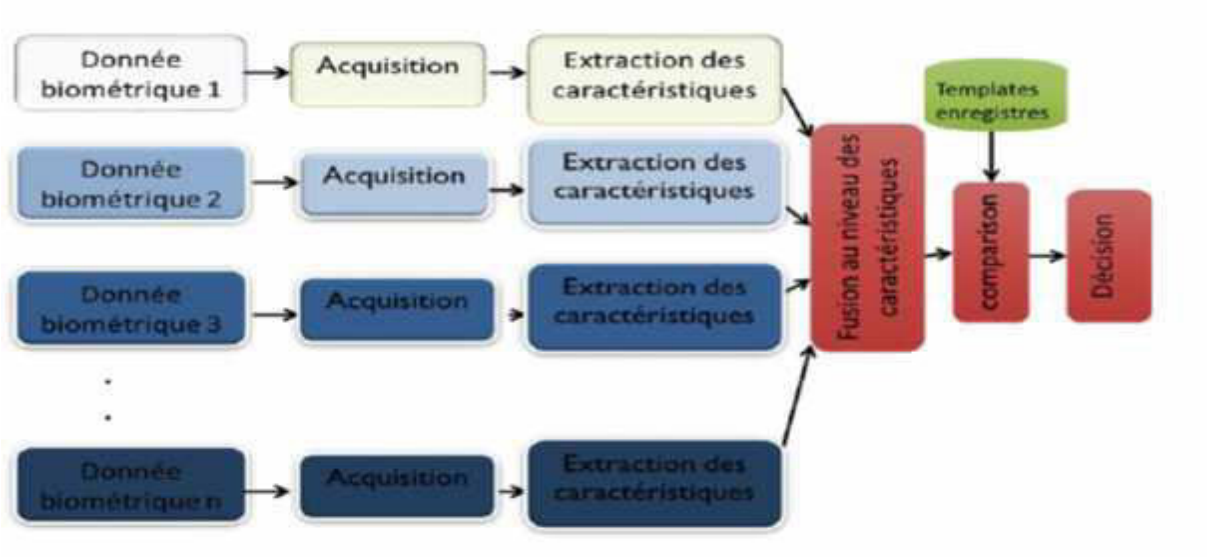

Figure 23 : Schéma de fusion au niveau du l'extraction des caractéristiques.

2.4.2 La fusion post-classification

La fusion post-classification peut se faire au niveau des scores issus des modules de comparaison ou au niveau des décisions. Dans les deux cas, la fusion est en fait un problème bien connu de la littérature sous le nom de "Multiple Classifier systems".

1) Niveau Décision (Decision Level)

La fusion au niveau des décisions est souvent utilisée pour sa simplicité. En effet, chaque système fournit une décision binaire sous la forme OUI ou NON que l'on peut représenter par 0 et 1, et le système de fusion de décisions consiste à prendre une décision finale en fonction de cette série de 0 et de 1. Les méthodes les plus utilisées sont des méthodes à base de votes telles que le OR (si un système a décidé 1 alors OUI), le AND (si tous les systèmes ont décidé 1 alors OUI) ou le vote à la majorité (si la majorité des systèmes ont décidé 1 alors OUI). On peut également utiliser des méthodes plus complexes qui pondèrent les décisions de chaque sous-système ou qui utilisent des classifieurs dans l'espace de décisions telles que BKS (Behaviour Knowledge Space). Dans [293], Verlinde présente un grand nombre de méthodes de fusion de décision. Ces méthodes de fusion au niveau des décisions sont très simples mais utilisent très peu d'information (0 ou 1).

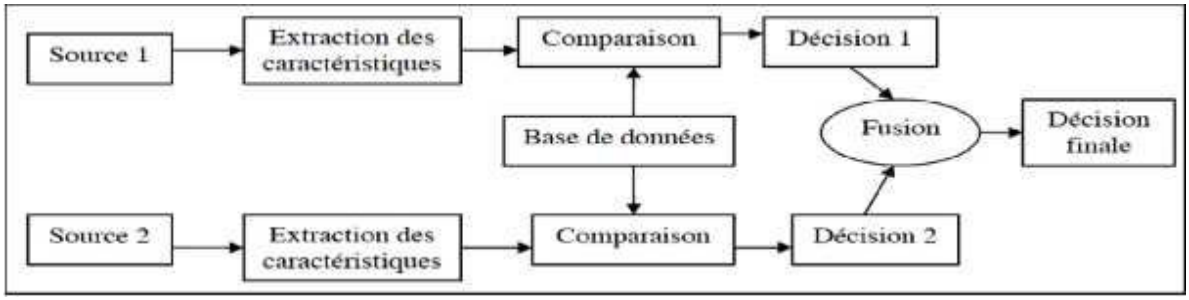

Figure 24 : Schéma de fusion au niveau de la décision.

2) Niveau Score (Score Level)

La fusion au niveau des scores est le type de fusion le plus utilisé car elle peut être appliquée à tous les types de systèmes (contrairement à la fusion pré-classification), dans un espace de dimension limité (un vecteur de scores dont la dimension est égale au nombre de sous-systèmes), avec des méthodes relativement simples et efficaces mais traitant plus d'information que la fusion de décisions. La fusion de scores consiste donc à la classification : OUI ou NON pour la décision finale, d'un vecteur de nombres réels dont la dimension est égale au nombre de sous-systèmes.

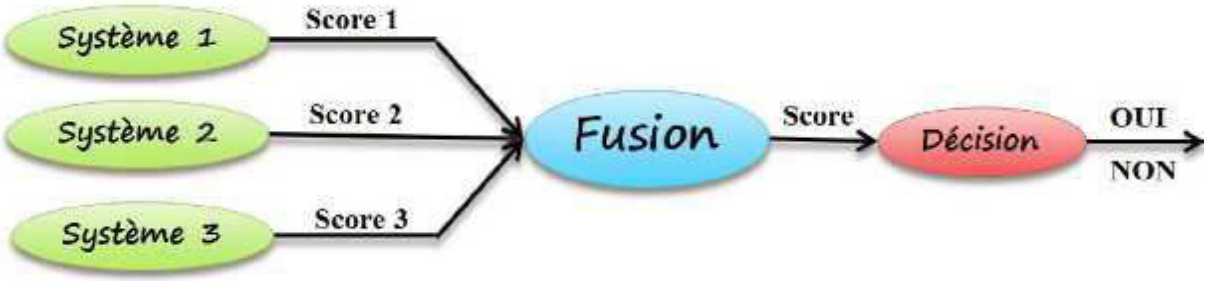

Figure 25 : Schéma de fusion au niveau de scores [19].

2.5 Principe de fonctionnement d'un système biométrique

En matière de fonctionnement, tous les systèmes biométriques fonctionnement comme suit :

1. **Capture des caractéristiques**

Collecte de certaines caractéristiques physiologique, comportementales ou biologiques présentée au moyen d'un terminal de capture biométrique, lequel restitue cette caractéristique sous la forme d'un échantillon biométrique capturé. La qualité du capteur peut grandement influencer les performances du système.

2. Extraction de caractéristiques

Cette phase comprend, en général ; un processus de segmentation visant à localiser l'information de la caractéristique dans l'échantillon biométrique capturé, un processus d'extraction de traits. Seuls les paramètres pertinents sont extraits de l'échantillon biométrique capturé et un processus de contrôle de qualité évalue la validité des échantillons.

3. Comparaison

Compare l'ensemble des caractéristiques extraites avec une ou plusieurs références préalablement stockées et les résultats de comparaison (degrés de correspondance) sont transmis au sous–système de décision. L'identité de l'utilisateur peut correspondre à l'identité recherchée ou pas.

4. Décision

Détermine si l'identité de l'utilisateur correspond ou non à l'identité proclamée (authentification) ou recherchée (identification).L'identification d'une personne est basée sur le degré de similitude entre les caractéristiques extraites et les modèles stockés.

2.6 Performance d'un système biométrique

Les performances d'un système biométrique sont données par la mesure de trois taux d'erreurs :

1. Le taux de faux rejet (''False Reject Rate'' ou FRR) : Ce taux représente le pourcentage d'utilisateurs censés être acceptés mais qui sont rejetées par le système. [10] :

$$TFR = \frac{\textit{nombre des clients rejeté}(FR)}{\textit{nombre total d'accés de clients}}$$

2. Le taux de fausse acceptation (''False Accept Rate'' ou FAR) : Ce taux représente le pourcentage d'utilisateurs censés ne pas être reconnus mais qui sont tout de même acceptées par le système.

$$TFA = \frac{\textit{nombredes imposteurs accepté}(FA)}{\textit{nombre total d'accés imposteurs}}$$

3. Le taux d'égale erreur (''Equal Error Rate'' ou EER) : Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courante. Ce Point correspond à l'endroit ou FRR=FAR, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations.

Un système fonctionnel aura un FRR le plus bas possible. Un système sûre aura un FAR le plus bas possible.

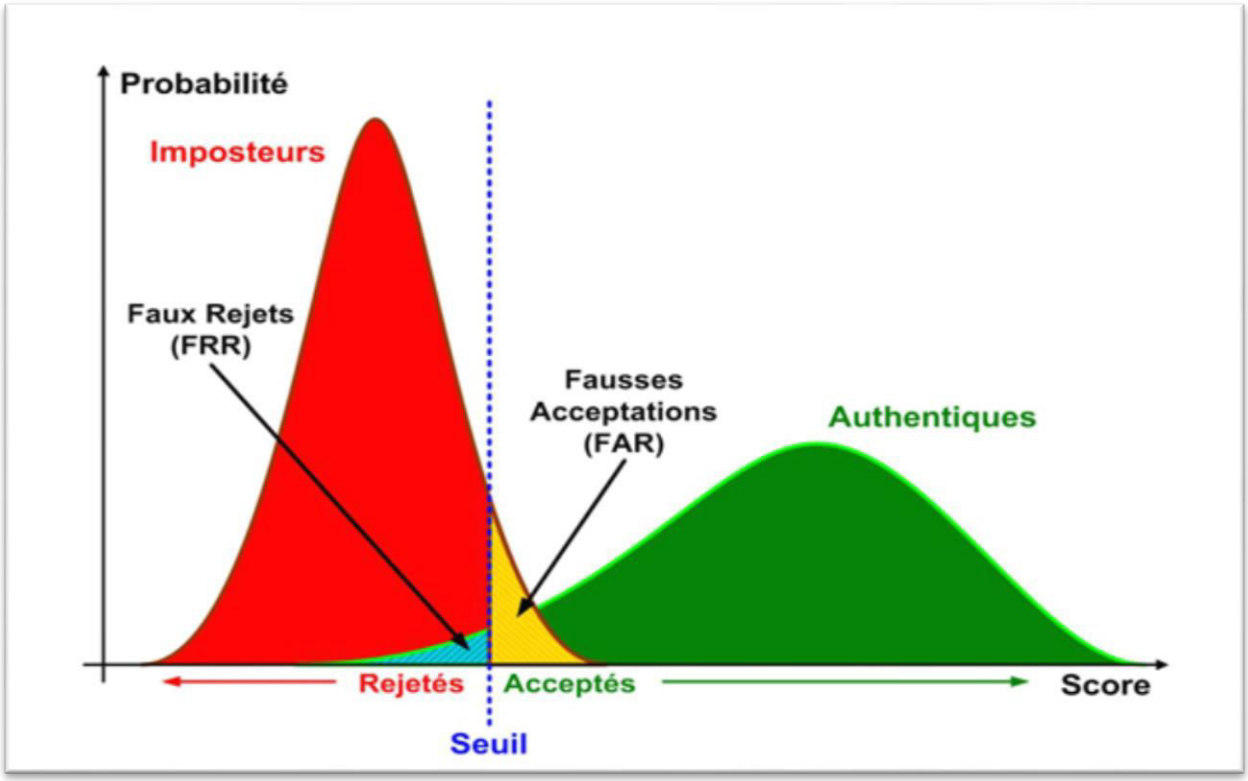

Figure 26 : Illustration du FRR et du FAR. [10]

3. Les avantages et les limites de la biométrie

3.1 Les avantages de la biométrie

La biométrie est une technologie récente et commence à être adoptée par de grands constructeurs de matériel informatique.

L'usage de la biométrie est un complément de l'utilisation des méthodes d'authentification comme des mots de passe, des badges, des cartes à puce.

- Suppression des mots de passe, Suppressions des clés :

Au lieu de retaper son mot de passe dès que le PC se met en veille, une simple pression de l'empreinte digitale sur le capteur
suffit et permet facilement de changer la session d'utilisateur.

- Utilisation d'une signature biométrique:

Grande sécurité, intransmissible à une autre personne.

Une identité vérifiée (Le destinataire est bien la personne autorisée à visualiser ou à utiliser les données).

Lors de transactions financières, il est capital de savoir quel moyen de paiement du consommateur est le plus sûr.

La biométrie offre le chaînon manquant dans la triade du problème de sécurité:

- Diminution de la fraude.
- Rehaussement de l'intégrité des informations et la sécurité.
- Réduction des attaques à l'égard des programmes gouvernementaux.
- Croissance de la confiance envers les systèmes de sécurité.
- Diminution des frais administratifs.
- Accélération des services.

3.2 Les limites de la biométrie:

La biométrie présente malheureusement un certain nombre d'inconvénients parmi eux : le problème de la qualité de l'authentification. Ces méthodes ne sont en effet pas toujours fiables à 100%, ce qui empêche des utilisateurs de bonne foi d'accéder à leur système. Car il s'agit bien là d'une des caractéristiques majeures de tout organisme vivant: on s'adapte à l'environnement, on vieillit, on subit des traumatismes plus ou moins importants, bref on évolue et les mesures changent.

Prenons le cas le plus simple, celui des empreintes digitales (mais la même chose s'applique à toute donnée physique). Suivant les cas, nous présentons plus ou moins de transpiration, la température des doigts n'est pas régulière. Il suffit de se couper pour présenter une anomalie dans le dessin de ses empreintes. Dans la majorité des cas, les mesures du capteur et du logiciel associé retourneront un résultat différent de la mesure initiale de référence. Or, il faut pourtant bien réussir à se faire reconnaître. En pratique, cela sera réalisé dans la plupart des cas car le système est amené à autoriser une marge d'erreur entre la mesure et la référence.

De manière générale, les faiblesses de ces systèmes ne se situent pas au niveau de la particularité physique sur laquelle ils reposent, mais bien sur la façon avec laquelle ils la mesurent, et la marge d'erreur qu'ils autorisent. Là encore, il convient de ne pas se laisser impressionner par une image illusoire de haute technologie - produit miracle.

De plus, les experts techniques mettent au passif de cette technologie, d'une part, son coût, d'autre part, la question de sa révocation. En effet, confronté à une personne qui a subtilisé un mot de passe ou une signature manuscrite, le titulaire du mot de passe ou de la signature peut facilement les remplacer ou les révoquer. La chose semble plus complexe pour une empreinte digitale ou rétinienne. Si un tiers s'approprie une identité biométrique du type empreintes digitales ou identité visuelle, il peut au moyen de ces identités biométriques passer tout type d'actes au nom de la victime. Comment la victime pourrait-elle alors révoquer sa propre empreinte digitale ou identité visuelle ? Les experts en sécurité sont partagés sur la question, même si, en majorité, ils semblent considérer que cette révocation est possible. Tous reconnaissent cependant la difficulté à mettre au passif cette protection technique.

Les données biométriques sont comparables à tout autre système de contrôle d'accès comme des mots de passe, …etc.

Car du point de vue du système informatique, ce ne sont rien d'autres que des séries de bits comme toute donnée. Autrement dit, la difficulté réside dans la contrefaçon de la caractéristique physique et biologique que l'on mesure.

Si la biométrie se généralise dans notre environnement, il est dangereux de penser qu'il s'agit de la réponse à tous les problèmes de sécurité. La biométrie, de par ses limites fonctionnelles, techniques et juridiques n'est en aucun cas synonyme de technologie miracle et de sécurité absolue.

- Les limites fonctionnelles:

Les systèmes d'authentification biométrique représentent une grande partie des limites fonctionnelles. En effet, les systèmes biométriques laissent la place à un certain nombre de faux rejets et de fausses acceptations. Ils ne peuvent à eux seuls garantir à 100% que seules les personnes autorisées pourront passer le contrôle. Ils ne peuvent même pas garantir qu'une personne autorisée ne sera pas rejetée par le système. Il y aura toujours une marge d'erreur à prendre en compte, ce qui n'est pas forcément très rassurant.

- Les limites techniques :

Bien que cela représente un travail assez conséquent, les données biométriques peuvent être imitées, notamment celles qui laissent des traces sur le passage de

l'individu telles que les empreintes digitales. Un individu mal intentionné peut récupérer les empreintes digitales sur un objet tenu par la victime, les imiter et tenter de passer le contrôle biométrique à l'aide de ces empreintes. De plus, les données biométriques sont dans la majeure partie des cas numérisées sur un support, de préférence individuel. Si ce support n'est pas protégé contre les intrusions et le piratage, tout le système biométrique tombe à l'eau.

Conclusion

Dans ce chapitre, nous avons présenté les technologies utilisées dans les systèmes biométriques pour l'identification de personnes. Nous avons aussi donné un aperçu sur les techniques de mesure de leurs performances. Cette étude nous a permis de constater que la reconnaissance de visage suscite de plus en plus l'intérêt de la communauté scientifique, car elle présente plusieurs challenges et verrous technologiques. Enfin, nous avons mis en évidence les différentes difficultés inhérentes à la reconnaissance automatique de visages, ce qui nous a permis de bien définir les problématiques traitées dans ce mémoire. Les techniques utilisées aux différentes étapes de la reconnaissance de visage sont détaillées dans le chapitre suivant.

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

TAB1 : R.P. Wildes, « *A system for automated iris recognition* », Proc. of 2nd IEEE Workshop on Applications of Computer Vision, pp. 121-128, Décembre 1994.

[1] : S. Prabhakar, S. Pankanti, and A. K. Jain. Biometric recognition : Security and privacy concerns. IEEE Security & Privacy, 1 :33–42, 2003. [cite p. 8]

[2] : J. Daugman. Recognizing Persons by Their Iris Patterns. In A. K. Jain, R. Bolle, and S. Pankanti, editors, Biometrics: Personal Identification in a Networked Society, pp. 103-121, Kluwer Academic Publishers, 1999.

[3] : N. Rudin, K. Inman, G. Stolovitzky, and I. Rigoutsos. Biometrics : Personal Identification in Networked Society, chapter DNA Based Identification, pages 287–309. Kluwer Academic Publishers, 2002. [cit´e p. 8]

[4] : International Biometric Group. http ://www.biometricgroup.com/, 2010. [cite p. 11, 15, 154]

[5] : L. O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. In Proceedings of the IEEE, volume 91, pages 2021–2040, 2003. [cite p. 11]

[6] : Fedias Meriem., "Combinaisons de données d'espaces couleurs et de méthodes de vérification d'identité pour l'authentification de visages", Université Mohamed Khi der – Biskra.

[7] : DANG Hoang Vu., "Biométrie pour l'identification", Rapport final, Institut de la Francophonie pour l'Informatique, Hanoï, Vietnam, 07 – 2005.

[8] : Nicolas MORIZET., "Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris", Thèse présentée pour obtenir le grade de Docteur, Ecole Nationale Supérieure des Télécommunications, Paris, 18 Mars 2009.

[9] : R. Brunelli and D. Falavigna. Person identification using multiple cues. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol17, pp.955-966, 1995.

[10] : Moulay Brahim Oussama, Arbaoui Mohamed Ibrahim., "Authentification des personnes par les articulations des doigts", UNIVERSITE KASDI MERBAH OUARGLA, 2015.

Chapitre 2

La reconnaissance faciale & d'empreinte palmaire avec les fractales

Introduction

L'objective de ce chapitre est de donner rapide état de l'art sur les méthodes les plus courantes pour la reconnaissance de visage et d'empreinte palmaire.

Ensuite on va définir une nouvelle méthode de reconnaissance biométrique nommée la dimension fractale qu'on va citer et expliquer son utilité et son principe de fonctionnement.

A. La reconnaissance du visage

1. Définition de la reconnaissance du visage

La reconnaissance de visages est la technique la plus commune et populaire. Elle reste la plus acceptable puisqu'elle correspond à ce que les humains utilisent dans l'interaction visuelle et par rapport aux autres méthodes la reconnaissance du visage s'avère plus avantageuse, d'une part c'est une méthode non intrusive, c'est-à-dire elle n'exige pas la coopération du sujet (en observant les individus à distance), et d'une autre part les capteurs utilisés sont peu coûteux (une simple caméra) contrairement à l'empreinte digitale et l'empreinte palmaire. Parmi les six attributs biométriques considérés par Hietmeyer [11], les caractéristiques faciales marquent un score de compatibilité le plus élevé dans un système MRTD («Machine Readable Travel Documents ») [12] ce score étant basé sur plusieurs facteurs d'évaluation tels que l'enrôlement, le renouvellement des données, les requis matériels et la perception des utilisateurs (Figure 1).

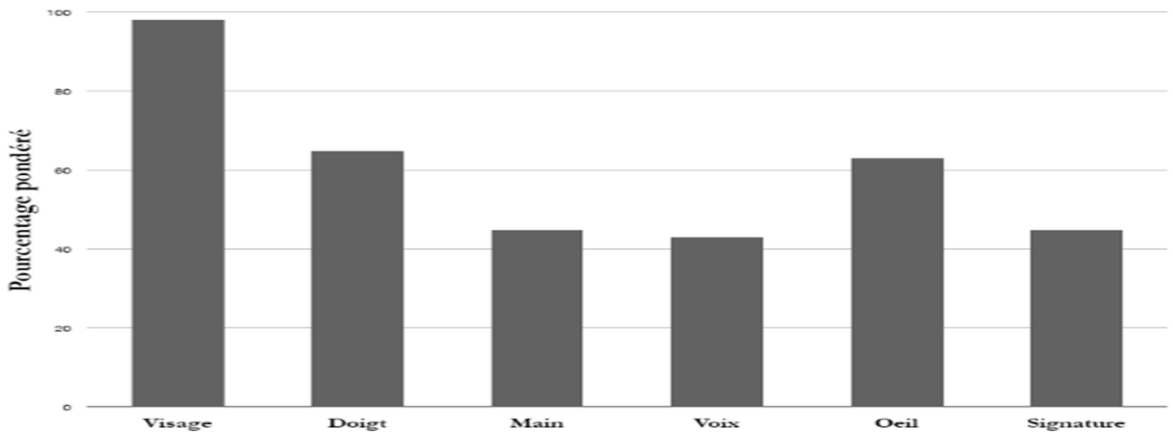

Figure 1 : Scores de compatibilité pour différentes technologies biométriques dans un système MRTD.

2. Processus d'un système de reconnaissance du visage

Tout processus de reconnaissance de visages doit prendre en considération plusieurs facteurs qui contribuent à la complexité de sa tâche, car le visage est une entité dynamique qui change constamment sous l'influence de plusieurs facteurs :

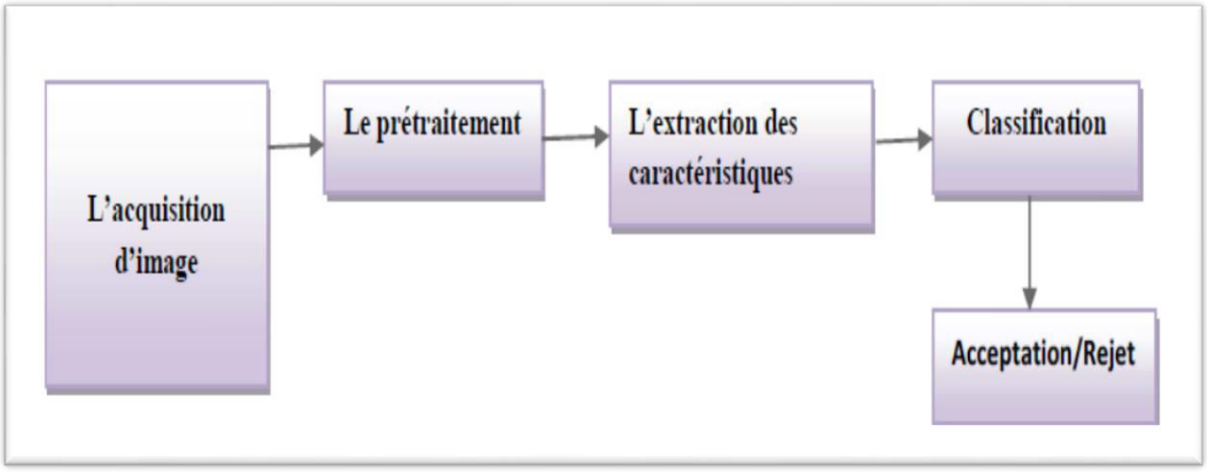

Figure 2 : Processus d'un système de reconnaissance.

2.1 Le Monde physique

Dans le Monde physique, il y'a trois paramètres à considérer : l'éclairage, la variation de posture et l'échelle. La variation de l'un de ces trois paramètres peut conduire à une distance entre deux images du même individu, supérieur à celle séparant deux images de deux individus différents.

L'image d'une personne dans un système de reconnaissance de visages suit les étapes suivantes

2.2 L'Acquisition de l'image

Le Codage consiste en l'acquisition d'image et sa diagonalisation, il comporte un risque de bruit et donne lieu à une représentation 2D (une image niveau de gris) pour un objet 3-D (le visage).

2.3 Les prétraitements

Dans le Prétraitement il faut éliminer le bruit par des techniques de traitement et de restauration d'images et procéder à une détection de visages, cette opération est très complexe, surtout dans le cas où l'image contient plusieurs images ou le cas de l'arrière-plan n'est pas neutre. Cette technique consiste à compenser les dégradations connues ou estimé et rétablir la qualité initiale de l'image.

2.4 L'extraction de paramètres

Il faut extraire de l'image les informations qui seront sauvegardées en mémoire pour être utilisées plus tard dans la phase de décision. Ces informations doivent être discriminantes et non redondantes.

2.5 La classification (Modélisation)

Cette étape consiste à modéliser les paramètres extraits d'un visage ou d'un ensemble de visages d'un individu en se basant sur leurs caractéristiques communes.

2.6 L'apprentissage

L'Apprentissage consiste à mémoriser les représentations calculées dans la phase de L'extraction de paramètres. Elle est en quelque sorte la mémoire du système.

2.7 La décision

La Décision pour estimer la différence entre deux images, il faut introduire une mesure de similarité.

3. Les méthodes utilisées pour la reconnaissance de visage

Les méthodes de reconnaissance de visages peuvent être classées en deux grandes catégories : les méthodes locales et globales [13]. Quelques principales d'entre elles seront présentées dans ce qui suit :

3.1 Les méthodes globales

Les méthodes globales basées sur des techniques d'analyse statistique bien connues. Dans ces méthodes, les images de visage (qui peuvent être vues comme des matrices de valeurs de pixels) sont utilisées comme entrée à l'algorithme de reconnaissance et sont généralement transformées en vecteurs, plus faciles à manipuler. L'avantage principal des

méthodes globales est qu'elles sont relativement rapides à mettre en œuvre. En revanche, elles sont très sensibles aux variations d'éclairement, de pose et d'expression faciale. Les principales méthodes existantes sont comme suit :

3.1.1 L'Analyse en Composante principale(ACP)

L'algorithme ACP appliqué au visage est né des travaux de MA. Türk et AP. Pentland au MIT Media Lab., en 1991 [14]. Il est aussi connu sous le nom de « Eigenfaces » car il utilise des vecteurs propres et des valeurs propres. Sa simplicité à mettre en œuvre contraste avec une forte sensibilité aux changements d'éclairement, de pose et d'expression faciale.

3.1.2 L'Algorithme LDA (Linear Discriminant Analysis)

Appliqué aux images en **1997** par Belhumer et al Yale de la Yale University aux USA, aussi connu sous le nom de Fisherfaces [15]. Contrairement à l'ACP, il permet d'effectuer une véritable séparation de classes.

3.1.3 Les réseaux de neurones

Les réseaux de neurones sont des modèles de calcul qui date des années 40. C'est une technique inspirée des réseaux de neurones biologiques pour exécuter des tâches calculatoires. Elle a la particularité de s'adapter, d'apprendre, de généraliser pour classer les données en entrée [16].

3.1.4 SVM (Machine à vecteurs de support)

Le principe de cette méthode est de trouver le meilleur hyperplan séparant aux mieux les points dans un espace de grande dimension et qui minimise le taux d'erreur total de classification [16].

3.2 Les méthodes locales(Géométrique)

Les méthodes locales consistent à appliquer des transformations en des endroits spécifiques de l'image, le plus souvent autour de points caractéristiques (coins des yeux, de la bouche, le nez,...). Elles nécessitent donc une connaissance à priori sur les images. Ces méthodes sont plus difficiles à mettre en place mais sont plus robustes aux problèmes posés

par les variations d'éclairement, de pose et d'expression faciale [17]. Les principales méthodes existantes sont :

3.2.2 EBGM (Elastic Bunch Graph Matching)

L'algorithme EBGM est né des travaux de Wiskott et al ,1997 [18]. À partir d'une image de visage, on localise des points caractéristiques (coins des yeux, de la bouche, nez,...etc.). Cette localisation peut se faire manuellement ou automatiquement à l'aide d'un algorithme

3.2.3 EingenFace modulaire

Cette méthode possède le même principe que les EigenFaces, mais appliquée à des parties précises du visage comme les yeux. Mais elle rencontre le problème de non précision lors de la localisation des points caractéristiques du visage avant l'application de la méthode.

3.2.4 Méthode de Markov caché

Les HMMs (Hidden Markov Models) sont appliqués à la reconnaissance du visage en considérant l'information du visage comme étant une séquence variable dans le temps [19].

3.3 Les approches hybrides

Plusieurs techniques peuvent parfois s'appliquer afin de résoudre un problème de reconnaissance des formes. Chacune d'entre elles possède évidemment ses points forts et ses points faibles qui, dans la majorité des cas, dépendent des situations (pose, éclairage, expressions faciales,….). Il est par ailleurs possible d'utiliser une combinaison de classificateurs basés sur des techniques variées dans le but d'unir les forces de chacun et ainsi pallier à leurs faiblesses [20].

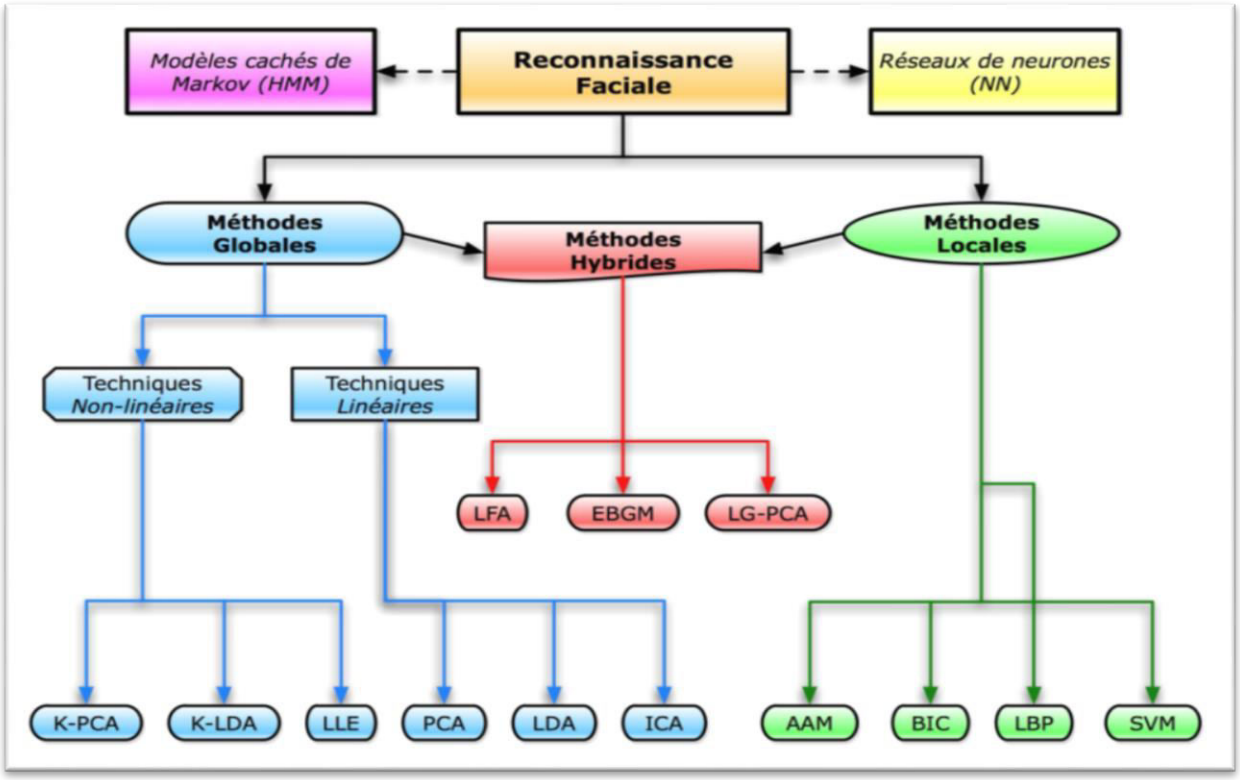

Figure 3 : Une classification des algorithmes principaux utilisés en reconnaissance faciale.

4. Performances d'un système de reconnaissances de visage

La performance d'un système biométrique peut se mesurer principalement à l'aide de trois critères : sa précision, son efficacité (vitesse d'exécution) et le volume de données qui doit être stocké pour chaque utilisateur et ces performances dépendent de plusieurs facteurs qui interviennent à plusieurs niveaux et qui peuvent limiter le degré de précision. Cependant, il serait judicieux de s'intéresser à ces facteurs avant de mesurer la performance d'un système de reconnaissance. Nous citons ici les principaux facteurs :

- L'environnement au moment de l'acquisition.
- Les différentes positions des capteurs.
- La qualité des capteurs.
- La mauvaise interaction entre l'utilisateur et les capteurs.

5. Difficultés de la reconnaissance de visages

Pour le cerveau humain, le processus de la reconnaissance de visages est une tâche visuelle de haut niveau. Bien que les êtres humains puissent détecter et identifier des visages dans une scène sans beaucoup de peine, construire un système automatique qui accomplit de telles tâches représente un sérieux défi. Ce défi est d'autant plus grand lorsque les conditions d'acquisition des images sont très variables. Il existe deux types de variations associées aux images de visages : inter et intra sujet. La variation inter-sujet est limitée à cause de la ressemblance physique entre les individus. Par contre la variation intra-sujet est plus vaste.
Elle peut être attribuée à plusieurs facteurs que nous analysons ci-dessous [21].

5.1 Changement d'illumination

Les variations d'éclairage rendent la tache de reconnaissance de visage très difficile. En effet, le changement d'apparence d'un visage du a l'illumination, se révèle parfois plus critique que la différence physique entre les individus, et peut entrainer une mauvaise classification des images d'entrée.

Figure 4 : Exemple de variation d'éclairage.

5.2 Variation de pose

Le taux de reconnaissance de visage baisse considérablement quand des variations de pose sont présentes dans les images. La variation de pose est considérée comme un problème majeur pour les systèmes de reconnaissance faciale. Quand le visage est de profil dans le plan image (orientation < 30°), il peut être normalisé en détectant au moins deux traits faciaux (passant par les yeux). Cependant, lorsque la rotation est supérieure à 30°, la normalisation géométrique n'est plus possible.

Figure 5: Exemples de variation de poses.

5.3 Les Expressions faciales

La déformation du visage qui est due aux expressions faciales est localisée principalement sur la partie inférieure du visage. L'information faciale se situant dans la partie supérieure du visage reste quasi invariable. Elle est généralement suffisante pour effectuer une identification. Toutefois, étant donné que l'expression faciale modifie l'aspect du visage, elle entraine forcement une diminution du taux de reconnaissance. L'identification de visage avec expression faciale est un problème difficile qui est toujours d'actualité et qui reste non résolu [19].

Figure 6 : Exemples de variation d'expressions.

5.4 Présence ou absence des composants structurels

La présence des composants structurels telle que la barbe, la moustache, ou bien les lunettes peut modifier énormément les caractéristiques faciales telles que la forme, la couleur, ou la taille du visage. De plus, ces composants peuvent cacher les caractéristiques faciales de base causant ainsi une défaillance du système de reconnaissance.

5.5 Les vrais jumeaux

Qui ont le même indicatif d'ADN, peuvent tromper les personnes qui ne les connaissent pas(les personnes familiers avec les jumeaux ont reçu une grande quantité d'information sur ces derniers et sont donc beaucoup plus qualifies à distinguer les jumeaux.). Il est peu probable que la vérification automatique de visage, ne pourra jamais détecter les différences très subtiles qui existent entre les jumeaux.

B. La reconnaissance de l'empreinte palmaire

1. Définition de l'empreinte palmaire

La reconnaissance d'empreintes palmaires est une méthode d'authentification biométrique basée sur les motifs uniques de diverses caractéristiques dans la paume des mains. Les systèmes de reconnaissance d'empreinte Palmaire utilisent un dispositif de numérisation ou une application basée sur une caméra, ainsi qu'un logiciel associé qui traite les données d'image d'une photographie de la paume d'un individu et la compare à un enregistrement stocké pour cette personne. Les empreintes de paume sont homologues aux empreintes digitales, y compris des détails similaires. Comme dans le cas de la numérisation d'empreintes digitales, les scanners à paume utilisent des méthodes optiques, thermiques ou tactiles pour faire ressortir les détails du relief des zones surélevées (appelées crêtes) et des branches (bifurcations) dans une image d'une paume humaine avec d'autres détails y compris les cicatrices, les plis et la texture. Ces trois méthodes reposent respectivement sur l'analyse de la lumière visible, l'analyse des émissions de chaleur et l'analyse de la pression. Palm scanners peuvent exiger que les individus touchent leurs mains à un écran ou sans contact.[22]

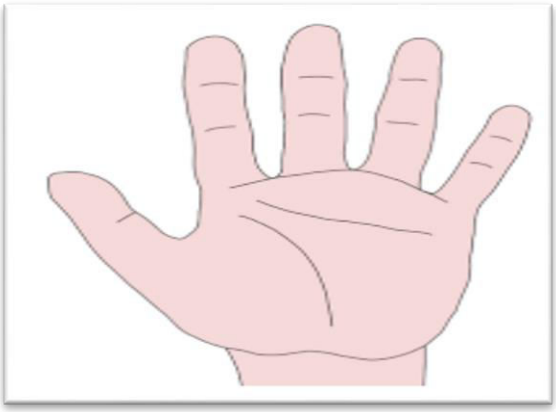

Figure 7 : Paume de la main.

2. Caractéristiques du système de reconnaissance de l'empreinte palmaire

Introduite par David Zhang et Shu (chercheurs et professeurs à l'université polytechnique de Hong Kong), depuis **1996** pour remédier aux problèmes liés à la non visibilité d'une empreinte digitale ou bien le coût élevé des appareils de capture des images de l'iris et de la rétine ou encore les faibles taux de reconnaissance des autres modalités biométriques, l'empreinte palmaire ou « Palmprint » est cette surface très large et interne de la main, elle contient plusieurs traits caractéristiques tels que les lignes principales, les plis et les textures [22].

Grace à cette large surface et l'abondance des traits caractéristiques, on prévoit que les Palmprint soient très robustes aux bruits et uniques à chaque individu.

Comparé aux autres caractéristiques physiques, l'identification par les empreintes palmaires (palmprint) à plusieurs avantages [23] :

- Traitement d'image à basse résolution.
- Peu de risque d'intrusion.
- Les traits des lignes sont stables.
- Taux élevé d'acceptation par les utilisateurs.

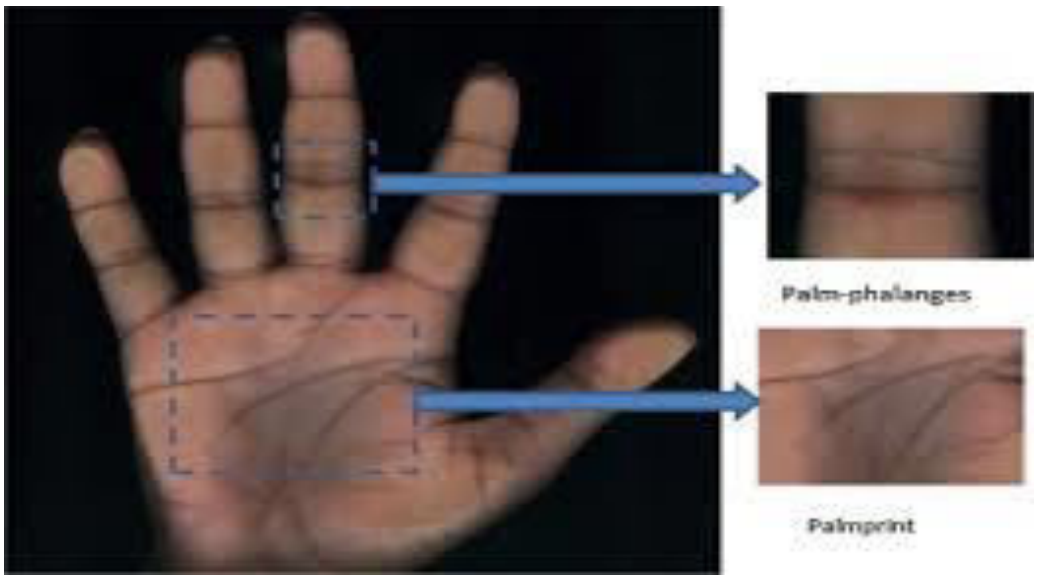

Figure 8 : Régions de la paume de la main.

Une empreinte palmaire est composée (d'après [22,23,24] de :

- **Les lignes principales:** la ligne de cœur, la ligne de vie et la ligne de tête.

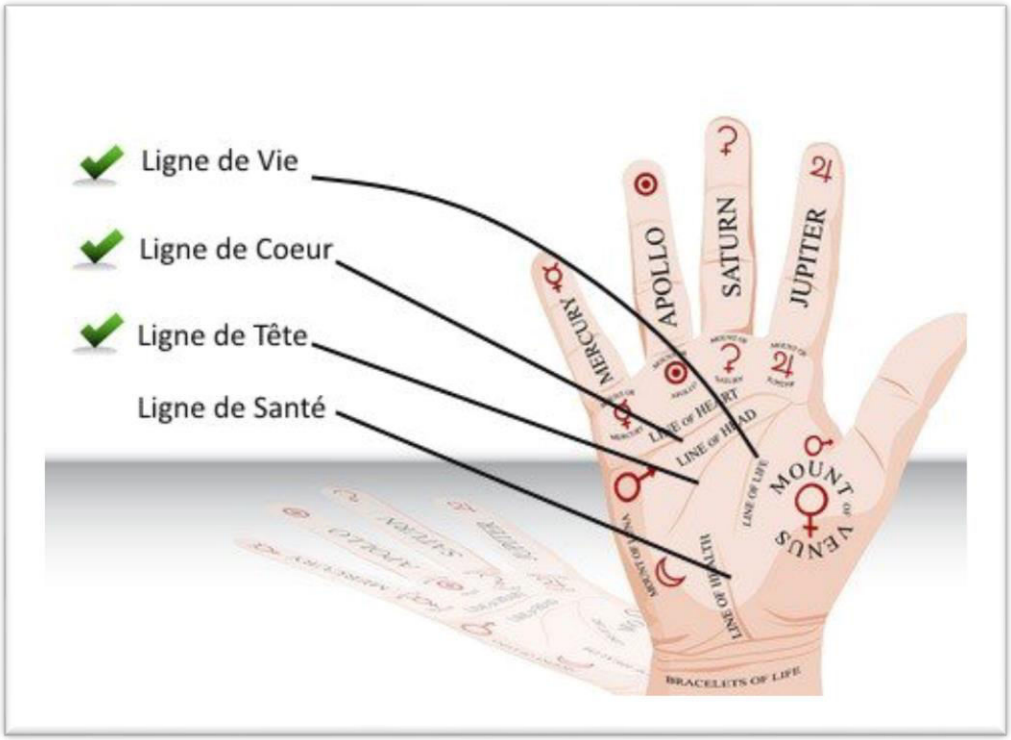

Figure 9: Lignes principales de la paume de la main.

- **Les régions:** doigt-racine (I), région intérieure (II) et région extérieure (III).

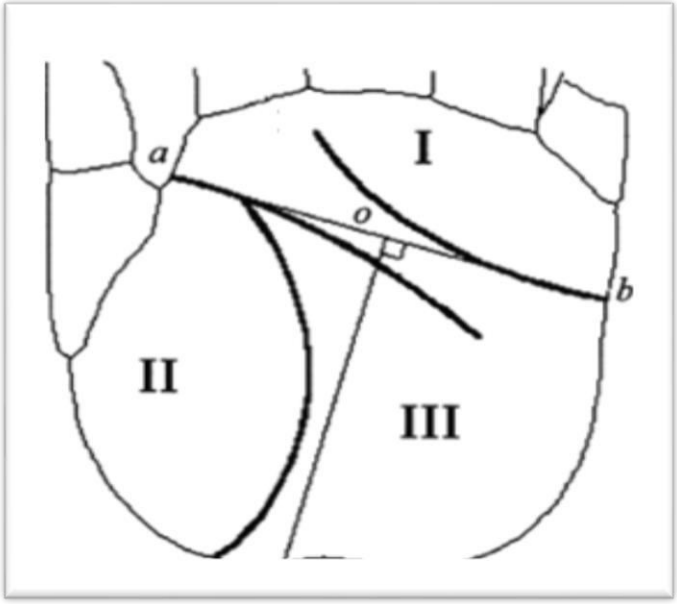

Figure 10 : Régions d'une empreinte palmaire: (**I-**Région de racine de doigt, **II-** Région de l'intérieur et **III-**Région de l'extérieur) et points de référence (**a**,**b**: Point final, **o**: leur point médian)

- **Les points de référence:** points d'extrémité à travers la paume et leur point médian. Ce sont les points a et b dans la Figure 11.
- **Caractéristiques géométriques:** la largeur de la paume, la longueur de la paume et la zone de la paume. Comme le montre la figure 11.

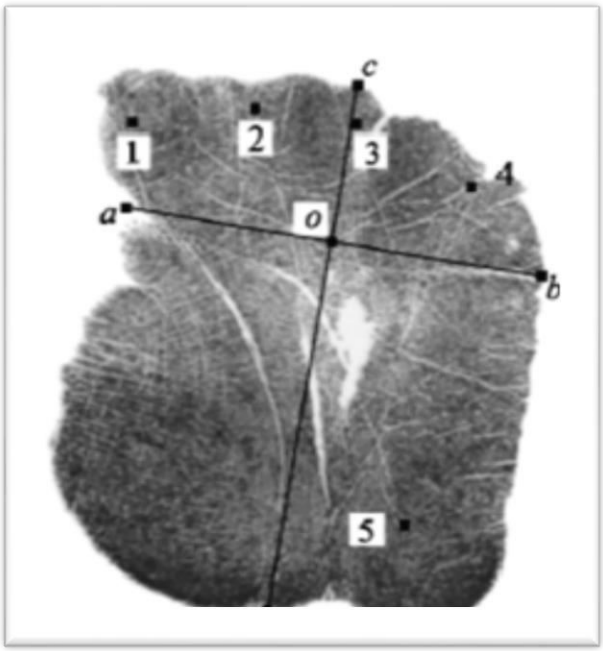

Figure 11 : Caractéristiques géométriques et points delta d'une empreinte palmaire, où (c, d) est la médiatrice du segment (a, b) et les points de 1 à 5 sont des points delta.

- **Caractéristiques de rides:** ces lignes autres que les lignes principales. Ils ont tendance à être plus minces et plus irréguliers. Elles sont classifie comme les rides grossières et les rides fines.

- **Caractéristiques du point Delta:** celles-ci sont définies comme le centre d'une région de type delta dans l'empreinte de la paume. (voir figure 10).

- **Les caractéristiques minuties:** Qui sont similaires à l'empreinte digitale type de fonctionnalités.

  En général, les entités géométriques, les entités de ligne principale et caractéristiques de rides peuvent être déterminées par une image technique de traitement de l'image.

  Détermination du point de référence: pour localiser les extrémités de chaque ligne principale.

3. Le processus de la reconnaissance d'empreinte palmaire

Semblable à la majorité des systèmes de reconnaissance biométriques, Le processus de la reconnaissance d'empreinte palmaire comporte quatre (4) étapes essentielles [25,31] :

- **L'acquisition d'image :** Consiste à capturer l'image de la paume de la main. Il existe deux méthodes distinctes d'acquisition de l'empreinte palmaire: Hors ligne et En ligne :

  Hors-ligne : L'identification par les palmprints peut être divisée en deux catégories, en ligne et hors ligne. Les recherches sur l'identification hors ligne par les palmprints ont été le centre d'intérêt principal durant les dernières années où tous les échantillons de palmprints étaient ancrés sur papier, ensuite transmis à l'ordinateur par un scanner numérique (voir figure 11). Due à la haute résolution relative aux images hors ligne des palmprints (plus de 500 dpi), quelques techniques utilisées pour les empreintes digitales peuvent être utiles pour l'identification hors ligne des palmprints où les lignes et les points de données ou points singuliers peuvent être extraits [26].

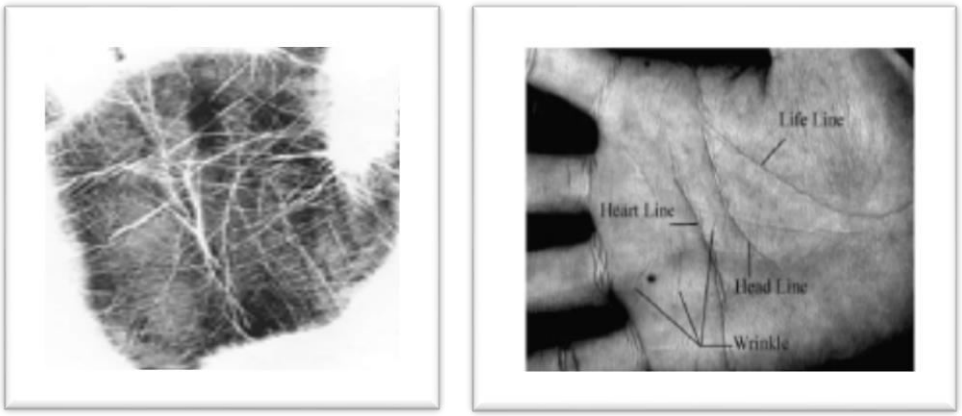

Figure 12 : Image hors ligne et en ligne de palmprint.

En ligne : Pour l'identification en ligne des palmprints, les échantillons d'images sont directement obtenus par un appareil de capture de palmprint. Il est évident que l'identification en ligne par les palmprints est beaucoup plus appropriée pour les applications en temps réel, c'est pour cela que notre intérêt c'est porté sur ce type d'identification [26].

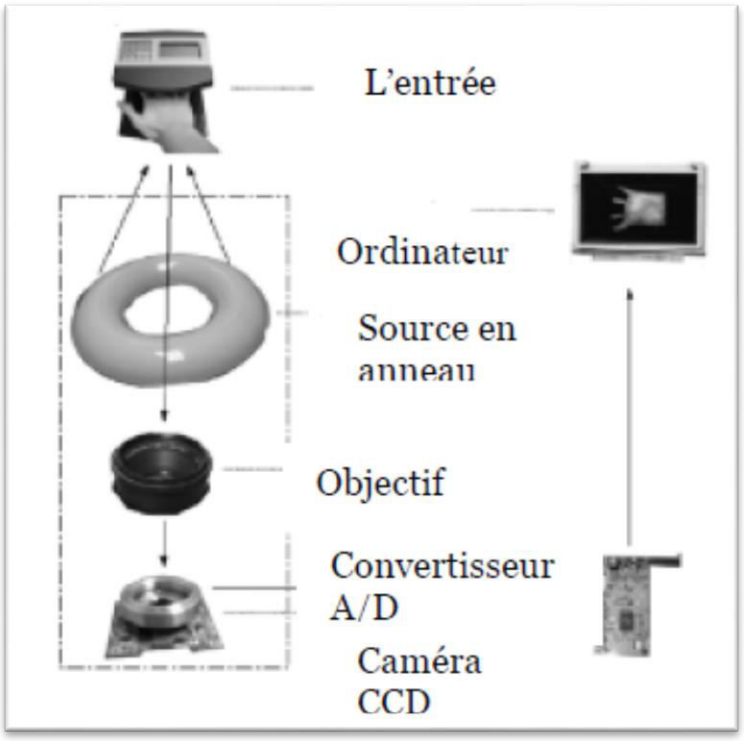

Figure 13 : Dispositif de capture de palmprints en ligne.

- **Le prétraitement :** Où un système de coordonnées est établi afin d'aligner l'image et segmenter la partie nécessaire appelée région d'intérêt pour en extraire les caractéristiques de l'empreinte palmaire acquis au cours de l'étape précédente [28].

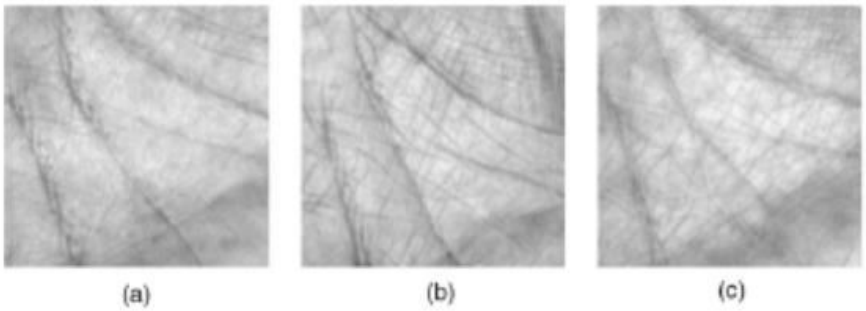

Figure 14 : Régions d'intérêts extraits d'une image palmprint.

- **L'extraction des caractéristiques :** L'extraction des caractéristiques est définie par un processus de conversion d'une image d'empreinte palmaire

capturée et prétraitée en une unique, distinctive et compacte forme de telle sorte qu'on puisse la comparer avec un enregistrement de référence [27,30].

- **La classification :** Qui va comparer cet ensemble de caractéristiques extraites dans l'étape précédente avec des enregistrements de références existants dans la base de données spécifique et ainsi trouver la classe à laquelle appartient cette image [29].

C. La reconnaissance biométrique avec la dimension fractale

1. Les fractales

En mathématiques, une fractale est un objet abstrait utilisé pour décrire et simuler des objets naturels, que la nature reproduit sans cesse au fil de l'évolution, ils sont dans nos poumons nos reins, nos vaisseaux sanguins, dans les fleurs, les plantes, les mouvements climatiques le rythme cardiaque, la vie cellulaire. [31]

Le concept de géométrie fractale, introduit par B.B. Mandelbrot, fournit en effet un cadre solide pour l'analyse des phénomènes naturels dans divers secteurs des sciences.

La notion de fractale en fait regroupe dans un cadre géométrique unique de nombreux travaux mathématiques antérieurs. Les objets concernés ont été inventés dès la fin du XIXe siècle par des mathématiciens comme Cantor, Peano ... Le terme «fractal» a été introduit par B.B. Mandelbrot (fractal, c'est à-dire qui a été fractionné à l'infini, du latin « fractus » dérivé du verbe «frangere», briser) [32].

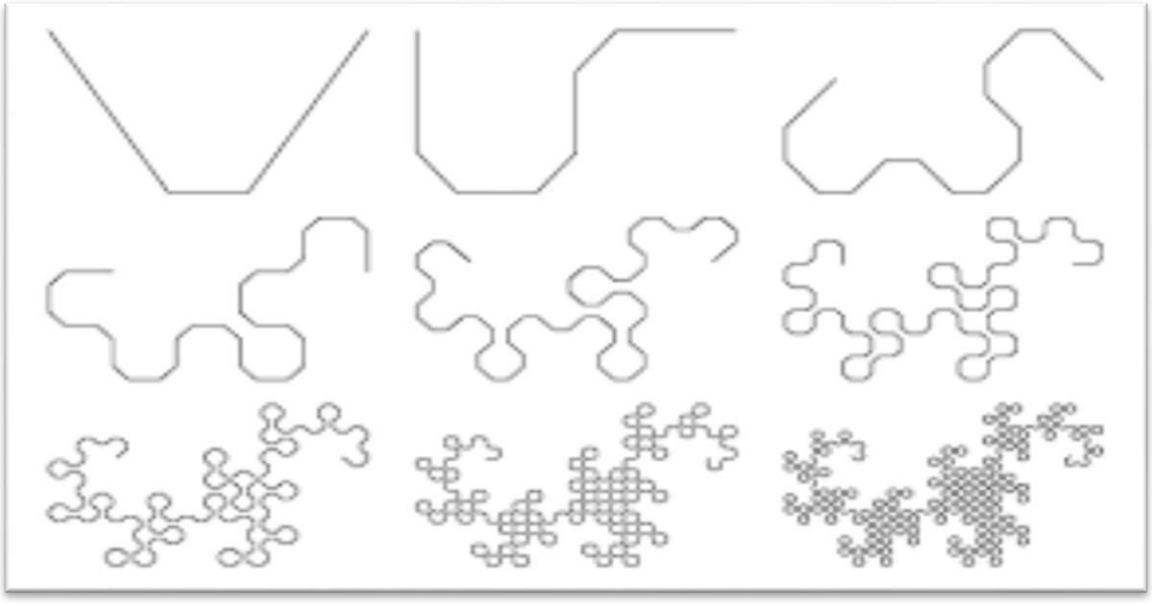

Figure 15 : Quelques schémas fractals.

2. Définition d'un objet fractale

Un fractal est un objet tel que chacun des morceaux reproduit en plus petit la structure du tout [33].

Une définition à la fois précise et générale d'un objet fractal est difficile, nous le définirons avec Mandelbrot comme un ensemble qui présente des irrégularités à toutes les échelles. C'est fondamentalement son caractère de concept géométrique qui en fait sa portée. La géométrie fractale est le complément qui manquait à la géométrie euclidienne : comme l'a fait remarquer Mandelbrot, les nuages ne sont pas des sphères, les montagnes des cônes, ni les îles des cercles et leur description nécessite une géométrisation adaptée. La notion de géométrie fractale est étroitement liée aux propriétés d'invariance par changement d'échelle : une structure fractale est la même « de près comme de loin » [34].

3. Caractéristiques d'un objet fractale

Un objet fractal possède au moins l'une des caractéristiques suivantes [35]:

- **irrégulier à toutes les échelles :** Un objet est irrégulier à toutes les échelles si, même en le regardant de plus en plus près (par exemple avec un zoom), il apparaît toujours irrégulier (non lisse) (figure 16). Les courbes différentiables n'ont pas cette propriété. Si on regarde de plus en plus près une courbe différentiable, au bout de quelques agrandissements, la portion de la courbe regardée a l'allure d'une droite (en fait, elle finit par se confondre avec sa tangente près du point regardé).

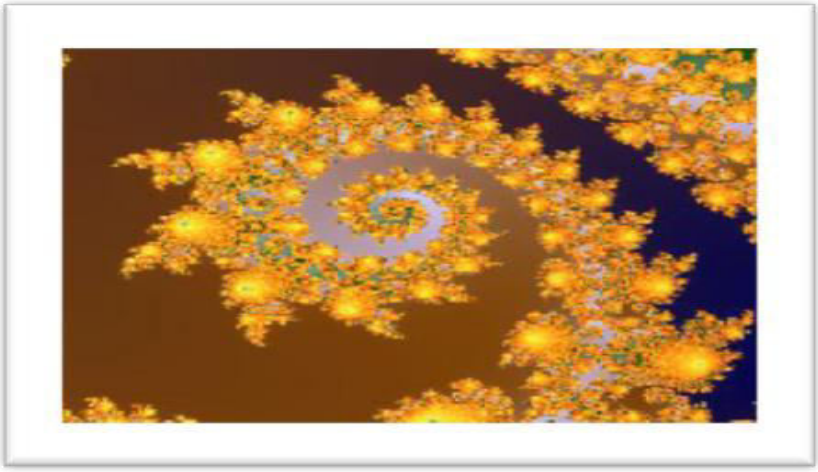

Figure 16 : image de synthèse représentant l'irrégularité d'un objet fractal

- **auto-similaire :** La géométrie fractale est basée sur la reproduction d'un même motif de plus en plus petit. En faisant un zoom sur un objet, on observe toujours exactement la même structure, quelle que soit l'échelle à laquelle on se trouve (figure17). On appelle cette propriété : l'auto-similarité.

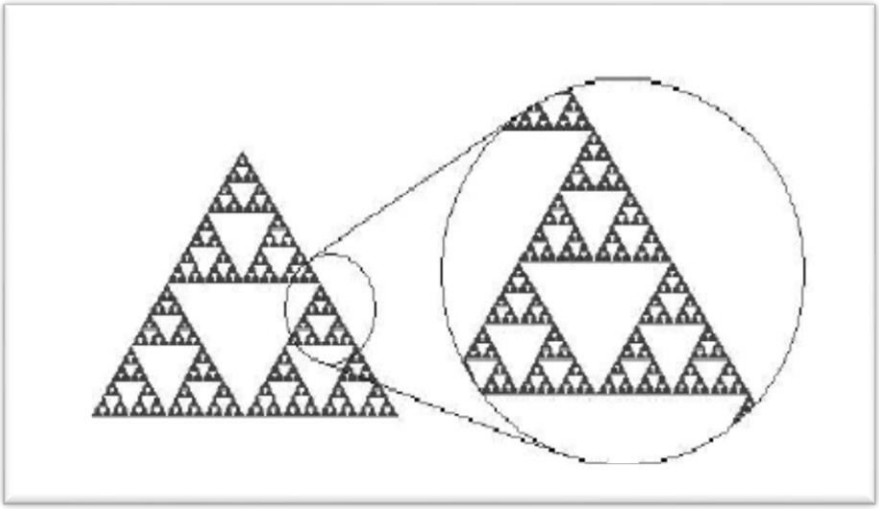

Figure 17 : objet fractal représentant l'auto similitude a différents échelles.

4. Classification des objets fractales

Nous pouvons distinguer 2 catégories de fractales, les fractales déterministes et les fractales non déterministes.

4.1. Fractales déterministes

Les fractales déterministes sont des figures géométriques de structure complexe dont la création ou la forme met en jeu des règles utilisant le fractionnement. Les courbes suivantes sont construites géométriquement ou avec des méthodes numériques. [37].

- **Ensemble de Cantor**

L'ensemble de Cantor (figure18) a été publié en 1883.

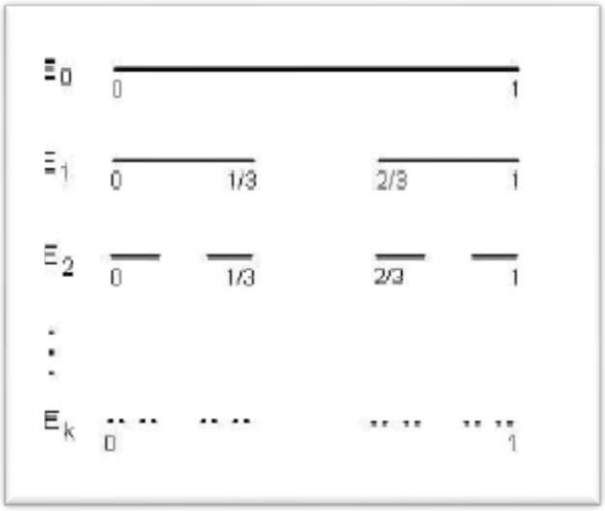

Figure 18: Ensemble de Cantor

Nous pouvons le construire en partant d'un segment [0 ; 1] dont nous enlèverons le tiers central. Ensuite, dans chacun des tiers restants, nous enlèverons son propre tiers central, et ainsi de suite jusqu'à l'infini [39].

- **Courbe de Von Koch**

La courbe de Von Koch (voir figure 19) ainsi que le flocon de Von Koch (figure 20) ont été publié en 1904.

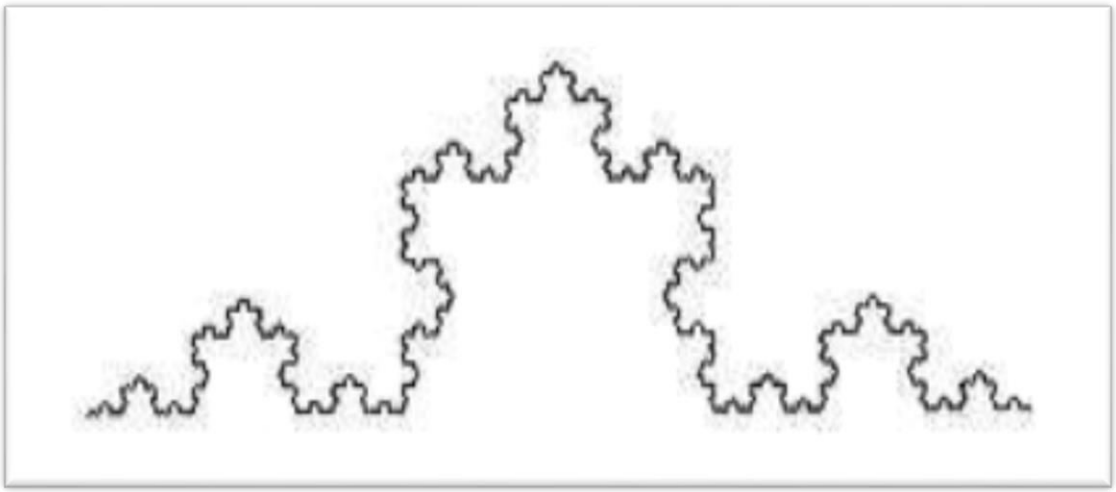

Figure 19: Courbe de Von Koch

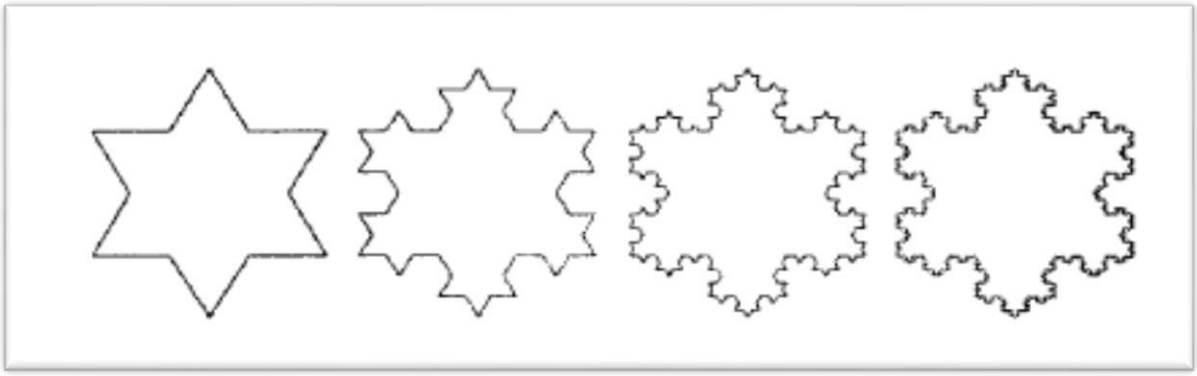

Figure 20: Flocon de Von Koch

A partir d'un segment de longueur un, nous remplaçons le tiers central par deux segments de même longueur que celui-ci. Au bout de cette première étape, nous obtenons une nouvelle figure. Nous pouvons itérer ce procédé infiniment en subdivisant chaque fois les segments en trois parties dont la partie centrale est remplacée par deux segments de même longueur qu'elle. Cette courbe est auto similaire et donc fractale car elle reste identique à elle-même quand nous la dilatons avec un grossissement égal à une puissance de trois [38].

- **Tamis de Sierpinski**

Le tamis de Sierpinski (voir figure 21) a été publié en 1915.

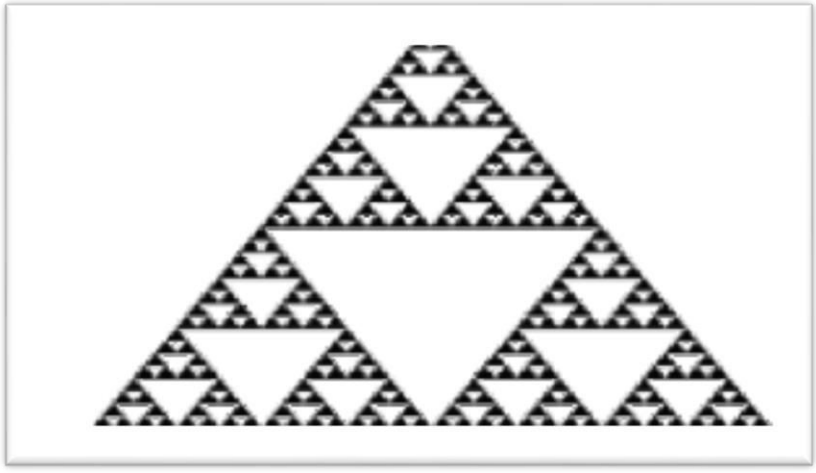

Figure 21: Triangle de Sierpinskien

Cet ensemble fractal utilise comme figure de départ un triangle équilatéral. En utilisant les milieux de ses côtés, nous définissons ainsi un nouveau triangle central que l'on enlève au triangle initial. En itérant ce procédé une infinité de fois, on obtient ainsi le triangle (ou fanion) de Sierpinski [38].

4.2. Fractales non déterministes

La nature fait bien les choses !

Par opposition aux fractales déterministes, il existe des fractales liées au hasard ou à des phénomènes aléatoires [40].

Les choux fleurs, les arbres, les nuages, les éclairs électriques, les montagnes, les poumons et les vaisseaux sanguins sont des fractales naturelles. Ces dernières sont tous les éléments et les phénomènes de la nature qui présentent des propriétés fractales. Cette catégorie regroupe donc les fractales qui se rapprochent le plus de notre quotidien [39].

Donnons à présent quelques exemples avec des figures.

- **La fougère**

La fougère (voir figure 22 et figure 23) possède un caractère fractal évident. Elle permet de démontrer que les fractales naturelles n'ont pas une complexité infinie (ici, la complexité se termine aux plus petites feuilles des plus petites branches) et que la propriété d'auto similitude, dans la nature, n'existe qu'avec une certaine approximation. (Bonhomme et al, 2008) [41].

Figure 22: la fougère

Figure 23: la fougère après grossissement.

- **Les vaisseaux sanguins**

Le réseau vasculaire est une organisation fractale, un labyrinthe complexe de bifurcations identiques entre elles sur des échelles de plus en plus petites (figure 24 et figure 25). Il apparaît ainsi un motif géométrique qui se répète sur des échelles différentes, il y a donc bien auto-similarité. Quelle que soit l'échelle à laquelle nous regardons cette structure, l'aspect paraît identique [42].

Figure 24 : réseau sanguin

Figure 25: réseau sanguin après grossissement

5. La dimension fractale

Nous savons tous qu'un point est une figure de dimension 0, qu'une ligne droite est un objet de dimension 1; qu'une surface plane est un objet de dimension 2; qu'un volume est de dimension 3... Mais qu'en est-il d'un objet fractal?

La dimension fractale est avant tout un paramètre permettant de quantifier la complexité d'un signal ou d'une image. Elle est un nombre réel quelconque. Pour déterminer la dimension fractale d'un objet il faut compter le nombre moyen de motifs répétés contenus dans une sphère de rayon k centrée en un point donné de l'objet. Ce nombre de motifs est donné par n = (k^d) et la dimension fractale est ainsi égale à : d= ln(n) / ln(k).

De façon intuitive, la dimension fractale indique un certain degré d'occupation de l'espace physique par une forme fragmentée, ramifiée, tortueuse (Lopes, 2009). Elle décrit la complexité d'une forme. Elle caractérise aussi le comportement auto-similaire d'une surface. Cette caractéristique n'est généralement pas acquise par les surfaces naturelles, mais elle est respectée en moyenne par les textures. Pour toutes ces raisons, la dimension fractale est dans la plus part des cas utilisée pour caractériser une texture (Nailon, 2010).

En fait, la dimension d'une fractale n'est pas entière. C'est d'ailleurs là-dessus que se base Benoît Mandelbrot pour définir une fractale. Un ensemble pour lequel la dimension de Hausdorff (ou dimension fractale) dépasse la dimension topologique. Mais cette définition

exclut des ensembles que certains considèrent comme des fractales. Aussi Sans entrer dans les détails, on peut penser qu'un objet bizarre comme la courbe de Koch, qui a une longueur infinie tout en ne remplissant qu'une région très limitée du plan, doit avoir des propriétés très particulières. En fait on peut démontrer que sa dimension est égale à log4/log3 (1.26). Presque tous les objets fractals ont des dimensions non entières. En résumé, une fractale peut donc être de dimension 0.63 c'est à dire à mi-chemin entre un point et une ligne (figure1.3), ou encore 1.26, entre une ligne et une surface (figure1.4). Par exemple, une ligne très contorsionnée (qui n'est pas forcément une fractale) se rapproche plus d'une surface que d'une ligne.

6. Méthodes de calcul de dimension fractale

L'attribut dimension fractale peut être exprimé par des relations d'échelles entre les structures géométriques et l'échelle d'analyse de ces structures. Plusieurs techniques de calcul de la dimension fractale sont proposées dans la littérature [43,44]. Lopes et Betrouni les ont classées en trois grandes approches.

- Approche basée sur le comptage des boites.
- Approches basée sur la mesure des surfaces.
- Approches basée sur le Mouvement Brownien Fractionnaire(FBM). (Harrouni et Guessoum2005).

Bien qu'elles soient toutes différentes, un principe de base est toujours respecté, il est résumé par les 3 étapes suivantes:

- Mesurer les quantités représentées par l'objet en utilisant différentes mesures.
- Tracer le logarithme des quantités mesurées en fonction du logarithme des tailles et approximer cette droite par régression linéaire.
- Estimer la **DF** comme étant la pente de la droite obtenue. (Guilmard, 2002)

6.1. Méthodes de comptage de boites

Ce sont les premières méthodes apparus et elles sont également les plus utilisées. Pour

chaque méthode l'algorithme consiste à subdiviser l'image en boites juxtaposées de côté ε puis calculer la dimension des boites qui est donnée par la relation suivante :

$$\text{Dim } F = \frac{\text{Log } N(\varepsilon)}{\text{Log } (1/\varepsilon)} \quad (1.2)$$

Ou F représente l'objet et N(ε) représente le nombre minimum de carrés recouvrant l'objet.

La dimension fractale n'est rien d'autre que la dimension des boites donnée par cette relation (1.2) (Zehani et al, 2011).

a. Comptage de boites « Box Counting»

Cette méthode a été proposée par Russel et all en 1980 c'est la plus utilisé et la plus simple elle est performante pour des images auto-similaires et n'est valable que pour des images noir et blanc (Russel et al, 1980).

Son principe est de recouvrir le signal par des boites de taille *r (*figure 26) et calculer la dimension fractales qui est donnée par :

$$\text{Dim } F = \lim_{r \to 0} \frac{\text{Log } N(r)}{\text{Log } r} \quad (1.3)$$

Ou N(r) représente le nombre de boites recouvrant complètement le signal.

Nous avons appliqué cet algorithme pour la courbe de Von Koch et on a trouvé une valeur proche de la valeur théorique '1.252'

Cette méthode présente cependant plusieurs limitations, du fait qu'elle nécessite l'utilisation d'une image binaire. Elle est sensible à la taille des boites.

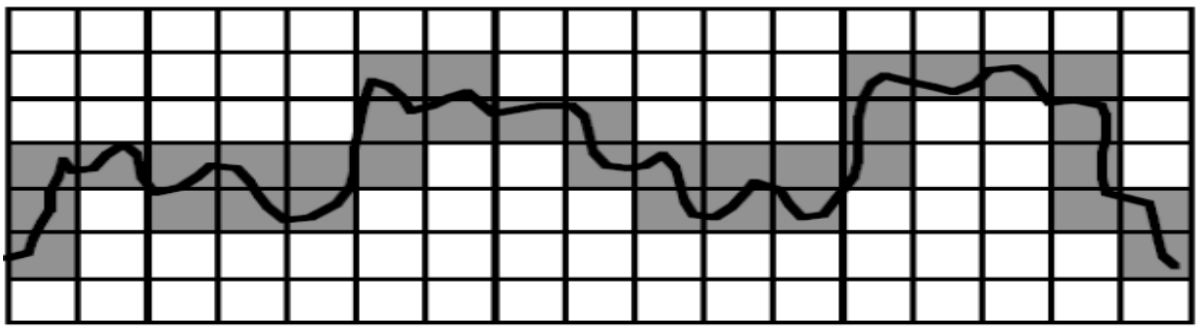

Figure 26: mesure de la dimension fractale d'une courbe par la méthode des boites.

b. Comptage différentiel de boites

Cette méthode a été proposée par Sarkar et Chaudhuri en 1992 dans le but de surmonter la contrainte rencontrée par la méthode de comptage de boites classique (Sarkar et Chaudhuri, 1992). Il y a eu plusieurs modifications de cette méthode par la suite (Sun et al.2006),(Cheng .1999),(Du ,Yeo. 2002),(Lee,Hsieh.2010).

Algorithme :

- L'image initiale est découpée en une image m x m
- L'image m x m est alors découpée en cellule s x s
- Le rapport d'homothétie est alors k = m / s
- On discrétise les niveaux de gris du même facteur d'homothétie que la dimension de l'image k = NG / s'
- On obtient des boites de s x s x s'empilées en trois dimensions (figure 27)
- Pour une colonne de boites (i,j) on regarde dans quelle boite indicée k se situe le niveaux max.
- Idem pour min dans la boite l
- On calculi $n(i,j) = l - k+1$
- On calcule Nr = Somme des nr(i,j)
- On dénombre le nombre de cellule n contenant une portion de contour.

d = log(n) / log(k)

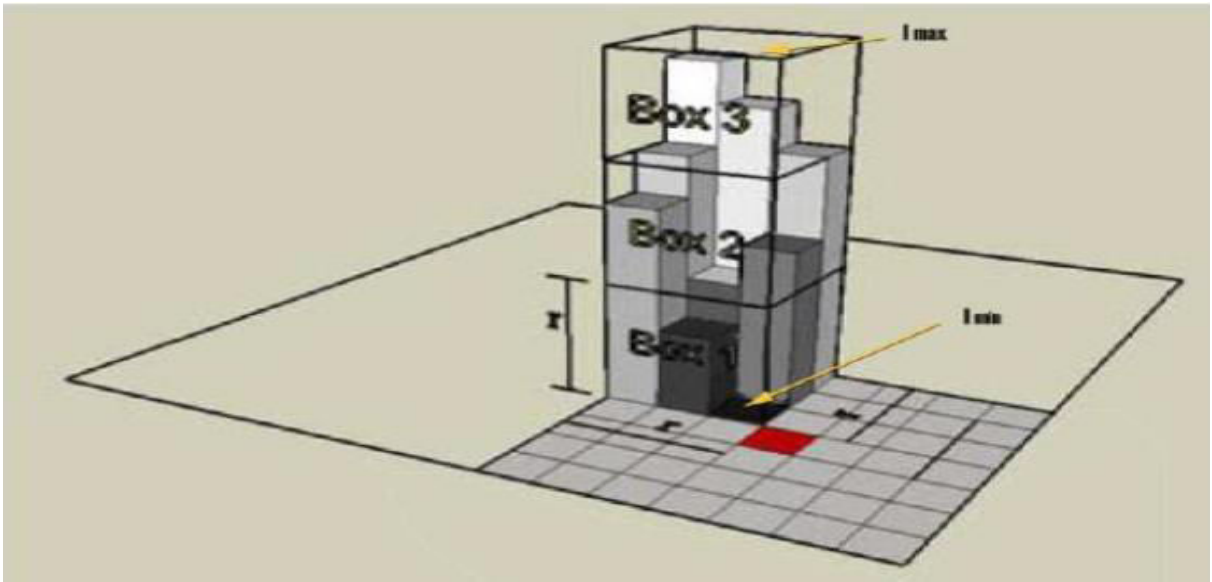

Figure 27:méthode comptage différentiel de boites

6.2. Méthodes de mesure d'air

Les méthodes dites de « mesure d'aire » utilisent des éléments structurants (triangle, carré, cercle..) et des opérations morphologiques (érosion, dilatation, …) à différentes échelles *r* et calculent l'aire *A(r)* de la surface étudiée à cette échelle. La DF est obtenue par régression linéaire de la pente de la courbe du logarithme de *A(r)* en fonction du logarithme de *r*. dans cette classe de méthodes, trois algorithmes sont les plus utilisés :

a. Méthodes des prismes triangulaires

La méthode de prisme triangulaire a été introduite par Clarke en 1986 (Clarcke, 1986) de la façon suivante :

Dans une image en niveau de gris, représentée dans un espace (O, X, Y, Z), chaque quatre pixels adjacents du plan (O,X,Y) constituent un carré (fenêtre d'analyse). Soit *abcd* ce carré de côté s et de centre *e*. l'idée est alors de calculer la surface du prisme triangulaire de chaque fenêtre d'analyse de taille *s*, puis de calculer la surface *As* qui correspond au total des surfaces de tous les prismes triangulaires obtenus.

La procédure se répète pour différentes tailles *s*, et la pente *p* de la droite de régression de l'ensemble de points (log s, log As) est calculée pour déterminer la dimension fractale D de l'image suivant l'équation : D= (2-P).

Un prisme triangulaire est obtenu en reliant les quatre niveaux de gris A, B, C, D ayant respectivement les positions a,b,c,d (angle de la fenêtre d'analyse) avec la valeur moyenne E correspondante (E est affectée à la position *e* du centre du carré). Sa surface représente la somme des surfaces des quatre triangles DEA, AEB, BEC, et CED qui le forment (figure 28).

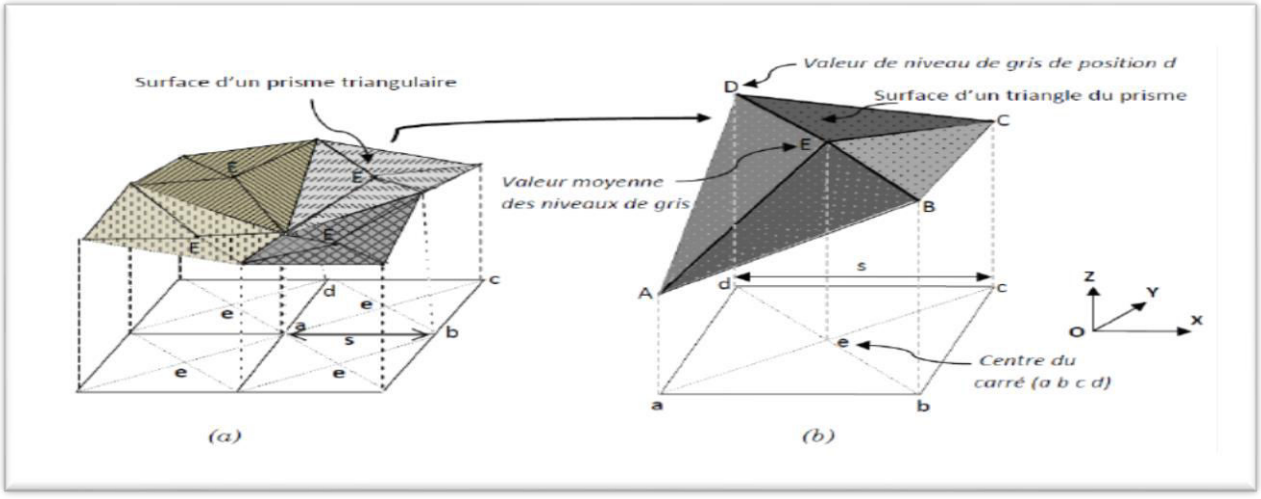

Figure 28 : méthode des prismes triangulaires

b. Méthodes de recouvrement des blancs

Le but de cette méthode est de calculer l'aire de la surface des niveaux de gris et ainsi d'estimer la DF de la surface 3D (Peleg et al 1984).

On considère tous les points dans un espace 3D (la troisième dimension étant le niveau de gris) séparés par une distance E, et une surface est recouverte donc avec un élément structurant d'épaisseur 2E. Cette couverture est déterminée par deux surfaces, l'une dite maximale obtenue par dilatation et l'autre minimale obtenue par érosion.

- **Avantages**

Si l'image avait ses niveaux de gris inversés, la DF estimée ne changerait pas.

- **Inconvénients**

Cette méthode donne de bonnes estimations seulement lorsque la valeur théorique de la DF est relativement faible (Asvestas et al, 1999).Le résultat de la DF dépend fortement du bruit dans l'image (Renaud, 2009).

Conclusion

Dans ce chapitre, nous avons expliqué les deux modalités qu'on va étudier dans notre mémoire, la reconnaissance de visage et l'empreinte palmaire.

Dans la première partie, Nous avons déterminé les techniques les plus populaires utilisées en reconnaissance du visage. Ces méthodes peuvent être classées en trois catégories :

1- Les méthodes globales : pour lesquelles les caractéristiques sont extraites directement de l'image du visage en entier.

2- Les méthodes locales : basées sur l'extraction de trait locaux du visage, tel que les yeux, le nez ou la bouche.

3- Les méthodes hybrides : fusion entre les deux premières méthodes.

Nous détaillerons plus tard le processus de reconnaissance de visage, le principe de fonctionnement d'un système de reconnaissance faciale, Enfin, nous motterons en évidence les différentes difficultés inhérentes à la reconnaissance de visages.

Dans la deuxième partie, Nous avons défini l'empreinte palmaire, ces caractéristiques biométriques et les types de reconnaissance, aussi nous avons déterminé le processus de reconnaissance palmaire.

Dans la dernière partie, Nous avons défini la nouvelle méthode nommée la dimension fractale qu'on va présenter sa définition, d'où elle est créée et comment l'utiliser dans notre projet de fin d'étude.

Nous détaillerons plus tard dans la conception, le processus de reconnaissance de visage et palmaire en utilisant les fractales avec leurs dimensions.

Chapitre 3

Conception

Introduction

Ce chapitre présente la partie la plus importante de cette étude. Le but de ce projet est de construire un système de vérification multimodale basé sur la fusion d'empreinte palmaire et du visage. La technique utilisée pour la reconnaissance des empreintes palmaires est la même pour la reconnaissance faciale, la méthode des dimensions fractales a été utilisée. Pour fusionner les deux sous-systèmes, le niveau score a été retenu.

Les parties suivantes présenteront les détails techniques de ce projet.

1. Le sous-système de reconnaissance faciale

La reconnaissance faciale est basée sur la méthode des dimensions fractales qui est détaillée dans les rubriques suivantes :

1.2 Méthode de Box Counting (Comptage des boites)

La notion de longueur « exacte » des éléments n'existe pas car ces derniers sont trop irréguliers. Ce qui a poussé **B. Mandelbrot** (1975) à introduire une nouvelle dimension qu'il nomme « dimension fractale », qui permettra de mesurer cette irrégularité.

On obtient le nombre de cases couvrant la trajectoire pour tous les niveaux de raffinement. C'est la boucle principale où le programme itère sur tous les niveaux de raffinement et, en attendant, de recueillir combien de boîtes sont nécessaires pour couvrir la trajectoire en fonction de l'indice de raffinement N pour $N_{min} \leq N \leq N_{max}$. Dans la boucle, le programme commence avec une grille de $[2N_{min} \times 2N_{min}]$ et se termine par une grille de $[2N_{max} \times 2N_{max}]$ cases, à chaque étape de raffinement augmenter le nombre de boîtes par un facteur de quatre. À chaque niveau de résolution croissante, le programme repose sur les routines 'get num' recouvrant les boîtes avec des boîtes () ou obtenir des boîtes de recouvrement num () pour effectuer le réel boîte-comptage. Les résultats du comptage des boîtes sont stockés dans les cases vectorielles, qui sont utilisées plus tard dans l'extraction réelle de l'estimation de la dimension fractale.

1.3 Procédure et implémentation de la méthode

Après la phase de prétraitement qui est due à la l'application d'un filtre gaussien qui suit la binarisation de l'image du visage, (voir figure 1 & 2)

Figure 1 : Image du visage à traiter

Figure 2 : Image du visage après filtrage gaussien

- Application d'une boucle 'For' sur la hauteur et la largeur de l'image.
- Pour chaque pixel, vérifier si ce dernier est 'Noir' c'est-à-dire qu'il à la valeur 0, ou 'Blanc' c'est-à-dire qu'il à la valeur 1.
- Si le pixel est Noir, on passe au pixel suivant, sinon (dans le cas où le pixel est Blanc) on compte la valeur initialisée par '0' et on incrémente d'une valeur « i=1 » et ainsi de suite jusqu'à la fin de la boucle.
- Après avoir eu le nombre total des blocs blancs, on applique la formule qui calcule la dimension fractale.

La formule de la dimension fractale est comme suit :

$$DimF = \frac{\text{Log } N(b)}{\text{Log } (r)}$$

Où : N(b) : représente le nombre des pixels blancs recouvrant l'objet.

r : représente le nombre dès la taille de l'image. (dans notre cas, la taille est 512).

- La dimension fractale est donc calculée, le résultat est un nombre réel qui définit le vecteur caractéristique de l'image.

2. Le sous-système de reconnaissance de l'empreinte palmaire

Semblable à la reconnaissance faciale en terme de calcul du vecteur caractéristique, ce dernier qui est calculé par la méthode de la dimension fractale, mais la seule différence concentre sur l'étape de prétraitement.

2.1 Traitement de l'empreinte palmaire

Après l'acquisition de l'image de l'empreinte palmaire, On doit trouver lés régions principales de la paume de la main, nommés les régions d'intérêt, ensuite extraire ces régions pour détecter les lignes principales en utilisant un filtre Sobel.

Figure 3 : Image d'une empreinte capturée.

Figure 4 : Région d'intérêt extraite d'une empreinte palmaire.

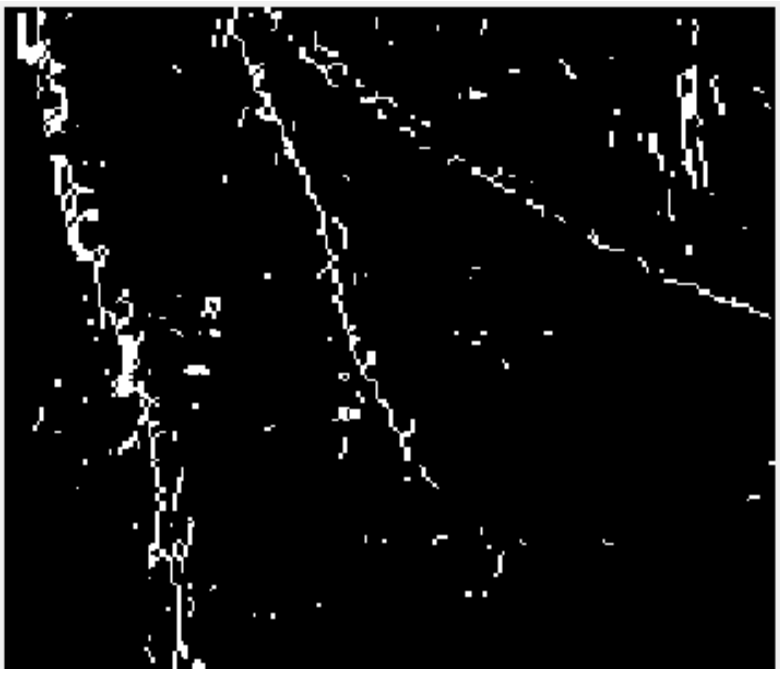

Figure 5 : Contour de la région d'intérêt.

2.2 La classification

La comparaison d'une empreinte palmaire avec une base d'empreintes consiste à réaliser l'accord entre une image d'empreinte provenant d'un enregistrement sur une fiche et une empreinte latente en utilisant les régions d'intérêt.

Le système de vérification d'identité est basé sur la comparaison de deux ensembles de régions, correspondants respectivement à deux paumes de la main à comparer.

Le système est donc capable de donner un indice de similitude ou de correspondance en utilisant la distance euclidienne entre l'image de test et les images d'apprentissage qui se trouvent dans la base de données.

3. La reconnaissance multimodale basée sur la fusion d'empreinte palmaire et du visage

Ajouter une modalité à un système biométrique, c'est ajouter une nouvelle source d'information. C'est pourquoi les systèmes multimodaux permettent d'obtenir de meilleurs résultats que les systèmes mono modaux correspondants. Ajouter des modalités permet également d'augmenter l'universalité du système.

Nous allons maintenant nous intéresser aux méthodes de fusion de scores. Les méthodes de fusion de scores combinent les informations au niveau des scores issus des modules de comparaison comme indiqué sur la **figure 6**.

Un système de fusion est constitué de deux modules, un module de fusion et un module de décision (voir **figure 7**). Le problème devient donc un problème de classification à 2 classes (OUI ou NON), Client ou Imposteur) à partir d'un vecteur de nombre réels dont la dimension est égale au nombre de sous-systèmes du système multi-algorithmes.

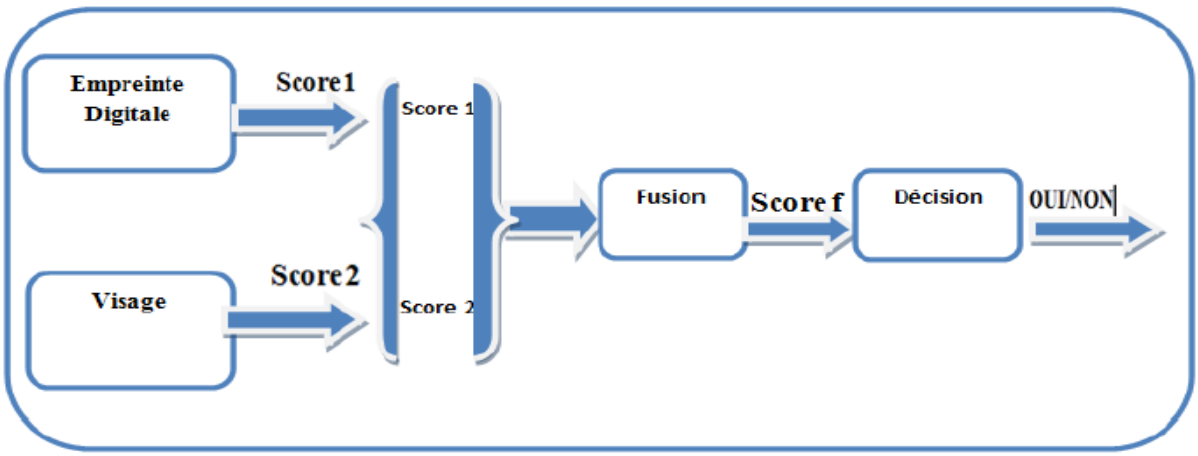

Figure 6 : Schéma de la fusion de scores.

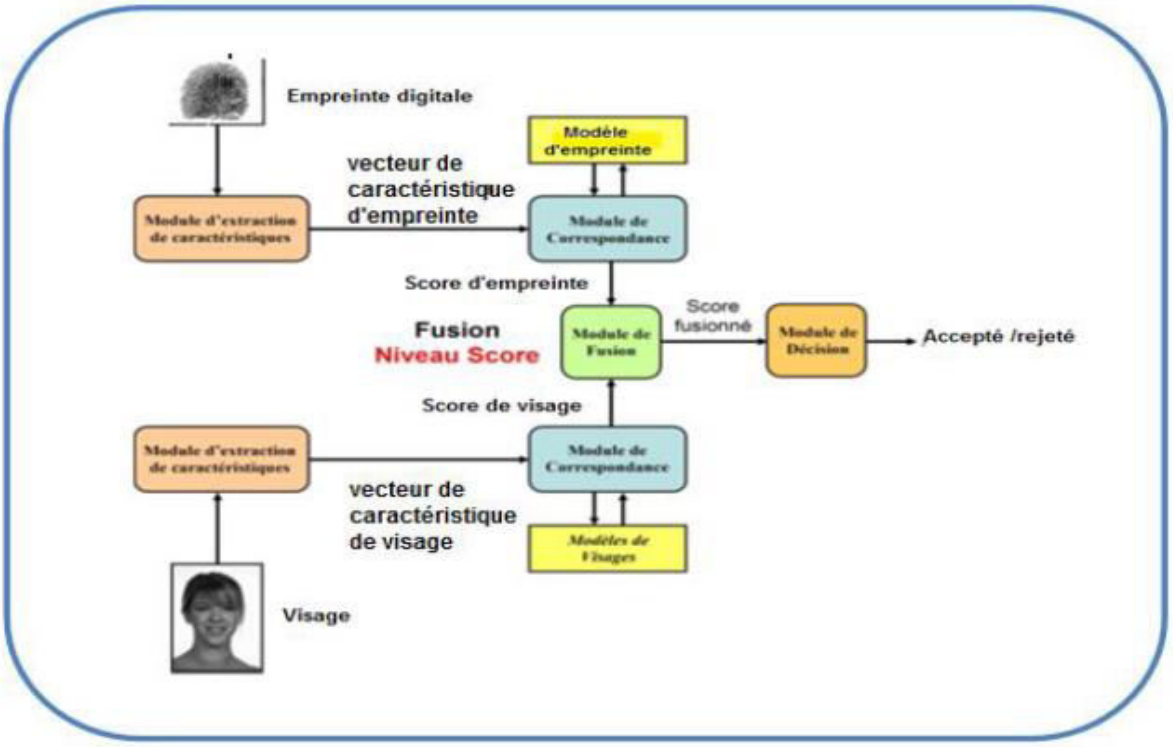

Figure 7 : Fusion au niveau score dans notre système biométrique multimodal.

Cette méthode est la plus utilisée car elle peut être appliquée à tous les types de systèmes, qu'ils sont un ensemble de sous-systèmes produisent après l'étape de comparaison. Les scores individuels sont combinés de manière à former un unique score, qui est ensuite utilisé pour prendre la décision finale. La fusion au niveau de score est appliquée par plusieurs méthodes, dans ce cas en utilise la règle de la somme pondérée.

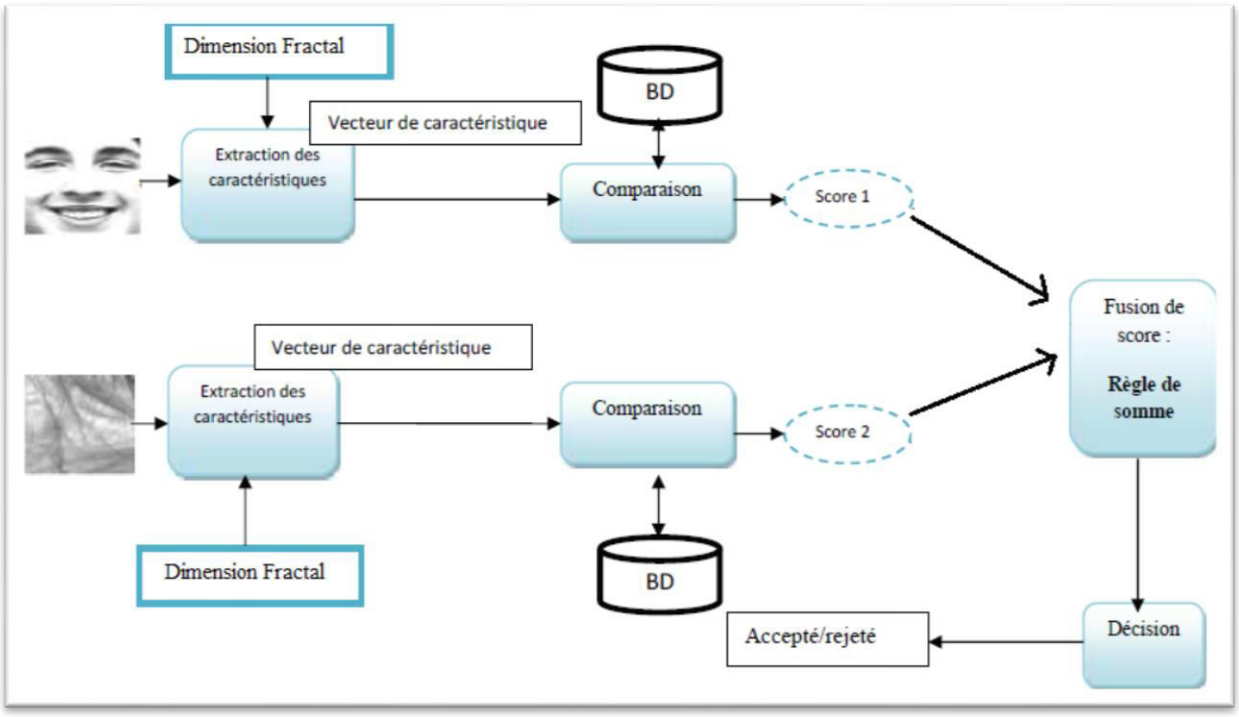

Figure 8 : Architecture de système multimodale au niveau des scores.

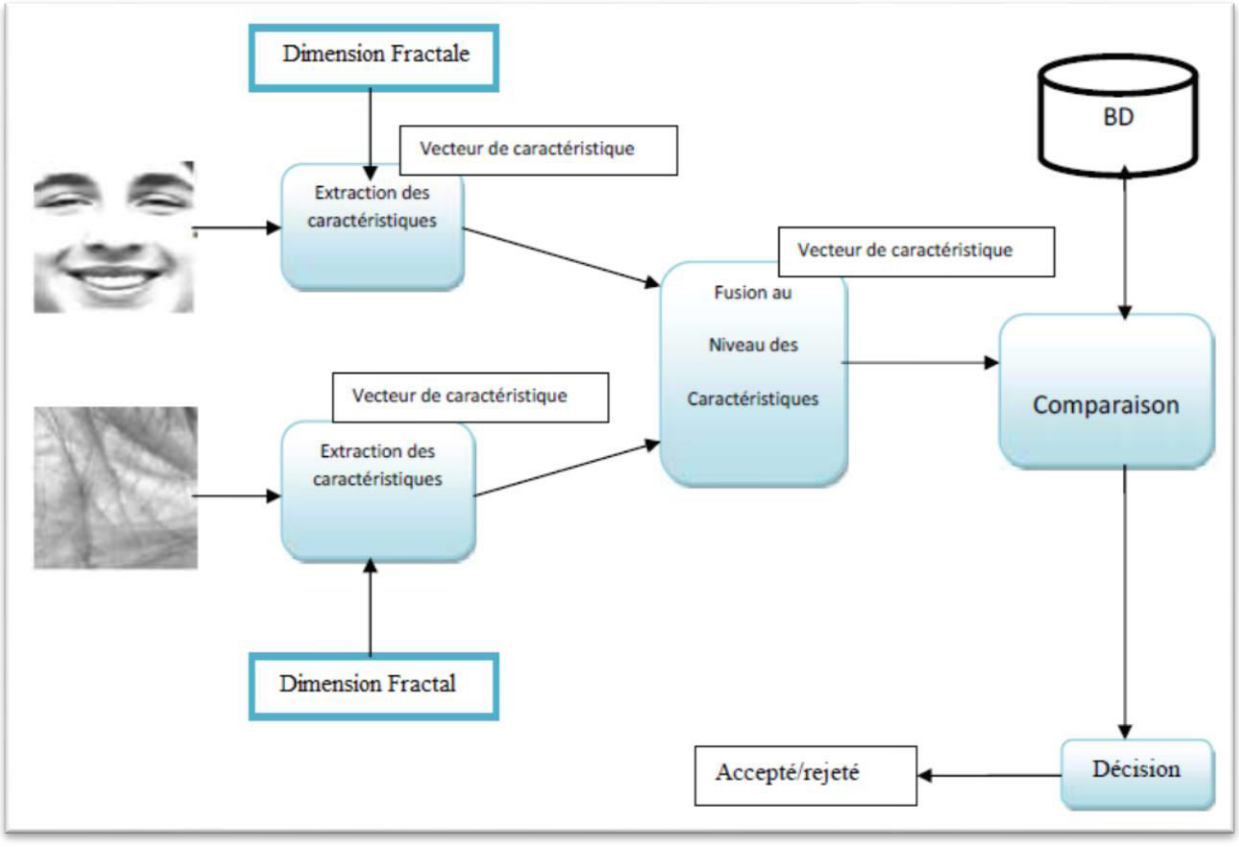

Figure 9 : Architecture de système multimodale au des caractéristiques.

Conclusion

Dans ce chapitre nous avons donné une représentation générale sur la méthode de la dimension fractale qu'on a utilisée dans ce projet.

Le processus des systèmes de reconnaissances est divisé en 3 étapes :

1- L'extraction de caractéristiques : pour obtenir les caractéristiques de chaque image acquise, en forme de vecteur, on doit calculer la dimension fractale de cette image puis on enregistre le vecteur formé pour passer à la prochaine étape de la classification.

2- La comparaison : cette étape se fait en calculant la mesure de similarité entre les vecteurs de caractéristiques enregistrées dans la base de données et les vecteurs de tests, qui sont calculées, par la distance euclidienne.

3- La fusion : la fusion de ces deux modalités a été utilisée dans plusieurs niveaux (au niveau des caractéristiques et au niveau des scores.).

Dans le chapitre suivant, on va implémenter cette nouvelle méthode pour distinguer l'efficacité de notre système puis constater ses résultats.

Introduction

Après avoir détaillé les différentes méthodes et approches utilisés pour modéliser notre système, on parlera dans ce chapitre de l'environnement de développement choisi pour implémenter l'ensemble des opérations et méthodes composant le processus de système de reconnaissance d'empreintes palmaire et de visage.

Ce système est réalisé sur la base de données AT&T (pour le visage) et CASIA-MS-PalmprintV1 (pour l'empreinte palmaire).

Afin d'évaluer l'efficacité de la méthode étudiée et les performances de notre système biométrique multimodale proposé, qui contient trois étapes reconnaissance d'empreinte palmaire, reconnaissance de visage et la fusion de ces deux modalités.

1. Les bases de données

1.1 Base de données uni-modale

- **Visage :**
  - **La base AT&T :** La base de données de visages AT&T (anciennement nommée ORL Database of Faces) a été développée dans le cadre d'un projet de reconnaissance de visages au sein du centre SVRG (Speech, Vision and Robotics Group) de l'Université de Cambridge. La base AT&T contient des images de visage (format PGM en niveau de gris) de 40 personnes, avec 10 images pour chacun (en total 400 images). Pour la plupart des sujets, les images ont été prises avec des variations différentes de l'apparence du visage : les expressions faciales (les yeux ouverts/fermés, souriant/pas souriant), les poses de tête et les détails du visage (avec ou sans lunette). Les images prises n'ont pas en commun les mêmes types de variation pour les différentes personnes de la base. En revanche, elles ont en commun la taille (512x 512) et le fond. Ces images sont organisées dans 40 répertoires (un pour chaque individu) nommé : s1, . . ., s40. Dans chacun de ces répertoires, il y a dix images de visage différentes pour chaque individu numéroté de 1 à 10. Un extrait de cette base est donné dans la figure 1.
    Cette base est téléchargeable via le lien suivant :
    « **http://www.cl.cam.ac.uk/research/dtg/attarchive/pub/data/att_faces.zip** »

Figure 1 : Extrait de la base AT&T.

- **Empreinte palmaire :**
  - **La base CASIA-MS-PalmprintV1 :** CASIA Multi-Spectral Palmprint Image Database V1.0 (ou CASIA-MS-PalmprintV1) est Publié afin de promouvoir la recherche et le progrès sur l'imagerie spectrale multiple de biométriques Modalités. CASIA Multi-Spectral Palmprint Image Database contient 5 502 images de palmaire capturées à partir de 312 sujets. Pour chaque sujet, nous recueillons des images de palmaire à partir des paumes de la main. Toutes les images de palmaire sont des fichiers JPEG au format gris de 8 bits grâce à notre dispositif de reconnaissance de palmaire (voir la figure 2). Dans notre travaille on prend seulement 40 personnes avec 8 images pour chacun (un total de 320 images). Ces images sont organisées dans 40 répertoires (un pour chaque individu) nommé : 1, . . ., 40. Dans chacun de ces répertoires, il y a 8 images de palm différentes pour chaque individu numéroté de 1 à 8.

    Cette base est téléchargeable via le lien suivant :

    « http://biometrics.idealtest.org/downloadDB.do?id=5 »

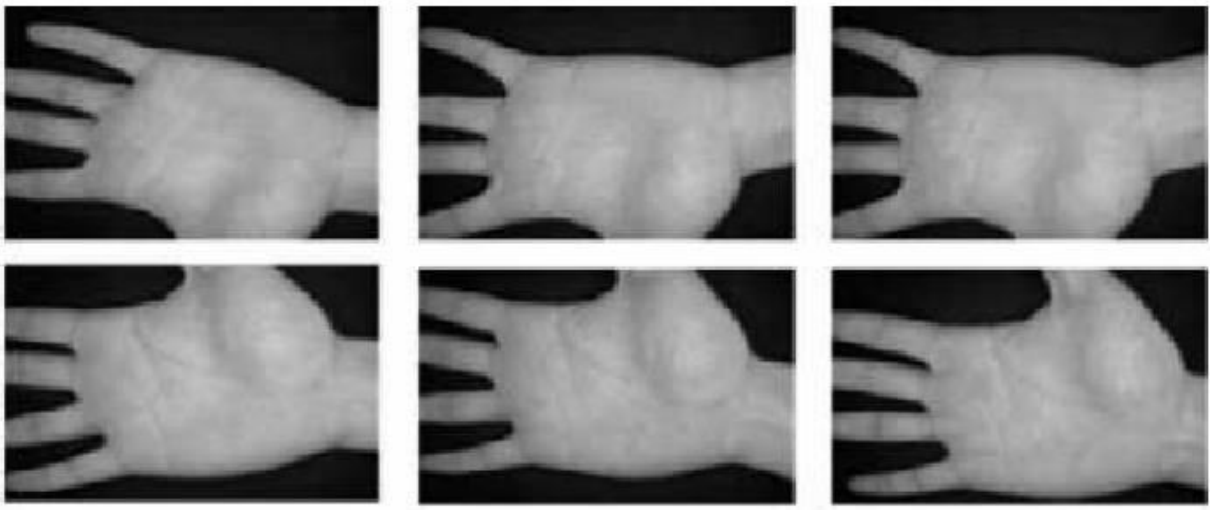

Figure 2 : la base CASIA-MS-PalmprintV1.

1.2 Base de données multimodale

Le problème majeur auquel nous sommes confrontés lorsqu'il s'agit de travailler en biométrie multimodale est le manque de bases de données et les bases disponibles sont payantes.

Cela implique alors la combinaison de modalités biométriques provenant de différente base de données. Cette opération provoque la création de ce que l'on appelle des utilisateurs virtuels.

1.2.1 Définition la base virtuelle

Est une base de données biométriques formée d'individus virtuels. Ces individus sont générés en associant une modalité biométrique d'une personne à une autre modalité biométrique d'une autre personne. Par exemple une personne virtuelle peut être formée à partir du visage d'une personne et de l'empreinte palmaire de quelqu'un d'autre.

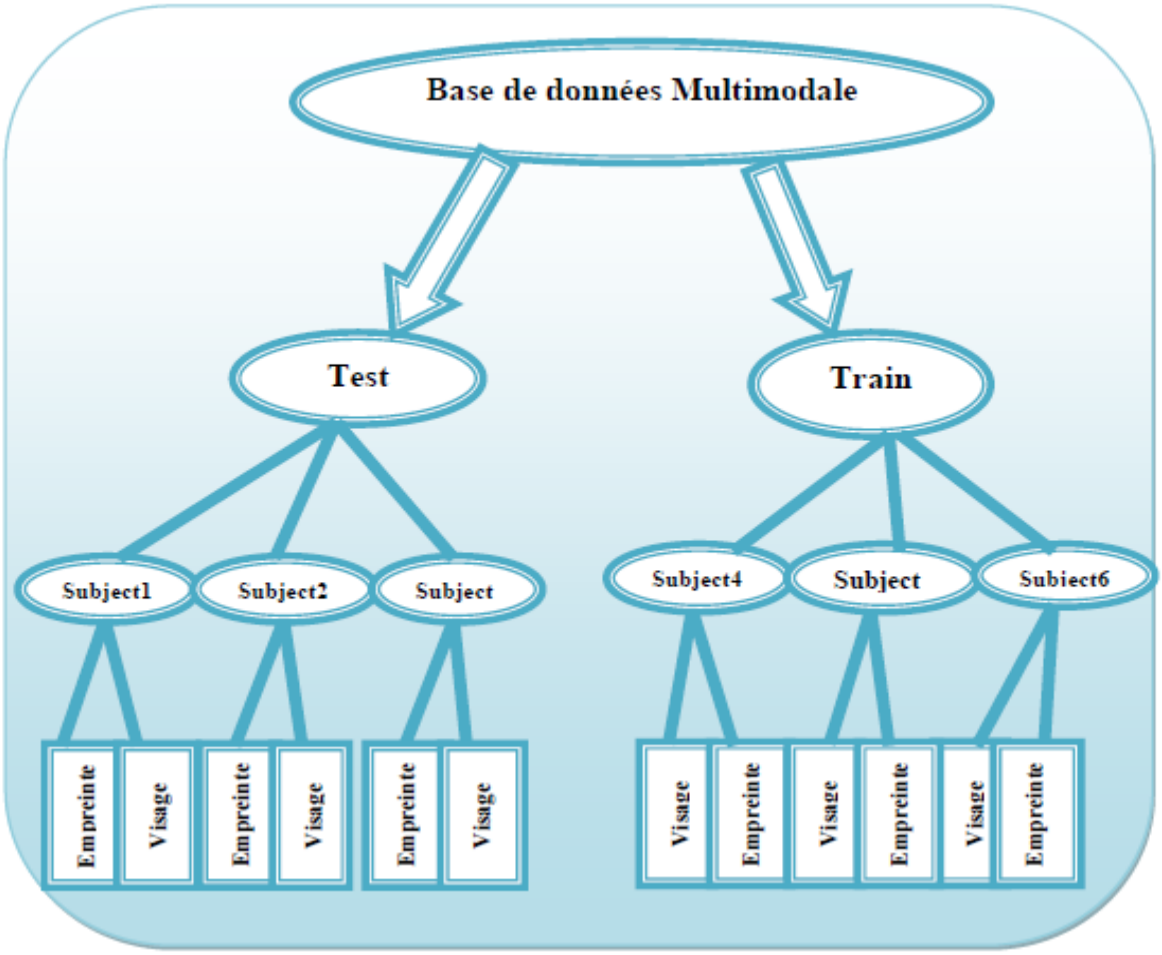

Figure 3 : La création d'une base multimodale.

2. Séparation de la base de données

Les 10 images de visage et les 8 images de l'empreinte palmaire sont divisées en deux groupes : un groupe pour effectuer l'enrôlement et l'autre pour tester les techniques et déterminer leurs performances. Mais il n'y a pas de règles pour déterminer ce partage de manière quantitative. Il résulte souvent un compromis tenant compte du nombre de données dont on dispose et du temps pour effectuer la reconnaissance. Dans les séries de test que nous avons effectué la base a été scindée de la façon suivante :

2.1 Visage

- **Images d'apprentissages** : Les sept premières images du visage de chaque personne servent pour la phase d'apprentissage.

- **Images Tests** : Les images restantes (8 ,9 et 10) de chaque individu nous ont servi pour la réalisation des différents tests.

2.2 Empreinte palmaire

- **Images d'apprentissages** : Les 8 premières images de l'empreinte de chaque personne servent pour la phase d'apprentissage.
- **Images Tests :** L'image restante (8) de chaque individu nous a servi pour la réalisation des différents tests.

Le but est d'évaluer le taux de reconnaissance de différents algorithmes présentés, en suivant un protocole de test basé sur la mesure du taux de reconnaissance.

$$\text{Taux de reconnaissance} = \frac{\text{Nombre d'images de test reconnues}}{\text{Nombre totale d'images de test}}$$

3. Environnement du travail

Dans cette section, nous présenterons les environnements matériel et logiciel de notre travail.

3.1 Outils de développement

Nous avons eu recours lors de l'élaboration de notre système à Matlab 2015b que nous présenterons ci-dessous.

- **Matlab r2015b**

Matlab et son environnement interactif est un langage de haut niveau qui permet l'exécution de tâches nécessitant une grande puissance de calcul et dont la mise en œuvre sera bien plus simple et rapide qu'avec des langages de programmation traditionnels tels que le C, C++. Il dispose de plusieurs boites à outils en particulier celle du traitement d'images « Image Processing ToolBox » qui propose un ensemble d'algorithme et d'outils graphiques de référence pour le traitement, l'analyse, la visualisation et le développement d'algorithmes de traitement d'images.

3.2 Environnement matériel

Afin de mener à bien ce projet, il a été mis à notre disposition un ensemble de matériels dont les caractéristiques sont les suivantes :

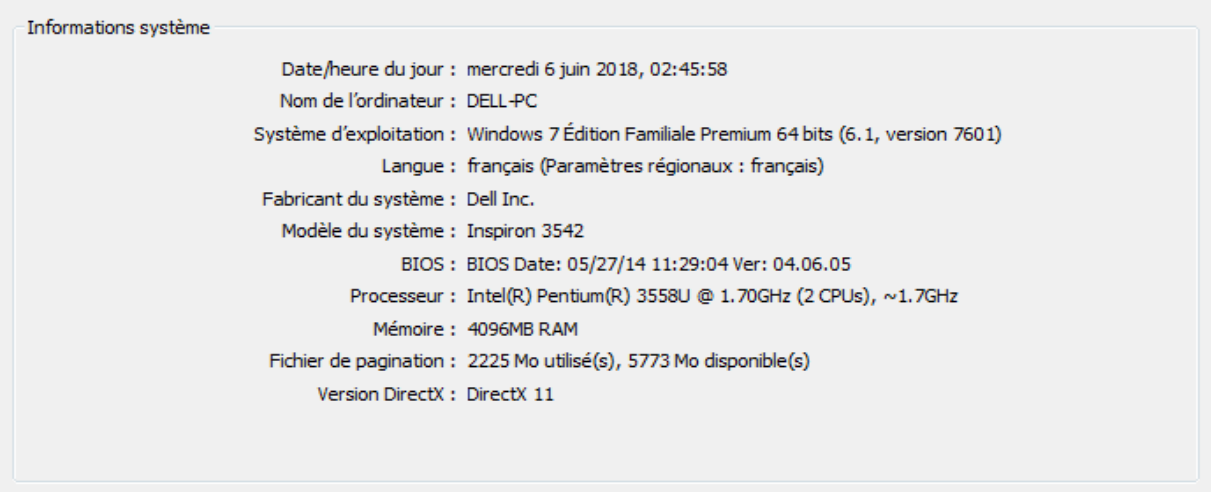

Figure 4 : Caractéristiques de l'ordinateur.

3 Développement de l'application

Dans cette partie, nous allons présenter les différentes phases de la réalisation de notre projet.

3.2 Interface principale

Cette interface représente l'interface d'accueil de notre application.

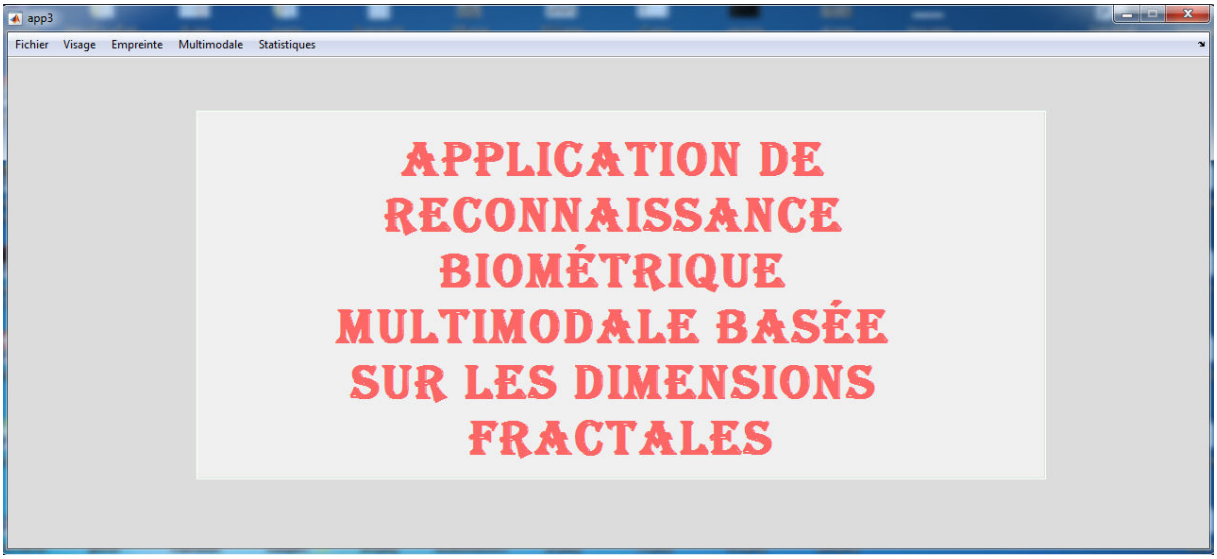

Figure 5 : Interface principale du système.

Lors du lancement de notre application, une fenêtre principale intitulée « Application de reconnaissance biométrique multimodale basée sur les dimensions fractales » s'affiche à l'écran .cette interface graphique est composée de cinq menus comme illustre la figure 5 Ci-dessus.

- Le menu « Fichier » : Contient un sous menu nommé « Quitter » , sa fonction est de fermer l'application suivi d'une boite de dialogue pour la confirmation ou pas de la fermeture.
- Le menu « Visage » : Qui redirige vers une interface de reconnaissance du visage en utilisant la dimension fractale.

3.3 Interface du visage

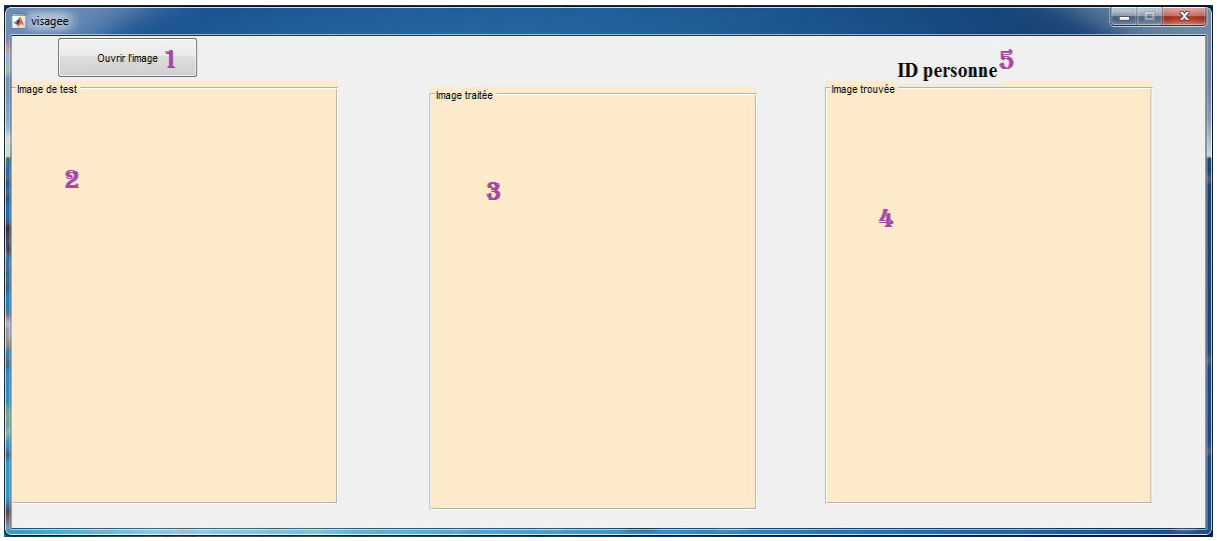

Figure 6 : Interface visage.

1. Bouton « Ouvrir l'image » : Pour ouvrir l'image du visage à reconnaître.
2. Panneau pour afficher l'image du visage sélectionné.
3. Panneau pour afficher l'image du visage après l'application du filtre Gaussien.
4. Panneau d'affichage de l'image de la personne reconnue.
5. « Edit Text » : Zone de texte pour afficher l'ID de la personne identifiée par le système.

Voici donc un exemple de reconnaissance faciale fait par notre système.

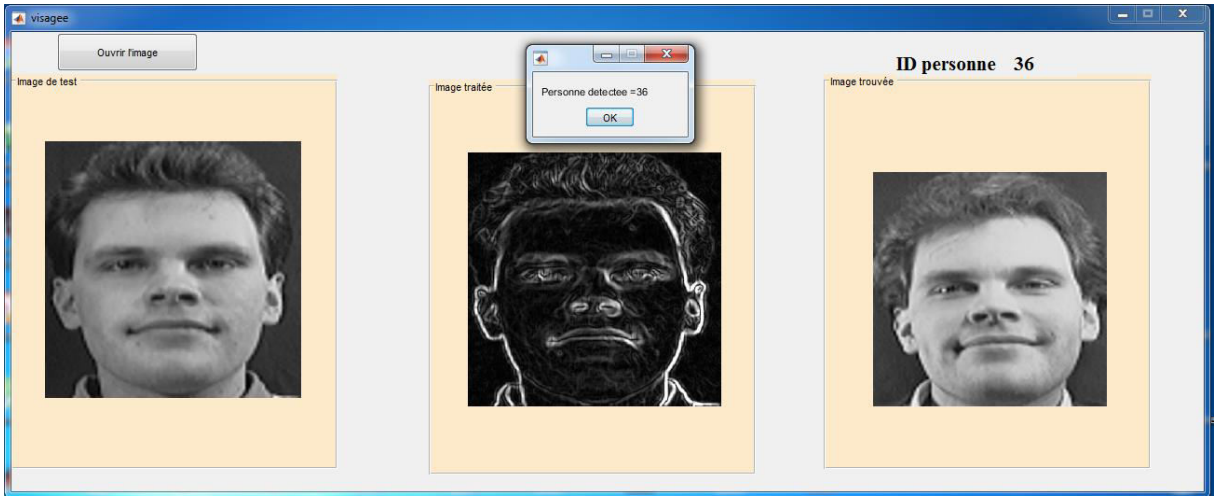

Figure 7 : Interface visage (2).

- Le menu « Empreinte » : Qui redirige vers une interface de reconnaissance de l'empreinte palmaire en utilisant la dimension fractale.
-

3.4 Interface Empreinte

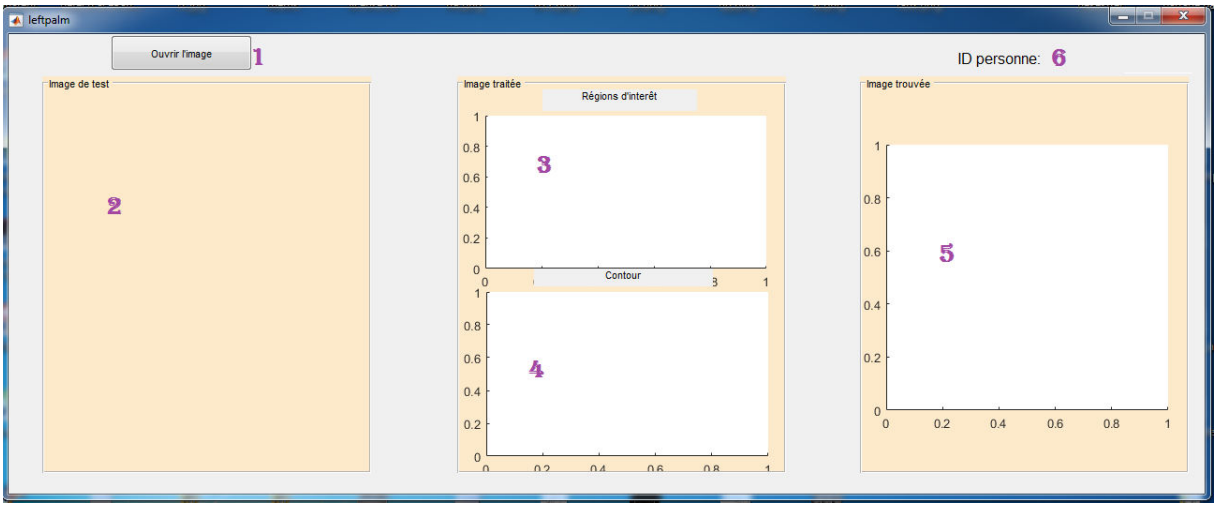

Figure 8 : Interface Empreinte palmaire.

1. Bouton « Ouvrir l'image » : Pour ouvrir l'image de l'empreinte à reconnaître.
2. Panneau pour afficher l'image de l'empreinte sélectionnée.
3. Panneau pour afficher la région d'intérêt de l'empreinte palmaire. .

4. Panneau pour afficher la région d'intérêt de l'empreinte palmaire après l'application du filtre Sobel.
5. Panneau pour afficher l'image de la personne dont l'empreinte le correspond.
6. « Edit Text » : Zone de texte pour afficher l'ID de la personne identifiée par le système de reconnaissance d'empreinte palmaire.

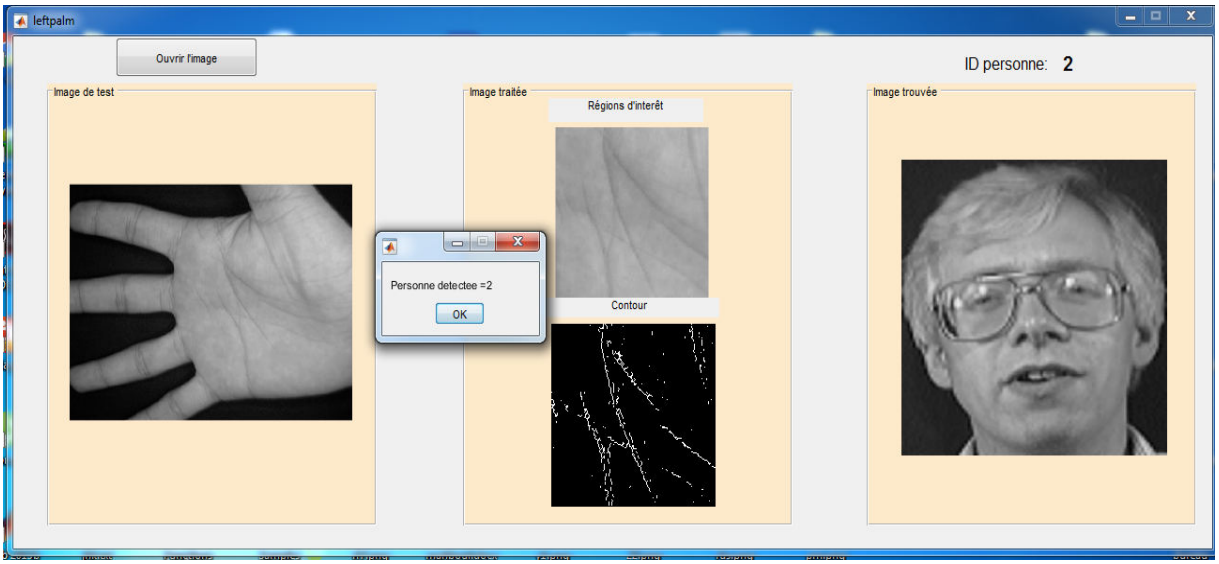

Figure 9 : Interface Empreinte palmaire(2).

- Le menu « Multimodale » : Qui redirige vers une interface de reconnaissance de l'empreinte palmaire et du visage en utilisant la dimension fractale.

3.5 Interface multimodale

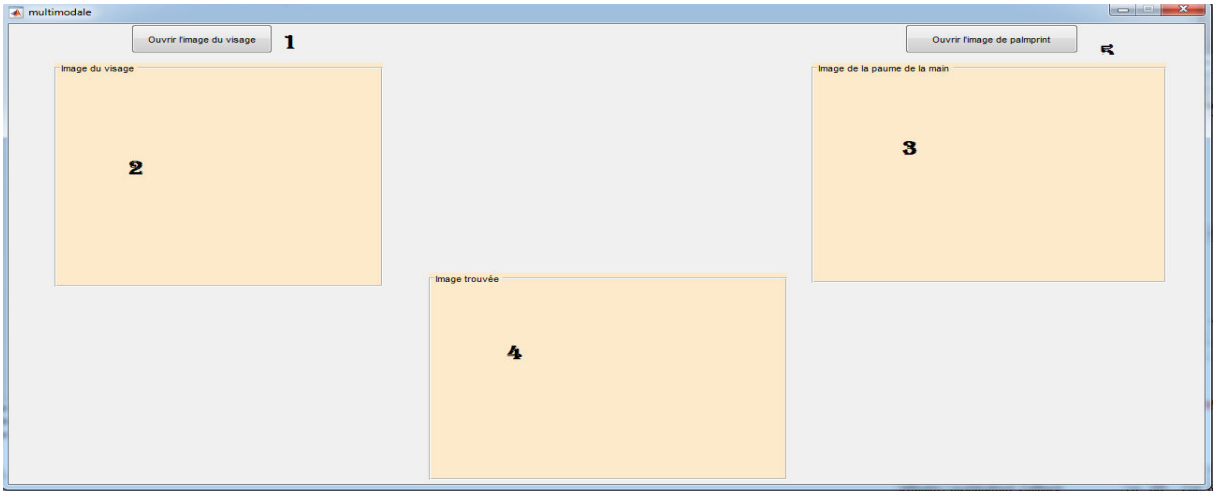

Figure 10 : Interface multimodale.

1. Bouton « Ouvrir l'image » : Pour ouvrir l'image du visage à reconnaître.
2. Panneau pour afficher l'image du visage sélectionné.
3. Panneau pour afficher l'image de l'empreinte palmaire sélectionnée.
4. Panneau pour afficher l'image de la personne correspondante après la fusion des deux modalités.
5. Bouton « Ouvrir l'image » : Pour ouvrir l'image de l'empreinte à reconnaître.

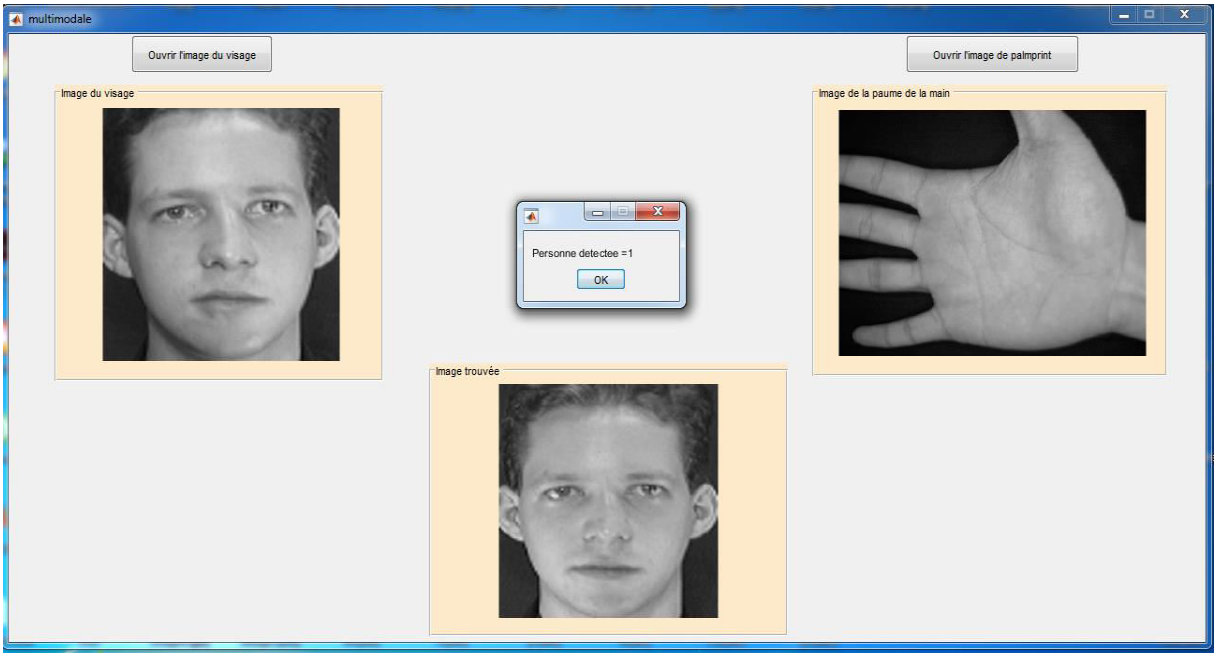

Figure 11 : Interface multimodale(2).

3.6 Interface Statistique

Pour calculer et afficher le taux de reconnaissance uni-modale et multimodale de notre application.

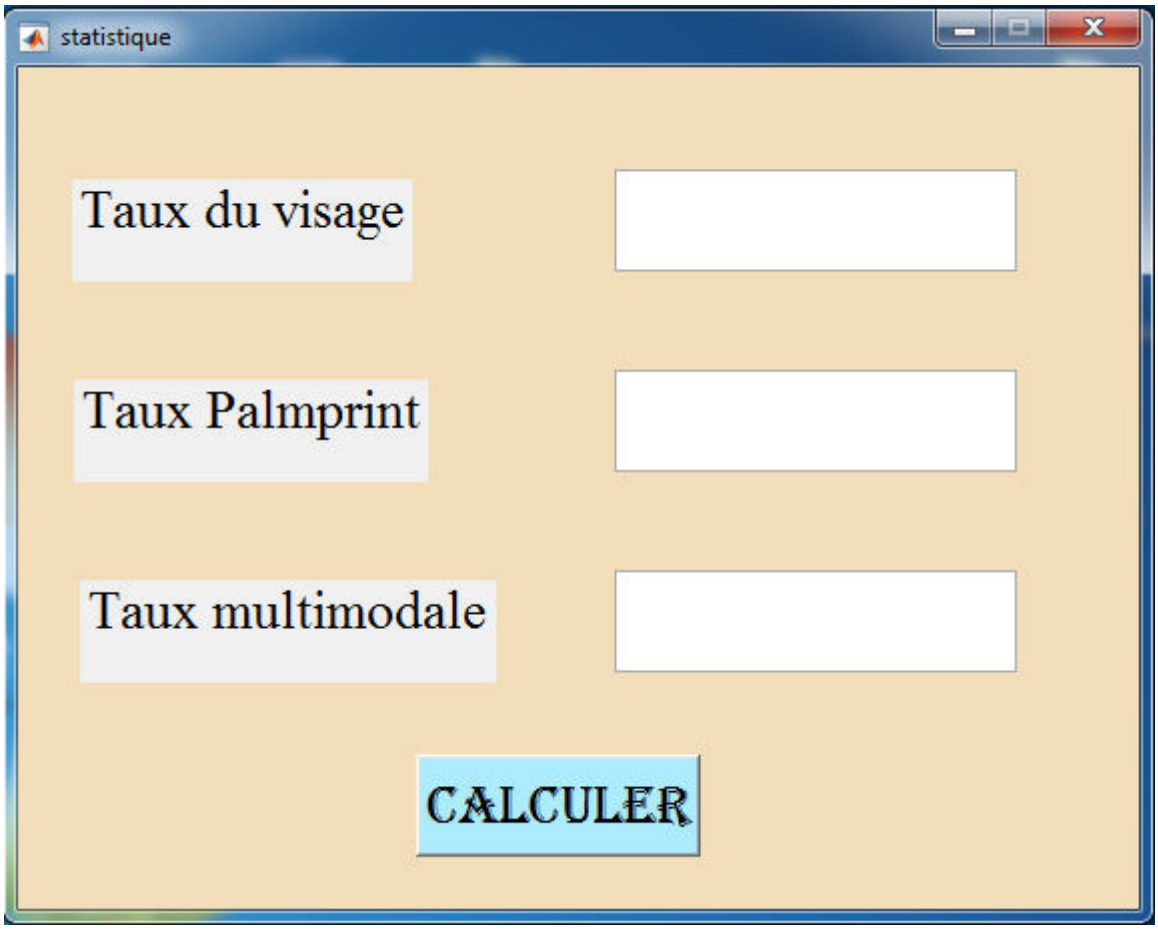

Figure 12 : Interface statistique.

4 Résultats Expérimentaux

4.2 Système uni-modal

Dans cette section, nous allons présenter les résultats de taux de reconnaissance pour une seule modalité biométrique (visage ou palmprint), en utilisant la dimension fractale.

Les méthodes	Taux de reconnaissance
Visage	91.66 %
Palmprint	80%

Tab 1 : Taux de reconnaissance unimodale.

4.3 Système multi-modal

Le but de la Multimodalité est d'améliorer le niveau de sécurité du système tel que le taux d'identification des modalités biométriques fusionnées soit supérieur au maximum des taux d'identification des modalités prises séparément. Ainsi, en utilisant les différentes modalités (visage et palmaire).

Les méthodes	Taux de reconnaissance
Visage	91.66 %
Palmprint	80 %
Multimodale	86 %

Tab 2 : Taux de reconnaissance multimodale.

5 Expérimentations et discussion

Pour évaluer l'efficacité de la méthode fractale décrite dans le chapitre 3, nous avons opté pour une validation sur les deux bases de données « CASIA-PalmprintV1 » pour les empreintes palmaire et « AT&T »pour le visage. Afin de faire la reconnaissance de ces deux modalités est défini comme suit : étant donnée une image dont on souhaite déterminer l'identité de la personne correspondante. Pour ce faire, il est nécessaire d'avoir des images de référence, sous la forme d'une base de données de toutes les personnes connues par le système (empreinte ou visage). A chaque image est associe un vecteur de caractéristiques, ces caractéristiques sont supposées être invariantes pour une même personne, et différentes d'une personne à l'autre. La reconnaissance consiste alors à comparer le vecteur de caractéristiques à reconnaitre avec celui de chaque empreinte ou visage de la base. Ceci permet de retrouver la personne ayant l'empreinte ou visage le plus ressemblant, qui est celui dont le vecteur est le plus similaire.

Conclusion

Dans ce chapitre, nous avons étudié et implémenté un système de reconnaissance multimodale empreinte digitale et visage, vu que ce système est basé sur la dimension fractale et que cette dernière est nouvellement utilisée dans le domaine biométrique, elle a eu le mérite d'être intégrée dans la reconnaissance biométrique grâce à sa précision, son efficacité et surtout ses taux élevés. Donc la dimension fractale pourra être utilisée sans aucune doute dans le reconnaissance biométrique et ses différentes modalités.

Conclusion Générale

Notre travail consiste à la conception et l'implémentation d'un système de la Biométrie Multimodale : empreinte palmaire et faciale.

Le système biométrique que nous avons proposé se base sur la fusion de deux modalités : empreinte palmaire et visage. Chaque modalité a de différentes méthodes. On a choisi la méthode de la dimension fractale dans l'extraction des caractéristiques pour l'empreinte digitale et la même méthode pour le visage.

Notre travail consiste à la mise au point d'un algorithme robuste destiné à reconnaître un individu par son empreinte palmaire et visage. Dans chaque système on a utilisé la même technique :

- Le niveau de fusion choisit est la fusion de score dans cette niveau les scores individuels sont combinés de manière à former un unique score qui est ensuite utilisé pour prendre la décision finale.

Nous estimons avoir réalisé un système répondant à l'objectif que nous nous sommes fixés au départ, à savoir la mise en œuvre d'un système permettant la reconnaissance d'individus et le contrôle d'accès.

Si la biométrie est un enjeu important au niveau économique, la recherche, en particulier dans le domaine de reconnaissance des visages et des empreintes offrent encore un champ d'investigations très ouvert.

References

[1] : S. Prabhakar, S. Pankanti, and A. K. Jain. Biometric recognition : Security and privacy concerns. IEEE Security & Privacy, 1 :33–42, 2003. [cite p. 8]

[2] : J. Daugman. Recognizing Persons by Their Iris Patterns. In A. K. Jain, R. Bolle, and S.

Pankanti, editors, Biometrics: Personal Identification in a Networked Society, pp. 103-

121, Kluwer Academic Publishers, 1999.

[3] : N. Rudin, K. Inman, G. Stolovitzky, and I. Rigoutsos. Biometrics : Personal

Identification in Networked Society, chapter DNA Based Identification, pages 287–

309. Kluwer Academic Publishers, 2002. [cit´e p. 8]

[4] : International Biometric Group. http ://www.biometricgroup.com/, 2010. [cite p. 11, 15, 154]

[5] : L. O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. In Proceedings of the IEEE, volume 91, pages 2021–2040, 2003. [cite p. 11]

[6] : Fedias Meriem., "Combinaisons de données d'espaces couleurs et de méthodes de vérification d'identité pour l'authentification de visages", Université Mohamed Khi der – Biskra.

[7] : DANG Hoang Vu., "Biométrie pour l'identification", Rapport final, Institut de la Francophonie pour l'Informatique, Hanoï, Vietnam, 07 – 2005.

[8] : Nicolas MORIZET., "Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris", Thèse présentée pour obtenir le grade de Docteur, Ecole Nationale Supérieure des Télécommunications, Paris, 18 Mars 2009.

[9] : revues.univ-biskra.dz/index.php/cds/article/view/455/422

[10] : Moulay Brahim Oussama, Arbaoui Mohamed Ibrahim., "Authentification des personnes par les articulations des doigts", UNIVERSITE KASDI MERBAH OUARGLA, 2015.

[11] : Hietmeyer, «Biometric identification promises fast and secure processing of airline passengers». The International Civil Aviation Organization Journal, Vol. 17, No. 9, pp. 10-11, 2000.

[12] : «Machine Readable Travel Documents (MRTD)».
2008. http://www2.icao.int/en/mrtd/Pages/default.aspx. valide le 12/07/2011

[13] : N. MORIZET, Thomas EA, Florence ROSSANT, Frédéric AMIEL, Amara AMAR « Revue des algorithmes PCA, LDA, et EBGM utilisé en reconnaissance 2D du visage pour la

biométrie » ; Institut Supérieur d'Electronique de Paris(ISEP), Département d'Electronique ; 2006.

[14] : S.Guerfi Ababsa "Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D ~~, thèse pour obtenir le titre de : Docteur de l'Université Evry Val d'Essonne spécialité : Science de l'ingénieur ; 2008.

[15] : N. MORIZET «Reconnaissance biométrique par fusion multimodale du visage et de l'iris », thèse de doctorat a l'Ecole National Supérieur de télécommunication, France ; 2009.

[16] : A. Mellakh «Reconnaissance des visages en conditions dégradées », thèse de doctorat a l'Ecole National Supérieur de télécommunication, France, 2009.

[17] : W.Hizem « Capteur intelligent pour la reconnaissance de visage », thèse de doctorat a l'Ecole National Supérieur de télécommunication et Université Pierre et Marie Curie- Paris G, France, 2009.

[18] : A. Chirikov, « Karhumen- Loeve, for face recognition »; Matlab code available at: http://mathworks.com/matlabcentral/fileexchange/ loadfile.do?

[19] : .Hazim Mohamed Amir et Nabi Rachid, thème reconnaissance de visages, Universités d?Avignon et du pays du Vaucluse IUPGMT 2006 /2007.

[20] : .A Lemieux <<système d?identification de personnes par vision numérique>>, université Laval, Québec décembre 2003.

[21] : https://carnets2psycho.net/pratique/livre1471601722.html// Livre ecrit par Raymond Bruyer

[22] : D. Zhang, W. K. Kong, J. You, M. Wong (2003): “Online Palmprint Identification”, IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 25, no. 9, pp. 1041-1050.

[23] : Xiao-Yuan Jing, David Zhang (2004): “A face and palmprint recognition approaches based on discriminant DCT feature extraction”, IEEE Transactions on Systems, Man, and Cybernetics, Part B 34(6), pp 2405-2415.

[24] : Xiang-Qian Wu, Kuan-Quan Wang and David Zhang (2002): "Wavelet Based Palmprint Recognition", Proceedings of the First International Conference on Machine Learning and Cybernetics, Beijing, pp. 1253- 1257.

[25] : Tee Connie, Andrew Teoh, Michael Goh and David Ngo (2003): “Palmprint Recognition with PCA and ICA”, Conference of Image and Vision Computing New Zealand 2003 (IVCNZ’03), pp 227-232.

[26] : A. Kumar, D.C.M. Wong, H.C. Shen and A.K. Jain (2003): “Personal Verification using Palmprint and Hand Geometry”, Proceedings of Fourth International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), pp 668-678.

[27] : C. Poon, D.C.M. Wong, H.C. Shen (2004): “A New Method in Locating and Segmenting Palmprint into Region-of-interest”, Proceedings of the 17th International Conference on Pattern Recognition 2004 (ICPR 2004). Vol. 4, pp. 533–536.

[28] : K. Y. E. Wong, G. Sainarayanan and Ali Chekima (2006): “Palmprint Authentication using Relative Geometric Features”, 3rd International Conference on Artificial Intelligent and Engineering Technology (ICAIET 2006), pp 743-748.

[29] : K. Y. E. Wong, G. Sainarayanan and Ali Chekima (2007): “Palmprint Identification Using Discrete Cosine Transform”, World Engineering Congress 2007, pp 85- 91.

[30] : K. Y. E. Wong, G. Sainarayanan and Ali Chekima (2007): “Palmprint Identification Using Wavelet Energy”, Intl. Conf. On Intelligent & Advanced Systems (ICIAS 2007), 25th - 28th Nov 2007.

[31] : K. Y. E. Wong, G. Sainarayanan and Ali Chekima (2007): “Palmprint Identification Using SobelCode”, Malaysia-Japan International Symposium on Advanced Technology (MJISAT 2007), 12th -15th Nov 2007

[32] : (Mandelbrot, 1975, 1977 et 1982) ; les livres de Barnsley (1988) et de Falconer

(1990) abordent également les aspects mathématiques. Parmi les livres traitant des fractales dans le domaine des sciences physiques

[33] : Les fractales, Art, Nature et Modélisation, Tangente Hors-série no. 8, ´Editions Poles (2004).

[34] : Barnsley M. F., Fractals everywhere, Academic Press (1988).

[35] : Cantor G., ¨Uber unendliche, lineare Punktmannigfaltigkeiten V, Mathematische

Annalen 21 (1883) pp. 545-591.

[36] : Euclide, Les quinze livres des éléments géométriques d’Euclide, traduit en français par D. Henrion, Paris, Veuve Henrion (1632) pp.1-3, 504.

[37] : Falconer K.J., Fractal geometry : Mathematical Foundations and applications,

(2003), John Wiley and Sons Ltd.

[38] : Gouyet J.-F., Physique et structures fractales, Masson (1992).

[39] : Hausdorff F., Dimension und Hausseres Mass, Mathematische Annalen 79 (1919) pp. 157-179.

[40] : Hutchinson J., Fractals and self-similarity, Indiana Journal of Mathematics 30

(1981) pp. 713-747.

[41] : Julia G., Mémoire sur l'itération de fonctions rationnelles, Journal de Mathématique Pure et Appliqué (1918) pp. 47-245.

[42] : http://library.thinkquest.org/26242/full/fm/fm7.html

[43] : (Guo et al. 2009)

[44] : (Lopes, Betrouni. 2009), (Zhou et Lam, 2005)