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

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

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

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

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

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

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

I. INTRODUCTION

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

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

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

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

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

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

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

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

II. Proposed encryption/Decryption method

A. PLCM chaotic map

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

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

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

B. Encryption scheme

The encryption process is detailed in the following steps:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Decryption scheme

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

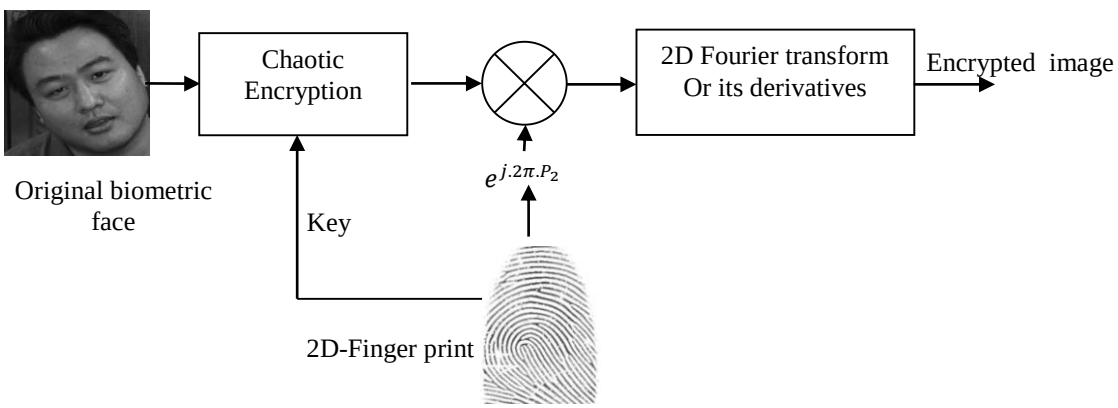


Fig. 1. Proposed encryption scheme.

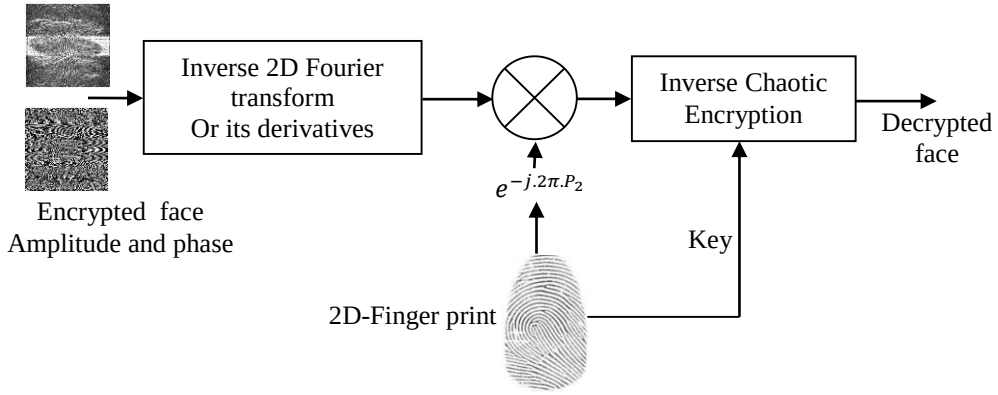


Fig. 2. Proposed decryption scheme.

III. Simulation Results and Security Analysis

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

A. *Histograms analysis*

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

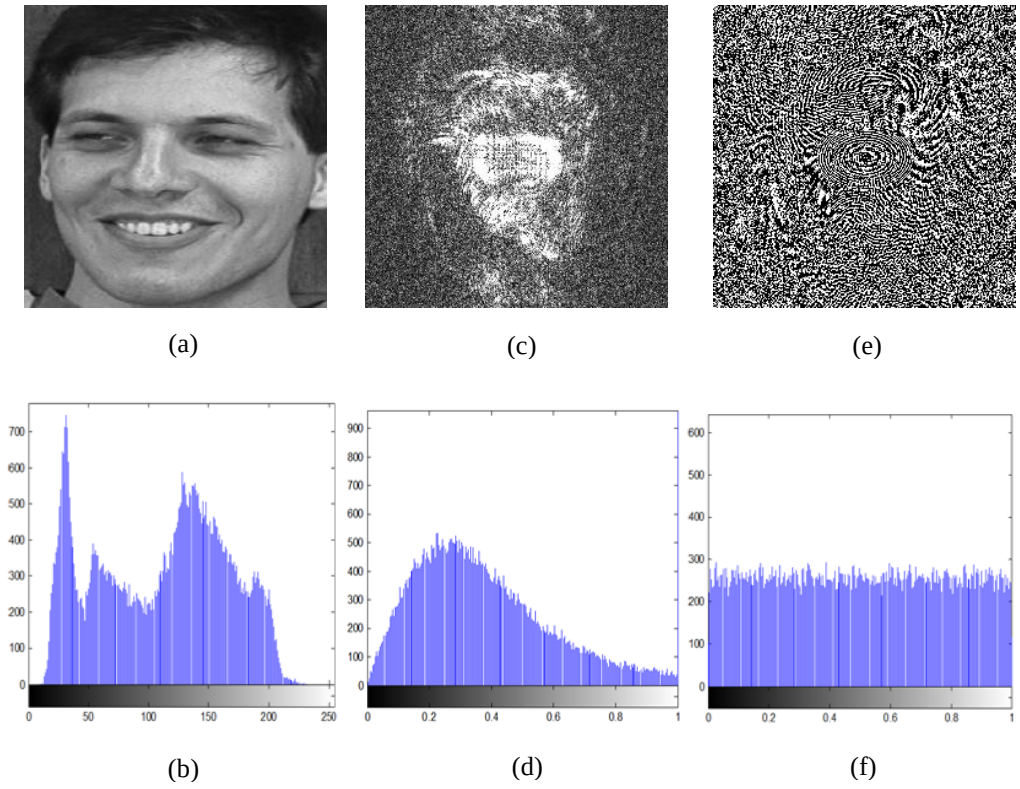


Fig. 3. Histogram analysis of biometric original image 1: The original face image 1 (a), original image histogram (b), the amplitude encrypted image (c), amplitude encrypted image histogram (d), phase encrypted image of (e), phase encrypted image histogram, (f).

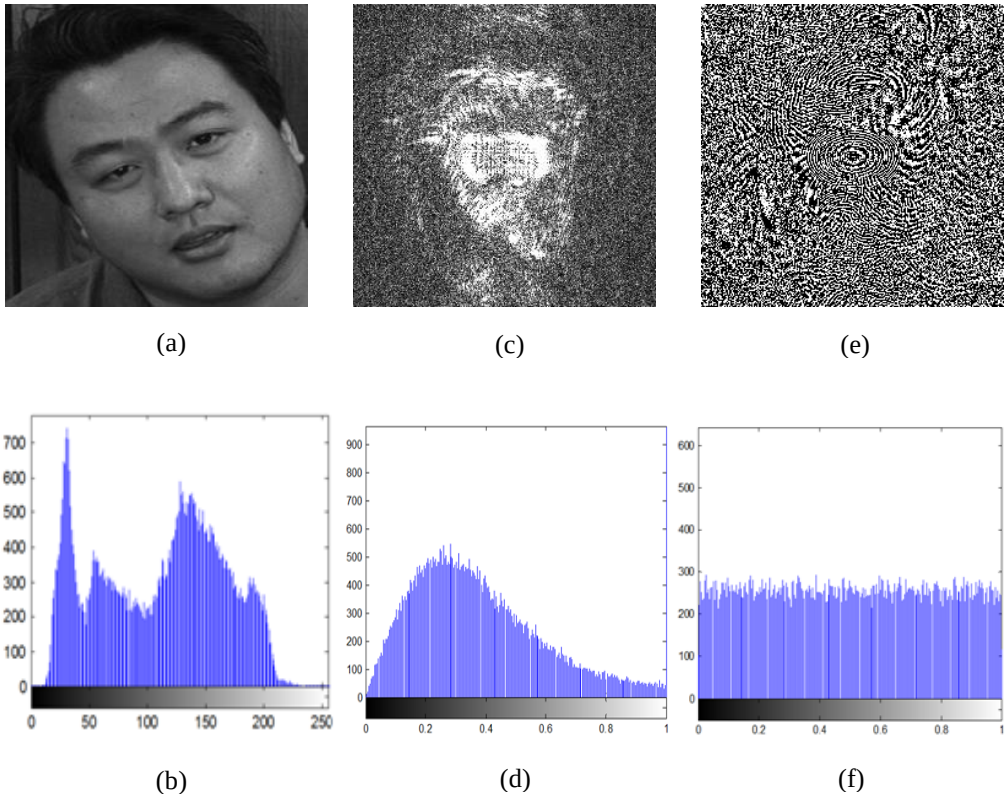


Fig. 4. Histogram analysis of biometric face image 2. The original face image 2 (a), original image histogram (b), the amplitude encrypted image (c), amplitude encrypted image histogram (d), phase encrypted image of (e), the phase encrypted image histogram, (f).

B. Correlation analysis

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

Table. 1. Correlation analysis

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

C. Loss data

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

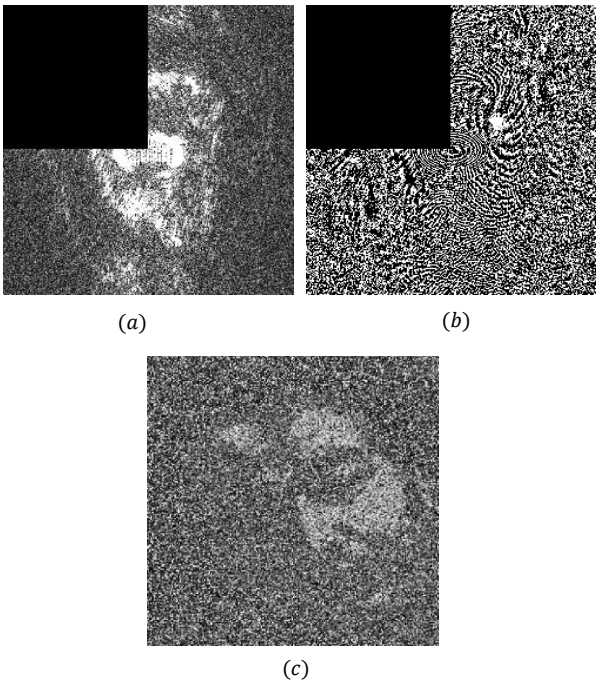
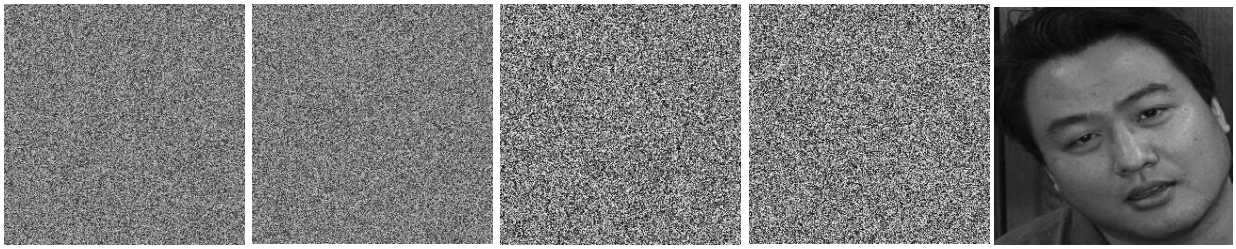


Fig.5. Loss data test: (a) Amplitude encrypted face with 25% loss data (b) Phase encrypted face with 25% loss data (c) The corresponding decrypted face with 25% loss data.

D. Sensitivity analysis



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

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

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

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

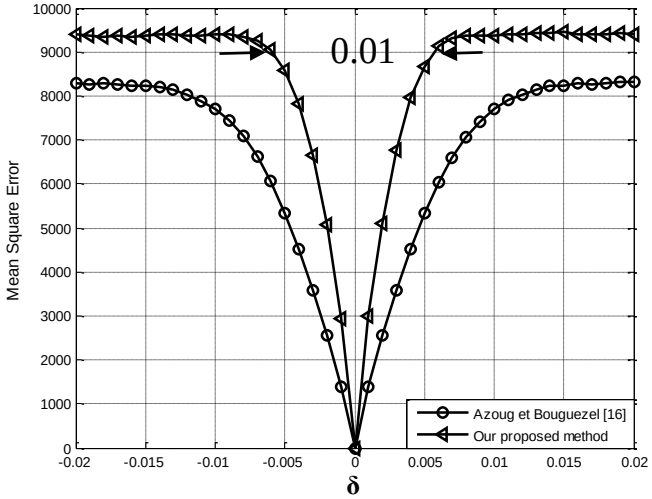


Fig. 7. The value of MSE of our method in terms of the deviation error δ compared with [16].

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

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

E. Key space

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

F. Statistical tests analysis

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

Table .2. NIST results

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

IV. CONCLUSION

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

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

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

REFERENCES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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