All Sciences Proceedings
http://as-proceeding.com/

2nd International Conference on Engineering, Natural and Social Sciences

April 4-6, 2023 : Konya, Turkey

https://www.icensos.com/

Nonlinear biometric pre-processing applied to image encryption scheme

Imane Kouadra*, Lahcene Ziet [2]

[1]Department of electronics/LEPCI Laboratory, University of Ferhat Abbes Setif1, Algeria
[2]Department of electronics/LEPCI Laboratory, University of Ferhat Abbes Setif1, Algeria

*imane.kouadra@univ-setif.dz

Abstract – In this paper, we propose an efficient preprocessing approach for an image encryption scheme based on a nonlinear function, namely the sigmoid function, applied to a permutation diffusion architecture. We introduce several chaotic functions and an original image fingerprint, which jointly form the encryption key of the proposed scheme. To evaluate the effectiveness of our algorithm, we use performance metrics such as mean square error (MSE), peak signal-to-noise ratio (PSNR), and correlation rate. Our results demonstrate the robustness of the proposed encryption scheme. In addition, the scheme is shown to be more efficient and superior to existing encryption schemes in the literature through cryptographic attacks.

Keywords – Nonlinear, Sigmoid Function, Pre-Encryption, Chaotic Map, Permutation-Diffusion

I. INTRODUCTION

Recently digital communication has become increasingly common in all areas of life, leading to a large amount of mutual information that is vulnerable to unauthorized use, resulting in damage to the information and the need for protection using various techniques such as digital watermarking [1], steganography [2], encryption [3], and biometric security databases [4]. Among the most commonly used information types are voice, video, and still images, with image information being the most widely exchanged information in communication systems and social networks, making it highly vulnerable to manipulation and misuse. Encryption techniques can be performed in two ways: spatial domain [5-7] based mainly on diffusion and permutation operations, or frequency domain using transforms [8-10] such as Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), and Discrete Cosines Transform (DCT)...etc. However, spatial image encryption has some shortcomings that have led researchers to develop advanced algorithms to improve security and address these issues. One interesting approach is the use of chaotic maps [11]. While classical chaotic maps, such as cubic, quadratic, and logistic, have shown some robustness over time, they have become increasingly fragile. Therefore, it is necessary to explore other more efficient and relevant solutions to combat cryptanalysis operations by using other types of nonlinear functions to strengthen the robustness of proposed systems [12-14]. In this context, we propose a hybrid biometric system that combines image and fingerprint according to an encryption structure based on pre-processing using the sigmoid function, which precedes the operations of diffusion and permutation. We will demonstrate the effectiveness of the proposed scheme against attacks through tests and simulations, comparing the results with previous works in the literature. The methodology of the work is as follows: firstly, we define the sigmoid functions in section 1, then present the encryption and decryption flowcharts in section 2. Section 3 discusses the work's valorization in addressing these challenges, and we conclude the paper with perspectives to improve this important axis.

II. PRELIMINARIES

In this section, we define the logistic chaotic map widely used in this paper, that on the one hand, on the other hand, we also define the non-linear function which is the sigmoid one and its inverse function.

A. *Logistic map*

The Logistic map is expressed as follows:

$$x_{i+1} = r.x_i(1 - x_i) \quad (1)$$

Where the initial condition parameter is x_0 and $r \in [3.99,4]$ is the control parameter .

B. *Sigmoid function*

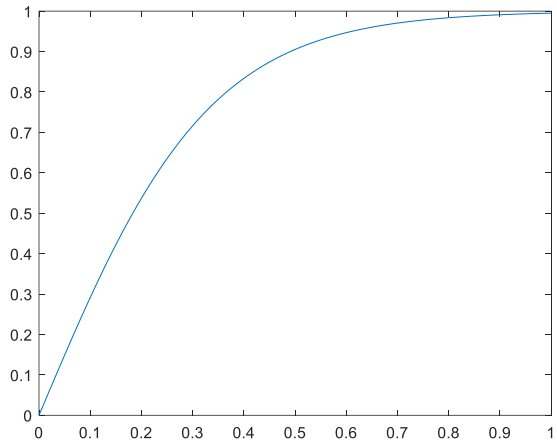


Fig.1 The plot of Sigmoid function with $\lambda = 6$

The sigmoid function is a non-linear reciprocal logistic function that can be expressed as a hyperbolic tangent function by:

$$f(x) = 1/(1 + e^{-x}) \quad (2)$$

for any real x.

The generalized form is expressed as follows:

$$f(\lambda x) = 1/\left(1 + e^{-\lambda x}\right) \quad (3)$$

To encrypt an image using a chaotic function by a nonlinear function called sigmoid whose interval which interests us is [0-1] or this function will be perfectly nonlinear if and only if the value of coefficient $\lambda = 6$ see the figure below

In the decoding phase it is enough to use the inverse function $(sigmoid^{-1})$ in this case it is only necessary to guess the values on y

In our work we use the sigmoid function with $\lambda = 6$, as show in fig.1.

Its inverse function is expressed as follows:

$$f^{-1}(x) = \log(x/1 - x)/\lambda \quad (4)$$

III. ENCRYPTION AND DECRYPTION SCHEMES

The following steps describe the proposed encryption scheme:

- Let I be the original image of size (m, n) and I' its corresponding finger print having the same dimensions as I.
- Resize the original image and its fingerprint into v and v'vectors of length $(1, m \times n)$ respectively.
- Generate two chaotic vectors C_0 and C_1based on the logistic map with respectively (x_0, r_0),(x_1, r_1) parameters of length $(1, m \times n)$.
- Let S be the result of the summation of the three vectors v,C_0, C_1 and S' its image through the sigmoid function, given by:

$$S' = sig(v + C_0 + C_1) = 1/\left[1 + exp\left(-(v + C_0 + C_1)\right)\right] \quad (5)$$

- Let IX be the vector representing the increasing order of the vector $v'$and let S_1 be the vector resulting from the rearrangement of the vector S'according to the order given by IX, this step is called the permutation phase .
- We generate a third chaotic vector C_2 of length $(1, m \times n)$, then we perform the XOR operation between this vector and the vector S_1 for obtaining the vector y according to the following formula:

$$y_k = \begin{cases} C_{2_k} \oplus S_{1_k}, & k = 1 \\ C_{2_k} \oplus S_{1_k} \oplus y_{1_{k-1}}, k = 1,2, \dots m \times n & \end{cases} \quad (6)$$

Finally, the encrypted image is obtained by reshaping y in to an $m \times n$ matrix.

The decrypted scheme takes the same path but in a reverse manner.

IV. RESULTS AND DISCUSSION

In this section, we present the simulation results of the proposed encryption algorithm, we used three biometric images of face [15] of size $(256\ x\ 256)$ with their corresponding

fingerprints [16].The simulations are performed through a personal laptop under Matlab 2016 environment.The parameters of the chaotic maps used are given as follows:$(x_0 = 0.45, r_0 = 3.99), (x_1 = 0.55, r_1 = 3.99)$ $(x_1 = 0.35, r_2 = 3.99)$. Figure 2 shows the biometric faces used and their histograms, figure 3 illustrates the proposed encryption scheme. As for the figure 4, it represents the encrypted faces with their histograms. The performance measures used for the evaluation of the proposed algorithm towards the different cryptographic attacks, namely the MSE, the PSNR and correlation rate are defined as follows:

$$PSNR = 10\log_{10}(d^2/MSE) \quad (7)$$

$$MSE = (1/m \times n) \times \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(I_0(i,j) - I_r(i,j)\right)^2 \quad (8)$$

With $d = 255$ (signal dynamic over 8 bits) and I_0 and I_r of size $m \times n$.

$$corr_{I_0 I_r} = \frac{cov(I_0, I_r)}{\sqrt{D_{I_0}} \times \sqrt{D_{I_r}}} \quad (9)$$

$$E(I_0) = \frac{1}{m \times n} \times \sum_{i=1}^{N} I_{0_i} \quad (10)$$

$$E(I_0) = 1/(m \times n) \times \sum_{i=1}^{m \times n} (I_{0_i} - E(I_0))^2 \quad (11)$$

$$cov(I_0, I_r) = \frac{1}{(m \times n) \times \sum_{i=1}^{m \times n}\left(I_{0_i} - E(I_0) \times \left(I_{r_i} - E(I_r)\right)\right)} \quad (12)$$

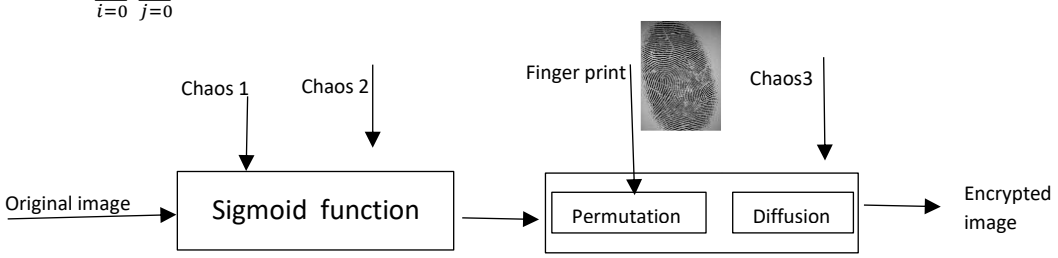


Fig. 2 The proposal encryption scheme

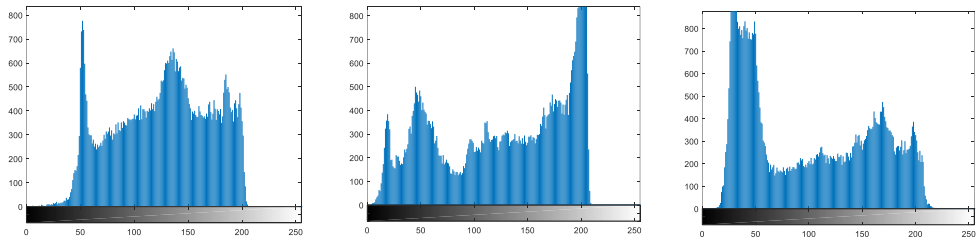
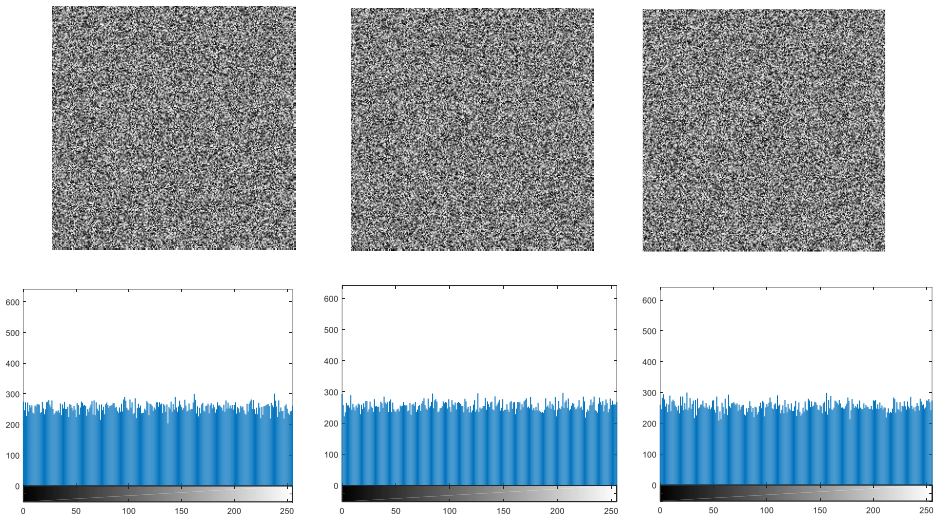


Fig. 3 Biometric test faces and their corresponding histograms

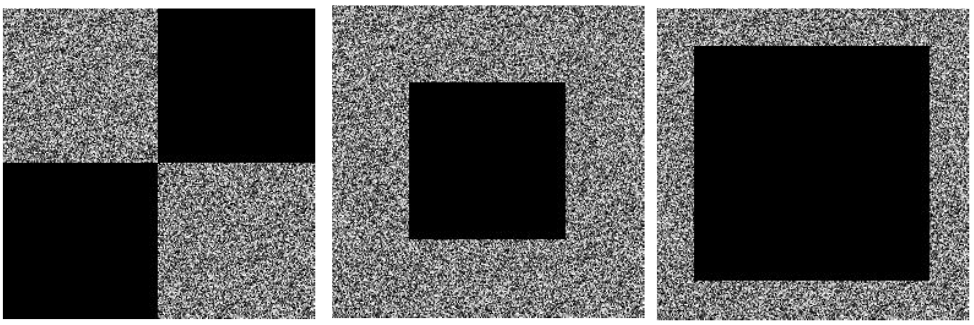


(a) (b) (c)

Fig.4 Encrypted test faces and their corresponding histograms

A. *Histogram analysis*

As illustrated in Figures 3 and 4, we start from three biometric test faces having different histograms Fig.3 and through the proposed algorithm, we obtain three encrypted images Fig.4 all having the same shape resembling a noisy image and the same histograms that look like a uniform white noise. It means that an attacker cannot extract any information from them that could reveal the proposed cryptographic system.



(a)

(b)

Fig.5 Loss data test. (a) Encrypted faces with 50%;25% and 75% respectively (b) The corresponding decrypted images

B. *Loss data test*

in this subsection, we assume that part of the information is lost during the transmission of the encrypted image between the transmitter and the receiver, consequently we will see the impact of this loss of information on the quality of the decrypted image Figure 6.a illustrates the different simulations with losses of 50%, 25% and 75% in the encrypted image, Figure 6.b represents the decrypted images corresponding to the losses mentioned. The decrypted images remain identifiable up to a loss rate of 75%. This confirms the robustness of the proposed algorithm with respect to the loss data test.

C. *Attack with a wrong fingerprint*

In this subsection, we assume that each biometric face has its own fingerprint of the same person. In this simulation we assume as illustrated in Figure 7.a has a test biometric face encrypted with its fingerprint which is part of the key space of the proposed algorithm. Figure 7.b represents the decrypted image with a fingerprint other than that used in the encryption phase, we notice that the decrypted image is completely noisy and indecipherable which qualifies the fingerprint as being a key decisive in the proposed algorithm.

(a)

(b)

Fig.6 Attack with a wrong fingerprint: (a) Face image with its corresponding fingerprint (b) The corresponding decrypted face image with the wright fingerprint and the wrong one respectively

D. *Correlation rate and other performance metrics*

Table1. Performance metrics

	PSNR	MSE	Corr
Face1	-43.3476	2.1615e+04	-0.0011
Face2	-43.350	2.1627e+04	-0.0065
Face3	-43.3475	2.1615e+04	-0.0038

In this subsection we used three performance measures to evaluate the robustness and the efficiency of the proposed algorithm which are the PSNR, MSE and the correlation rate. The table below summarizes all obtained results. We note that the PSNR is very degraded, the MSE is of very high value and the correlation rate is close to zero, which confirms the validity of the proposed algorithm.

E. *Sensitivity analysis*

In what follows, we assume that the encryption key is composed of the parameters of the chaotic map and the fingerprint (f_0) of the person having the face to encrypt $k(x_0, r_0, x_1, r_1, x_2, r_2; f_0)$. During decryption we also assume that the decryption key is $k'(x'_0, r'_0, x'_1, r'_1, x'_2, r'_2; f_0)$. For the sensitivity analysis, we make a minor variation in one of the elements of the encryption key and we keep the others as they are. We repeat this operation in turn. We note that the limit of appearance of the image is of the order of $10^{-16}$for the ri and 10^{-17} for the xi so the precision of ri is 10^{15} and that of xi is 10^{16} the figure (6) illustrates the different cases discussed.

F. *Key space analysis*

Considering the sensitivity results obtained in the previous subsection, we have shown that the precision in the chaotic parameters (x_i, r_i) is 10^{16}, and 10^{15} respectively. As for the precision of the fingerprint is 2^8, or the key space is as follows: $10^{15} \times 10^{15} \times 10^{15} \times 10^{16} \times 10^{16} \times 10^{16} \times 2^8 = 10^{93} \times 2^8 = 2^{287}$. This is sufficient compared to the value required encryption $= 2^{100}$.

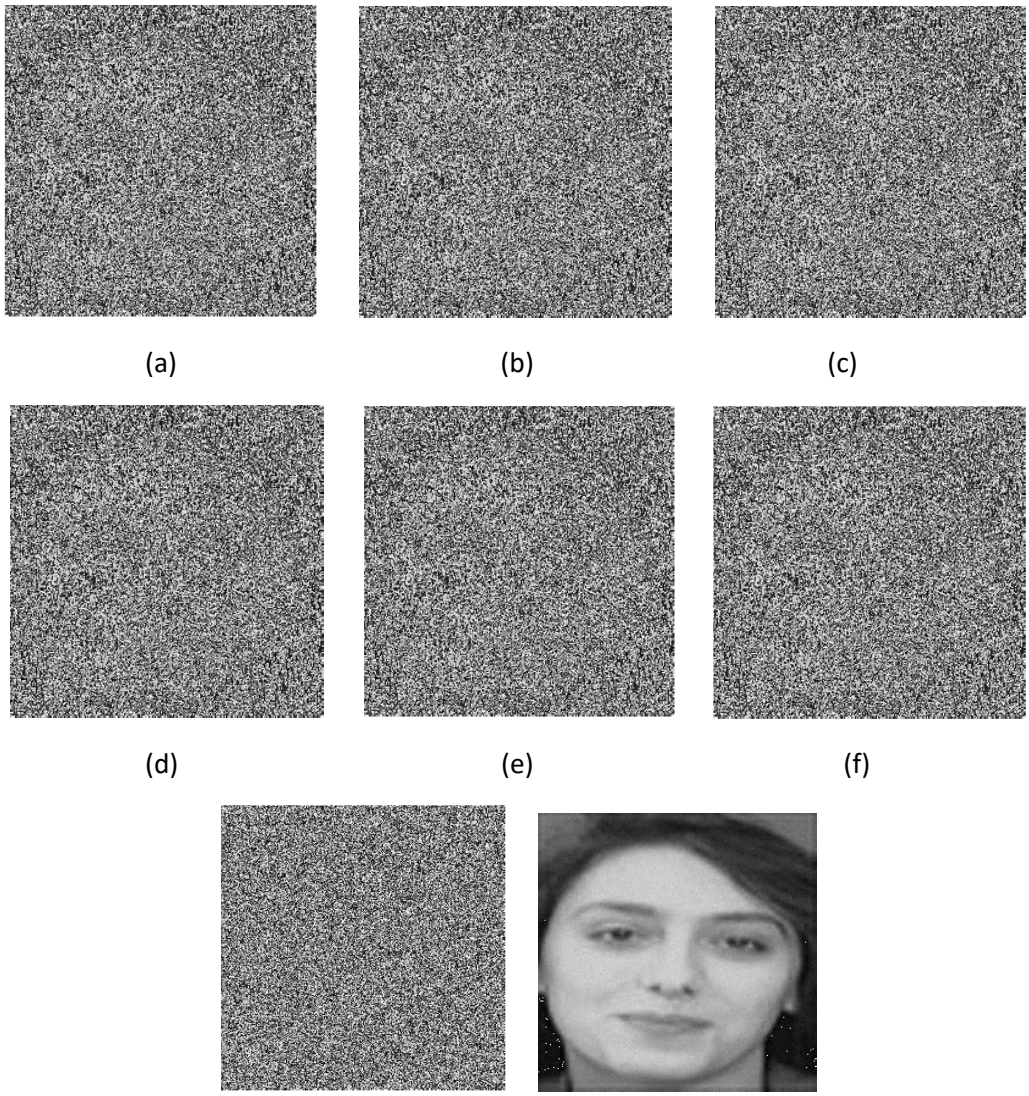


Fig.7 Sensitivity analysis: (a)$x'_0 = x_0 + 10^{-16}(b)\ r'_0 = r_0 + 10^{-15}$ (c)$x'_1 = x_1 + 10^{-16}(d)\ r'_1 = r_1 + 10^{-15}$ (e)$x'_2 = x_2 + 10^{-16}(f)\ r'_2 = r_2 + 10^{-15}$ (g) Decrypted Face2 with wrong fingerprint (h) Decrypted Face2 with correct fingerprint.

V. CONCLUSION

In this manuscript we have proposed a biometric face encryption scheme based on chaotic functions and permutation diffusion architecture. .Moreover, we carried out the permutation phase according to an ascending order given by the fingerprint of the face of the person to be encrypted. The simulation results using the various performance measures proved the effectiveness of the proposed scheme and also confirmed its robustness against cryptographic attacks carried out.

ACKNOWLEDGMENT

The authors would like to thank the General Directorate for Scientific Research and Technological Development of the Algerian Republic in general, LEPCI laboratory of Setif university.

REFERENCES

[1] J. A. P. Artiles, D. P. B.Chaves, C.Pimentel,"Robust image watermarking algorithm using chaotic sequences," *Journal of Information Security and Applications* ., vol. 68, pp.103219,Aug.2022.

[2] P. C. Mandal, I.Mukherjee, G.Paul, and B. N. Chaterji,"Digital image steganography: A literature survey," *Information sciences* ., vol. 609, pp.1451-1488,Sep.2022.

[3] A. Yahi, T.Bekkouche, M. El Hossine. Daachi, and N. Diffellah,"A color image encryption scheme based on 1D cubic map,"*Optik.*, vol. 249, pp.168290,Jan.2022.

[4] A. K. Trivedi, D. M. Thounaojam, S. Pal, "Non-Invertible cancelable fingerprint template for fingerprint biometric,"*Computers & Security.*, vol. 90, pp.101690,March.2020.

[5] X. Wang, X. Chen., "An image encryption algorithm based on dynamic row scrambling and Zigzag transformation,"*Chaos, Solitons & Fractals.*, vol. 147, pp.110962,June.2021.

[6] L. Xu, X. G. Zhili, J. Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion,"*Optics and Lasers in* E*ngineering.*, vol. 91, pp.41-52,april.2017.

[7] C. Han, "An image encryption algorithm based on modified logistic chaotic map ,"*Optik.*, vol. 181, pp.779-785,March.2019.

[8] Y. Su, W. Xu., T. Li,J.Zhao, and S. Liu, "Optical color image encryption based on fingerprint key and phase-shifting digital holography,"*Optics and Lasers in*

[9] M. A. Ben Farah , R. Gesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation,"*Optics & Lasers* Technology., vol. 121, pp.105777,Jan.2020.

[10] G. Qu, X.Meng, Y. Yin, and al "Optical image encryption based on hadamard single-pixel imaging and Arnold transformation ,"*Optics and Lasers in* E*ngineering.*, vol. 137, pp.106392,Feb.2021.

[11] R. Parvaz , M. Zarebnia, "Acombination chaotic system and application in color image encruption,"*Optics & Lasers* Technology., vol. 101, pp.30-41,May.2018.

[12] T. Bekkouche , S. Bouguezel, "A recursive non-linear pre-encryption for opto-digital double random phase encoding,"*Optik.*, vol. 158, pp.940-950,April.2018.

[13] S. E. Azzoug, S. Bouguezel, "A non-linear preprocessing for opto-digital image encryption using multiple-parameter discrete fractional Fourier transform, *«Optics Communications.*, vol. 359, pp.85-94,Jan.2016.

[14] J. Lang, R. Tao, Y. Wang "Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function,"*Optics Communications.*, vol. 283, pp.85-94,May.2010.

[15] https://paperswithcode.com/dataset/orl

[16] http://www.comp.polyu.edu.hk/~csajaykr/myhome/database_request/ContactlessFP/