All Sciences Proceedings

1st International Conference on Pioneer and Innovative Studies

June 5-7, 2023 : Konya, Turkey

ICPIS

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

https://as-proceeding.com/index.php/icpis

Encryption face area in color images using Chaotic Maps

Imane Kouadra*, Mehamal Bouchra, Tewfik Bekkouche and Lahcene Ziet

Department of electronics/LEPCI Laboratory, University of Ferhat Abbes Setif1, Algeria
Department of Electronics/LEPCI Laboratory, University of Ferhat Abbes Setif1, Algeria
Department of electronics/ETA Laboratory, University Mohamed El Bachir El Ibrahimi of Bordj Bou Arreridj, Algeria
Department of electronics/LEPCI Laboratory, University of Ferhat Abbes Setif1, Algeria

**imane.kouadra@univ-setif.dz*

Abstract **–** This paper introduces a region-based selective image encryption technique using a chaotic approach. The aim is to address the growing need for secure face image transmission and storage in various applications where image information requires protection from unauthorized access. Existing image encryption schemes often rely on generating randomness in the image to hide the content, but they can be time-consuming during the encryption and decryption processes. Therefore, an efficient algorithm is crucial to ensure practicality and effectiveness. To tackle this challenge, the proposed technique focuses on selectively encrypting and reconstructing facial regions in images. By identifying the importance of face images in applications where security is critical, the proposed method offers a targeted approach to encryption. This selective encryption allows for improved efficiency in both encryption and decryption processes, reducing computational complexity and enhancing overall performance. The experiments demonstrate the successful encryption and reconstruction of face images, highlighting the preservation of facial details and the robustness of the encryption against attacks. These results confirm the suitability of the proposed technique for applications that require secure face image transmission and storage.

Keywords –Face Detector, RBG Images, Logistic Maps, Permutation-Diffusion, Encryption Region

I. INTRODUCTION

In keeping with modern technology and information crowding. Communication technology is advancing exponentially [1]. Thanks to developments in almost all scientific fields and the emergence of new relevant applications. What makes the individual in constant need of communication tools is due to the confidentiality and value of the information it carries [2]. Among the most shared and used information, we have text messages, voice messages, images, videos ... etc. Image information exchange is becoming increasingly prevalent in communication systems and social networks [1]. which is exposed to unauthorized uses, which harms information and thus leads to the need to protect it [3]. Digital images are different from textual information due to their high volume of data and redundancy [4]. Several researchers have developed advanced algorithms to improve security and address the shortcomings of spatial image encryption [7]. In the 1960s, meteorologist Edward Lorenz released a new theory to the world, that called chaos theory, known as the "butterfly effect". This theory studies the conduct of dynamical systems, of which Lorenz confirmed that it is impossible to predict the evolution of these long-term systems, without knowing the initial conditions in detail. Chaotic systems are generally characterized by ergodicity, sensitivity to initial conditions, control parameters, and random behavior [5-6]. The use of chaotic maps, including classical ones such as logistic and quadratic maps has shown a precarious robustness in face encryption using the permutation diffusion architecture. Generally securing images is to encrypt the entire image. However, in some cases, encrypting the entire image may result in a large size number of redundant operations. In practice, in

many applications, the individual prefers to protect the private portrait information in the image, so encrypting the entire image would be unnecessary [11]. Therefore, In this context, we propose a Viola-Jones algorithm to detect face region. So much the face is the most modal which ensures the recognition of the publishers. Then chaotic encryption is recommended for this zone using permutation-diffusion operations [12].

Our work is structured into three main sections. Firstly, we focus on detecting the face zone in a color image, followed by its decomposition into three primary zones. Then, in the second section, we delve into the encryption and decryption phase. The third section is dedicated to presenting the simulation results and discussions. We conclude with our findings and discuss possible avenues for further research.

II. PRELIMINARIES

In this section, we will provide definitions for the Logistic chaotic map, a widely utilized concept in this paper. Additionally, we will introduce the permutation-diffusion architecture, as they play a crucial role in our analysis.

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. *Permutation-diffusion Operations*

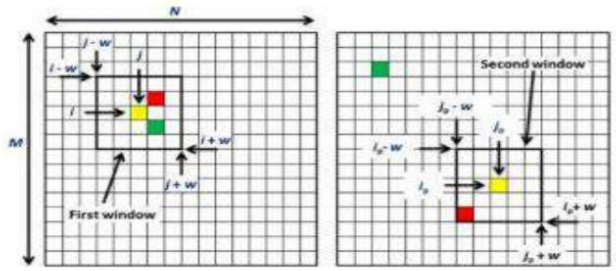

Fig. 1 Pixel permutation

The principle of the permutation or transformation technique is to restructure the arrangement of the pixels by changing their positions according to a predetermined order given by the chaotic map. This makes it possible to satisfy the diffusive property by dispersing the repetitions in the image. Diffusion allows changing of the character of the pixel by applying the XOR operation between the matrix E and the key H as shown in Fig.1 using the following formula:

$$Q(i,j) = \big(E(i,j) \oplus H(i,j)\big) \quad (2)$$

Where:$(i,j) = 1,2,3,\ldots..n$, and $\oplus$ is the XOR operator.

III. ENCRYPTION AND DECRYPTION SCHEMES

The following steps describe the proposed encryption scheme:

- Let Y be the original color image of size $(m,n,3)$.
- We apply the face detection function based on the Viola-Jones algorithm which gave the delimitation face named bbox [bbox (1), bbox (2), bbox (3), bbox (4)].
- Extract the face area with $(m',n',3)$ size called it Z .
- Decompose this face area into three channels Zr, Zg, Zb represented by red channel, green channel, and blue one.
- All processing below is effect by each channel alone.
- Reshape each Z into v vector of length $(1, m' \times n')$.
- Applied permutation-diffusion architecture which consists to generate the first chaotic vector C_0 based on the Logistic map with (x_0, r_0) parameters of length $(1, m' \times n')$.
- 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 here the permutation phase.
- We generate a second 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:

$$y_k = \begin{cases} C_{2_k} \oplus S_{1_k}, & k = 1 \\ C_{2_k} \oplus S_{1_k} \oplus y_{1_{k-1}}, & k = 2, \ldots m' \times n' \end{cases} \quad (3)$$

- Finally, the encrypted image is obtained by reshaping y into an $m' \times n', 3$ matrices. Then, we concatenate the three obtained results and placed them in their shape to get an encrypted face image.

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

IV. RESULTS AND DISCUSSION

The simulation is performed under MATLAB 2016a environment using a personal laptop with 4G RAM memory capacity. The test images are extracted respectively from the databases [13]. We also used the chaotic Logistic map having parameters $(x_0, r_0) = (0.25, 3.99)$ and $(x_1, r_1) = (0.35, 3.99)$. Fig. 2 illustrates the simulation results, in fact, Fig. 2.a represents the original test images. Fig. 2.b represents the areas delimiting the faces of the test images and their corresponding encrypted faces in Fig. 2.c. The location of the encrypted area is well illustrated in the full image in Fig. 2.d.

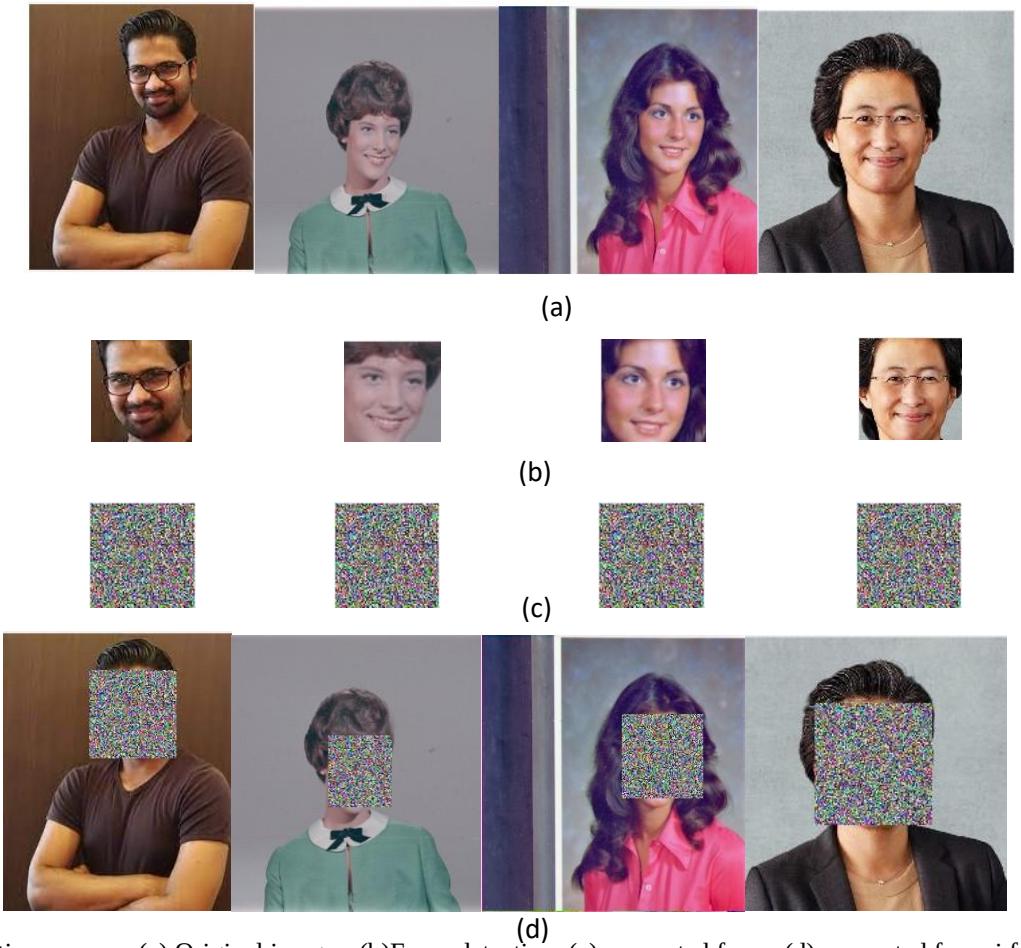

Fig. 2 Encryption process, (a) Original images, (b)Faces detection, (c) encrypted faces, (d) encrypted faces i full images.

To objectively evaluate the proposed algorithm, we have used the following performance measures: the peak signal-to-noise ratio (PSNR) and the correlation rate (Corr2) defined respectively by:

$$PSNR = 10\log_{10}(d^2/MSE) \quad (4)$$

$$MSE = (1/m \times n) \times \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(\mathrm{Z}(i,j) - \mathrm{y}(i,j)\right)^2 \quad (5)$$

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

$$corr_{Zy} = \frac{cov(Z,y)}{\sqrt{D_Z} \times \sqrt{D_Z}} \quad (6)$$

$$E(Z) = \frac{1}{m' \times n'} \times \sum_{i=1}^{N} Z_i \quad (7)$$

$$E(Z) = 1/(m' \times n') \times \sum_{i=1}^{m' \times n'} (Z_i - E(Z))^2 \quad (8)$$

$$cov(Z,y) = \frac{1}{(m' \times n') \times \sum_{i=1}^{m' \times n'} \left(Z_i - E(Z_i) \times \left(Z_i - E(y)\right)\right)} \quad (9)$$

In the following, the faces of Fig. 2.b are denoted from left to right by face1, face2, face3, and face4 respectively. Their corresponding encrypted faces are also shown in Fig. 2.c. Table 1 summarizes the results of calculating the PSNR and the correlation rate between the faces and their encrypted ones. We

clearly notice that the PSNR is of the order of -40dB and the correlation rate is close to zero value commonly for the four cases.

Table 1. Performance measures

	PSNR	MSE	Corr2
Face1	-40.0482	74.9929	0.0009279
Face2	-38.3180	119.2119	0.0073
Face3	-39.6937	112.2490	-0.0147
Face4	-40.2560	119.7424	0.0053

This confirms the degree of degradation caused by the proposed algorithm and proves its efficiency with respect to performance measures.

A. *Histogram analysis*

In this subsection, as illustrated in Fig. 3, we notice that each original face has its own histogram which differs from the others, while the encrypted faces all have the same histogram which looks like uniform white noise. This confirms that a potential attacker cannot derive any information that can reveal the original face. Therefore, we prove the effectiveness of our proposed algorithm against the histogram analysis test.

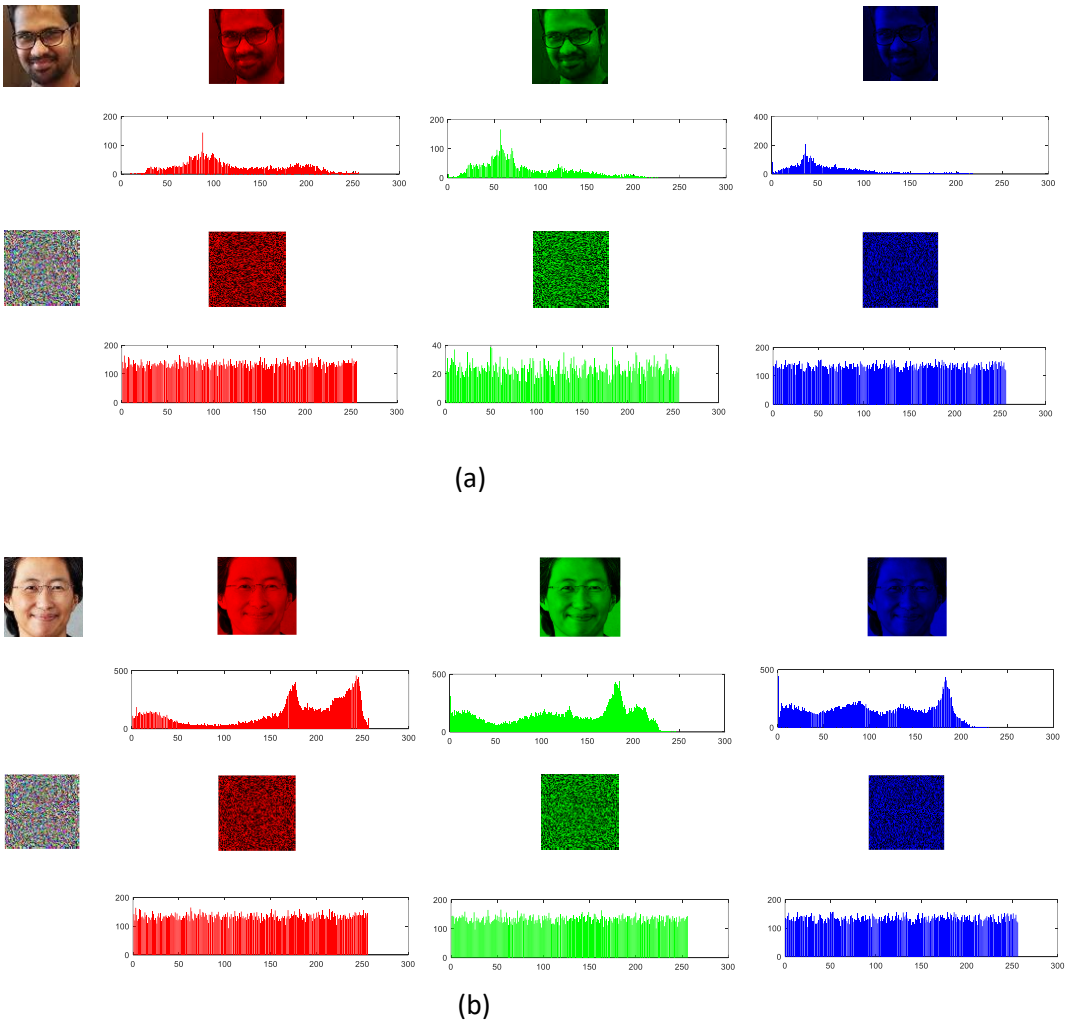

Fig. 3 Histogram analysis: (a) original face 1; its corresponding face 1 encrypted image and their histograms (b) original face 4; its corresponding face 4 encrypted image and their histograms

B. *Loss data test*

In this subsection, we explore the results where a portion of the information is lost while transmitting the encoded image from the sender to the receiver.

Consequently, we examine the impact of this information loss on the quality of the encrypted image. Fig. 4 illustrates various simulations demonstrating different levels of loss (12.5%, 25%, and 50%) in the encrypted image, along with the corresponding encoded images for each loss level. Despite the data loss, the decrypted images remain recognizable up to a certain loss rate. This verifies the resilience of the suggested algorithm in the face of a 75% data loss test.

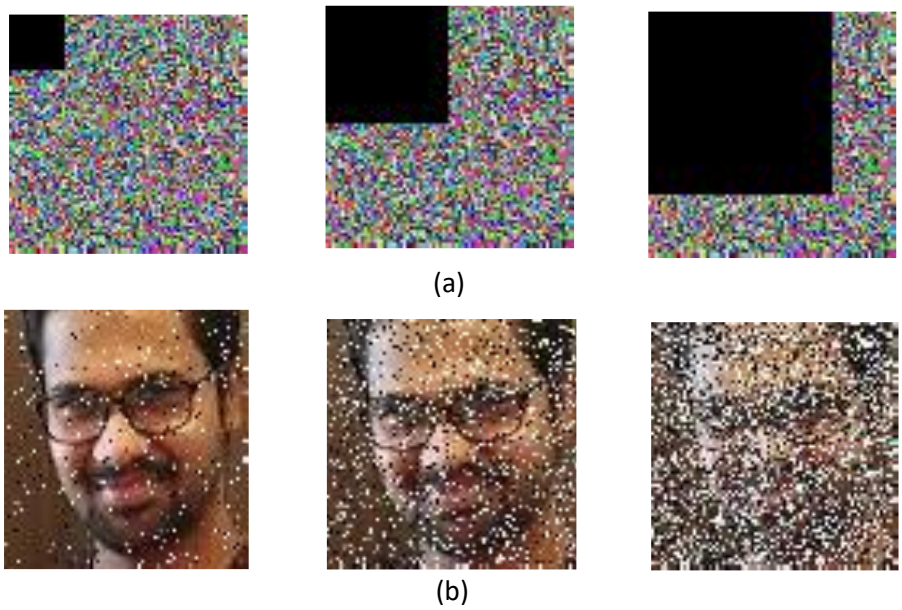

Fig. 4 Loss data test: (a) Encrypted face 1with 12.5% data loss;50% data loss and 75% respectively (b) Their corresponding decrypted faces

C. *Sensitivity analysis*

The encryption key is composed of the parameters x_i , r_i. In our proposed algorithm we assume that the encryption key is designated by $k = (x_0, r_0, x_1, r_1)$, the corresponding decryption key is $k' = (x_0', r_0', x_1', r_1')$. In the case where $k = k'$, the decrypted face is the same as the encrypted one. Now, we assume that one of the key parameters has undergone a variation of $10^{-15}$and the others remain as they are. We will see the impact on the decrypted face following this variation on the encrypted one. We will repeat the same procedure on all the parameters of the key in turn. The Fig. 5 below summarizes the obtained results.

Fig. 5 Sensitivity analysis: Decrypted face 1 with (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) $k = k'$

D. *Keyspace analysis*

For a secure encryption system, it is essential to have sensitivity to secret keys. Sensitivity to secret keys implies that even slight modifications made by an attacker to the keys will render the decryption algorithm unable to retrieve the original image. Regarding the precision of the input field, which is 256, the key space is calculated as follows:

$$(10^{15}) \times (10^{16}) \times (10^{15}) \times (10^{16}) = (10^{62}) \times (2^3) = (2^{186}).$$

This value is deemed sufficient when compared to the required encryption value of (2^{100}).

V. CONCLUSION

In this paper, we proposed a facial encryption algorithm based on the Viola-Jones detection principle. It consists of extracting the face from the entire image and then encrypting the resulting face using the permutation-diffusion architecture. The simulation results performed on several test images have proven the effectiveness of the proposed method against different cryptographic attacks. Even more, the performance measures found also confirmed the reliability and robustness of the proposed algorithm.

ACKNOWLEDGMENT

The authors would like to thank the General Directorate for Scientific Research and Technological Development of the Algerian Republic in general, without forgetting also the material and scientific support of LEPCI and ETA laboratories of Setif and Bordj Bou Arreridj Universities respectively.

REFERENCES

[1] J. Wang, L.Liu, M.Xu, and X.Li " A novel content-selected image encryption algorithm based on the LS chaotic model," *Journal of King Saud University Computer and Information Sciences* ., vol. 34, pp. 8245-8259, Nov.2022.

[2] A. Yahhi,"développement d'Algorithmes de Cryptage d'Images à Base des Suites Chaotiques ," Mthesis,University of mohamed el bachir el ibrahimi, Bordj Bou Areridj, Algeria, Fev. 2023.

[3] P. Murali, G.Niranjana, A.J.Paul,and J.S.Muthu "Domain-flexible selective image encryption based on genetic operations and chaotic maps," *The visual computer* ., vol. 39, pp. 1057–1079, Feb.2022.

[4] 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.

[5] 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.

[6] 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 Engineering.*, vol. 137, pp.106392, Feb. 2021.

[7] 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.

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

[9] G. Ye, and X. Huang, "Spatial image encryption algorithm based on chaotic map and pixel frequency," *science china information sciences*., vol. 61, pp. 058104, Nov.2017.

[10] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new Beta chaotic maps," *Optics and lasers engineering*., vol. 96, pp. 39-49, Sep.2017.

[11] B. Wang, X. Yingjie Xie, C. Zhou, S. Zhou, and X. Zheng "Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps," *Optik*., vol. 127, pp. 3541-3545, Apr.2016.

[12] D. Herbadji, A. Belmeguemia, N. Derouiche, and H. Liu,"Colour image encryption scheme based on enhanced quadratic chaotic map," *IET image processing*., vol. 61, pp. 058104, Jan.2020.

[13] GB. Hung , M.MattarT.Learned-Miller, a data base forstuding face recognition in unconstrained environments.