MALAYSIAN JOURNAL OF COMPUTING AND APPLIED MATHEMATICS (2020) 3 (2) 54-59

DOI: *https://doi.org/10.37231/myjcam.2020.3.2.55*

Article: Received 29.08.2020; Accepted 21.11.2020; Published 22.12.2020

A NEW EFFICIENT APPROACH BASED ON CHAOTIC MAP FOR IMAGE ENCRYPTION

Ali HADOUDA[a,✉], Najia TRACHE[b], Mohamed Fayçal KHELFI[c]

[a,b,c]RIIR Laboratory, Faculty of Exact and Applied Sciences, Universite Oran1, BP 1524 El M'Naouer, Oran, Algeria

✉ *alihadouda111@gmail.com*

Abstract: The protection and security of data and information have become of paramount importance in the deferential areas including imaging, so it is best to protect them before transmitting them. Today, various types of techniques and methods based on Chaotic Encryption are used to overcome several types of threats. In this paper, we propose a new efficient image encryption system using a new simple function permutation pixels(confusion) of an image and a chaotic generator map, the proposed cryptosystem based on three steps: confusion, shuffling, diffusion. In the confusion step, the pixels of the original image is swapped by a simple permutation function. In the shuffling step, the confusing image is devised over four blocks as each block of pixels of the image is mixed, allowing to give more unpredictability. In the diffusion step, the shuffling image is diffused by combining chaotic sequence generated from the chaotic generator map used. The evaluation parameters used are: Number of Pixel Rate Changes (NPCR), Unified Average Change Intensity (UACI), Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE).

Keywords: *Image Encryption, Chaotic Generator, Permutation of Pixels, NPCR, UACI*.

1. INTRODUCTION

The security needs of real life always remain increasing. For this reason, many people have developed cryptographic systems to achieve these needs. When we talk about cryptography several interpretations arise which can be used to achieve the flexibility, compliance, and privacy of data that is a requirement in today's systems. Mathematicians and scientists, starting from Shanon's that date back to 1949 [1] have proposed several cryptographic algorithms up to now like AES, DES, RSA [9,10].

All recent work for data security uses Shannon's basic techniques [1,2] that can be classified into two main categories: the transformation of values (confusion) and permutation of positions (diffusion). The combination between them is also possible. Chaos-based encryption algorithms [3] are considered good for practical use as they provide a good combination of high speed, good security, and computational power. Several ways for decreasing effects of Solak's attack or eliminating its possibility were proposed. There are many chaosbased encryption algorithms which introduce the image security in different principle. In [4] A new efficient image cryptosystem based on combination of confusion and diffusion with FRFT to provide the best performance. The proposed algorithm uses Arnold cat map for confusion with the development of a new Henon chaotic map for diffusion in FRFT. In [5] a new method of encryption/decryption based on chaos and confusion-diffusion architecture. They also developed a new algorithm based mostly on two standard chaotic maps, a logistics map, and a sine map. This method is applied for simple and medical images to produce an encrypted image. In [6] they have tried to use a chaotic map to its full potential to build a strong encryption scheme that can withstand any intrusion, and ensure safety of the image. This Image encryption algorithm proposed using mathematical octave tool and verified by the use of a variety of test series.

In [7] a new chaos-based cryptosystem has been proposed for securing images based on Arnold cat map and Henon chaotic map. The Arnold cat map and the Henon map are two discrete chaotic maps that are used in this scheme and the bit shuffling and pixel shuffling are reversible transformations that are performed using the Arnold cat map with various secret parameters. In [8], a new efficient image encryption algorithm using a set of chaotic maps has been proposed, consists of three steps: confusion, shuffling, and

diffusion as shown in Fig. 1. In confusion step, the original image is confused by using Arnold cat chaotic map. In shuffling step, the pixels of the confused image are shuffled to add more randomness. Finally, the shuffled image is diffused by a key image generated by combining sequences generated from set of Henon chaotic maps.

This paper is organized as follows, the next section describes the main structure of the proposed cryptosystem, and in its subsections, the details of the used cryptosystem components are described. Section 3 presents the security and the influence of the change of the pixels on the clear image by the proposed cryptosystem analysis results.

2. THE PROPOSED SCHEME

The proposed encryption as in Fig. 2 shows the block diagram of our proposed encryption which consists of three steps. In the first step, the image pixels of size N*N is confused based on our simple function of permutation developed. In the pixel permutation, the pixels are shuffled without any alteration in value and histogram. Therefore, the initial conditions and control parameters of this function serve as the first secret key (number iterations of permutation on the image pixels). Our new function used is a simple function to swap the pixels (x,y) of the original image in a new pixel location (x',y') in the permuted image as follow:

For each pixel (x,y) :
x'=x+y, y'=x'+x and b(x',y')= a(y,x) where b(x',y') is the new pixels location in the shuffled image b, a(x,y) is the pixels location of the original image a. In the second step [8] the confused image is devised over four blocks, each block of pixels of the confused image is mixed as follow (Fig.1):

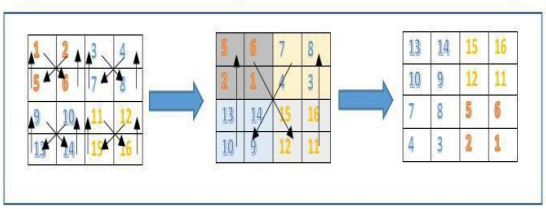


Fig. 1 Pixel shuffling [8].

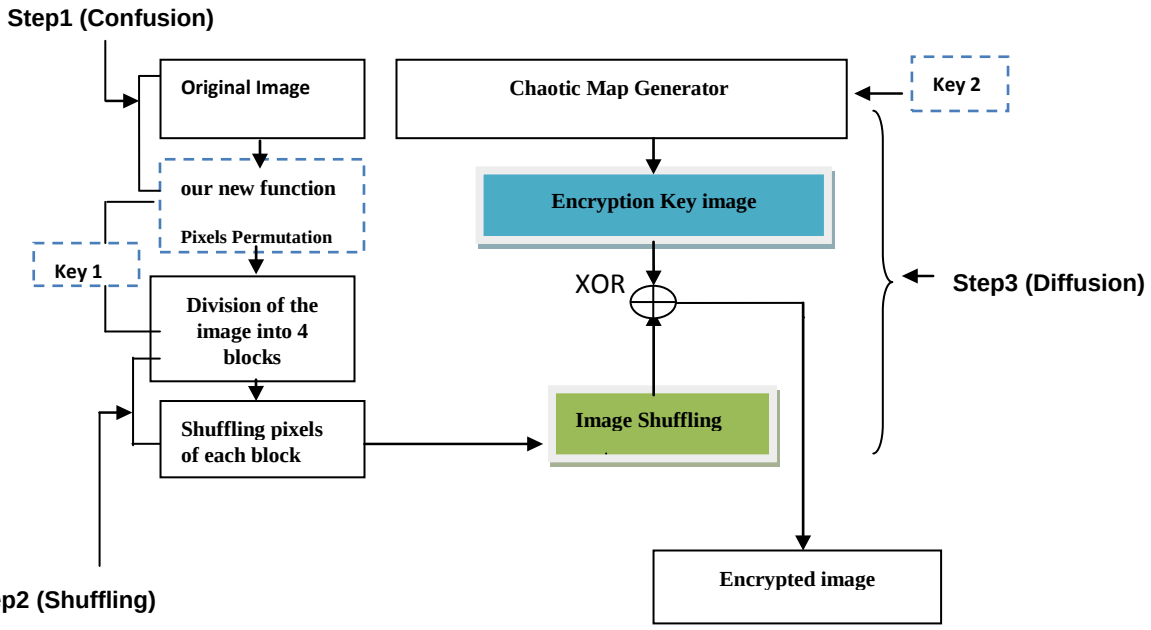


Fig. 2 Our proposed cryptosystem.

Step 1: Divide the image into 4 blocks.
Step 2: Each block is shuffled in a predefined order (e.g. the block (1,2,5,6) is shuffled).
Step 3: Step 2 is repeated until it reaches the last quad.
Step 4: Each entire quad is considered as a single cell and shuffled in a predefined order (e.g entire quad (5,6,2,1)) is shuffled to be (13,14,10,9) as shown in Fig. 2, we have divide the step three into two parts:
1- We adopt a henon chaotic map to generate encryption key images and change the pixel values of the image. The developed Henon chaotic map is obtained by the equation (1)[4]:

$x_{i+1} = (r \times x_i + y_i) \bmod 1$

$y_{i+1} = x_i - b,\ \ i=0,1,2,\ldots$ (1)

where b=0.3, r [0, ∞].The parameter r, the parameter b, initial value x_0 and the initial value x_1 may represent the second key, and the parameters are selected as b=0.3, r=1.4, x_0=0.02, x_1=0.08.
2- The shuffling image is X-ORed with the encryption key image.

3. SECURITY ANALYSIS

A cryptosystem is said to be reliable if one has the possibility of resisting attacks from intruders, interceptors or any other form of enemies. In this article, we will evaluate the security of crypto by several families of cryptoanalytic:

A- NPCR and UACI Analysis:

NPCR means the change rate of the number of pixels of the cipher image when only one pixel of the plain image is modified. the unified average changing intensity, (UACI) measures the average intensity of differences between the plain image and ciphered image, The NPCR and UACI of these two images are defined in equations (4), (5) [11,12]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\ \% \qquad (2)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\ \% \qquad (3)$$

where D(i,j) is defined as

$$D(i,j) = \begin{cases} 0, & if\ (C_1(i,j) = C_2(i,j)) \\ 1, & if\ (C_1(i,j) \neq C_2(i,j)) \end{cases}$$

W and H are the width and height of encrypted image $C_1(i,j)$ and $C_2(i,j)$, are the pixel's value of the original and the encrypted image respectively.

B-Histogram:

To prevent the access of information to attackers, it is important to ensure that encrypted and original images do not have any statistical similarities. The histogram analysis clarifies how the pixel values of image are distributed. We test the histogram analysis of the proposed encryption algorithm using five plain images as shown in Fig. 3 [15].

4. ANALYSIS & QUALITY PERFORMANCE MEASURES

PSNR and MSE Analysis [13,14]**:**

A. Peak Signal to Noise Ratio (PSNR):

PSNR is the ratio between the most feasible power of a signal and the power of damage noise that change the reliability of its representation. Because many signals have an extremely wide dynamic range, PSNR is usually specified in terms of the logarithmic decibel (dB) scale. The PSNR can be computed as follows:

$$PSNR = 10 \times \log_{10} \frac{255 \times 255}{\frac{1}{H \times W} \sum_{X=0}^{H-1} \sum_{y=0}^{W-1} [f(x,y) - g(x,y)]^2} \quad (4)$$

where H and W area part of the height and widthof the image, severally; and f(x,y) and g(x,y) area section the graylevels situated at coordinate (x,y) of the first image and attacked image, respectively.

B. Mean Square Error (MSE):

It is considered as an average squared difference between the original image and distorted image. It is calculated by the formula given below:

$$MSE = \frac{1}{n} \sum_{i=1}^{n} (\hat{Y}_i - Y_i)^2 \quad (5)$$

where, $\hat{Y}_i$ is the distorted image and the Y is the original image[14].

5. EXPERIMENTAL RESULTS

The proposed algorithm uses only one round for confusion, pixel shuffling and diffusion. All the simulation experiments have been carried out using MATLAB R2014a on Core i3, 4 GB RAM PC. The number of shuffled blocks in the shuffling stage is 64, and the number iterations of permutation on the image pixels is 5. The following experiment used four images (Lena, Cameraman, Pepper, and House). These images encrypted with their resolution 256*256.

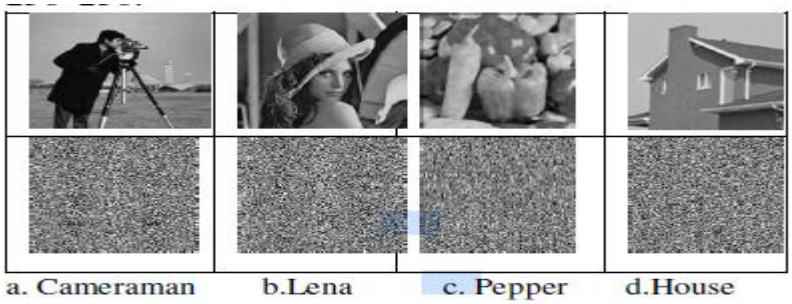
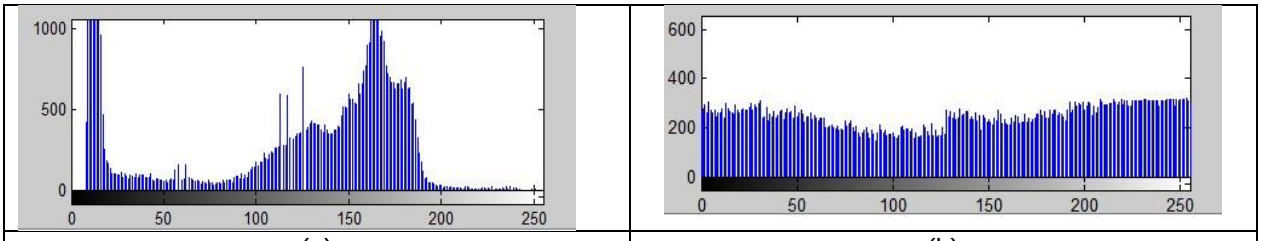


Fig. 3. Original and Encrypted Images



(a) (b)

Fig 4. Histogram Analysis ((a) original image, (b) encrypted image)

Table 1. NPCR and UACI Analysis

image	NPCR (**Our**)	UACI (**Our**)	NPCR **Ref.[6]**	UACI **Ref.[6]**
Cameraman	99,64%	32,11%	99.30	33.65

Lena	99,62%	31,29%	99.61	33.50
Pepper	99,65%	31,20%	99.56	33.46
House	99,63%	28,97%	99.58	33.48

Table 2. PSNR and MSE (after encryption)

image	PSNR (db)	MSE
Cameraman	35.47	2.8347×10^{-4}
Lena	31.83	6.5482×10^{-4}
Pepper	32.49	$2{,}1\times 10^{4}$
House	31.20	7.5735×10^{-4}

Tables 1 and 2 shows that the result obtained by our cryptosystem is better than the results found by [6].

6. CONCLUSION

In this paper, we have designed and tested an effective new approach based on three steps. The cryptosystem proposed uses a simple function of permutation of the pixels of the image and the characteristics of the high sensitivity of the chaotic systems for the initial values by producing the secret key of the chaotic generator usable in our cryptosystem. The results of the security analysis of four images demonstrate the resistance of our cryptosystem. For our future work, we will use our proposed cryptosystem in this paper in the image watermarking.

References

[1]. Shannon, C E. Communication theory of secrecy system, Bell System Technical Journal, 1949, 28:656-715.
[2]. Yang, M, Bourbakis, N and Li, S. Data-image-video encryption, in IEEE Potentials, 2004, 23(3):28-34.
[3]. Gao, T, Chen, Z. A new image encryption algorithm based on hyper-chaos, Physics Letters A, 2008, 372(4):394–400.
[4]. Mursi, M F M, Ahmed, H E H, El-samie, F E A, El-aziem, A H A. Image Encryption Based on Development of Hénon Chaotic Maps Using Fractional Fourier Transform, International Journal of Strategic Information Technology and Applications, 2014, 5(3): 98-106.
[5]. Madani, M, Bentoutou, Y. Cryptage d'images médicales à la base des cartes chaotiques, International Conference Colloque Tassili SCCIBOV, (2015).
[6]. Mondal, B, Mandal, T. A Nobel Chaos based Secure Image Encryption Algorithm, International Journal of Applied Engineering Research, 2016, 11(5):3120-3127.
[7]. Soleymani, A, Nordin, M J. and Sundararajan, E. A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map, The Scientific World Journal, 2014, 2014, Article ID 536930, 21 pages.
[8]. Abdullah, H N, Abdulkareem H. Image Encryption Using Hybrid Chaotic Map, International Conference on Current Research in Computer Science and Information Technology (ICCIT), Slemani, Iraq. 2017.
[9]. Mahajan, P, Sachdeva A. A Study of Encryption Algorithms AES, DES and RSA for Security, Global Journal of Computer Science and Technology Network, Web & Security, 2013, 13.
[10]. Preetha M, Nithya M. A Study and Performance Analysis of RSA Algorithm, International Journal of Computer Science and Mobile Computing, 2013. 2(6):126 – 139.
[11]. Kwok, H S, Tang, W K S. A fast image encryption system based on chaotic maps with finite Precision representation, Chaos Solitons Fractals, 2007, 32(4):1518–1529.
[12]. Borujeni, S E, Eshghi, M. Chaotic image encryption design using tompkins-paige algorithm, Hindawi Publishing Corporation Mathematical Problem in Engineering, 2009, Article ID 762652, 22 pages.

[13]. Saini, L K, Shrivastava, V. Survey of Digital Watermarking techniques and its Applications, International Journal of Computer Science Trend and Technology, 2014, 5(3):70-73.
[14]. Kalra, G S, Talwar, R, Sadawarti, H. Comparative Analysis of Blind Digital Image Watermarking Utilising Dual Encryption Technique in Frequency Domains, World Journal of Computer Application and Technology, 2013, 1(2): 35-40.
[15]. Mohamed, M A, Abdel-Atty H M, Aboutaleb, A M, Abdel-Fattah, M G, Samrah, A S. Hybrid Watermarking Scheme for Copyright Protection using Chaotic Maps Cryptography, International Journal of Computer Applications, 2015, 126(4):13-26.