All Sciences Proceedings

1st International Conference on Modern and Advanced Research

July 29-31, 2023 : Konya, Turkey

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

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

An Algorithm for Image encryption based on chaotic maps

Herbadji Djamel[1] , Herbadji Abdarrahmane[1], Ismail Haddad[3] , Belmeguenaï Aïssa[3] ,Nadir Derouiche[3] , Hichem Kahia[4]

[1]*Independent Researcher, Algeria*
[3] *Laboratoire de Recherche en Electronique de Skikda, Universit´e 20 Aout 1955 Skikda, ˆ BP 26 Route d'El-hadaeik, Skikda 21000, Algeria*

[*]*(herbadjidjamel@gmail.com)*

Abstract – In recent years, the use of chaotic maps in encryption has become an attractive research area, due to the advantages of chaotic maps that make it suitable for use in cryptography. In this paper we present a new image encryption algorithm based on dividing the image into four equal elements, where the direction and the key of encryption of each element is different from other ones. Firstly, Arnold s Cat Map is used to permute the positions of the image pixels. Secondly, the permutated image is divided into four equal elements; thirdly, the content of each image element is diffused by performing the XOR bit operation among two image elements sequentially. Finally, the first element of the produced image is diffused by using the Henon Map. Each element is diffused by performing the XOR bit operation with the element that came before it. The decryption operation uses the secret key and the first element permutated to decrypt the encryption image to obtain the original image. The algorithm is validated using security analysis, and the experimental results demonstrate that the algorithm is simple and effective.

Keywords – Encryption , Chaos

I. INTRODUCTION

Nowadays, Technology plays a crucial role in everyday life, especially the internet. The internet is now widely used by most people for a wide range of services, including sharing information. It has been applied in several areas as an essential infrastructure for businesses and institutions in a wide range of sectors, such as healthcare, energy and transport.

The transmission of digital information requires great secrecy especially for digital images, knowing that the internet does not provide the necessary protection for the transmitted information. This has led to the encryption of digital images in order to ensure more secure transmission via the internet.

Encryption means changing information or data from its original formula to another type of information completely different from the first one [1]. The use of traditional encryption algorithms such as Rivest-Shamir-Adleman (RSA), advanced encryption standard (AES) and data encryption standard (DES) have become insufficient to encrypt a digital image[2] ,due to its special features such as huge data flow and interdependence between the pixels of the digital image [1][3] [4].Therefore many researchers have proposed several digital image encryption algorithms to prevent unauthorized access. Among the most widely used and known methods of encryption are the methods adopted on chaos due to their features such as randomness and its high sensitivity to initial conditions and control parameters, non-linear dynamic system and unpredictable manners[5].

Many researchers have been suggested different image encryption algorithms based on Chaos[1-11] .Zang et al. [6] proposed a multiple-image encryption algorithm based on mixed image element and permutation .Rim Zahmoul et al. [7]

proposed image encryption based on new Beta chaotic maps. Asia Mahdi et al. [8] proposed a Color Image Encryption and Decryption using Pixel Shuffling with the Henon Chaotic System. Yannick Abanda et al. [9]proposed a Image encryption by chaos mixing.

This work proposes a new algorithm to the encryption of image intended to be transferred on an insecure channel. The algorithm is simple and very easy to implement for image encryption and decryption.

This paper is organized as follows; the first section is a historical introduction, the second section presents the chaotic maps. In the third section we will present with details the new proposed image algorithm. In the fourth section we present the experimental results and finally the conclusion is given in section 5.

II. CHAOTIC MAPS

A. Arnold Cat Map System

Arnold's Cat Map transformation is used to permute the pixels of image; this map is defined by[10].

$$\begin{pmatrix} x\prime \\ y\prime \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & p*q+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod\ N. \quad (1)$$

where p and q are control parameters, N is the number of pixels in one row of the image, I_{N*M}, x and y are the original location of the image pixel and, x' and y' are new location of the image pixel. A permitted image can be obtained by iterating M*N times, where M*N is the size of the image I_{N*M}.

B. Henon Chaotic System

Henon Chaotic System is used to generate Pseudo-random sequence, by iterating r*c times, where ($r = \frac{M}{2}, c = \frac{N}{2}$) and M*N is the size of the original image IN*M., M*N is the size of the image IN*M.

This map is given by the following equation [11].

$$\begin{cases} x_{n+1} = 1 - ax^2{}_n + y_n \\ y_{n+1} = bx_n \end{cases} \quad (2)$$

Where a and b are the control parameters which are regarded as secrete keys, x_0, y_0 are the initial values.

III. THE PROPOSED ENCRYPTION ALGORITHM

A. Generating Key by Chaos

To encrypt the original images, we generate a Chaotic matrix a chaotic K_{r*c} can be generated by the Henon Chaotic system.

This is obtained by using Equation (2) .

Step 1: Choosing the initial values of the Henon Chaotic system, and the number of the iteration is r * c, a chaotic sequence X= { x_1 , $x_{2,\ldots\ldots}$ X_{r*c} } .

Step 2: Generating a chaotic integer sequence by using Equation (3).

$$Y_i = floor\ [(x_i * 10^{14}) \bmod 256]. \quad (3).$$

Where $x_i \in X$ and i =1,2,…, r*c.

Step 3: Convert the consequence of the integer values Y to matrix K_{r*c}.

A. Algorithm of image encryption

Fig. 1 and Fig. 2 illustrate the block diagram of the proposed algorithm. The encryption direction of each element of the image as follows:

Step 1: Generating the permutation.

Arnold's Cat Map is used to permute the pixels' location by using Equation (1) ,the iteration number is m*n.

Step 2: Divide the permuted image into four equal elements I^1_{r*c} , I^2_{r*c} , I^3_{r*c} , I^4_{r*c} .

Step 3 : Encrypting each element with the element which is adjoined to it with $\oplus$ operation to obtain cipher image elements I'^1_{r*c} , I'^2_{r*c} , I'^3_{r*c} , I'^4_{r*c} .

The ciphering direction of each element is Different from the other element as shown in Fig. 1.

To encrypt the content of image elements, we calculate:

$I'^1_{r*c} = I^1_{r*c} \oplus I^2_{r*c}$.

$I'^2_{r*c} = I^2_{r*c} \oplus I^4_{r*c}$.

$I'^3_{r*c} = I^3_{r*c} \oplus I^1_{r*c}$.

$I'^4_{r*c} = I^4_{r*c} \oplus I^3_{r*c}$.

Step 4: Encryption of the content of each element of the image resulting from the previous step with $\oplus$ operation to obtain cipher image elements J^1_{r*c} , J^2_{r*c} , J^3_{r*c} , J^4_{r*c} . The ciphering direction of each element is defined from the other part as shown in Fig. 1 as:

$$J^1_{r*c} = I'^1_{r*c} \oplus K_{r*c} \quad .$$

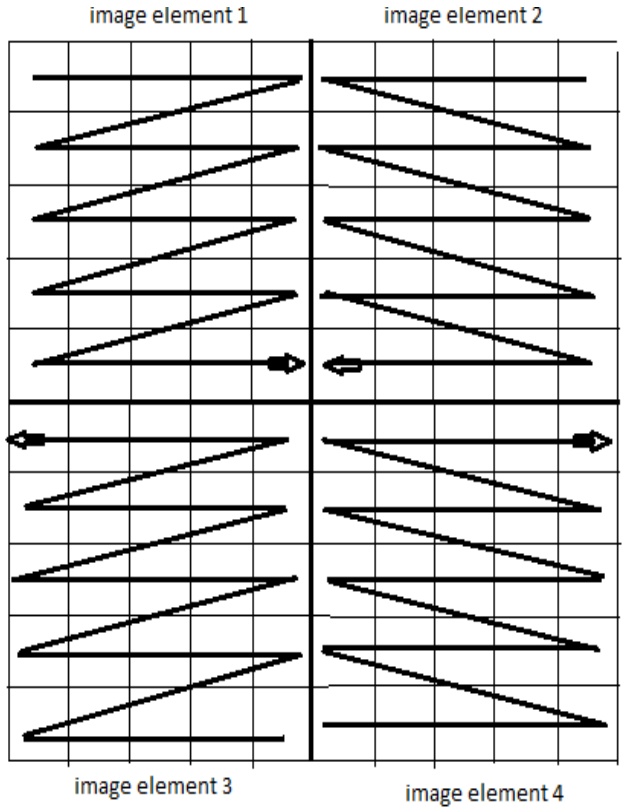
$$J^4_{r*c} = I'^4_{r*c} \oplus J^1_{r*c} \quad .$$

$$J^3_{r*c} = I'^3_{r*c} \oplus J^4_{r*c} \quad .$$

$$J^2_{r*c} = I'^2_{r*c} \oplus J^3_{r*c} \quad .$$

Where $\oplus$ is the XOR bit operation between two element of the image, and J^1_{r*c} , J^2_{r*c} , J^3_{r*c} , J^4_{r*c} .are the encrypted image elements.

Step 5: Combining encrypted image elements.



II. EXPERIMENTAL RESULTS

There are many kinds of attacks, such as statistical attacks and differential attacks[12].

In this section we discuss the performance of the proposed algorithm through the obtained results; we will use some types of tests to measure the performance of the proposed algorithm. These are:

The number of pixel change rate (NPCR), the unified average changing intensity (UACI), the correlation analysis, and the PSNR (Peak Signal to Noise Ratio) and MSE (mean square error) tests and information entropy evaluation.

A. Histogram analysis

The number of pixels corresponding to each color intensity and the distribution of the pixels in an image are represented by a histogram [13].

From the histograms of Fig. 4, used for the analysis, this figure shows clearly move of the encrypted image towards a uniform distribution. Thus, the difference from the original image is very significant.

Therefore the histogram of the encrypted image does not contain statistical information for use in statistical attacks.

B. Correlation coefficient

The similarity degree between two variables is indicated by correlation methods[14]. This coefficient is particularly useful for computing the cryptosystem's quality, Correlation coefficient is given by [15][16], [17].

$$corr = \frac{cov(x,y)}{\sqrt{D(x)D(Y)}} \quad (3)$$

Where X and Yare the sets composed of N pixel gray values, $x_i \in X$ and $y_i \in Y$, are two adjacent pixels,

$$E(X) = \frac{1}{N}\sum_{i=1}^{N} x_i, \quad D(X) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(X)]^2$$

and

$$cov(X,Y) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(X)][y_i - E(Y)].$$

Table 1 shows that the obtained correlation coefficients of the encrypted image are quite close to the value of 0, while correlation coefficients of the original image are quite close to the value of 1, thus, the encrypted image the highly independent of the original image. Therefore, the proposed algorithm secures the images against statistical attacks.

Table 1: Correlation coefficients of adjacent pixels.

image	Direction	original image	Encrypted image	(Ref.[4])
Elaine	Horizontal	0.985	-0.0015	0.0003
	Vertical	0.983	**-0.0011**	−0.0010
	Diagonal	0.974	**-0.0015**	0.0043
Boat	Horizontal	0.9381	-0.0016	0.0003
	Vertical	0.9713	**-0.0029**	0.0020
	Diagonal	0.9221	**-0.0016**	0.0043
Baboon	Horizontal	0.8665	**-0.0032**	−0.0033
	Vertical	0.7586	**-0.0018**	0.0021
	Diagonal	0.7261	**-0.0019**	0.0057

C. Information Entropy

The entropy of image determines how the pixel values are distributed. If the image pixel values are completely random, the value of entropy is 8, which is the ideal value [9] [18].

The information entropy is given by the following formula:

$$E(m) = -\sum_{i=0}^{255} \Pr(mi) \log_2 \Pr(mi) . \quad (4)$$

Where Pr(mi) denotes the probability of symbol mi .The expression of entropy is in bits.

Table 2 shows that the obtained Information Entropy of encrypted image are quite close to the theoretical value is 8, Therefore , the proposed encryption method is secure upon the entropy attack.

Table 2: Information Entropy Analysis of various Images

Image	Original	Encrypted	(Ref. [4])	(Ref. [5])
Boat	7.1914	**7.9993**	7.9992	7.9993
Man	7.1925	7.9992	-	7.9998
Elaine	7.504	**7.9992**	7.9992	7.9992
Baboon	7.357	**7.9994**	7.9993	-
Lena	7.2894	**7.9992**	-	7.9991
Couple	7.0543	7.9992	7.9994	7.9993

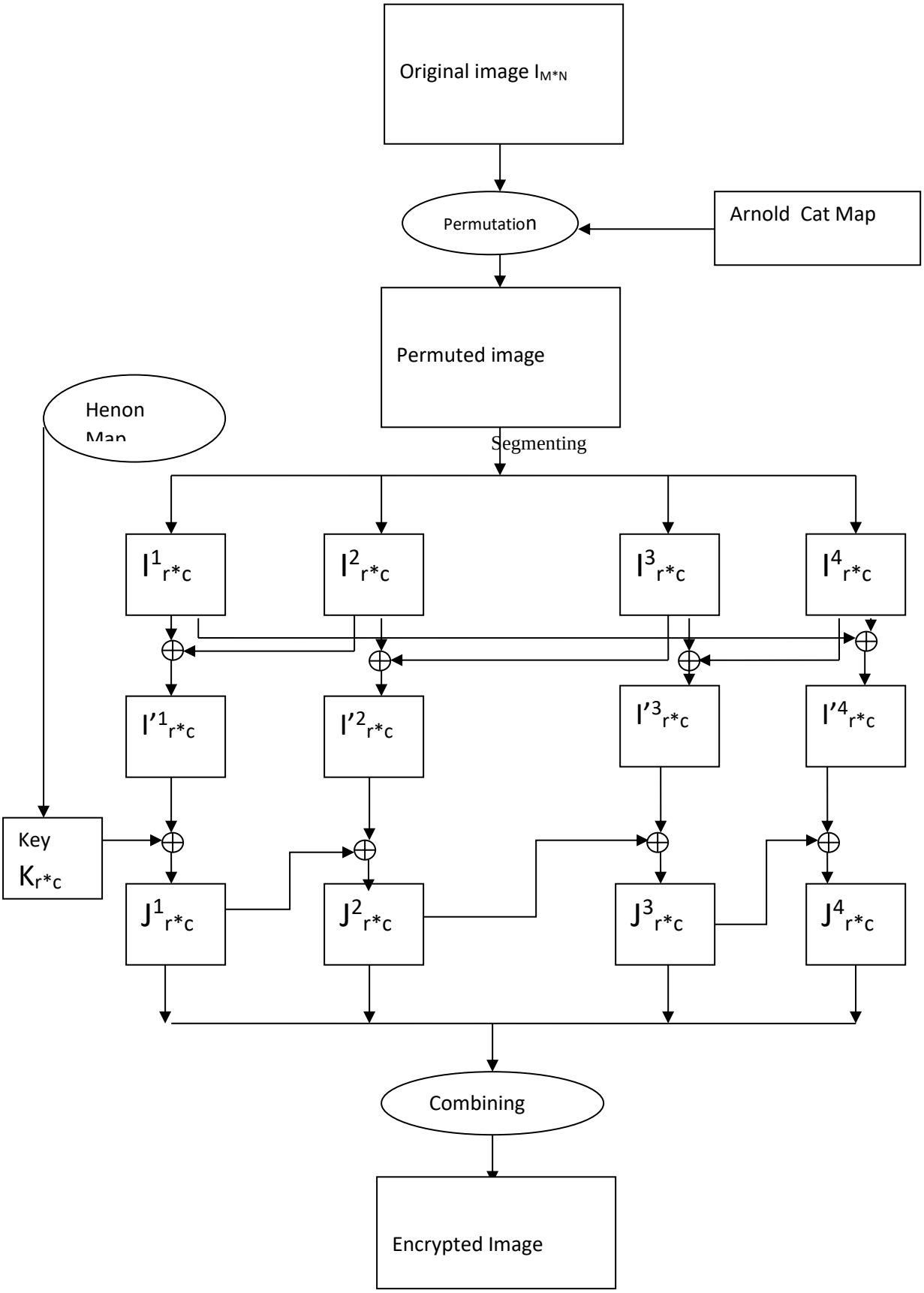


Fig.2. Block diagram of proposed Image encryption scheme

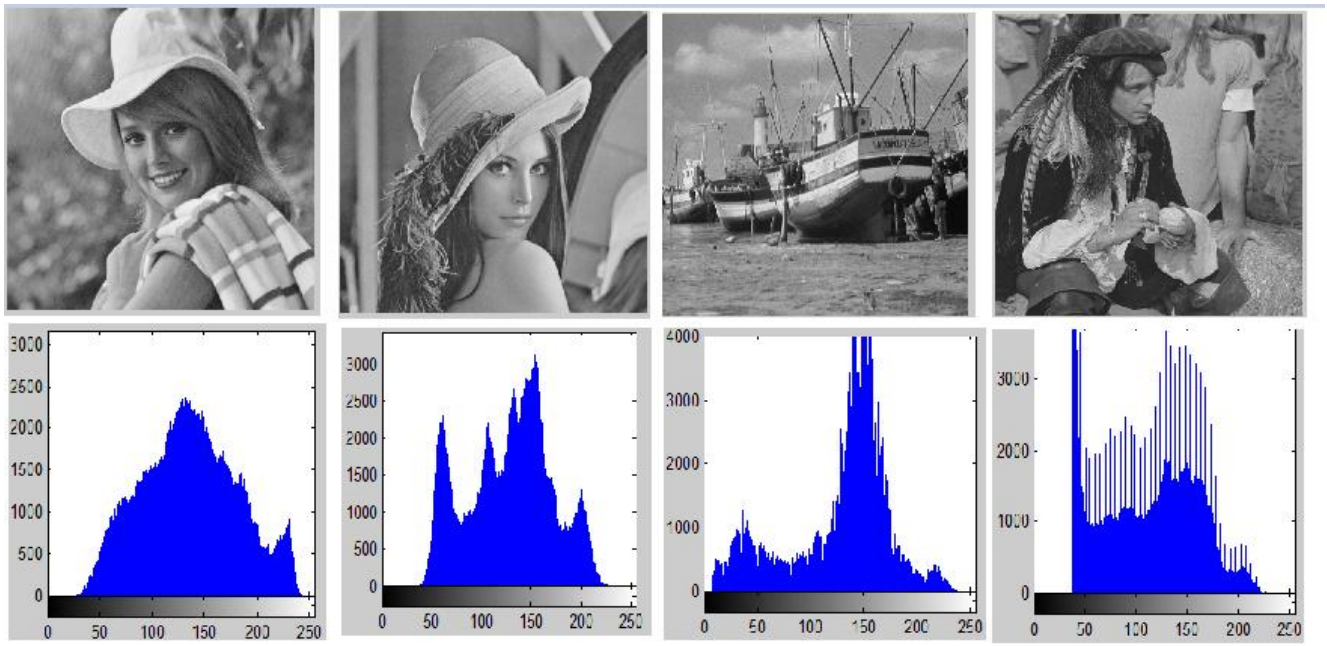


Fig. 3.Respectively : original images of ‘Elaine’, ‘lena’, ‘Boat’, ‘Man’ and their histograms.

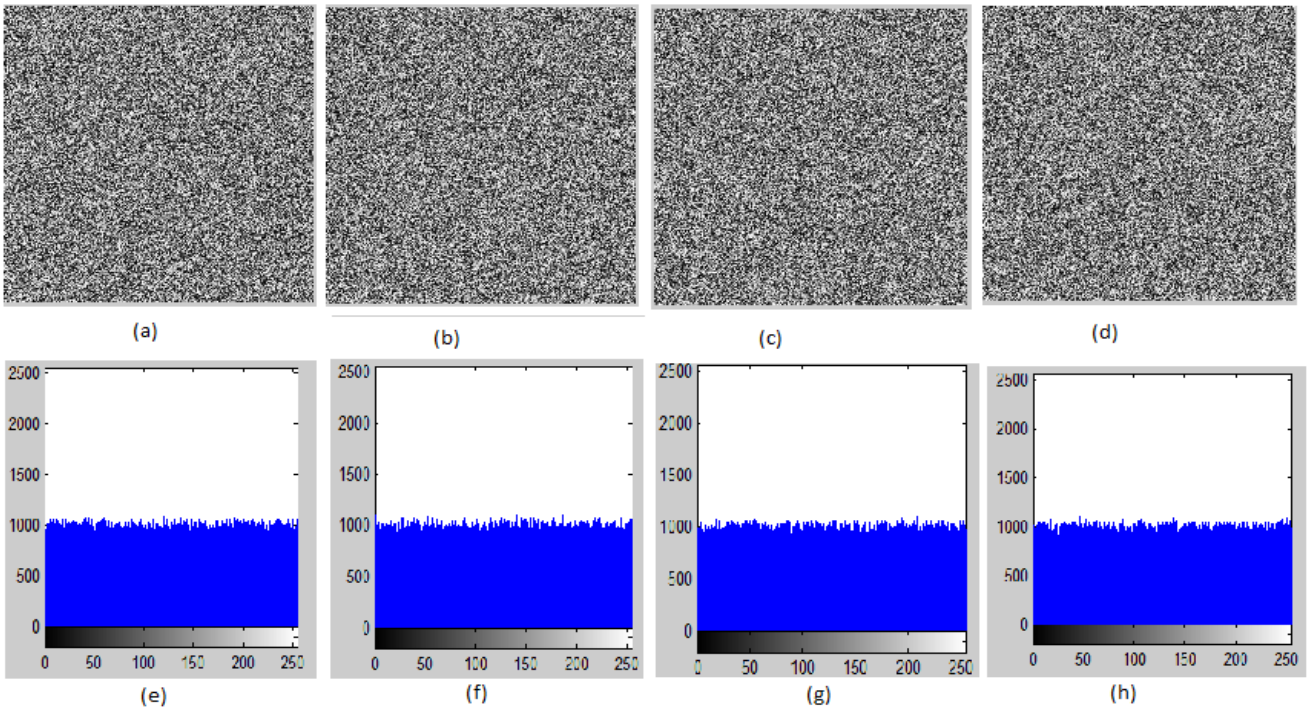


Fig. 4.Respectively(from left to right): encrypted images of ‘Elaine’, ‘lena’, ‘Boat’, ‘Man’ and their histograms.

D. NPCR and UACI tests

The Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are two percentages used to determine the effect of changing the value of one pixel from the original image to the encryption image [19] .

The NPCR of these two images is defined by:

$$NPCR(M\ C) = \frac{1}{h*w}\sum_{i\ j} D(i,j) * 100\%. \quad (5)$$

Where D(i, j) = 0, if C_1(i, j) = C_2(i, j) and

D(i, j) = 1, if C_1(i, j) $\neq$ C_2(i, j), C_1(i, j) and C_2(i, j) , whose corresponding original image have only one pixel difference [12].

The differences in average intensity between the encrypted image and the original image is measured using UACI (Unified Average Changing Intensity) which can be computed with the following formula [12][20]:

$$UACI = \frac{1}{h*w}\sum_{i\ j} \frac{D(i\ j)}{255} * 100\%. \quad (6)$$

Table 3 and 4 give the test results of NPCR(%) and UACI(%).

The results proved the effectiveness of the algorithm against differential attacks, because the resulting values are within the values found in[21]

Table 3: NPCR of Various Images

image	Our Algorithm	(Ref. [4])	(Ref. [5])
Boat	99.60%	99.60%	99.62%
Elaine	99.59%	99.61%	99.62%
Lena	99.60%	%	99.62%

Table 4: UACI of Various Images

image	Our Algorithm	(Ref. [4])	(Ref. [5])
Boat	28.98%	33.49%	33.51%
Elaine	28.50%	33.44%	33.47%
Lena	28.61%	%	33.48%

E. Key space analysis

A good encryption system, the key space size must be sufficient large to grant the success of brute- force attacks, the key space for the algorithm is the total number of keys is used in the encryption process. This proposed algorithm has following secret keys: the initial values x_0,y_0 and control parameters a ,b of the Henon Chaotic System, control parameters p, q of the Arnold's Cat Map. For a sufficient security to make the brute-force attack infeasible ,the key space size should be k > 2^{100} [22][23].

Supposing that the keys precision is 10^{-15}, so the final key space is $10^{15*6} = 10^{90}$. Therefore, this final key space size is large enough to resist the brute-force attack.

F. Peak signal to noise ratio analysis

The Peak Signal to Noise Ratio (PSNR) is one of the most important measurements are used to evaluate an encryption quality[24]. It is used to calculate the difference between the pixels of the original image and the encrypted image depending on the Mean Square Error (MSE) [14],

PSNR is defined as decibel scale; MSE and PSNR are denoted by:

$$MSE = \frac{1}{m*n}\sum_{i=1}^{n}\sum_{j=1}^{m}\big(C(i,j) - M(i,j)\big)^2 \quad (6).$$

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \quad (7).$$

Where M(i, j) and C(i, j) are the gray level of the pixels at the i-th row and j-th column of a m*n original image and encrypted image, respectively. The lower value of PSNR represents better encryption quality.

Table 5: PSNR values of encrypted image

Images	PSNR (our new approach)	PSNR(Ref. [5])
Boat	**9.29**	9.40
Man	9.10	8.04
Baboon	9.50	-
Elaine	**9.27**	9.32
Couple	**7.25**	9.66

Table 4 shows PSNR values that the obtained the PSNR value between the original image and the encrypted, the results demonstrate that the proposed encryption algorithm have a better resistance, due to small PSNR values.

III. CONCLUSION

In this paper, a novel algorithm has been proposed for encryption images by using two Chaotic Maps. Arnold's Cat Map has been used to change the positions of pixels of the image and the Henon Chaotic Map has been used to generate a sequence of random values that use bit XOR operation, for changed pixel value of image.

The image was divided into four equal elements. This paper defines the direction of encryption of each element of the image, and also the key used to encrypt each element of the image.

Differential and statistical analyzes have been conducted, the results demonstrated the robustness of the algorithm against many of the known attacks.

References

[1] M. A. Mokhtar, N. M. Sadek, and A. G. Mohamed, "Design of image encryption algorithm based on different chaotic mapping," in *Radio Science Conference (NRSC), 2017 34th National*, 2017, pp. 197–204.

[2] H. Huang and S. Yang, "Colour image encryption based on logistic mapping and double random-phase encoding," *IET Image Process.*, vol. 11, no. 4, pp. 211–216, 2016.

[3] L. Liu, S. Miao, H. Hu, and M. Cheng, "N-phase logistic chaotic sequence and its application for image encryption," *IET Signal Process.*, vol. 10, no. 9, pp. 1096–1104, 2016, doi: 10.1049/iet-spr.2015.0522.

[4] H. N. Abdullah and H. A. Abdullah, "Image encryption using hybrid chaotic map," in *Current Research in Computer Science and Information Technology (ICCIT), 2017 International Conference on*, 2017, pp. 121–125.

[5] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A Novel Color Image Encryption Scheme Using Rectangular Transform-Enhanced Chaotic Tent Maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.

[6] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on mixed image element and permutation," *Opt. Lasers Eng.*, vol. 92, pp. 6–16, 2017.

[7] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new Beta chaotic maps," *Opt. Lasers Eng.*, vol. 96, pp. 39–49, 2017.

[8] A. Mahdi, N. Alzubaidi, and N. D. K. Al-shakarchy, "Color Image Encryption and Decryption Based Pixel Shuffling with 3D Blowfish Algorithm," vol. 3, no. 7, pp. 336–343, 2014.

[9] Y. Abanda and A. Tiedeu, "Image encryption by chaos mixing," *IET Image Process.*, vol. 10, no. 10, pp. 742–750, 2016, doi: 10.1049/iet-ipr.2015.0244.

[10] C. Fu, O. Bian, H. Jiang, L. Ge, and H.-F. Ma, "A new chaos-based image cipher using a hash function," in *Computer and Information Science (ICIS), 2016 IEEE/ACIS 15th International Conference on*, 2016, pp. 1–9.

[11] A. M. N. Alzubaidi, "Color Image Encryption and Decryption using Pixel Shuffling with Henon Chaotic System," *Int. J. Eng.*, vol. 3, no. 3, 2014.

[12] M. Dridi, M. A. Hajjaji, B. Bouallegue, and A. Mtibaa, "Cryptography of medical images based on a combination between chaotic and neural network," *IET Image Process.*, vol. 10, no. 11, pp. 830–839, 2016.

[13] O. P. Verma, M. Nizam, and M. Ahmad, "Modified multi-chaotic systems that are based on pixel shuffle for image encryption," *J. Inf. Process. Syst.*, vol. 9, no. 2, pp. 271–286, 2013.

[14] H. M. Al-Mashhadi and I. Q. Abduljaleel, "Color image encryption using chaotic maps, triangular scrambling, with DNA sequences," in *Current Research in Computer Science and Information Technology (ICCIT), 2017 International Conference on*, 2017, pp. 93–98.

[15] L. Abraham and N. Daniel, "Secure image encryption algorithms: A review," *Entropy*, vol. 100, no. 2, 2013.

[16] D. Herbadji *et al.*, "A New Image Encryption Scheme Using an Enhanced Logistic Map," in *2018 International Conference on Applied Smart Systems (ICASS)*, 2018, pp. 1–6.

[17] D. Herbadji, N. Derouiche, A. Belmeguenai, N. Tahat, and S. Boumerdassi, "A new colour image encryption approach using a combination of two 1D chaotic map," *Int. J. Electron. Secur. Digit. Forensics*, vol. 12, no. 4, pp. 337–356, 2020.

[18] C. Fu, G. Zhang, O. Bian, W. Lei, and H. Ma, "A novel medical image protection scheme using a 3-dimensional chaotic system," *PLoS One*, vol. 9, no. 12, p. e115773, 2014.

[19] A. Belmeguenai, O. Berrak, and K. Mansouri, “Image Encryption using Improved Keystream Generator of Achterbahn-128.,” in *VISIGRAPP (3: VISAPP)*, 2016, pp. 335–341.

[20] D. Herbadji, N. Derouiche, A. Belmeguenai, A. Herbadji, and S. Boumerdassi, “A Tweakable Image Encryption Algorithm Using an Improved Logistic Chaotic Map.,” *Trait. du Signal*, vol. 36, no. 5, pp. 407–417, 2019.

[21] Y. Wu, J. P. Noonan, and S. Agaian, “NPCR and UACI randomness tests for image encryption,” *Cyber journals Multidiscip. journals Sci. Technol. J. Sel. Areas Telecommun.*, pp. 31–38, 2011.

[22] G. Alvarez and S. Li, “Some basic cryptographic requirements for chaos-based cryptosystems,” *Int. J. Bifurc. Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[23] D. Herbadji, A. Belmeguenai, N. Derouiche, and H. Liu, “Colour image encryption scheme based on enhanced quadratic chaotic map,” *IET Image Process.*, vol. 14, no. 1, pp. 40–52, 2020.

[24] M. Dridi, M. A. Hajjaji, and A. Mtibaa, “Hardware implementation of encryption image using Xilinx System Generator,” in *Sciences and Techniques of Automatic Control and Computer Engineering (STA), 2016 17th International Conference on*, 2016, pp. 772–775.