Bulletin of Electrical Engineering and Informatics
Vol. 10, No. 4, August 2021, pp. 2100~2109
ISSN: 2302-9285, DOI: 10.11591/eei.v10i4.2924

Image confusion and diffusion based on multi-chaotic system and mix-column

Amal Abdulbaqi Maryoosh, Zahraa Salah Dhaif, Raniah Ali Mustafa
Computer Science Department, Collage of Education, Mustansiriyah University, Baghdad, Iraq

Article Info

Article history:

Received Mar 3, 2021
Revised May 13, 2021
Accepted Jun 17, 2021

Keywords:

Arnold cat map
Image encryption
Image permutation
Lorenz system
Mix-column

ABSTRACT

In this paper, a new image encryption algorithm based on chaotic cryptography was proposed. The proposed scheme was based on multiple stages of confusion and diffusion. The diffusion process was implemented twice, first, by permuting the pixels of the plain image by using an Arnold cat map and, the second time by permuting the plain image pixels via the proposed permutation algorithm. The confusion process was performed many times, by performing the XOR operation between the two resulted from permuted images, subtracted a random value from all pixels of the image, as well as by implementing the mix column on the resulted image, and by used the Lorenz key to obtain the encrypted image. The security analysis tests that used to exam the results of this encryption method were information entropy, key space analysis, correlation, histogram analysis UACI, and NPCR have shown that the suggested algorithm has been resistant against different types of attacks.

Corresponding Author:

Amal Abdulbaqi Maryoosh
Department of Computer Science
Collage of Education
Mustansiriyah University, Baghdad, Iraq
Email: amalmaryoosh@uomustansiriyah.edu.iq

1. INTRODUCTION

Due to the rapid growth of IT and computer networks, massive quantities of data are being interchanged over different network types. The main portion of transmitted digital data, that has been either private or confidential, needs the security techniques to provide wanted protection. Thus, security became a significant case during the transmission and storage of digital data [1]. Recently, numerous image encryption algorithms that were based on chaos theory have been designed and implemented, because of the desirable features which make them appropriate for image encryption such as pseudorandomness, arbitrary behavior, and sensitivity to control parameters and initial conditions [2].

Recently, several studies have emerged in the field of image encryption using chaotic systems such as, Narendra K. *et al*. [1] who have proposed algorithm for the encryption of gray-level images by the use of a confidential key of 128-bits size. At first, image quality was degraded by mixing up procedure. The resulting image was separated to key dependent dynamic blocks and, furthermore, those blocks were exceeded by key dependent substitution and diffusion procedures. A total of sixteen rounds were utilized in the encryption algorithm. Apeksha Waghmare *et al.* [3] designed a cryptographic algorithm that was based on ACM and logistic map. They used the cat map for the permutation operation and the Logistic map for the key generation. Ekhlas A. and Tayseer K. [4] proposed a novel chaotic permutation and substitution technique for image encryption. In this algorithm they made a combination of the block cipher and the chaotic map. The proposed algorithm was utilized to encrypt and decrypt a block of 500 bytes. Every block was initially permuted through utilizing the hyper-chaotic map and thereafter the result was substituted by utilizing the 1-D Bernoulli map. Eventually, the resulted block has been XORed with the key block. Qi Zhang *et al*. [5] implemented an algorithm for image encryption based upon chaotic sequences that have been created by the Lorenz system. Kayhan C. and Erol K. [6] was proposed an innovative image encryption method based on the Lorenz chaotic system and pixel shuffling. For the pixel shuffling process, they have used two initial vectors, one of columns and another of rows. Firstly, they performed the XOR operation between the initial column vector and image columns, then XORed the initial row with image rows to generate encrypted image. Ali Soleymani *et al*. [7] presented a new encryption system for images security depending on ACM and Henon maps. The system used ACM for a bit- and pixel-level permutation cases on the plain and encrypted images, while the Henon map created cipher images and specified parameters for permutations. Sura F. [8] proposed a novel system for grayscale image encryption. She divided the image evenly into four blocks, every one of the blocks was rotated 90^o in a clockwise orientation. The confusion was implemented by generating a permutation sequence, and the diffusion was implemented by generating a masking sequence for the alteration of image pixel values. Four various chaotic map variants were utilized, one for every block and those were Cross map, Quadratic map, the Ikeda map, and Chebyshev map. Finally, through commingle the 4 encrypted blocks, the cipher-image has been acquired. Ibtisam A. and Sarab M. [9] suggested a colored image encryption scheme based on a combination of 1D logistic and Sine chaotic maps. Behrang Chaboki and Ali Shakiba [10] proposed a chaotic-based image encryption algorithm, they used chaotic coupled lattice mapping for permutation and use a sorting approach to construct the diffusion matrix. Arwa Benlashram *et al.* [11] were used image pixel shuffling and the 3D chaotic map to propose a new method of image encryption. Ahmed M. Elshamy *et al.* [12] proposed a hybrid encryption technique for image encryption by using the Baker map, the Arnold cat map, and the Henon map, they applied each to a single channel. Ehsan Hasanzadeh and Mahdi Yaghoobi [13] were used S-box, fractals, and hyper chaotic dynamical systems to propose a colored image encryption method. Muna KH. and Sura Mazin [14] proposed an algorithm for image encryption by using the ElGamal public key algorithm and the 3D Arnold cat map. Using the proposed 2D chaotic map and discrete wavelet transform (DWT), Ibrahim Yasser *et al.* [15] proposed a new method for image encryption.

By combining the chaotic scheme with mix-column, a new color image encryption algorithm is proposed in this paper. This algorithm increases the security and efficiency of image encryption via high confusion that provided by XOR operation, mixcloumn and, the Lorenz system and high diffusion that was provided by the permutation method and ACM. The remainder of this paper has been organized in the following manner. The methods that were used in the proposed algorithm will be explained in section 2. The proposed system has been explained in detail in section 3. Section 4 demonstrates the security analysis. Finally, in section 5, the conclusions are presented.

2. CHAOTIC SYSTEM

This paper used two chaotic systems, which are, Arnold cat map [16] and the Lorenz system [17] that were employed in the proposed system for the key generation.

2.1. Arnold cat map

Arnold's cat map is a two-dimension chaotic map which can be utilized to alter the position of the pixel of the image without eliminating any information from that image [18], This 2-D transformation depends upon a matrix that has a determinant of 1, making this conversion reversible and described as [19]:

$$I = \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & P \\ Q & PQ+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ n \quad (1)$$

Where, P and Q are integers and (x, y) is the original position which has been mapped to the new position (x', y'). This conversion is utilized for the randomization of the original arrangement of bits or pixels in an image. Yet, after enough reiteration, the original image has been reconstructed. Inverse mapping using (2) is a decryption phase procedure to convert the scrambled image to the input image. The number of repetitions in the permutation phase should be equal to the number of repetitions of the reverse transmutation [20]. In (2) shows the reverse mapping:

$$I' = \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} PQ+1 & -P \\ -Q & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} mod\ n \quad (2)$$

2.2. Lorenz system

The Lorenz system, which initially has been researched by E. Lorenz in 1963, is a dynamic scheme which has been described through the following non-linear scheme of ordinary differential equations (ODEs) [21]:

$$\begin{aligned} x' &= \alpha(y - x) \\ y' &= (\beta x - y - xz) \\ z' &= (xy - \gamma z) \end{aligned} \tag{3}$$

The actual numbers α, β, γ have been known as control parameters, while x, y, z have been known as the status variables. As shown in Figure 1, the scheme presents a periodic behavior for parameters value α=10, γ=8/3 and β=28.

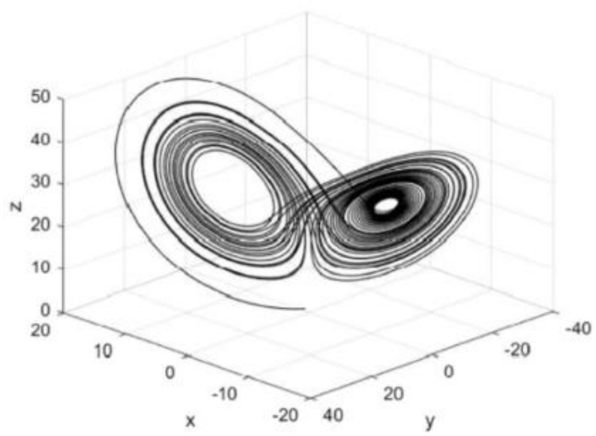


Figure 1. The plot of the Lorenz system along x–y–z axis, for α=10, γ=8/3, β=28

3. PROPOSED SCHEME

The proposed scheme contains six major steps, which conitain multiple steps of diffusion and confusion, that are:

a. The first stage is the diffusion process, which will be implemented twice. In the first one, the plain image is permuted by ACM that has been explained in the section (2.1), and in the second one is the plain image is permuted by the proposed permutation method which will be explained in the section (3.1).
b. The second stage is the confusion which will be implemented four times. The first one, is by implementing XOR operation between the results of the two permutation output. The second one, is by subtracting the random value in the range of [0-255] from all image pixels and this value is saved in a parameter will be used with chaotic parameters as a key. The third one, divides the resulting image to many blocks each block in size 16-byte and implement mix-column for each one. After that, collecting the blocks to generate the resulting image. Finally, implements the XOR operation between the resulting image and the Lorenz key to generate the encrypted image. Figure 2 illustrates the structure of the proposed model.

3.1. Permutation method

The permutation is a very important stage for impeding the rising correlation amongst image pixels to increment the encrypted image security. In this method, we relied on scrambling columns and rows depending on the sum invariance of row and column through a circular shift process. In the beginning, the plain image is divided into three bands (red, green, and blue) and shift each row in each band by the total sum of the row and column's pixel values and save the result in a variable, then implementing the same method in each column and saving the result in another variable has been performed. After that, transpose operation has been implemented for each band and the previous steps have been repeated for each row and column in each band, then, collecting the bands to generate the resulting image. Table 1 illustrate the permutation method of 5x5 sub-image and Figure 3 shows Lena image permutation by ACM, permutes Lena image by the permutation method, and XOR operation between two methods.

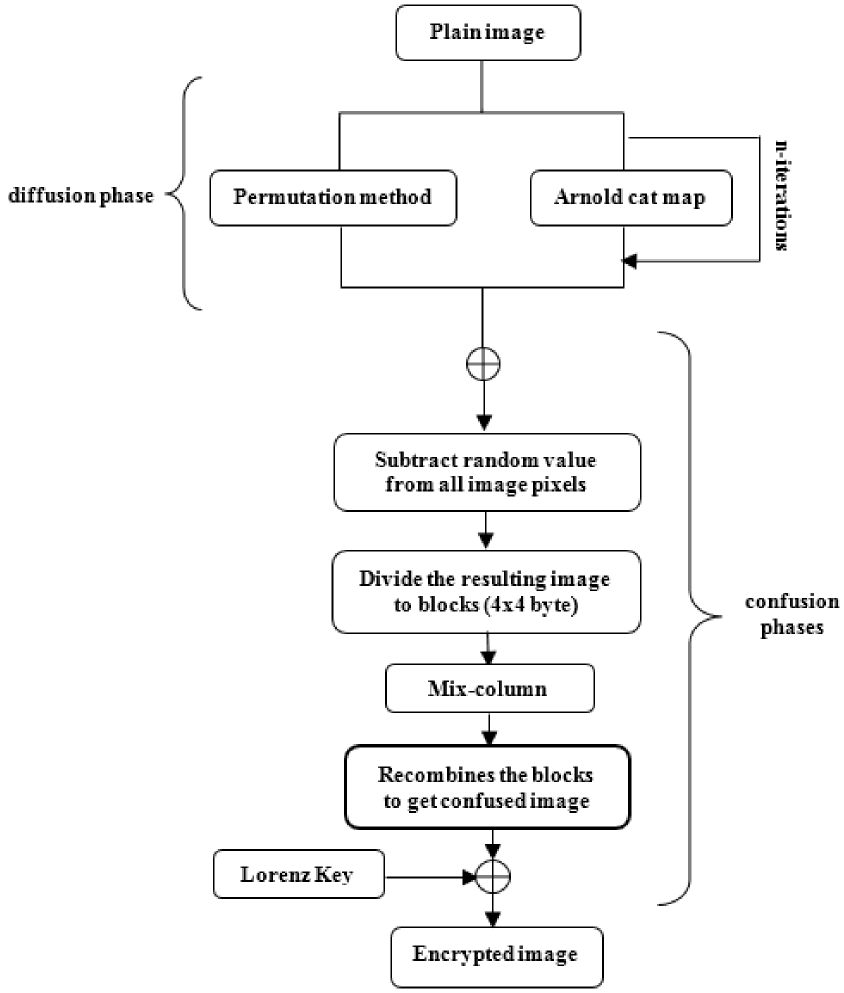
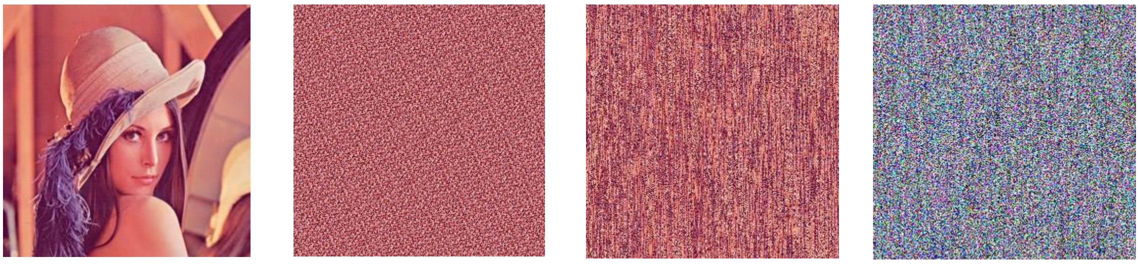


Figure 2. General structure of the proposed scheme



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

Figure 3. These figures are; (a) Plain Lena image, (b) Lena image permutation by ACM, (c) Lena image permutation by proposed permutation method, (d) XOR operation between two permutation methods

Table 1. Image permutation method

Original pixel location					The new pixel location				
216	159	162	283	215	99	283	129	224	187
190	245	111	129	154	142	215	154	180	159
187	191	224	180	182	198	96	216	182	156
198	192	156	150	148	245	148	192	190	150
96	107	138	99	142	138	162	111	107	191

3.2. Mix-column

In this scheme, the mix-column transformation matrix has been implemented in the AES algorithm which has been explained in detail by [22]. The mix-column transformation is applied to a block of columns one by one. It is performed by transforming each column of four bytes and takes it as input, which contains 4 bytes, and outputs a totally different 4 bytes by transforming the original column. Each byte in the product matrix is the summation products of bytes of one row and one column. The resultant matrix is the same as the input block size. Figure 4 explains the mix-column transformation process and Figure 5 shows the mix-column implementation of Lena's image.

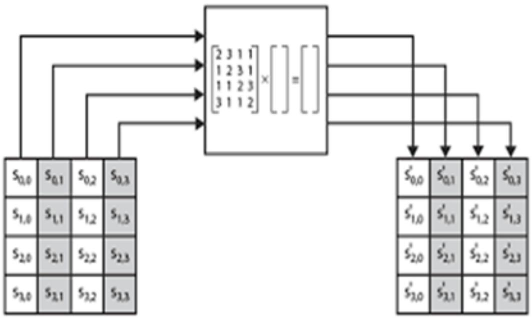
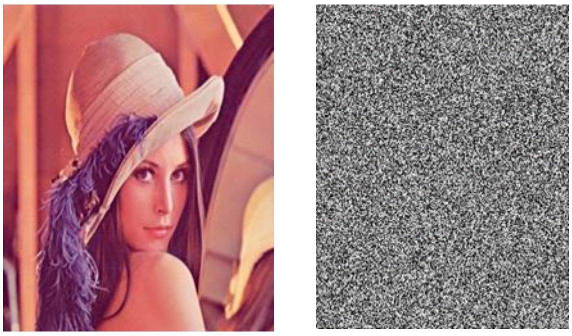


Figure 4. The mix-column transformation process



(a) (b)

Figure 5. These figures are; (a) Lena plain image, (b) mix-column implementation on Lena image

3.3 Proposed algorithm

In this section, the encryption and decryption algorithm will be explained:

a. Encryption algorithm

Input: plain image (*img*), *Lorenz_key*
Output: encrypted image (*c*)
Step1: read a colored image (*img*)
Step2: $p_1 \leftarrow$ ACM(*img*)
Step3: for $i \leftarrow 1{:}m$
            for $j \leftarrow 1{:}n$
                $r \leftarrow$ circular_shift (*img*)
            end
        end
        $t \leftarrow$ transpose (r)
        for $i \leftarrow 1{:}m$
            for $j \leftarrow 1{:}n$
                $p_2 \leftarrow$ circular_shift (t)
            end
        end
Step4: $x \leftarrow$ XOR (p_1, p_2)
Step5: *rand* $\leftarrow$ (random value [0,255])
        $s \leftarrow x$ - *rand*
Step6: divided (s) to blocks in size *4* x *4*
Step7: for $i \leftarrow 1{:}4$
            for $j \leftarrow 1{:}4$
                $M \leftarrow$ Mix-column(s)
            end
        end
    Step8: $k \leftarrow$ collects the blocks
Step9: $c \leftarrow$ XOR (*Lorenz_key*, *k*)

b. Decryption algorithm

Input: encrypted image (*c*), *Lorenz_key*
Output: plain image (*img*)

Step1: read an encrypted image (*c*)
Step2: $k \leftarrow$ XOR (*Lorenz_key, c)*
Step3: divided (*k*) to blocks in size *4* x *4*
Step4: for $i \leftarrow 1{:}4$
 for $j \leftarrow 1{:}4$
 $M \leftarrow$ Inv_Mix-column(*k*)
 end
 end
Step5: $b \leftarrow$ collect the blocks
Step6: $s \leftarrow b + rand$
Step7: $t_1 \leftarrow$ Inv_transpose (*s*)
 for $i \leftarrow 1{:}m$
 for $j \leftarrow 1{:}n$
 $p_1 \leftarrow$ Inv_circular_shift (t_1)
 end
 end
Step8: $p_2 \leftarrow$ Inv_ACM(*s*)
Step9: $x \leftarrow$ XOR (p_1, p_2)

4. RESULTS AND DISCUSSION

In this section, we review the results of the series of tests to proof the efficiency of the proposed method. The evaluation consists of many practical experiments. The experiments are performed via MATLAB R2013a on a computer with Intel Core i7 CPU 1.99 GHz, 8 GB of RAM.

4.1. Key space analyses

Key space size is the aggregate number of various keys which may be utilized in the encryption and decryption. The key space has to be large enough in order to resist against robust attacks, which makes the finding of the key very hard for the attackers. In the systems that were based on chaotic systems, key space increases by increasing the number of parameters and the chaotic system size. In this approach, the key space is $(10^{14})^6$ which is nearly equal to 2^{279} and it's sufficient to resist each type of brute-force attacks. Table 2 shows the key space compared to some related works.

Table 2. Key space comparison

schemes	Ehsan H. *et al.* [13]	Narendra K. *et al.* [1]	Ünal Ç. *et al.* [2]	Ekhlas A. *et al.* [4]	Kayhan Ç. *et al.* [6]	Proposed scheme
Key space	$>2^{128}$	2^{128}	10^{98}	2^{213}	10^{45}	2^{279}

4.2. Information entropy analysis

One of the very important measures to compute the randomness is information entropy. It can be computed by:

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) \log_2 \frac{1}{p(m_i)} \tag{4}$$

In (4), m is a sample, n is the number of samples, and p (m) is the likelihood of symbol m. The ideal value of H (m) can be obtained according to (4) is 8, this indicates that random information in the image [23]. The values of information entropy that has been obtained from the proposed system are closer to eight, this shows that the suggested scheme has good randomness. Table 3 shows the values of information entropy for the different plain images and Table 4 shown the information entropy comparison with some of the related works.

4.3 Correlation analysis

The correlation among contiguous pixels in the normal image is always strong, and the correlation coefficient values are so close to 1. For this reason, the correlation must be decreased significantly in an efficient encryption algorithm and the value extremely close to 0 [21]. The correlation coefficients can be calculated for three orientations, which are diagonal, horizontal, and vertical shown in below.

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{5}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{6}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{7}$$

Table 3. Entropy of the plain and encrypted image information

Images	Entropy	
	Plain image	Encrypted image
Flower	7.7666	7.9989
Tree	7.6659	7.9989
Splash	7.3795	7.9990
Sky	7.9339	7.9992
Lena	7.7599	7.9992
Garden	7.7955	7.9989
Pepper	7.7124	7.9989
Birds	7.7472	7.9990
Horse	7.6143	7.9991
Cat	7.6596	7.9990

Table 4. Information entropy comparison for Lena image

Schemes	Ehsan H. *et al.* [13]	Arwa B. *et al.* [11]	Ekhlas A. *et al.* [4]	Kayhan Ç. *et al.* [6]	Proposed Scheme
Entropy	7.9992	7.9901	7.9988	7.9993	7.9992

In (5), x and y represent values of 2 contiguous pixels in an image. Figure 6 illustrates the diagonal, horizontal, and vertical correlation coefficients in the plain and encrypted Lena image, and Table 5 displays the results of the correlation for different plain and encrypted images. Table 6 lists the comparison of the correlation coefficients with some of the related works.

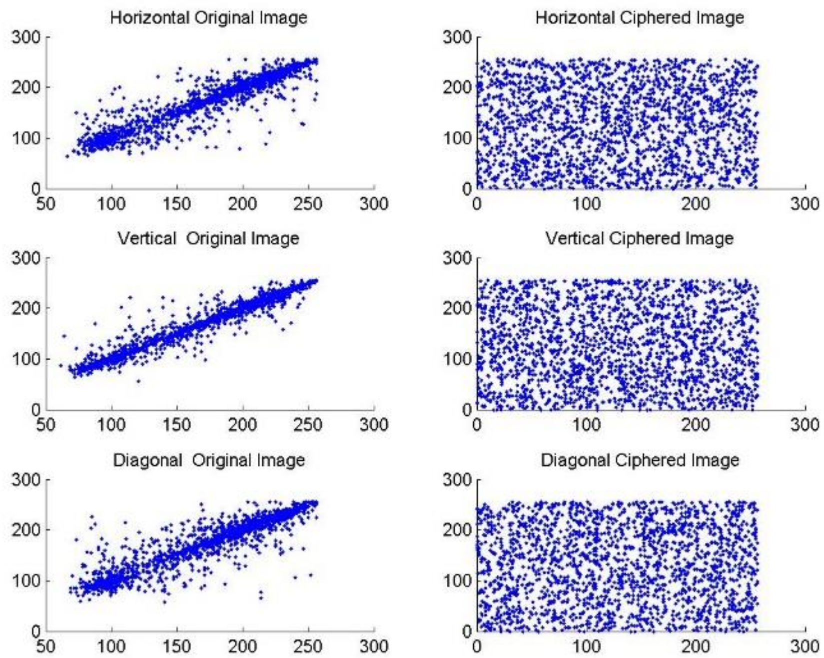


Figure 6. The correlation of two neighboring pixels in the plain and encrypted Lena image

Table 5. The correlation coefficient of encrypted images

Images	Correlation		
	Horizontal	Vertical	Diagonal
Flower	-0.0060	0.0047	0.00007
Pepper	0.0035	0.0012	0.0057
Lena	0.0048	-0.0016	0.0040
Birds	0.0034	0.0061	0.00009
Garden	-0.00024	-0.0019	0.0066
Horse	0.00007	0.0042	-0.00002
Tree	0.0078	-0.0072	0.0064
Sky	-0.00001	-0.0036	0.0011
Cat	-0.00002	0.0035	0.0041
splash	-0.0026	-0.0027	0.00002

Table 6. Correlation coefficient comparison

Correlation	Ehsan H. *et al.* [13]	Arwa B. *et al.* [11]	Ekhlas A. *et al.* [4]	Proposed scheme
Horizontal	0.0204	- 0.0127	-0.0002	0.0048
Vertical	-0.0124	- 0.0242	0.0008	-0.0016
Diagonal	-0.0895	NA	0.0087	0.0040

4.4. Resisting differential attack analysis

In cryptography, a pixel from a plain image is compared to a pixel from a cipher image to obtain the beneficial relation, that moreover defines the secret key. This type of analysis has been known as the differential attack cryptanalyses [24]. This study used the number of unified averaged modified intensity (UACI) values and the pixels change rate to determine the effect of changing a small portion of the pixels in the normal image of the encrypted image (NPCR). The NPCR index can be used to estimate the number of pixels in the original image that have the same location in the encrypted image, and it is determined as follows:

$$NPCR = \frac{\sum_{i,j} d(i,j)}{w \times h} \times 100\% \tag{8}$$

Where, the image width (w) and height (h), C1(i, j) & C2(i, j) are two encrypted images whose corresponding plain images I1(i, j) & I2(i, j) have only 1-pixel value variation. D(i, j)=0, if C1(i, j)=C2(i, j); otherwise D(i, j)=1.

The UACI index is utilized for knowing the influence of the encrypted image in the case where one-pixel has been changed in the plain image, and it has been determined according to:

$$UACI = \frac{1}{w \times h}\left(\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right) \times 100\% \tag{9}$$

The optimum value of UACI and NPCR are 33.46 and 99.61 [25]. In this paper we implement NPCR and UACI measures on ten colored images and the results of two indicators are near to idealistic value. Table 7 shown the results of UACI and NPCR in the suggested scheme. Table 8 shows the UACI and NPCR comparison with some of the related works.

Table 7. UACI and NPCR indicator of plain and encrypted images

Images	UACI	NPCR
Flower	33.59	99.60
Tree	34.01	99.58
Splash	33.98	99.62
Sky	33.81	99.61
Lena	32.51	99.62
Garden	33.35	99.61
Pepper	34.10	99.61
Birds	33.76	99.61
Horse	33.37	99.61

Table 8. UACI and NPCR indicator comparison

Indicators	Ehsan H. *et al.* [13]	Arwa B. *et al.* [11]	Kayhan Ç. *et al.* [6]	Ekhlas A. *et al.* [4]	Proposed scheme
UACI	33.42	33.60	6.0158	33.39	32.51
NPCR	99.61	99.65	17.92	99.49	99.62

4.5. Histogram analysis

The histogram analysis has been utilized in order to explain the diffusion and confusion characteristics of the encryption algorithm. Figure 7 shows the difference in the image distribution between the plain and encrypted tree images.

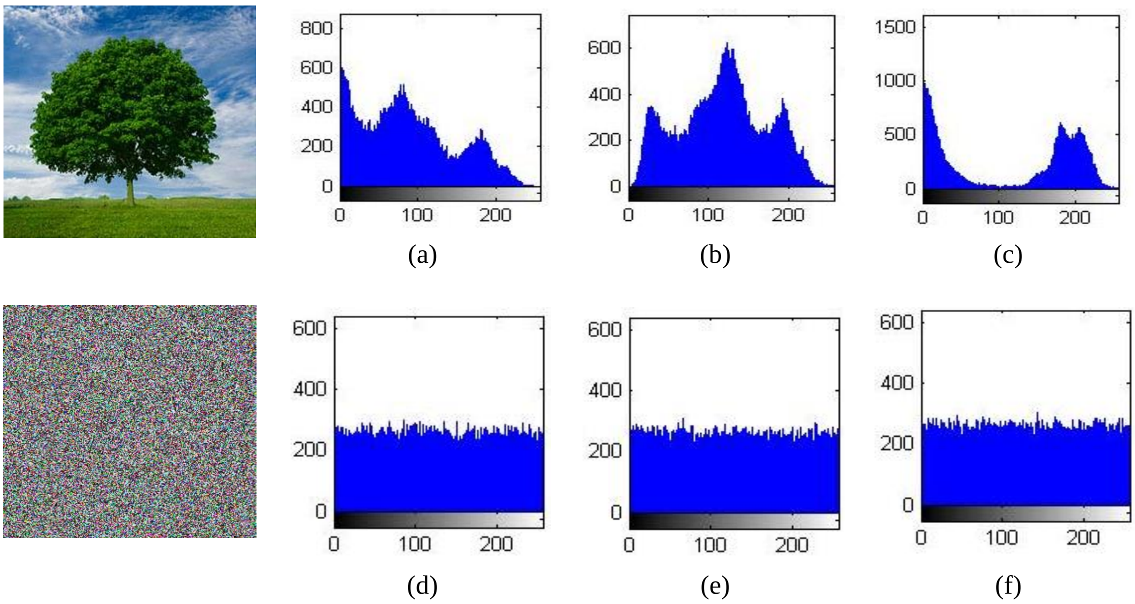


Figure. 7. Histogram analysis; (a), (b) and (c) are the histogram of (red, green and blue) of plain tree image, (d), (e) and (f) are the histogram of (red, green and blue) of encrypted tree image

5. CONCLUSION

In the present paper, a new image encryption algorithm was suggested to provide a high security level of image encryption, based upon the combinations of permutation method, the chaotic system and mix-column. Whereas the random permutation method provides a high level of diffusion, and mix-column process provides high confusion. Also, the use of the chaotic system offers high randomness, key sensitivity, and confusion. The effectiveness of this method has been confirmed by the experimental results above. It can be seen that according to these results, the suggested system shows high resistance against the statistical and differential attack types.

ACKNOWLEDGEMENTS

The authors would like to thank Mustansiriyah University **(**www.uomustansiriyah.edu.iq**)** Baghdad, Iraq for its support in the present work.

REFERENCES

[1] N. K. Pareek, V. Patidar, and K. K. Sud b, "Diffusion–substitution based gray image encryption scheme", *Digital Signal Processing*, vol. 23, No. 3, pp. 894-901, 2013, doi: 10.1016/j.dsp.2013.01.005.

[2] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-Box", *Chaos Solitons and Fractals*, vol. 95, pp. 92–101, 2017, doi: 10.1016/j.chaos.2016.12.018.

[3] A. Waghmare, A. Bhagat, A. Surve and S. Kalgutkar, "Chaos Based Image Encryption and Decryption", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 5, Issue 4, April 2016.

[4] E. A. Albahrani and T. K. Alshekly, "New Chaotic Substation and Permutation Method for Image Encryption", *International Journal of Applied Information Systems (IJAIS)*, Vol. 12, No. 4, pp. 34-39, July 2017, doi: 10.5120/ijais2017451698.

[5] Q. Zhang, Y. Guo, W. Li and Q. Ding, "Image Encryption Method Based on Discrete Lorenz Chaotic Sequences", *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 7, Number 3, pp. 576-586 May, 2016.

[6] K. Celİk and E. Kurt, "A new image encryption algorithm based on lorenz system," *2016 8th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2016, pp. 1-6, doi: 10.1109/ECAI.2016.7861097.
[7] A. Soleymani, M. J. Nordin and E. Sundararajan, "A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map", *Hindawi Publishing Corporation the Scientific World Journal*, Vol. 2014, doi: https://doi.org/10.1155/2014/536930.
[8] S. F. Yousif, "Grayscale image confusion and diffusion based on multiple chaotic maps," *2018 1st International Scientific Conference of Engineering Sciences - 3rd Scientific Conference of Engineering Science (ISCES)*, 2018, pp. 114-119, doi: 10.1109/ISCES.2018.8340538.
[9] Ibtisam A. Taqi and Sarab M. Hameed, "A new Color Image Encryption based on multi Chaotic Maps", *Iraqi Journal of Science*, Vol. 59, No.4B, pp: 2117-2127, 2018, doi: 10.24996/ijs.2018.59.4B.17.
[10] Behrang Chaboki and Ali Shakiba, "An image encryption algorithm with a novel chaotic coupled mapped lattice and chaotic image scrambling technique", *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 21, No. 2, pp: 1103-1112, 2021, doi: 10.11591/ijeecs.v21.i2.pp1103-1112.
[11] Arwa Benlashram, Maryam Al-Ghamdi, Rawan AlTalhi and Pr. Kaouther Laabidi "A novel approach of image encryption using pixel shuffling and 3D chaotic map", *Journal of Physics: Conference Series*, 2020, doi: 10.1088/1742-6596/1447/1/012009.
[12] Ahmed M. Elshamy, *et al.*, "Color Image Encryption Technique Based on Chaos", *16th International Learning & Technology Conference 2019, Procedia Computer Science 163*, pp. 49–53, 2019, doi: https://doi.org/10.1016/j.procs.2019.12.085.
[13] Ehsan Hasanzadeh and Mahdi Yaghoobi, "A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys", *Multimedia Tools and Applications*, 2019. doi: 10.1007/s11042-019-08342-1.
[14] Muna K H. Al naamee and Sura Mazin Ali, "Improved El Gamal public key cryptosystem using 3D chaotic maps", *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, pp. 404-411, February 2021, doi: https://doi.org/10.11591/eei.v10i1.2124.
[15] Ibrahim Yasser, *et al.*, "A New Image Encryption Scheme Based on Hybrid Chaotic Maps", *Hindawi, Complexity*, Volume 2020, doi: https://doi.org/10.1155/2020/9597619.
[16] E. Hariyanto and R. Rahim, "Arnold's Cat Map Algorithm in Digital Image Encryption," *International Journal of Science and Research (IJSR)*, Volume 5 Issue 10, pp. 1363-1365, October 2016. doi: 10.21275/ART20162488.
[17] Jianghong Bao and Qigui Yang, "Period of the discrete Arnold cat map and general cat map", *Nonlinear Dyn*, 70:1365–1375, 2012. doi: 10.1007/s11071-012-0539-3.
[18] A M H Pardede, *et al.*, "Digital Image Security Application with Arnold Cat Map (ACM)", *IOP Conf. Series: Journal of Physics: Conf. Series*. Vol: 1114, no: 1, p. 012059, 2018. doi: 10.1088/1742-6596/1114/1/012059.
[19] Anak Agung, *et al.*, "Chaos-Based Image Encryption Using Arnold's Cat Map Confusion and Henon Map Diffusion", *Advances in Science, Technology and Engineering Systems Journal*, vol. 6, no. 1, pp. 316-326, 2021.
[20] Tu Li, *et al.*, "A new image encryption algorithm based on optimized Lorenz chaotic system", *Concurrency Computat Pract Exper*, 2020. doi: https://doi.org/10.1002/cpe.5902.
[21] O. M. Al-Hazaimeh, Mohammad Fawaz Al-Jamal, and Nouh Alhindawi, "Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys", *Neural Computing and Applications*, Augest 2017. doi: 10.1007/s00521-017-3195-1.
[22] William Stallings, "Cryptography and Network Security", *principles and practice 5th edition, Pearson Education*, Inc., 2011.
[23] L. Hongjun and W. Xingyuan,"Color image encryption based on one-time keys and robust chaotic maps," *Computers and Mathematics with Applications 59*, pp. 3320_3327, 2010. doi: https://doi.org/10.1016/j.camwa.2010.03.017.
[24] L. Xu, ZhiLi, Jian Li, and Wei Hua, "A novel bit-level image encryption algorithm based on chaoticmaps", *Optics and Lasersin Engineering* 78, pp. 7–25, 2016. doi: https://doi.org/10.1016/j.optlaseng.2015.09.007.
[25] G. Ye, *et al.*, "A Chaotic Image Encryption Algorithm Based on Information Entropy, "*International Journal of Bifurcation and Chaos*, Vol. 28, No. 1, pp. 1-11, 2018. doi: https://doi.org/10.1142/S0218127418500104.