Image encryption based on combined between linear feedback shift registers and 3D chaotic maps

Salah Taha Allawi[1], Nada Abdul Aziz Mustafa[2]
[1]Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq
[2]Information Technology Unit, College of Languages, Baghdad University, Baghdad, Iraq

Article Info

Article history:

Received May 22, 2022
Revised Jan 24, 2023
Accepted Feb 4, 2023

Keywords:

3D chaotic maps
Colour image
Image encryption
Linear feedback shift register
Statistical tests

ABSTRACT

Protecting information sent through insecure internet channels is a significant challenge facing researchers. In this paper, we present a novel method for image data encryption that combines chaotic maps with linear feedback shift registers in two stages. In the first stage, the image is divided into two parts. Then, the locations of the pixels of each part are redistributed through the random numbers key, which is generated using linear feedback shift registers. The second stage includes segmenting the image into the three primary colors red, green, and blue (RGB); then, the data for each color is encrypted through one of three keys that are generated using three-dimensional chaotic maps. Many statistical tests (entropy, peak signal-noise ratio (PSNR), mean square error (MSE) and correlation) were conducted on a group of images to determine the strength and efficiency of the proposed method, and the result proves that the proposed method provided a good level of safety. The obtained results were compared with those of other methods, and the result of comparing confirms the superiority of the proposed method.

Corresponding Author:

Salah Taha Allawi
Department of Computer Science, College of Science, Mustansiriyah University
Baghdad, Iraq
Email: salah.taha@uomustansiriyah.edu.iq

1. INTRODUCTION

With the great and rapid technological development in various fields, including computers and data transfer, images are exposed to many risks and security threats, especially when transmitted through unsecured channels over the internet [1], [2]. Particularly in times of war, the confidentiality and security of transmitted information play an essential role in success [3]. Encrypting is an effective way to protect an image's data before sending it to the receiver [2], [4]. The main purpose of the image encryption process is to transform it into another form so that no one can know its content without owning the original key [5]. Traditional algorithms used in data encryption, such as data encryption standard (DES), advanced encryption standard (AES), and Rivest-Shamir-Adleman (RSA), are not suitable for image encoding because of image properties such as the strong relationships between adjacent pixels and high redundancy [6]–[8]. According to Shannon in his 1945 classified report, techniques for the basic encryption system can be classified into two categories: diffusion, and confusion [9]. Using chaotic maps is one method that has been suggested in the image encoding process because of its essential properties, such as sensitivity to initial values of control parameters, excellent pseudo-randomness, and determinism [10].

Encrypting images using chaotic maps takes place in two stages. Redistributing the locations of pixels without changing the data in the first stage. Changing the values of pixels to achieve certain information protection in the second stage [11], [12]. For the encryption algorithm to be strong and the encrypted image more confusing, researchers suggested combining the redistribution of pixel locations with the changing of pixel values [13]. This paper suggests a new color image cryptography approach based on combining linear feedback shift register (LFSR) and chaotic maps such that images can be sent safely over unsecured internet channels. Recently, many encryption systems that rely on chaotic maps have been suggested.

Li *et al.* [14] proposed a new method to encrypt images using 3D chaotic maps. The keys are generated using 3D chaotic maps, and these keys are used to redistribute the locations of pixels in the first stage. In the second stage, the three keys are changed so they can change the pixel's data and obtain an encrypted image. In relevant research, Lagmiri et *al*. [15] introduced a new and effective method for encrypting color images using chaotic behavior. Where redistributing the locations of pixels is in the first stage. While in the second stage, the pixel data resulting from the first stage are changed through the developed map called Nahrain, which depends on chaotic behavior. Similarly, Abdullah and Abdullah [16] introduced a new and effective method for encrypting color images using chaotic behavior. Redistributing the locations of pixels is carried out in the first stage, while in the second stage, the pixel data resulting from the first stage are changed through the developed map called Nahrain, which depends on chaotic behavior. Allawi and Abbas [17] presented a method for encrypting color images based on the combination of 2D and 3D chaotic maps in two stages. In the first stage, 2D chaotic mapping is used to redistribute the locations of the pixels. While in the second stage, 3D logistic maps are used to change the values of the pixel data. Finally, Huang *et al.* [18] introduced a new encryption method that depends on color image data in the creation of keys that are used in redistributing the locations of pixels and changing the pixel values, which depends mainly on chaos. Thus, an encrypted image resistant to differential attacks can be obtained efficiently.

This paper presents a new encryption method that combines 3D chaotic maps and LFSRs. The rest of this paper is arranged as shown in; an explanation of the proposed method is given in section 2. Section 3 presents and discusses the results. Finally, the conclusions are presented in section 4.

2. METHOD

This section presents details of the proposed method, which comprises two stages, confusion and diffusion. The mechanism for generating the random numbers is explained using LSFRs to change the image pixel locations (confusion). Then, the details of the data encoding method using 3D chaotic maps are described (diffusion). Figure 1 shows the general outline of the proposed method.

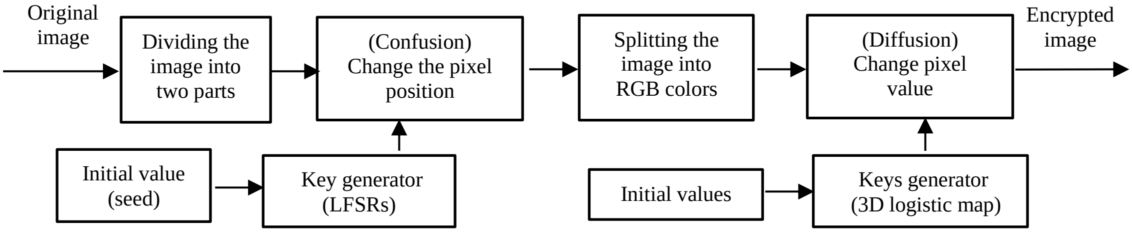

Original image
Dividing the image into two parts
(Confusion) Change the pixel position
Splitting the image into RGB colors
(Diffusion) Change pixel value
Encrypted image
Initial value (seed)
Key generator (LFSRs)
Initial values
Keys generator (3D logistic map)

Figure 1. General outline of the proposed method

2.1. Encryption stage

This stage is divided into two parts. The first is the confusion stage, which involves changing the locations of image pixels by generating a set of non-repeating random numbers using LFSRs. Second, in the diffusion stage, the pixel data are changed using 3D chaotic maps.

2.1.1. Changing the pixel's position (confusion)

Neighboring pixels in the image have strong correlations in all directions. Therefore, at this stage, work is being done to destroy this correlation between the pixels. In the begging, the inputting color image is divided into two equal parts (upper UP and lower LW) with size Sk. Second, using LFSRs that comprise three registers with different lengths (29, 31, 33) and different taps (2, 7, 13), (1, 2, 3), (11, 13, 22), respectively, key K is generated that contains non-repetitive random numbers with size Sk. The same key is used to redistribute the locations of the pixels in each part. Figure 2 shows the form LFSR used to generate the random numbers. In this stage, we get a distorted image because of the changed locations of the pixels without changing the image's original data.

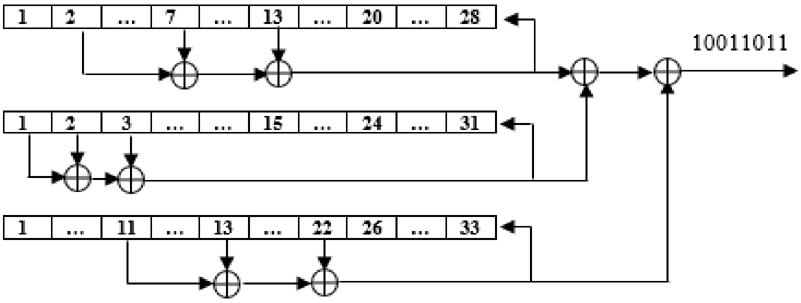


Figure 2. LFSR form with different taps

2.1.2. Changing the pixel values (diffusion)

This stage relies mainly on 3D chaotic maps to improve the level of security in the encryption system. The image data is encoded by changing the pixel values at this stage. Although the 1D chaotic maps are quite effective show complex chaotic behavior, still their orbits can be predicted by using chaotic signal estimation technologies. A three-dimensional map has better chaotic properties than a one-dimensional map. According to (1)-(3) illustrate the 3D logistic map [19], [20].

$$x_{i+1} = \alpha x_i(1 - x_i) + \beta y_i^2 x_i + \gamma z_i^3 \tag{1}$$

$$y_{i+1} = \alpha y_i(1 - y_i) + \beta z_i^2 y_i + \gamma x_i^3 \tag{2}$$

$$z_{i+1} = \alpha z_i(1 - z_i) + \beta x_i^2 z_i + \gamma y_i^3 \tag{3}$$

Where (α, γ, and β) are three parameters ($0 < \gamma < 0.015$), ($0 < \beta < 0.022$), ($3.68 < \alpha < 3.99$) and $z_{0,} y_0, x_0$ can take the value between (0, 1).

We isolate the image colors that result from the previous stage to the three basic components red, green, and blue (RGB) in the first step. The 3D chaotic maps in (1), (2), and (3) generate three keys (*Kr*, *Kg*, *Kb*), each used to encrypt a specific color. Image data encryption is performed by applying an XOR process between the data of each color, with the key corresponding to where the value of each point is changed in the second step. The result is an encrypted image that can be sent to the desired location. Algorithm 1 shows the stage of redistribution of positions and change of data values for all pixels of the image (encryption stage).

Algorithm 1. Encryption stage

```
Input: Original image.
Output: Encrypted image.
1: Entering a color image (P) with a size (M x N)
2: Dividing the input image into two equal parts (UP, LW).
3: Converting each part of the image to a 1D array with a size (Sk)
4: Giving the initial value to the LFSRs
5: Using the LFSRs to generate a key containing random numbers of size (SK).
6: Redistributing the pixel position for each part by using the key generated in the previous
   step.
7: Recombining the parts of an image (UP, LW) to form the image (IP).
8: Isolating the image (IP) to the three primary colors (RGB).
9: Convert the data of each color into a 1D array (Ar, Ag, Ab).
10: Generating three keys (Kr, Kg, Kb) by using the 3D chaotic map
11: The XOR operation executes between the keys and the data of colors (Kr, Ar), (Kg, Ag), (Kb,
    Ab).
12: Recombining the colors after executing the previous step to form the encrypted image
    (IPE).
13: The result is an encrypted image.
```

2.2. Decryption stage

To decode the data and restore the original image, a series of operations are performed, in which all operations performed in the encryption phase are reversed and the same initial values are used. The decoding phase involves restoring the original value of the point through the use of 3D chaotic maps. The original position of each pixel was restored by the use of LFSR. Algorithm 2 describes the steps for decoding the data and reconstructing the original image.

Algorithm 2. Decryption stage

```
Input: Encrypted image
Output: Original image
Input the encrypted image
Splitting the encrypted image into the three essential colors (RGB)
Converting the data of each color into a one-dimensional array.
Generating three keys by using the 3D Logistic maps.
The XOR operation executes between the keys and the pixel’s value.
Reshape the image by combining the three arrays after executing the previous step.
Dividing the image into two equal parts.
Generating the key of random numbers by using the LFSRs.
Use the key of the random numbers to get the original position for all the pixels in each
   part.
Reshape the original image by combining the two parts after executing the previous step.
```

3. RESULTS AND DISCUSSION

The proposed method was tested on a group of colored images: Lena, Baboon, Barbara, and Pepper of size (256×256). In the permutation stage, we used three registers of different lengths (29, 31, 33) and different taps (13, 7, 2), (3, 2, 1), (22, 13, 11,) respectively, and each register had a unique initial value(seed). The number of sequences bits required to generate each number depended on the number of pixels in one-half of the image size. Thus, the number of bits required to generate the numbers varied according to the image size.

For example, if half of the image size was 1000 pixels, we needed 10 bits for each number, but if half of the image size was 2000 pixels, we required 11 bits. The generated random numbers key was used to change the locations of the image pixels, where the same key was used for each part. In the diffusion stage, the 3D logistic map was used with the following initial parameters: γ=0.015, β=0.02, α=3.84, z_0=0.97, y_0=0.67 and x_0=0.97. Figure 3 shows the original images that were used in the experiment, and Figure 4 shows encrypted images that result from the experiment. To know the strength and effectiveness of the method, many statistical tests were conducted on the images used in the experiments.

Figure 3. The original images used in experiments

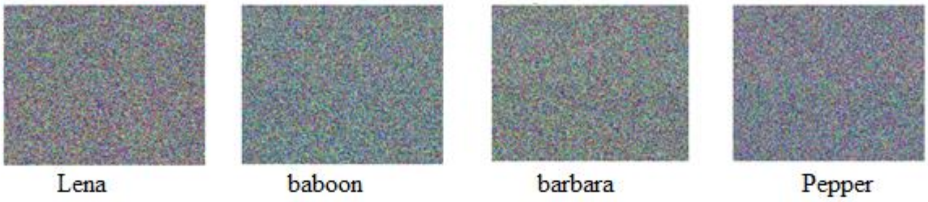


Figure 4. The encrypted images that result from experiments

3.1. Histogram analysis

The primary purpose of the histogram is to determine the distribution of the pixels of the image and obtain relevant information. The encryption process aims to remove the differences between the pixels, which prevents the attacker from obtaining information that helps to reveal the image [21], [22]. Figure 5 explains a histogram of Lena’s original image. Figure 6 explains a histogram of Lena’s encrypted image. The resulting histogram of the encrypted image is regular, making it difficult for unauthorized parties to get any information to recreate the original image.

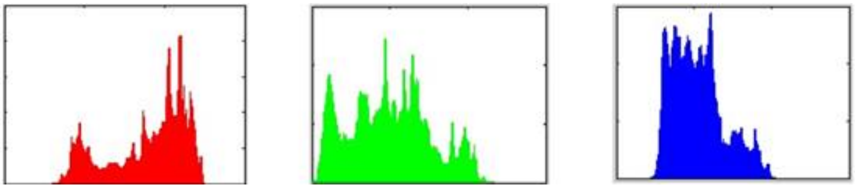


Figure 5. The result of the histogram analysis of the original image

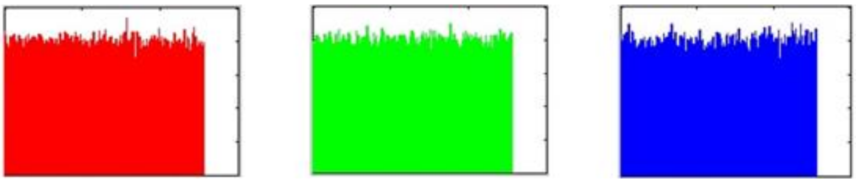


Figure 6. The result of the histogram analysis of the encrypted image

3.2. Entropy

Entropy estimates the strength of the proposed encryption system in terms of its ability to distort the encoded images. The entropy value is calculated as the average amount of data produced by a truly random source of data. As shown in (4) illustrates the mathematical formula for calculating entropy [23], [24].

$$H(p) = -\sum_{i=0}^{255} q(p_i)\, log_2\, q\,(p_i) \qquad (4)$$

Where $q(p_i)$ is the probability of (p_i), and the entropy $H(p)$ is described by bits.

The value of the entropy of the encrypted image as it approaches 8 indicates the strength of the encryption system. Table 1 illustrates the entropy values got from implementing the method on the experiment images. Through the results, we notice that the value of entropy for all original images deviates from the optimal value. While the value of entropy for all encrypted images is 7.99, which is very close to the optimal value and this shows the strength of the proposed method.

Table 1. Entropy values for the experiments image

image	Original image	Encrypted image
Lena	7.33	7.99
Baboon	7.57	7.99
Barbara	7.51	7.99
Peppers	7.33	7.98

3.3. Unified average changing intensity and number of pixel change rate tests

Statistical tests used to determine the ability of the encrypted image to resist statistical attacks are unified average changing intensity (UACI) and number of pixel change rate (NPCR). NPCR determines the rate of change that occurs between the pixels of the original image and the encrypted image. UACI calculates the difference between the original and encrypted images [24], [25]. As shown in (5)-(7) are the mathematical formulas for calculating the UACI and NPCR values.

$$UACI = \frac{1}{R*C}\left[\sum_{i,j}\frac{|D_1(i,j)-D_2(i,j)|}{255}\right] * 100 \qquad (5)$$

$$NPCR = \frac{\sum_{i,j} M(i,j)}{R*C} * 100 \qquad (6)$$

$$M(ij) = \begin{cases} 0, \ if\ D_1(i,j) = D_2\,(i,j) \\ 1, \ if\ D_1(i,j)\ \neq D_2\,(i,j) \end{cases} \qquad (7)$$

Where $D_1(i, j)$ is the encrypted image and $D_2(i, j)$ is the original image, R is the image height and C is the image width. Table 2 shows the NPCR and UACI values for the images used in the experiments after applying the proposed method. Through the results, we notice the value of NPCR and UACI are very close to the ideal values. This indicates the ability of this method to resist various statistical attacks.

Table 2. UACI and NPCR for the experiments image

Image	NPCR			UACI		
	Red	Green	Blue	Red	Green	Blue
Lena	99.69	99.64	99.69	35	32	33
Baboon	99.65	99.63	99.64	31	30	32
Barbara	99.62	99.63	99.65	30	32	33
Peppers	99.63	99.60	99.65	30	34	37

3.4. PSNR analysis

Another critical test to assess the strength and effectiveness of the proposed method involves calculating the MSE and PSNR. For an encryption algorithm to be robust, the MSE should be high, and the PSNR should be less than 10. Equations (8) and (9) are the mathematical formula for calculating the PSNR and MSE [26], [27].

$$MSE = \frac{1}{mn}\sum_{ij}(D(i,j) - R(i,j))^2 \tag{8}$$

$$PSNR = 10log_{10}\left(\frac{H^2}{MSE}\right) \tag{9}$$

Where *MSE* is the mean square error of an image, *D*(*i*,*j*) is the encrypted image, and *R*(*i*,*j*) is the original image, (*i*,*j*) are the coordinates and *H* is the range of pixels in the image [27]. Table 3 demonstrates the PSNR and MSE values got from applying the proposed method to the experimental images. The results obtained demonstrate the power and efficiency of this method.

Table 3. PSNR and MSE for the experiments image

image	PSNR			MSE		
	Red	Green	Blue	Red	Green	Blue
Lena	7.502	8.313	9.060	115.58	95.88	80.72
Baboon	8.700	9.208	8.361	87.70	78.02	94.83
Barbara	8,886	8.668	8.210	84.92	88.36	98.18
Peppers	8.959	7.738	7.003	82.62	109.46	129.73

3.5. Correlation analysis

The bonding strength between the adjacent pixels in the horizontal, vertical, or diagonal direction of the original image is considerable. A good encryption system destroys this bonding strength, which should be close to zero to protect the system from statistical attacks. Correlation analysis is used to determine the strength of the encrypting system. According to (10), (11) and (12) are the mathematical formula for calculating the correlation coefficient values [23], [28], [25]:

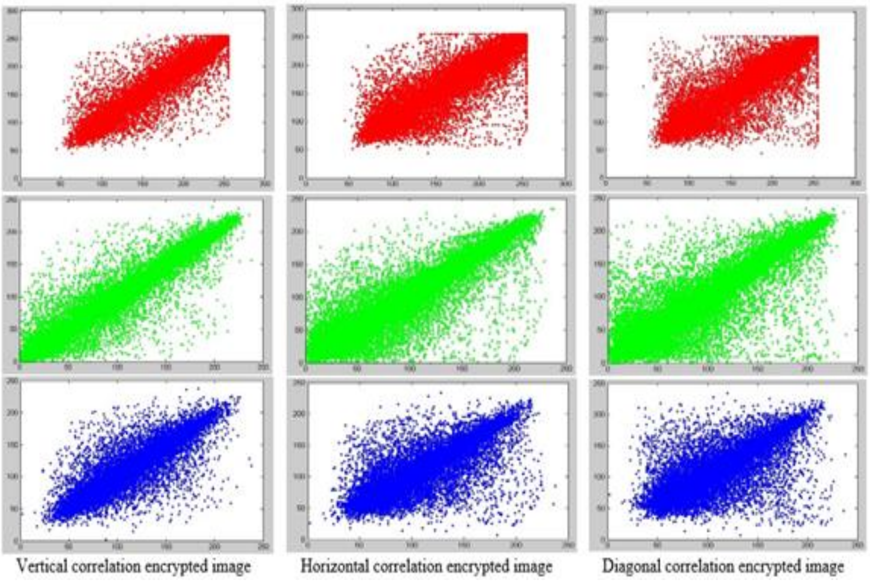
$$r_{u,v} = \frac{F\ ((u-F(u))(v-F(v)))}{\sqrt{H(u)H(v)}} \tag{10}$$

$$F(u) = \frac{1}{N}\sum_{i=1}^{N} u_i \tag{11}$$

$$H(u) = \frac{1}{N}\sum_{i=1}^{N}(u_i - F(u))^2 \tag{12}$$

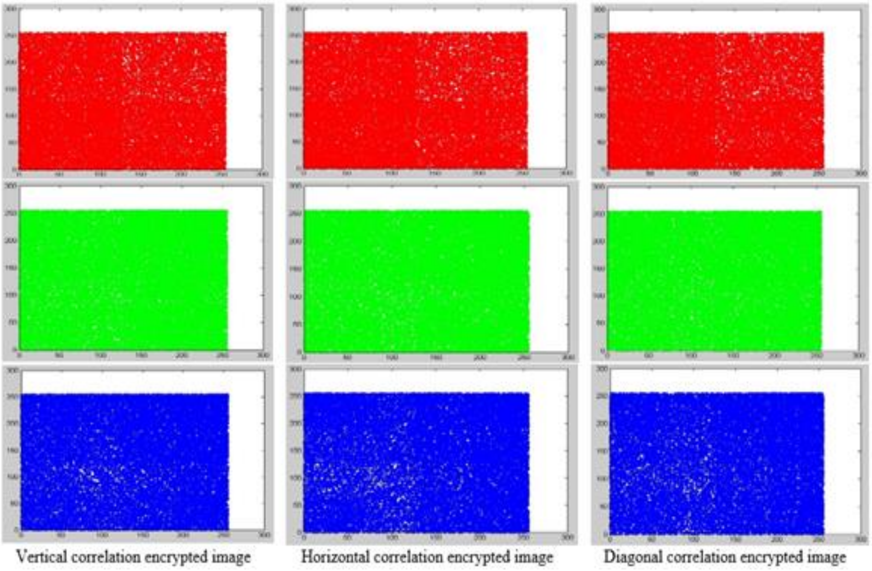
where *F*(*u*) and *H*(*u*) are the mathematical expectation and covariance, respectively. The correlation value of the original image is close to 1. The cryptosystem is considered stronger if its correlation value is close to 0 [28].

The proposed method achieves a correlation value close to zero, which indicates the high strength of this method. Figure 7 shows the result of applying the correlation test to the original ‘Lena’ image in the diagonal, vertical, and horizontal directions. Figure 8 shows the result of applying the correlation test to the encrypted ‘Lena’ image in the diagonal, vertical, and horizontal directions. Tables 4 and 5 show the correlation coefficients for all images used in the experiments before and after applying the method.



Vertical correlation encrypted image Horizontal correlation encrypted image Diagonal correlation encrypted image

Figure 7. Result of the correlation test for the original Lena image



Vertical correlation encrypted image Horizontal correlation encrypted image Diagonal correlation encrypted image

Figure 8. Result of the correlation test for the encrypted Lena image

Table 4. Correlation coefficients values for the original images

Image	Horizontal			Vertical			Diagonal		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lena	0.9184	0.9227	0.8491	0.9523	0.9551	0.9120	0.8945	0.8993	0.8153
Baboon	0.8792	0.8167	0.8894	0.8246	0.7344	0.8473	0.8161	0.7183	0.8322
Barbara	0.9018	0.8827	0.9029	0.9173	0.9061	0.9219	0.8704	0.8457	0.8713
Peppers	0.9112	0.9607	0.9262	0.9303	0.9628	0.9367	0.8674	0.9366	0.8933

Table 5. Correlation coefficients values for the encrypted images

Image	Horizontal			Vertical			Diagonal		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lena	0.0115	-0.0035	-0.0254	0.0116	-0.0027	0.0041	0.0023	-0.0031	-0.0006
Baboon	0.0084	0.0054	-0.0061	-0.0009	-0.0031	-0.0011	-0.0009	-0.0006	0.0023
Barbara	0.0036	-0.0076	-0.0024	0.0061	0.0048	-0.0059	0.0055	-0.0043	0.0064
Peppers	-0.0078	-0.0072	-0.0051	0.0093	-0.0014	0.0034	0.0098	0.0013	0.0057

Over the past period, many methods have been introduced that were used to encrypt data. A comparison was made between a group of related methods and the proposed method in the results of the tests (PSNR, MSER, entropy, and coloration) tests that were implemented on Lina's image. The results of this comparison prove the efficiency and strength of the proposed method. Table 6 shows the results of this comparison.

Table 6. A comparison between the proposed method and some other methods

Method	Entropy	NPCR	UACI	Correlation		
				Horizontal	Vertical	Diagonal
Proposed method	7.99	99.67	33.33	-0.0058	0.0043	-0.0004
Guodong *et al.* [29]	7.99	99.62	33.39	---	---	---
Chunyuan *et al.* [30]	7.99	99.62	33.41	-0.0012	-0.0027	-0.0033
Salah *et al.* [31]	7.99	99.64	32.66	0.0096	-0.0071	-0.0079
Muhammad *et al.*[32]	7.99	99.59	33.12	-0.0024	-0.0018	-0.0025
Sarab *et al.* [33]	7.99	99.62	33.60	-0.0001	0.0002	-0.0001

4. CONCLUSION

Through the results obtained after implementing the proposed method on a group of experimental images and comparing them with the results of other methods, the proposed method achieved better efficiency and effectiveness. The use of random number generators at work increases the robustness and strength of the encryption system and prevents unauthorised persons from accessing the data. The results of the tests indicate that the randomness resulting from the use of LFSR and random maps provides a good level of security. The entropy test on the Lena image resulted in an entropy value of 7.99, which is close to 8. In addition, NPCR and UACI were 99.67 and 33.33, respectively, showing that the proposed method is powerful against various attacks. The resulting images do not provide opportunities for attackers to learn any information about the original images. To develop the work, DNA bases will be used to encode the data.

ACKNOWLEDGEMENTS

The authors would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq), Baghdad, Iraq, for supporting this work. They also appreciate the constructive comments of reviewers.

REFERENCES

[1] B. T. Ahmed, “A systematic overview of secure image steganography,” *International Journal of Advances in Applied Sciences (IJAAS)*, vol. 10, no. 2, pp. 178-187, Jun. 2021, doi: 10.11591/ijaas.v10.i2.pp178-187.

[2] L. Li, Y. Luo, S. Tang, L. Cao, and X. Ouyang, “Image encryption algorithm using chaotic maps and cellular automata,” *ICST Transactions on Security and Safety*, vol. 7, no. 26, Oct. 2020, doi: 10.4108/eai.21-6-2021.170238.

[3] W. Andre, “Efficient adaptation of the Karatsuba algorithm for implementing on FPGA very large scale multipliers for cryptographic algorithms,” *International Journal of Reconfigurable and Embedded Systems (IJRES)*, vol. 9, no. 3, pp. 235-241, Nov. 2020, doi: 10.11591/ijres.v9.i3.pp235-241.

[4] A. H. Khaleel and I. Q. Abduljaleel, “Chaotic image cryptography systems: a review,” *Samarra Journal of Pure and Applied Science*, vol. 3, no. 2, pp. 129–143, Sep. 2021, doi: 10.54153/sjpas.2021.v3i2.244.

[5] M. Es-Sabry, N. E. Akkad, M. Merras, A. Saaidi, and K. Satori, “A new image encryption algorithm using random numbers generation of two matrices and bit-shift operators,” *Soft Computing*, vol. 24, no. 5, pp. 3829–3848, 2020, doi: 10.1007/s00500-019-04151-8.

[6] D. A. Q. Shakir and A. J. Dawood, “3D chaos graph deep learning method to encrypt and decrypt digital image,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 25, no. 2, pp. 941-951, Feb. 2022, doi: 10.11591/ijeecs.v25.i2.pp941-951.

[7] A. A. Karawia and Y. A. Elmasry, “New encryption algorithm using bit-level permutation and non-invertible chaotic map,” *IEEE Access*, vol. 9, pp. 101357–101368, 2021, doi: 10.1109/ACCESS.2021.3096995.

[8] S. N. Prajwalasimha and L. Basavaraj, “Performance analysis of transformation and bogdonov chaotic substitution based image cryptosystem,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 188–195, 2020, doi: 10.11591/ijece.v10i1.pp188-195.

[9] Z. Deng and S. Zhong, “A digital image encryption algorithm based on chaotic mapping,” *Journal of Algorithms and Computational Technology*, vol. 13, pp. 1–11, 2019, doi: 10.1177/1748302619853470.

[10] M. K. Khairullah, A. A. Alkahtani, M. Z. B. Baharuddin, and A. M. Al-Jubari, “Designing 1D chaotic maps for fast chaotic image encryption,” *Electronics*, vol. 10, no. 17, Aug. 2021, doi: 10.3390/electronics10172116.

[11] R. Parameshachari and S. M. Chandramouli, “Building enhanced chaotic map encryption method for medical information system,” *Journal of System and Management Sciences*, vol. 11, no. 1, pp. 176–192, Mar. 2021, doi: 10.33168/JSMS.2021.0111.

[12] S. Patel and T. Veeramalai, “Image encryption using a spectrally efficient halton logistics tent (HaLT) Map and DNA encoding for secured image communication,” *Entropy*, vol. 24, no. 6, Jun. 2022, doi: 10.3390/e24060803.

[13] L. M. H. Yepdia, A. Tiedeu, and G. Kom, “A robust and fast image encryption scheme based on a mixing technique,” *Security and Communication Networks*, vol. 2021, pp. 1–17, Feb. 2021, doi: 10.1155/2021/6615708.

[14] C. Li, G. Luo, and C. Li, “An image encryption scheme based on the three-dimensional chaotic logistic map,” *International Journal of Network Security*, vol. 21, no. 1, pp. 22–29, 2019, doi: 10.6633/IJNS.201901 21(1).04.

[15] S. N. Lagmiri, N. Elalami, and J. Elalami, "Color and gray images encryption algorithm using chaotic systems of different dimensions," *International Journal of Computer Science and Network Security*, vol. 18, no. 1, pp. 79–86, 2018.

[16] H. A. Abdullah and H. N. Abdullah, "FPGA implementation of color image encryption using a new chaotic map," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 13, no. 1, pp. 129-137, Jan. 2019, doi: 10.11591/ijeecs.v13.i1.pp129-137.

[17] S. T. Allawi and M. M. Abbas, "A new method for image encryption based on 2D-3D Chaotic Maps," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 18, no. 11, pp. 39–43, 2020.

[18] L. Huang, S. Cai, M. Xiao, and X. Xiong, "A simple chaotic map-based image encryption system using both plaintext related permutation and diffusion," *Entropy*, vol. 20, no. 7, Jul. 2018, doi: 10.3390/e20070535.

[19] M. S. Fadhil, A. K. Farhan, and M. N. Fadhil, "Designing substitution box based on the 1D logistic map chaotic system," *IOP Conference Series: Materials Science and Engineering*, vol. 1076, no. 1, Feb. 2021, doi: 10.1088/1757-899X/1076/1/012041.

[20] Y. Hu and R. Tian, "Image encryption and decryption based on chaotic algorithm," *Journal of Applied Mathematics and Physics*, vol. 08, no. 09, pp. 1814–1825, 2020, doi: 10.4236/jamp.2020.89136.

[21] F. A. Salman and K. A. Salman, "Enhanced image encryption using two chaotic maps," *Journal of ICT Research and Applications*, vol. 14, no. 2, Dec. 2020, doi: 10.5614/itbj.ict.res.appl.2020.14.2.3.

[22] S. Askar, A. Karawia, A. Al-Khedhairi, and F. Al-Ammar, "An algorithm of image encryption using logistic and two-dimensional chaotic economic maps," *Entropy*, vol. 21, no. 1, Jan. 2019, doi: 10.3390/e21010044.

[23] C. Rekha and G. N. Krishnamurthy, "An optimized encryption algorithm and F function with dynamic substitution for creating S-box and P-box entries for blowfish algorithm," *Computer Science and Information Technologies (CSIT)*, vol. 2, no. 1, pp. 16–25, Mar. 2021, doi: 10.11591/csit.v2i1.p16-25.

[24] S. T. Allawi, "Image encryption based on chaotic mapping and random numbers," *Journal of Engineering and Applied Sciences*, vol. 14, no. 19, pp. 6954–6958, Oct. 2019, doi: 10.36478/jeasci.2019.6954.6958.

[25] S. Agarwal, "Secure image transmission using fractal and 2D-chaotic map," *Journal of Imaging*, vol. 4, no. 1, Jan. 2018, doi: 10.3390/jimaging4010017.

[26] N. Chaudhary, T. B. Shahi, and A. Neupane, "Secure image encryption using chaotic, hybrid chaotic and block cipher approach," *Journal of Imaging*, vol. 8, no. 6, 2022, doi: 10.3390/jimaging8060167.

[27] A. Yousif and A. H. Kashmar, "Key generator to encryption images based on chaotic maps," *Iraqi Journal of Science*, vol. 60, no. 2, pp. 362–370, 2019, doi: 10.24996/ijs.2019.60.2.16.

[28] M. D. Al-Hassani, "A novel technique for secure data cryptosystem based on chaotic key image generation," *Baghdad Science Journal*, vol. 19, no. 4, pp. 905–913, Aug. 2022, doi: 10.21123/bsj.2022.19.4.0905.

[29] G. Ye, K. Jiao, C. Pan, and X. Huang, "An effective framework for chaotic image encryption based on 3D logistic map," *Security and Communication Networks*, vol. 2018, pp. 1–11, Oct. 2018, doi: 10.1155/2018/8402578.

[30] C. Liu and Q. Ding, "A color image encryption scheme based on a novel 3D chaotic mapping," *Complexity*, vol. 2020, pp. 1–20, Dec. 2020, doi: 10.1155/2020/3837209.

[31] S. T. Allawi and D. R. Alshibani, "Color image encryption using LFSR, DNA, and 3D chaotic maps," *International Journal of Electrical and Computer Engineering Systems*, vol. 13, no. 10, pp. 885–893, Dec. 2022, doi: 10.32985/ijeces.13.10.4.

[32] M. Tanveer *et al.*, "Multi-images encryption scheme based on 3D chaotic map and substitution box," *IEEE Access*, vol. 9, pp. 73924–73937, 2021, doi: 10.1109/ACCESS.2021.3081362.

[33] I. A. Taqi and S. M. Hameed, "A new beta chaotic map with DNA encoding for color image encryption," *Iraqi Journal of Science*, vol. 61, no. 9, pp. 2371–2384, Sep. 2020, doi: 10.24996/ijs.2020.61.9.24.

BIOGRAPHIES OF AUTHORS

Salah Taha Allawi earned a B.Sc in Computer Science from Mustansiriyah University in 1992 and an MSc in Computer Science from Iraq Commission for Computers & Informatics, Informatics Institute for Postgraduate Studies in 2004. He is an associate professor at the Computer Science Department, College of Science, Mustansiriyah University. His research areas are image processing and information security. He has published a many research papers in local and international refereed journals as an author. He can be contacted at email: salah.taha@uomustansiriyah.edu.iq.

Nada Abdul Aziz Mustafa earned a BSc in Computer Science from Baghdad University, College of Education Ibn AL-Haitham in 2000 and an M.Sc in Computer Science from University of Sulymaina in 2010. She is a lecture at the College of languages, Baghdad University. Her research areas are image processing and information security. She has published a many research papers in local and international refereed journals as an author or co-author. She can be contacted at email: nada@colang.uobaghdad.edu.iq.