

First Libyan international Conference on Engineering Sciences & Applications (FLICESA_LA)
13 – 15 March 2023, Tripoli – Libya

Integration of 3D Chaotic Maps for Color Image Encryption

Nuha Omran Abokhdair
Computer Science Department,
Faculty of Science,
University of Zawia,
Zawia, Libya
abo.khdeir@zu.edu.ly

Ebtesam Rajeb Khather
Computer Science Department,
Faculty of Science,
University of Zawia,
Zawia, Libya
e.rajeb@zu.edu.ly

Mohamed Ab. Sultan
Department of Electrical and
Electronics Engineering
Higher Institute of Science and
Technology Zawia, Libya
abo_sultan2020@yahoo.com

Abstract— The use and transmission of color images have become common and more significant, which requires protection from unauthorized access. This research is presented to increase color image security through an image encryption algorithm. The proposed algorithm uses circle map for key generation, 3D logistic map for confusion and 3D henon map for diffusion. To enhance the sensitivity of a plain-image, SHA-1 is employed in our proposed method to calculate the hash value and use it as an input to circle map. Set of tests are used to evaluate the proposed algorithm. These tests include Key sensitivity, Information entropy, Correlation analysis, NPCR, and UACI. The experimental results show that the algorithm improves encryption efficiency; It has good security performance and can resist common attack methods.

Keywords—3D henon map, 3D logistic map, confusion, diffusion, Chaotic Map.

I. Introduction

Information security is becoming a more important factor in data transmission and storage nowadays[1]. This information consists of text, audio, image and other multimedia. Images have a wide application in the daily life of most of us. However, the more extensive the use of the images, the more important is their security [2]. Conventional encryption schemes such as DES, 3DES, RC5, AES, and RSA have many applications in text encryption, but they are not sufficient to fulfill the security requirements of image encryption. Images have different features such as their large size and high correlation among pixels[3][4].

Cryptographic algorithms using chaotic maps have attracted a great deal of attention and become an important topic[5]. Chaotic maps are used in confusion and diffusion mechanisms, which show excellent performance in image encryption techniques for their unpredictability and randomness[6]. Liu and Suoxia[7] proposed an encryption technique for grayscale images. This technique is based on logistic map with varying parameter to improve the weaknesses of logistic map, including small key space and uneven distribution of sequences, and to resist the phase space reconstruction attack. The experimental results show that the proposed algorithm is highly secure against attacks. Liu and et al. proposed a color image encryption algorithm based on two logistic maps[5]. The researchers use stream cipher for its

security and speed. The results show advantages of high-level security and large key space. Rui, in [3] presented an algorithm use 1D logistic map to confuse the addresses of a color image pixels and global diffusion to permute the bit-matrix which makes the three elements influence each other effectively without neglecting the relativity between R, G and B. Experiments show that this algorithm has some good properties such as easy to implement, large key space, and excellent encryption effect with just one round of iteration. Gorji and et al.[8] Presented an image encryption method based on Logistic and Tent chaotic maps and permutation-diffusion architecture. Results obtained from evaluation show that image encryption using this method is resistant against various attacks, including salt and pepper noise, data loss and universal search attack. Mondal and Mandal in[9] presented greyscale image encryption algorithm for secure encryption and efficient transmission of data. This algorithm is divided into three stages including: the random number generation process, the image permutation process and the substitution process. The results of this algorithm for Lena image, the entropy was 7.9967 a, average correlation coefficient 0.00296, NPCR and UAC was 99.61 and 33.50 respectively. The proposed encryption algorithm in ref [10] is based on Henon map. This algorithm is based on fully layered encryption technique to provide higher level of confidentiality. The researcher does not exhibit NPCR and UACI in result analyzing. The average calculation of correlation and entropy determine the quality of encrypted image. In ref [11], the researcher proposed an algorithm for grayscale image encryption based on Nested Piece Wise Linear Chaotic Map. This method combines pixel shuffling, bit shuffling, and diffusion. The cipher image generated by this method is the same size as the plain image and is suitable for practical use in the secure transmission of confidential information over the Internet.

From the related work, it is noted that the current image encryption systems depend on the chaotic system but mostly in low-dimensional domains. This low dimension have disadvantages like limited security and provide small key space. high dimension like 3D maps offer greater security against cryptanalytic attack [12]. In this paper, a new chaotic based encryption scheme for color images is proposed. This scheme uses the 3D logistic map for image scrambling; 3D

Henon is used for value transformation and circle map for key generation.

This paper is organized as follows: Section 2 briefly introduces the basic theory of the proposed algorithm. Section 3 describes the proposed encryption algorithm; the proposed system performance measures and security analysis are given in Section 4. And finally, we summarize our conclusions in Section 5.

II. BASIC THEORY OF THE PROPOSED ALGORITHM

A. 3D Logistic Map

The logistic map is a three dimensions chaos function and given by the following equation[13]:

$$\begin{aligned} X_{i+1} &= \lambda x_i(1 - X_i) + \beta y_i^2 x_i + \alpha z_i^3 \\ y_{i+1} &= \lambda y_i(1 - y_i) + \beta z_i^2 y_i + \alpha x_i^3 \\ z_{i+1} &= \lambda z_i(1 - z_i) + \beta x_i^2 z_i + \alpha y_i^3 \end{aligned} \tag{1}$$

When $0.35 < \lambda < 3.81$; $0 < \beta < 0.022$; $0 < \alpha < 0.015$ are set, the 3D logistic map (1) exhibits a chaotic behavior if the initial values $x_0, y_0, z_0 \in (0, 1)$. In the proposed method the control parameters λ, β, α are used as keys. The values are obtained chaotically from circle map, and x_0, y_0, z_0 are equal to 1.

B. 3D Henon Map

Henon chaotic map was discovered in 1978, it is mathematical in nature, and is used as a privet key stream cipher cryptographic system. The 3D Henon map has reversibility and simple geometric vision. Additionally, it will be lessening the errors in the calculation because its coefficient is an integer, and can be represented by the following formula[14]:

$$\begin{aligned} X_{i+1} &= \alpha - y_i^2 - bz_i \\ y_{i+1} &= x_i \\ z_{i+1} &= y_i \end{aligned} \tag{2}$$

Where $1.54 < |a| < 2$, $0 < |b| < 1$ and the range of x_0, y_0, z_0 between 0 and 1. In the introduced method $a=1.7$, $b=0.1$ and x_0, y_0, z_0 are the keys generated by circle map.

C. Circle Map

The circle map is a dynamic system, which is initially determined by Andrey Kolmogorov. It is a simplified model that is used to determine the mechanical rotors. The Equation denotes the formula to calculate the circle map, which is a simplified model in electronics. Mathematically, the circle map is represented by (3)[15]:

$$X_{i+1} = \left\{ X_i + b - \left(\frac{a}{2\pi} \right) \sin(2\pi x_i) \right\} \text{mod}(1) \tag{3}$$

In this situation, the circle map is used for key generation where $a=0.2$, $b=0.5$, $x_0=1$.

III. THE PROPOSED SCHEME

In this section, we are going to illustrate the proposed encryption algorithm. As shown in Fig. 1, this algorithm consists of three phases namely: key generation, confusion

and diffusion. The key produced from key generation step is used as input into confusion and diffusion steps. Using one cycle of confusion-diffusion is insecure for image encryption. Therefore, to enhance the security of the proposed algorithm, more than one round of confusion-diffusion is employed in the proposed method.

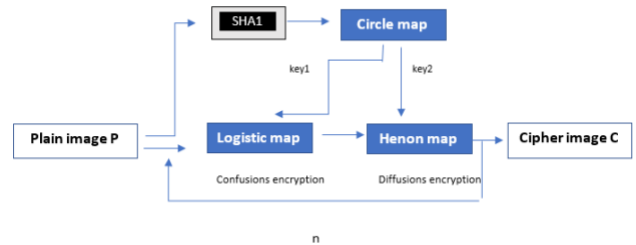


Fig. 1. Block diagram of the proposed image encryption algorithm.

A. Key Generation

This phase is used to generate the parameters of the key, which are used, along with the image, as inputs to confusion and diffusion phases.

SHA-1 is firstly applied on the plain-image p. the obtained hash vector h consist of 160 bits (20 bytes), that is divided into six factors by the following equations:

$$\begin{aligned} h1 &= \frac{\sum_{i=1}^3 h(i)}{\sum_{i=1}^3 h(i)+1} \\ h2 &= \frac{\sum_{i=4}^6 h(i)}{\sum_{i=4}^6 h(i)+1} \\ h3 &= \frac{\sum_{i=7}^9 h(i)}{\sum_{i=7}^9 h(i)+1} \\ h4 &= \frac{\sum_{i=10}^{12} h(i)}{\sum_{i=10}^{12} h(i)+1} \\ h5 &= \frac{\sum_{i=13}^{16} h(i)}{\sum_{i=13}^{16} h(i)+1} \\ h6 &= \frac{\sum_{i=14}^{20} h(i)}{\sum_{i=14}^{20} h(i)+1} \end{aligned} \tag{4}$$

Secondly, all h_i values produced in the previous step are set as initial values of the circle map where h_1, h_2 and h_3 are used to represent x_i in (3) to generate the keys of logistic map. h_4, h_5 and h_6 are used to generate the keys of henon map. circle map generates chaotic numbers between 0 and 1, where $a=0.2$ and $b=0.5$. a and b are considered as control parameters.

B. Confusion Stage

the logistic map is used to confuse the image by applying (1). The initial values x_1, y_1 and z_1 are set to one and the parameters λ, β and α are extracted from the circle map as h_1, h_2 and h_3 , respectively.

To increase the randomness degree, the initial iterated values should be discarded. All the decimal numbers within x_i, y_i and z_i are transferred using the following equation:

$$\begin{aligned} x_i &= [x_i * 10^{14}] \text{mod } n \\ y_i &= [y_i * 10^{14}] \text{mod } m \\ z_i &= [z_i * 10^{14}] \text{mod } 3 \end{aligned} \tag{5}$$

Then, these values are used to perform a circular permutation for the plain image P along the row, column and color channel, respectively. After completing the permutation operation, permuted image A can be obtained.

C. Diffusion Stage

using a permutation only scheme is not secure image encryption algorithm due to the invariance of the statistical property as it only changes the pixel positions. Therefore, to ensure the security, a diffusion operation for the permuted image is applied using 3D henon map. The iteration is achieved using the initial conditions $\alpha = 1.7$ and $b = 0.1$. the Parameters h4, h5 and h6, that obtained from circle map, are set to x_1, y_1 and z_1 in the henon map, respectively.

All the elements in x_i, y_i and z_i should be transformed into integer numbers between 0 and 255 through the next Equation to satisfy the pixel interval.

$$\begin{aligned} x_i &= [x_i * 10^3] \bmod 256 \\ y_i &= [y_i * 10^3] \bmod 256 \\ z_i &= [z_i * 10^3] \bmod 256 \end{aligned} \tag{6}$$

The elements x_i, y_i and z_i are rearranged to form matrix V, which has the same dimensions as the original image, and added to permuted image A. Finally, cipher image C is obtained after both permutation and diffusion are completed.

IV. EVALUATION TESTS

In order to evaluate the performance of the proposed algorithm, five color images are selected for encryption, refer to Fig. 2. There are many tests used to analyze the effect of the proposed technique on the ciphered image and the recovered image. The experiments are performed on a computer with Intel Quad-Core i7-8550U CPU, 16G RAM with Windows 10 using MATLAB. The original images are encrypted with different number of rounds. The encrypted image is recovered using the decryption algorithm. As shown in Fig. 3, The original image and the decrypted one are equal for each pixel which shows that the proposed algorithm is lossless algorithm.

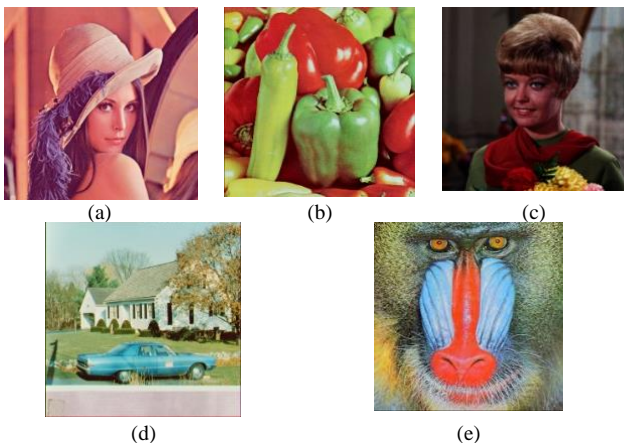


Fig. 2. Original test images: (a)Lena, (b) Pepper, (c) Woman, (d) House and (e) Baboon

A. Statistical Analysis

1) Histogram and Entropy Analysis

Information entropy is the most significant feature of randomness. Entropy is a statistical parameter that is defined to measure the uncertainly and randomness of a package of data. the information entropy of the ciphered image should be close to 8, in order to consider its histogram as sufficiently uniform[16][17] [18]. Equation (7) is used to calculate the entropy H(m) of a plaintext message m.

$$H(m) = \sum_{i=0}^{L-1} p(m_i) \log \frac{1}{p(m_i)} \tag{7}$$

Where L is the total number of symbols, $p(m_i)$ represents the probability of occurrence of symbol m_i and log denotes the base 2 logarithm so that the entropy is expressed in bits.

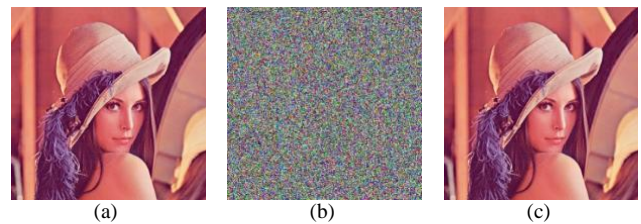


Fig. 3. Image encryption result. (a) original image; (b) encrypted image; (c) decrypted image;

Table I illustrates the entropy values for a set of cipher images with different confusion-diffusion rounds. The results proved that the entropy values of encrypted images using all number of rounds are close to 8. Moreover, until three rounds, the entropy value is increased while the number of rounds is increased in most of test images.

TABLE I. ENTROPY VALUES OF ENCRYPTED IMAGES

Rounds Image	1	2	3	4	5
Lena	7.9990	7.9991	7.9990	7.9991	7.9991
Baboon	7.9986	7.9987	7.9988	7.9986	7.9989
Woman	7.9984	7.9989	7.9989	7.9991	7.9991
House	7.9995	7.9998	7.9998	7.9997	7.9998
peppers	7.9997	7.9997	7.9998	7.9997	7.9998

Fig. 4 shows the histograms of the RGB channels in the original image in fig.4 (a) and the histograms encrypted image after four rounds of confusion and diffusion is shown in fig. 4(b). it is clearly obvious that the histograms of the encrypted image are uniform.

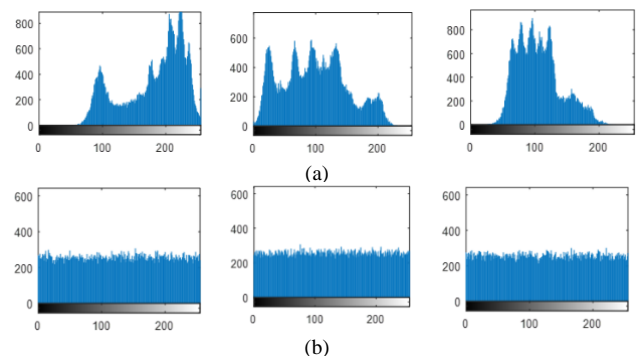


Fig. 4. Histogram analysis of Lena. (a) Histogram of the original image; (b) Histogram of the encrypted image

2) Correlation analysis

In plain image each pixel is usually highly correlated with its adjacent pixels either in horizontal, vertical or diagonal

rounds Image	1	2	3	4	5
Lena	-0.0030968	-0.01259	0.0147	-0.0033	0.010611
Baboon	-0.0116111	0.0005	0.02068	0.001756	0.023111
Woman	-0.0023667	-0.00284	0.015033	-0.00766	0.022467
House	-0.0166444	-0.00446	-0.00917	0.002186	0.003333
peppers	0.00005667	0.001933	-0.00164	0.003943	-0.01029

directions. In contrast, the correlation between adjacent pixels in cipher image must be very low in robust cipher systems. Equation (8) is used to calculate the correlation of adjacent pixels.

$$cov(u, v) = E \{ (u - E(u))(v - E(v)) \}$$

$$r_{uv} = \frac{cov(u, v)}{\sqrt{D(u)}\sqrt{D(v)}} \tag{8}$$

Where u and v are pixel values of two adjacent pixels, $E(u) = \frac{1}{P} \sum_{i=1}^P u_i$, and $D(u) = \frac{1}{P} \sum_{i=1}^P (u_i - E(u))^2$.

The correlation coefficient close to zero indicates that low correlation exists between the pixels. Table II shows the value of correlation coefficients in the set of cipher images with different rounds.

TABLE II. CORRELATIONS OF THE ENCRYPTED IMAGES

Illustrated in Fig. 5 is the visual correlation distribution of adjacent neighboring plain-image pixel in horizontal, vertical and diagonal direction for Lena while Fig. 6 is the visual correlation distribution of encrypted pixel using four rounds in horizontal, vertical and diagonal direction. As shown in Fig. 5, the plain-image neighboring pixels are clustered along a straight line meaning pixel values along each direction has high correlation. Meanwhile as shown in Fig. 6, the encrypted image pixel values are scatter all over the entire space meaning the correlation of pixel values for each direction in the encrypted image drastically reduce.

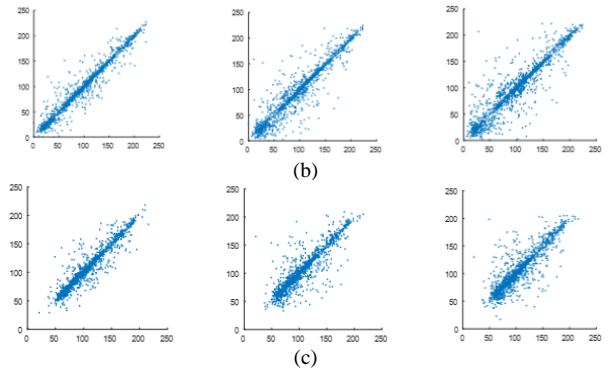
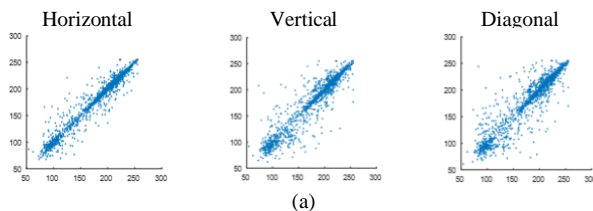


Fig. 5. Correlations of two adjacent pixels in Lena plain-image. (a) Red; (b) Green; (c) Blue

According to the results, four rounds of the proposed algorithm provide the best correlation results. Therefore, to balance between entropy results and correlation results, it is advised to perform four rounds of confusion and diffusion.

B. Differential Attack Analysis

The two measurements are mostly used to evaluate the effect of the change of one pixel in the plain image on the all cipher image[17].

1) Rate of Change of Pixel Number (NPCR)

NPCR means the change rate of the number of pixels of ciphered image while one pixel of plain-image is changed[17].

$$NPCR = \sum_{i,j} \frac{D(i,j)}{w * H} \times 100 \tag{9}$$

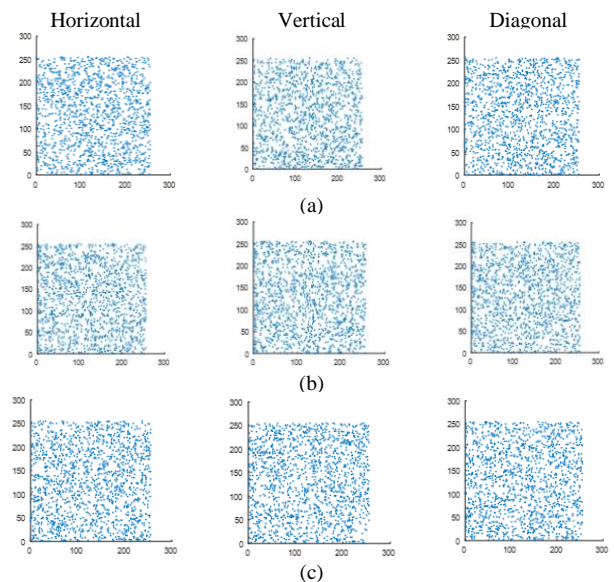


Fig. 6. Correlations of two adjacent pixels in the cipher-image. (a) Red; (b) Green; (c) Blue

The value of one pixel of plain-image is changed. Experimental results are shown in Table III.

TABLE III. THE NPCR RESULTS OF THE PROPOSED IMAGE ENCRYPTION ALGORITHM

Rounds Image	1	2	3	4	5
Lena	0.9960	0.9963	0.9962	0.9960	0.9961
Baboon	0.9959	0.9959	0.9960	0.9961	0.9961
Woman	0.9962	0.9960	0.9963	0.9961	0.9960
House	0.9961	0.9961	0.9963	0.9962	0.9962
peppers	0.9962	0.9961	0.9960	0.9962	0.9961

2) Unified Average Changing Intensity (UACI)

UACI calculates the total number of pixels that have been changed in the cipher images obtained for the plain image and its modified plain image at the same location[17][19].

$$UACI = \frac{1}{w * H} (\sum \frac{|c_1(i,j) - c_2(i,j)|}{225}) \times 100 \quad (10)$$

Table IV illustrates the UACI values for set of cipher image for number of rounds.

The results in table III and IV prove that the proposed algorithm is resistant against differential attack.

TABLE IV. THE NPCR RESULTS OF THE PROPOSED IMAGE ENCRYPTION ALGORITHM

Rounds Image	1	2	3	4	5
Lena	0.3332	0.3342	0.3342	0.3345	0.3349
Baboon	0.3326	0.3334	0.3347	0.3351	0.3340
Woman	0.3347	0.3348	0.3346	0.3347	0.3339
House	0.3337	0.33467	0.3346	0.3347	0.3344
peppers	0.3337	0.3346	0.3342	0.3354	0.3348

C. Key sensitivity

A good cryptosystem should be sensitive to a small change in secret keys i.e. a small change in secret keys in decoding process results into a completely different decoded image. . Figure 5 shows the sensitivity results. It is observed from Figure 5 that the proposed algorithm is highly sensitive to encryption keys. Therefore, the encrypted plain image can only be recover with the correct key.

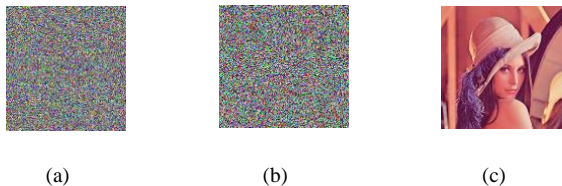


Fig. 7. Key sensitivity results. (a) Decrypted with key 1; (b) Decrypted with key 2; (c) Decrypted with correct key

V. CONCLUSION

In this paper, a secure chaotic-based color image encryption algorithm is proposed. The algorithm consists of three chaotic maps. Circle map is used for generating the encryption key, 3D logistic map is used for confusion process, and 3D henon map is used for diffusion process. The performance of the proposed algorithm was then evaluated

using different tests including information entropy, histogram analysis, adjacent pixels correlation coefficient, key sensitivity, NPCR and UACI as metric. The results gained confirmed that the proposed algorithm shows a good encryption performance with high security level, better robustness and resistance to attacks.

REFERENCES

- [1] H. Rathod, M. S. Sisodia, and S. K. Sharma, 'Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)', vol. 1, no. 3, pp. 7–13.
- [2] I. F. Elashry, 'Homomorphic image encryption', no. July, 2009, doi: 10.1117/1.3167847.
- [3] H. Liu and X. Wang, 'Color image encryption based on one-time keys and robust chaotic maps', Comput. Math. with Appl., vol. 59, no. 10, pp. 3320–3327, 2010, doi: 10.1016/j.camwa.2010.03.017.
- [4] L. Rui, 'New algorithm for color image encryption using improved 1D logistic chaotic map', Open Cybern. Syst. J., vol. 9, pp. 210–216, 2015, doi: 10.2174/1874110X01509010210.
- [5] H. Liu, X. Wang, and A. Kadir, 'Image encryption using DNA complementary rule and chaotic maps', Appl. Soft Comput. J., vol. 12, no. 5, pp. 1457–1466, 2012, doi: 10.1016/j.asoc.2012.01.016.
- [6] A. M. Alabaichi, 'Color Image Encryption using 3D Chaotic Map with AES key Dependent S-Box', vol. 16, no. 10, pp. 105–115, 2016.
- [7] S. Liu, J. Sun, and Z. Xu, 'An improved image encryption algorithm based on chaotic system', J. Comput., vol. 4, no. 11, pp. 1091–1100, 2009, doi: 10.4304/jcp.4.11.1091-1100.
- [8] R. B. Gorji, 'A new image encryption method using chaotic map', vol. 2, no. 2, pp. 251–256, 2015.
- [9] B. Mondal and T. Mandal, 'A nobel chaos based secure image encryption algorithm', Int. J. Appl. Eng. Res., vol. 11, no. 5, pp. 3120–3127, 2016.
- [10] L. Liu and S. Miao, 'A new image encryption algorithm based on logistic chaotic map with varying parameter', Springerplus, pp. 1–12, 2016, doi: 10.1186/s40064-016-1959-1.
- [11] R. Kumar and B. Raisen, 'A New Approach of Colour Image Encryption Based on Henon like Chaotic Map', vol. 3, no. 6, pp. 14–20, 2013.
- [12] A. Jolfaei and A. Mirghadri, 'An image encryption approach using chaos and stream cipher', J. Theor. Appl. Inf. Technol., vol. 19, no. 2, pp. 117–125, 2010.
- [13] P. N. Khade and P. M. Narnaware, '3D Chaotic Functions for Image Encryption', Int. J. Comput. Sci. Issues, no. May 2012, 2012.
- [14] E. Albhrany and T. Alshekly, 'A New Key Stream Generator Based on 3D Henon map and 3D Cat map', no. February, 2017.
- [15] H. Lu, X. Wang, Z. Fei, and M. Qiu, 'The effects of using chaotic map on improving the performance of multiobjective evolutionary algorithms', Math. Probl. Eng., vol. 2014, 2014, doi: 10.1155/2014/924652.
- [16] A. Soleymani, M. J. Nordin, and E. Sundararajan, 'A chaotic cryptosystem for images based on Henon and Arnold cat map', Sci. World J., vol. 2014, no. October, 2014, doi: 10.1155/2014/536930.
- [17] P. R. Sankpal and P. A. Vijaya, 'Image encryption using chaotic maps: A survey', Proc. - 2014 5th Int. Conf. Signal Image Process. ICSIP 2014, no. February, pp. 102–107, 2014, doi: 10.1109/ICSIP.2014.80.
- [18] N. O. Abokhdair, 'An Experimental Study of the Effect of AES in Combination with 2D Lower Triangular Chaotic Map', no. March, pp. 3–7, 2018.
- [19] N. O. Abokhdair, A. B. A. Manaf, and M. Zamani, 'Integration of chaotic map and confusion technique for color medical image encryption', in 6th International Conference on Digital Content, Multimedia Technology and its Applications, 2010, pp. 20–23.

