j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 6, No:4. 2023

Journal Selection › Manuscript Preparation › Manuscript Submission › Peer-review & Revision › Acceptance › Copy editing English editing › Proofreading › Publishing
Rejection
OPEN ACCESS

An Image Encryption Method Based on Lorenz Chaotic Map and Hunter-Prey Optimization

[1*]Qutaiba K. Abed, [2]Waleed A. Mahmoud Al-Jawher

[1]*Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatics, Baghdad, Iraq*

[2]*College Engineering, Uruk University, Baghdad, Iraq.*

phd202130682@iips.edu.iq

Abstract Through the development of communication technology, fast and efficient tools are required to practically secure the process of data exchange in securing images. This paper presents a new method of encryption for protecting images against many attacks from unsafe public networks. Lorenz chaos map is used to generate a sequence of random numbers for each stage depending on the initial parameters. The Hunter Prey optimization algorithm is applied in order to obtain these parameters to use them based on the original image. Therefore, the random sequence number generated by the Lorenz chaotic map will be different from one image to another. That will make it unpredictable and very difficult to discover the process of encryption. The results of simulation experiments demonstrate that the encryption algorithm have passed the plaintext sensitivity test with the NPCR of 0.99785 and the UACI of 0.33623. As well as the correlation coefficient test values in the three directions gave the values of (v = -0.0007, h = -0.0000, d = 0.0005). Also, the calculated information entropy test value was 7.9983. These results demonstrate that this algorithm is very strong enough to withstand the various types of attacks that images can be exposed during transmission on the Internet or any public network. The security analysis's comparison of the proposed changes to similar ones revealed that the proposed encryption system is more efficient.

Crossref 10.36371/port.2023.4.3

Keywords: *Hunter pray algorithm, Image encryption, Lorenz chaotic map, Parameter adjustment*

1. INTRODUCTION

The widespread use of information technology and the network's popularity have increased our awareness of the significance of secure data transfer. Digital images, a crucial medium for the transfer of information, can be secured in one of two ways: information concealment or encryption [1]–[13]. Image encryption has its roots in the early classical encryption theory [14]–[25]. However, due to the differences in the storage methods and inherent properties of digital images and texts, such as high redundancy, high correlation, and a significant amount of data between adjacent pixels, traditional encryption techniques like RSA (Rivest Shamir Adleman) and DES (Data Encryption Standard) are no longer helpful [26], [27]. Thus, several academics have put forth a variety of encryption techniques [28]–[31]. These technologies primarily rely on wavelet compression [32], [33], chaotic systems [34]–[36], cellular automata [37]–[39], and DNA computing [40]–[41].

Numerous areas of chaos research have advanced significantly[42]. Chaos satisfies the criteria for image encryption because of its properties, including great sensitivity to beginning circumstances and control settings and intrinsic unpredictability[43]–[45]. This type of encryption typically involves the two phases of diffusion and scrambling. Since Matthews et al.[46] proposed a time pad for communications encryption utilizing one-dimensional chaotic maps, they used several chaotic system-based image encryption techniques. To address the security flaws in the schemes presented by Gao He Chen [47] and Rhouma and Belghith[48] , for instance, Fuh GwoJeng et al. [49] and others developed an image encryption system based on a hype-chaos. Image encryption using a one-time key and two potent chaotic maps was shown by Liu et al. [50]. A high-dimensional chaotic image encryption system using a perceptron model was proposed by Wang et al. [51]. The security of encryption techniques can be improved by using complex, chaotic systems, such as hyper-chaotic systems or high-dimensional ones, to produce chaotic sequences with higher unpredictability.

In recent years, the swarm intelligence optimization method has been extensively researched in human intelligence, such as associative memory, perception and recognition due to its remarkable performance in parallelism, resilience, evolution, and other aspects [52]. Numerous image encryption academics have also taken notice of it. For instance, Wang et al. [53] suggested an optimization technique for a DNA coding and image encryption system. They created an encryption method by choosing the critical sequence using PSO, using a DNA mask, and rapidly shuffling plaintext

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 6, No:4. 2023

Journal Selection › Manuscript Preparation › Manuscript Submission › Peer-review & Revision › Acceptance › Copy editing English editing › Proofreading › Publishing
Rejection
OPEN ACCESS

DNA coding to function. An image encryption technique based on a DNA chaos map and genetic algorithm (GA) was suggested by Enayatifar R et al. Enhancing the DNA mask quality produced the best mask that works with pure images. Wang, J. et al. [54]suggested a novel framework employing the population-based particle swarm optimization technique to increase the encryption speed. However, the encryption method can't effectively fend off a differential attack because there is a poor connection between the plaintext image and the scrambled phase key. In the techniques above, a frequent issue is that the produced data has poor pseudo-randomness and ergodicity, which results in inadequate security performance. Additionally, the conventional swarm intelligence algorithm is stuck in local optimization due to parameter selection and early convergence.

When a slight change in the chaos parameters, it gives a different output, and the challenge is selecting the optimum chaos parameters to obtain the best output. The duty of hunter-prey optimization through the generation is to find the best parameters for the Lorenz chaotic map. The optimization will be based on the objective function that will produce the best pseudorandom numbers that could be used in the diffusion and confusion processes. Such hybrid technique in the security will result in a strong secure system against various types of attacks. The main contribution of current paper can be sumarized as follows:

(1) A new encryption system is developed, and the dynamical analyses are studied. The proposed algorithm is implented by combining a Lorenz chaotic map with the Hunter prey optimization.

(2) The Hunter Prey Optimizer was used for diffusion coefficients, and confusion operations in the proposed system. Attackers have to search over a far wider range of potential keys as a result, it will make the algorithm more difficult to crack.

(3) Hunter-prey optimizer is used to determine which encrypted image parameters lower the correlation between adjacent pixels. This improves the algorithm's resistance to statistical attacks.

(4) The practical results have shown this method is effective in the encryption and decryption process with a higher chaotic range, and a higher complexity compared to the traditional chaotic maps.

(5) A number of encryption analysis methods, which include the correlation coefficient, PSNR, MSE, entropy are used to assess the security of the proposed system. Results confirm better security of encryption of the proposed merged technique than those available.

The rest of this paper is structured of the following sections as follows: design and dynamical analyses of Lorenz chaotic map system are provided in Section section 2, hunter-prey optimization algorithms in section 3 the proposed Encryption process method described in section 4. The decryption process in section 5, Experimental results of the security measures of the proposed technique using several encryption security analysis tools is provides in section 6. Finally, the conclusion in given in section 7.

2. THE LORENZ CHAOTİC MAP SYSTEM

A random sequence generator called chaotic is extremely sensitive to the beginning values. As a result, this randomness is unexpected because even a tiny change in the initial numbers might significantly impact the final result. The Lorenz system used in this work [55] is the optimum model for a chaotic system. The three dependent variables in Lorenz's chaotic system were designated as x, y, and z. Three equations make up Lorenz's chaotic map.

$$x = \sigma^{x}(y - x)$$

$$y = \gamma^{x}x - x^{x}z - y \qquad (1)$$

$$z = x^{x}y - b^{x}z$$

Where σ = 10, γ = 28, and b = 8/3, The Hunter prey optimization algorithm will select the other parameters.

3. HUNTER-PREY OPTIMIZATION ALGORITHMS

It's a good idea to get inspiration from nature when attacking challenges. Organisms engage in interactions with one another in the natural world. One of the interactions in nature was between the hunter and the prey. The most notable biological observations are those of hunters and prey, and there is a heated argument over this among environmental scientists. There are numerous ways to catch prey. Some scenarios have evolved into algorithms. The hunter chooses the prey farthest away from the swarm since the prey is a swarm and the hunter is seeking it. The hunter locates his prey, chases it, and eventually captures it. The prey is simultaneously looking for food and finding a safe location to hide from predators. The optimal answer for the goal function is where we believe to be the safe place.[56]

The reasons behind the selection of the Hunter-prey optimization in the current application is inspired by the behavior of predator animals such as lions, leopards and wolves, and preys such as stag and gazelle. There are many scenarios of animal hunting behavior, and some of them have transformed into optimization algorithms. The reasons behind the selection of the Hunter-prey optimization in the current application since it has the advantages of a rapid convergence rate and a significant optimization capacity. As well as at present, researchers have achieved good results in optimizing mathematical functions and constrained engineering applications with this algorithm.

All optimization approaches have an identical overall structure. The objective function is then calculated for each member of the original population, which is first randomly selected. Equation (2) generates the positions of each member of the beginning population at random within the search space.

$$x_i = \text{rand}\,(1, d) \cdot * \,(ub - lb) + lb \qquad (2)$$

The fitness function can be used to determine whether a solution is excellent or terrible, but it takes more than one run to find the ideal answer. For the purpose of directing search agents to the best location, a search mechanism needs to be established and used repeatedly. Equation (3) is suggested for the hunter search method.

$$x_{i,j}(t+1) = x_{i,j}(t) + 0.5\left[\left(2CZP_{pos(j)} - x_{i,j}(t)\right) + \left(2(1-C)Z\mu_{(j)} - x_{i,j}(t)\right)\right]. \qquad (3)$$

The hunter's location is updated using equation (3), where l is the mean of all positions, Ppos is the prey position, x (t) is the current position, and Z is an adaptive parameter determined by equation (4).

$$\begin{aligned} P &= \vec{R}_1 < C; IDX = (P == 0); \\ Z &= R_2 \otimes IDX + \vec{R}_3 \otimes (\sim IDX) \end{aligned} \qquad (4)$$

The random vectors R1 and R3 are in the interval [0,1]. P is a random vector with the number of problem variables as its values, 0 and 1. A random number in the interval [0,1] is R2. The vector R1's index number, IDX, satisfies the condition (P == 0). Over the course of iterations, the value of C, the balance parameter between exploration and exploitation, drops from 1 to 0.02. C is computed in this way:

$$C = 1 - it\left(\frac{0.98}{\text{MaxIt}}\right) \qquad (5)$$

where MaxIt is the maximum value of the current iteration. it is the highest possible number of reruns. The prey's position (Ppos) is determined by first utilizing Eq. (6) to determine the average position (μ), and then calculating the separation between each search agent and this mean position

$$\mu = \frac{1}{n}\sum_{i=1}^{n} \vec{x}_i \qquad (6)$$

the distance determined by applying Eq. (7), which uses the Euclidean distance.

$$D_{euc(i)} = \left(\sum_{j=1}^{d} \left(x_{i,j} - \mu_j\right)^2\right)^{\frac{1}{2}} \qquad (7)$$

Using Equation (8), prey (Ppos) is defined as the search agent that is furthest away from the mean of positions.

$$\vec{P}_{pos} = \vec{x}_i \mid i \text{ is index of Max (end)sort } (D_{\text{euc}}). \qquad (8)$$

The method will have late convergence if we always take into account the search agent with the highest distance from the average position (μ) in each iteration. The hunting scenario states that the prey dies when taken by the hunter, and the hunter then moves on to the next victim. Eq. (9) is a decreasing mechanism that we investigate in order to solve this problem.

$$\text{kbest} = \text{round}\,(C \times N) \qquad (9)$$

where N is the number of search agents. Now, we change Eq. (8) and calculate the prey position as Eq. (10)

$$\vec{P}_{\text{pos}} = \vec{x}_i \mid \text{ i is sorted } D_{\text{euc}} \text{ (kbest)} \qquad (10)$$

We think that the optimal global location is the optimum safe position since it will boost the prey's chances of survival and allow the hunter to choose a different target. The recommended equation (11) is used to update the prey position.

$$x_{i,j}(t+1) = T_{pos(j)} + CZ\cos\,(2\pi R_4) \times \left(T_{pos(j)} - x_{i,j}(t)\right) \qquad (11)$$

where x (t) is the current position of the prey, x (t+1) is the next position of the prey, Tpos is the optimum global position, Z is an adaptive parameter calculated by Eq. (4), and R4 is a random number in the range [-1, 1]. choosing the hunter and prey in this algorithm in Eqs. (3) and (11) as Eq. (12)

$$x_i(t+1) = \begin{cases} x_i(t) + 0.5\left[\left(2CZP_{\text{pos}} - x_i(t)\right) + (2(1-c)Z\mu - x_i(t))\right] & \text{if } R_5 < \beta (12a) \\ T_{pos} + CZ\cos\,(2\pi R_4) \times \left(T_{\text{pos}} - x_i(t)\right) & \text{else } (12b) \end{cases} \qquad (12)$$

where b is a regulatory parameter, and R5 is a random number in the interval [0, 1]. The value of b is set at 0.1 in this study. When the R5 value is less than b, the search agent is regarded as a hunter, and Eq. (12a) is used to update its next location; when the R5 value is more than b, the search agent is seen as prey, and Eq. (12b) is used to update its next position.

4. THE PROPOSED ENCRYPTION SYSTEM

This system used a new encryption method by merging Lorenz's chaotic map with the Hunter Prey optimization algorithm. The Hunter prey algorithm improves the initial parameters of the Lorenz chaotic map and chooses the best among them based on the original image. As a result, the parameters could generate the best initial chaos numbers. This leads to the lowest correlation for confusion and the highest entropy for the diffusion of the encrypted image. The two objective functions are used one for diffusion and the other for confusion. Lorenz's chaotic map was used to generate random numbers to make diffusion and confusion for each pixel of the image. It uniforms the pixels through diffusion. These operations will be explained in detail through the following steps:

Step 1: Input the original image.
Step2: convert the original image into one dimension (1D)
Step3: Apply Hunter prey optimization to get Lorenz chaotic map parameters (X_1, X_2, and X_3) which produce the random numbers for shuffling the image as follows:

a. Generate the initial populations, and the dimension of each element is three parameters (Y1, Y2, and Y3).

b. These parameters are used with the Lorenz chaotic map to generate pseudorandom numbers (R) to diffuse the image.

c. Diffuse the image by using the pseudorandom numbers.

$$img2= img \oplus R \qquad (13)$$

where img2 is the diffusion image, img is the original image, and R is a vector of random numbers generated by chaos.

d. Evaluate the result of the diffused image using the entropy objective function using the following equation.

$$\text{maximum } E=\text{entropy (img2)}. \qquad (14)$$

where E is entropy, the value of the fitness.

e. Update the parameters of the population.

f. Repeat the same process until you finish the whole iterations.

g. Get the optimal solution that achieves the maximum output through the objective function in order to produce the diffused image.

Step 5 Confuse the image to get the minimum correlation between pixels as follows.

a. Generate the initial population, and the dimension of each element will include three values (X1, X2, and X3) for using it as initial parameters for the Lorenz chaotic map.

b. Lorenz chaotic map used with the parameters (X1, X2, and X3) for generating a vector 1D of chaos numbers for image shuffling.

c. Sort the vector of 1D ascending and get the index (idx) of all locations as a vector of one dimension.

d. Shuffle the image by using the index vector (idx) through the following equation.

Img3=img2 (idx (:))   (15)

where img3 is the shuffled image and img2 is the diffused image

e. Evaluate the result of the Lorenz chaotic map by using the correlation objective function

C=|H_correlation(img3) +V_correlation (img3) +D_correlation (img3)| (16)

C represents the fitness value, representing the total horizontal, vertical, and diagonal correlation, H_correlation is the horizontal correlation, V_correlation is the vertical correlation, and D_correlation is the diagonal correlation.

f. Update the parameters and evaluate the result by using the same objective function.

g. Continue until you reach the end of iterations and get the optimal parameters for Lorenz's chaotic map to shuffle the image.

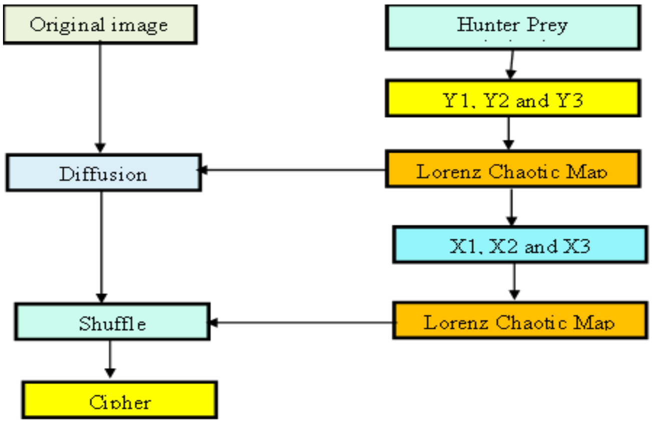


Fig 1: *Block diagram of the proposed encyption system*

5. DECRYPTION PROCESS

The same encryption procedures are used for decryption but in reverse. Utilize the three parameters with the Lorenz chaotic map to generate the identical random numbers used in the encryption phase. using the three keys (X1, X2, and X3) to reverse the scrambled image and using the three keys (Y1, Y2, and Y3) to produce the random numbers is also necessary to reverse the diffusion of the image and get the original image before the encryption process.

6. EXPERIMENTAL RESULTS

Numerous tests were carried out and presented in this section to evaluate the proposed system's effectiveness and performance.

6.1 Entropy

The unpredictability of the sequence is reflected in the information entropy. The information entropy of the image is the most significant, and the optimum entropy value for 256 gray levels is 8 when the likelihood of each gray value in the image is equal. The gray value distribution is more uniform. The calculating formula is as follows:

$$H(s) = -\sum_{i=1}^{255} PP(ssi)\log_2\left(\frac{1}{PP(ssi)}\right) \qquad (17)$$

Where ssi is the pixels' gray level, PP (ssi) is the probability of the ssi happening.

Analyzing entropy is possible. Thirty iterations of the suggested algorithm were performed on the original image. The entropy for the images that were encrypted is shown in

j. port. sci. res.
ISSN: 2616-7441 (Online)
ISSN: 2616-6232 (Print)
ISSN: 2616-7220 (USB)
INTERNATIONAL IDENTIFIER FOR SERIALS

Journal port Science Research
Available online www.jport.co
Volume 6, No:4. 2023

Table 1. After computation, the algorithm's information entropy was 7.9983, demonstrating that the distribution of gray values is uniform and that the probability of each pixel value appearing is quite close together. Additionally, it shows the algorithm's respectable degree of attack resistance, its ability to endure exhaustive attacks and its successful encryption. Table 2 displays a comparison of information entropy with other recent sources.

Table 1. *The entropy of the cipher image*

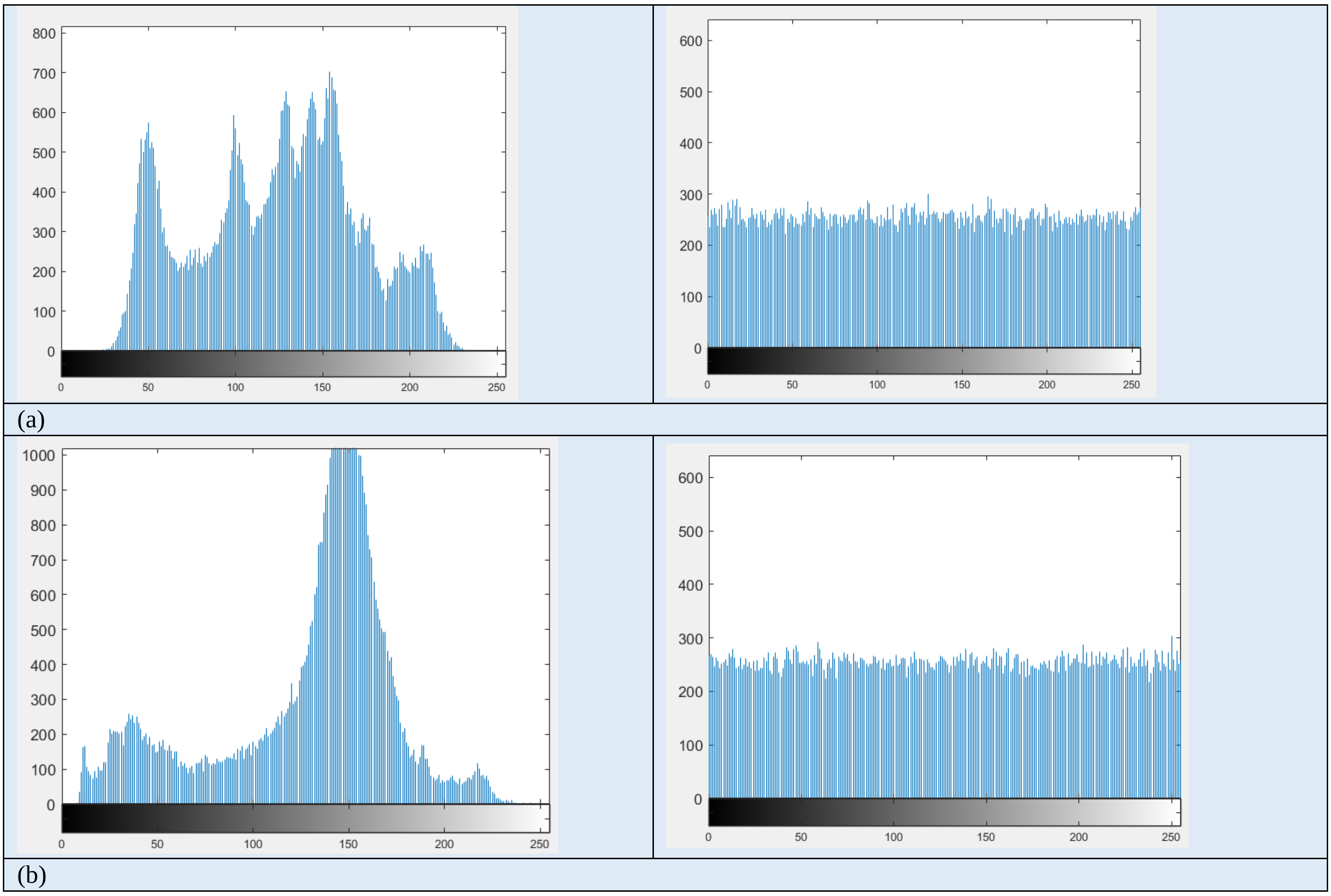
Image name	**Entropy**
Lena	7.9983
Boat	7.9980
Cameraman	7.9981
Peppers	7.9982
Baboon	7.9983

Table 2 *compares information entropy*

Algorithm	entropy
proposed	7.9983
Ref [13]	7.9974
Ref [33]	7.9895
Ref [34]	7.9879

6.2 Histogram analysis

The histogram may intuitively display the image's resistance to assault. The original image's pixel values have an uneven probability distribution, making it more vulnerable to attack. The suggested encryption approach produces a consistent and erratic probability distribution of the image's pixel values, making identifying the initial image's patterns challenging. A stronger resilience against exhaustive assaults can be attained using the method described in this algorithm. Using 256×256 pixel images to check the histogram of the encrypted image is illustrated in Fig. 2.



(a)

(b)

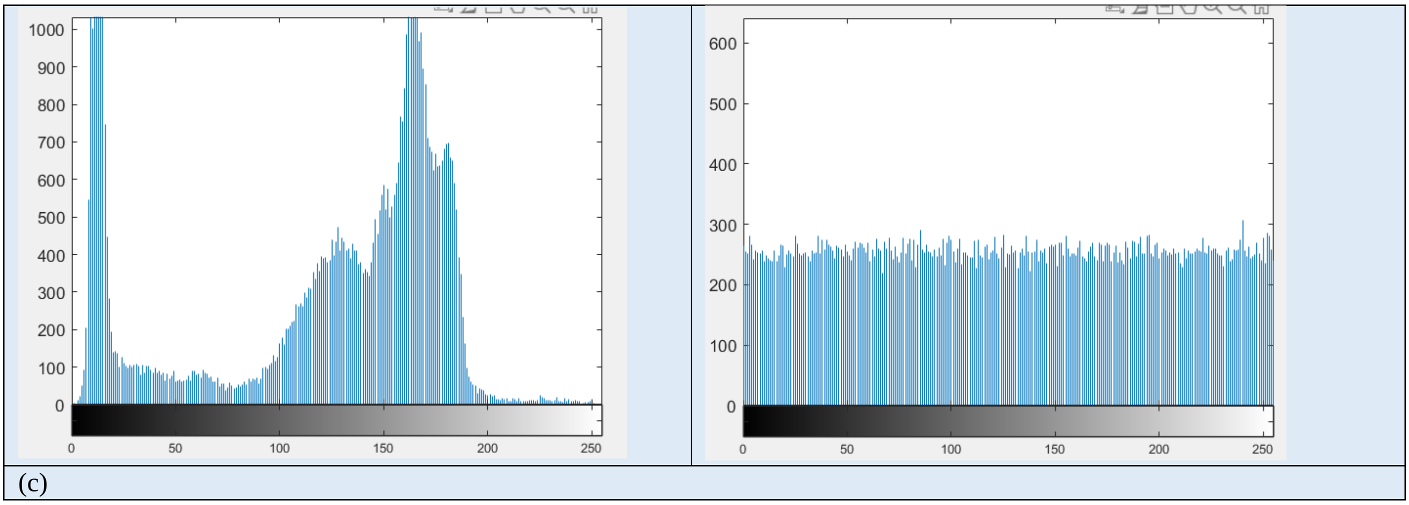


Fig 2. The original and encrypted images histogram: (a)Lena, (b)Boat, (c)Cameraman

6.3 Correlation coefficient analysis

The correlation coefficient is the value used to check the strength of the encrypted images when statistical attacks are subjected. The correlation is high between the original image pixels. In contrast to the encrypted images, the correlations between pixels are minimal. Therefore, the observed correlation decrease between pixels indicates the algorithm's ability to encrypt effectively. The ciphertext image's random pixel distribution in each direction is dispersed in all directions with essentially no association. With the use of the following equation, the correlation can be calculated:

$$(1+x)^n = \frac{|cov(\mathrm{x},\mathrm{y})|}{\sqrt{D(x)}^{\times}\sqrt{D(y)}}$$

Subject to:

$$\mathrm{c(x,y)} = \frac{1}{Z}\sum_{k=0}^{n}(xi - EE(x)(yi - EE(y))) \quad (18)$$

$$EE(x) = \frac{1}{N}\sum_{i=1}^{N} xi$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(xi - EE(x)\right)^2$$

Where the pixel number is Z, and two adjacent pixels' Gray levels are x and y, the algorithm is implemented on the original images for 30 runs. According to the computation findings in Table 3, the neighbouring pixels in the crowded ciphertext image seldom correlate with one another. Table 4 compares the correlation coefficient comparison findings to demonstrate the effectiveness of the suggested approach.

***Table 3** displays the pixel correlations in the cipher image*

Image name	correlation		
	v	h	d
Lena	-0.0007	-0.0000	0.0005
Boat	-0.0004	0.0002	-0.0003
Cameraman	-0.0007	-0.0006	-0.0000
Peppers	0.0013	-0.0000	0.0002
Baboon	0.0002	-0.0002	-0.0001

***Table 4** Comparison of correlation coefficients between adjacent pixels of plaintext and ciphertext*

SSS	proposed	Ref [32]
vertical	-0.0007	-0.0079
horizontal	-0.0000	0.0076
diagonal	0.0005	-0.0098

6.4 UACI and NPCR analysis

A Number Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are two metrics used to evaluate the resilience of the image encryption algorithm against different types of attacks. UACI and NPCR are calculated by a small change in the initial keys from hunter prey optimization. Encrypt two images before and after the change in the initial keys (Enc1 and Enc2). After that, the two encrypted images (Enc1 and Enc2) are compared with each other to find any relationship between the original image and the encrypted image. table 5 shows the NPCR and UACI for the image that is encrypted with two keys slightly different. That indicates how sensitive the algorithm is. The outcomes of comparing with other methods are displayed in Table 6.

$$\text{NPCR} = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{D(Enc1ij, Enc2ij)}{M \times N}$$

Subject to:

$$D(Enc1ij, Enc2ij) = \begin{cases} 0 & \text{if } Enc1i,j = Enc2i,j \\ 1 & \text{if } Enc1i,j \neq Enc2i,j \end{cases}$$

$$\text{UACI} = \frac{1}{M \times N \times 255} \sum_{i=1}^{M} \sum_{j=1}^{N} |\, D(Enc1ij, Enc2ij)|$$

Where M is the width and N is the height of the image.

Table 5. *The NPCR and UACI of encrypted images*

	UACI	NPCR
Lena	0.33623	0.99785
Boat	0.33522	0.99669
Cameraman	0.33454	0.99629
Peppers	0.33472	0.99559
baboon	0.33361	0.99575

Table 6. *Comparing with other algorithms*

	UACI	NPCR
proposed	0.33623	0.99785
Ref [7]	0.3356	0.9974
Ref [12]	0.3331	0.9946
Ref [13]	0.3346	0.9961

6.5 The Analysis of the Keyspace

A suitably sizeable key space is necessary for an image encryption system to be secure against brute-force assaults. The number of potential outcomes from which a key can be produced. To protect the encrypted image against intrusions, the critical space has to be expanded. This approach creates the initial values X1, X2, and X3 for the Lorenz chaotic map. This method is resistant to brute force assaults and has a key space is 2^{128}. Due to the chaotic system's significant initial values sensitivity, even little changes might lead to an incorrectly decrypted image during the decryption process.

6.6 Occlusion and Noise Attack Analysis

Data corruption may occur in real applications where the cipher is affected and corrupted in the transfer process. Occlusion and noise refer to the data corruption which the encryption algorithm must be able to withstand and recover the encrypted image information. Fig 3 shows the effect of cipher images by occlusion attack and their decrypted. The original image was retrieved from different test cases that confirmed the algorithm could withstand the attack of the occlusion. To ensure the stability of the encryption algorithm against noise attacks, different types of noises (Salt & Pepper and Speckle) were applied with different levels of density on the encrypted image and the decrypted image, as shown in Table 7. From the results obtained, it was found that the algorithm's attack ability to withstand the noise attack.

Table 7*: ability to withstand the different type of noise attack*

Salt and pepper	Intensity		0.00003	0.00005	0.00007	0.00009
	PSNR (dB)	Lena	78.2338	72.2302	69.2199	66.2096
Speckle Noise	Intensity		0.000002	0.000003	0.000004	0.000005
	PSNR (dB)	Lena	41.4700	40.2759	39.7939	39.0954

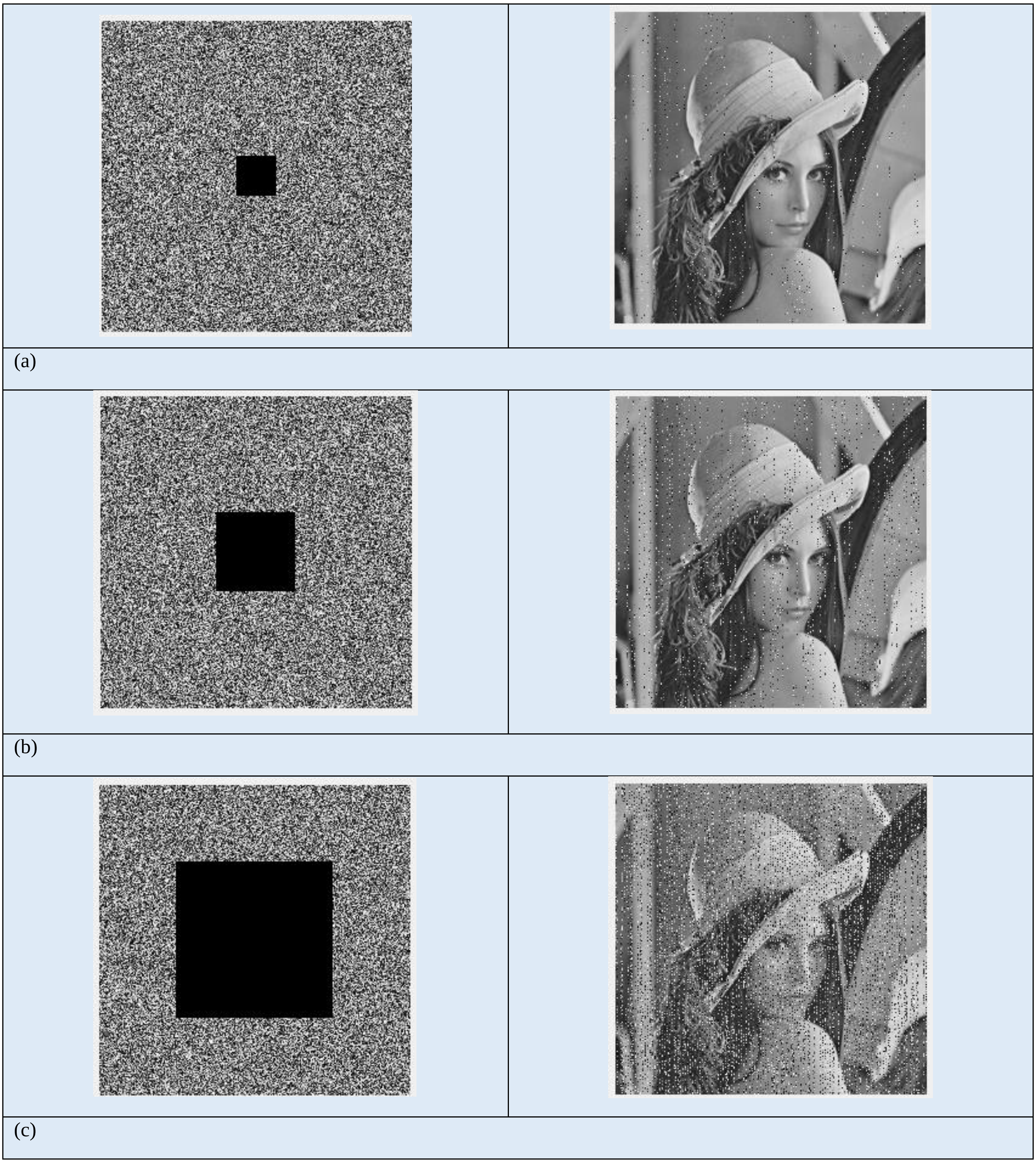


Fig. 3 *Occlusion attacks on cipher image of Lena. (a) noise size 32×32 pixels, (b) noise size 64×64 pixels and (c) noise size 128×128 pixels*

7. CONCLUSION

The proposed encryption algorithm offered a novel two-step approach for secure image communication. The Lorenz Chaos map initial key values were created using the Hunter-Prey Optimization algorithm to create pseudo-random sequences for diffusion and confusion techniques. Based on the results obtained, the application of this proposed encryption algorithm on five grayscale images showed an effective and a high secure performance. The proposed method has more resistant to attacks. This was concluded from the flowing obtained result where the sensitivity test of the NPCR was 0.99785 and the UACI was 0.33623. The Lena image's correlation coefficient in three directions were (v = -0.0007, h = -0.0000, d = 0.0005). The entropy criterion was a significant additional evaluation criterion. As well as the suggested algorithm yields an information entropy value of 7.9983. However, developing an algorithm that increases this value to 8 is still feasible, which is the best-case scenario .

Today’s encryption systems of course will be of key based. This necessitates that the data will be usable only to those with permission to access it. This can be achieved by introducing encryption key through hybrid transformation like Walidlet transform [58] or mixed transform [59]. This idea will be the future work that provides new encryption structures. As another future research can be suggested through providing securities for OFDM systems [60-62] When a credentialed person or machine is ready to access that data, a decryption key is used to make it readable again. Therefore, more powerful encryption methods can be created using multiwavelet transforms [63-65]. Organizations will need to prepare for the adoption of superior emerging encryption technologies as they become available for practical use.

REFERENCES

[1] S. Thakur, A. K. Singh, S. P. Ghrera, and M. Elhoseny, “Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications,” *Multimed Tools Appl*, vol. 78, pp. 3457–3470, 2019.

[2] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher, “Image Encryption Algorithm Based on Arnold Transform and Chaos Theory in the Multi-wavelet Domain”, International Journal of Computers and Applications, Vol. 45, Issue 4, pp. 306-322, 2023.

[3] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher ”Hybrid image encryption algorithm based on compressive sensing, gray wolf optimization, and chaos” , Journal of Electronic Imaging, Volume 32, Issue 4, Pages 043038-043038, 2023.

[4] K. M. Hosny, M. M. Darwish, K. Li, and A. Salah, “Parallel multi-core CPU and GPU for fast and robust medical image watermarking,” *IEEE Access*, vol. 6, pp. 77212–77225, 2018.

[5] T. Xiang, J. Hu, and J. Sun, “Outsourcing chaotic selective image encryption to the cloud with steganography,” *Digit Signal Process*, vol. 43, pp. 28–37, 2015.

[6] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher,”URUK 4D DISCRETE CHAOTIC MAP FOR SECURE COMMUNICATION APPLICATIONS” Journal Port Science Research, Vol. 5, Issue 3, PP. 131-141, 2023.

[7] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher, “Image Encryption Algorithm Based on Arnold Transform and Chaos Theory in the Multi-wavelet Domain” International Journal of Computers and Applications, Volume 45, Issue 4, Pages 306-322, 2023.

[8 T. Xiang, J. Hu, and J. Sun, “Outsourcing chaotic selective image encryption to the cloud with steganography,” *Digit Signal Process*, vol. 43, pp. 28–37, 2015.

[9] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher, “WAM 3D discrete chaotic map for secure communication applications” International Journal of Innovative Computing, Volume 13, Issue 1-2, Pages 45-54, 2022.

[10] H. Ghanbari-Ghalehjoughi, M. Eslami, S. Ahmadi-Kandjani, M. Ghanbari-Ghalehjoughi, and Z. Yu, “Multiple layer encryption and steganography via multi-channel ghost imaging,” *Opt Lasers Eng*, vol. 134, p. 106227, 2020.

[11] S. E. El-Khamy, N. O. Korany, and A. G. Mohamed, “A new fuzzy-DNA image encryption and steganography technique,” *IEEE Access*, vol. 8, pp. 148935–148951, 2020.

[12] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher” Hybrid image encryption algorithm based on compressive sensing, gray wolf optimization, and chaos” Journal of Electronic Imaging, Volume 32, Issue 4, Pages 043038-043038, 2023.

[13] K. Y. Hu, J. Wang, and Y. Wang, “Image encryption based on block compression sensing and the improved magic square transformation,” *Laser Technology*, vol. 43, no. 4, pp. 96–102, 2019.

[14] G. Cheng, C. Wang, and C. Xu, “A novel hyper-chaotic image encryption scheme based on quantum genetic algorithm and compressive sensing,” *Multimed Tools Appl*, vol. 79, no. 39–40, pp. 29243–29263, 2020.

[15] Zahraa A Hasan, Suha M Hadi, Waleed A Mahmoud, “Speech scrambler with multiwavelet, Arnold Transform and particle swarm optimization” Journal Pollack Periodica, Volume 18, Issue 3, Pages 125-131, 2023.

[16] Ali Akram Abdul-Kareem, Waleed Ameen Mahmoud Al-Jawher “A Hybrid Domain Medical Image Encryption Scheme Using URUK and WAM Chaotic Maps with Wavelet–Fourier Transforms” Journal of Cyber Security and Mobility, Pages 435–464-435–464, 2023.

[17] M. Z. Talhaoui, X. Wang, and M. A. Midoun, “Fast image encryption algorithm with high security level using the Bülban chaotic map,” *J Real Time Image Process*, vol. 18, pp. 85–98, 2021.

[18] J. Deng, M. Zhou, C. Wang, S. Wang, and C. Xu, “Image segmentation encryption algorithm with chaotic sequence generation participated by cipher and multi-feedback loops,” *Multimed Tools Appl*, vol. 80, pp. 13821–13840, 2021.

[19] W. A. Mahmoud Al-Jawher Zahraa A Hasan, Suha M. Hadi “Speech scrambling based on multiwavelet and Arnold transformations” Indonesian Journal of Electrical Engineering and Computer Science, Volume 30, Issue 2, Pages 927-935, 2023.

[20] W. A. Mahmoud Al-Jawher, Zahraa A Hasan, Suha M. Hadi ”Time Domain Speech Scrambler Based on Particle Swarm Optimization” International Journal for Engineering and Information Sciences, Vol. 18, Issue 1, PP. 161-166, 2023.

[21] M. Zhou and C. Wang, “A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks,” *Signal Processing*, vol. 171, p. 107484, 2020.

[22] Qutaiba K Abed, Waleed A Mahmoud Al-Jawher “ANEW ARCHITECTURE OF KEY GENERATION USING DWT FOR IMAGE ENCRYPTION WITH THREE LEVELS ARNOLD TRANSFORM PERMUTATION” Journal Port Science Research, Volume 5, Issue 3, Pages 166–177, 2022.

[23] Qutaiba K Abed, Waleed A Mahmoud Al-Jawher “A Robust Image Encryption Scheme Based on Block Compressive Sensing and Wavelet Transform” International Journal of Innovative Computing, Volume 13, Issue 1-2, Pages 7-13, 2022.

[24] Y. Zhou, W. Cao, and C. L. P. Chen, “Image encryption using binary bitplane,” *Signal Processing*, vol. 100, pp. 197–207, 2014.

[25] A. Elghandour, A. Salah, and A. Karawia, “A new cryptographic algorithm via a two-dimensional chaotic map,” *Ain Shams Engineering Journal*, vol. 13, no. 1, p. 101489, 2022.

[26] Z. Hua, S. Yi, and Y. Zhou, “Medical image encryption using high-speed scrambling and pixel adaptive diffusion,” *Signal Processing*, vol. 144, pp. 134–144, 2018.

[27] H. Liu and A. Kadir, “Asymmetric color image encryption scheme using 2D discrete-time map,” *Signal Processing*, vol. 113, pp. 104–112, 2015.

[28] H. Shen, F. Yu, C. Wang, J. Sun, and S. Cai, “Firing mechanism based on single memristive neuron and double memristive coupled neurons,” *Nonlinear Dyn*, vol. 110, no. 4, pp. 3807–3822, 2022.

[29] F. Yu, X. Kong, A. A. M. Mokbel, W. Yao, and S. Cai, “Complex dynamics, hardware implementation and image encryption application of multiscroll memeristive Hopfield neural network with a novel local active memeristor,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 70, no. 1, pp. 326–330, 2022.

[30] F. Yu *et al.*, “Dynamic analysis and application in medical digital image watermarking of a new multi-scroll neural network with quartic nonlinear memristor,” *The European Physical Journal Plus*, vol. 137, no. 4, p. 434, 2022.

[31] F. Yu *et al.*, “Dynamic analysis and audio encryption application in IoT of a multi-scroll fractional-order memristive Hopfield neural network,” *Fractal and Fractional*, vol. 6, no. 7, p. 370, 2022.

[32] J. Liu, M. Zhang, X. Tong, and Z. Wang, “Image compression and encryption algorithm based on compressive sensing and nonlinear diffusion,” *Multimed Tools Appl*, vol. 80, pp. 25433–25452, 2021.

[33] X. Lv, X. Liao, and B. Yang, “A novel scheme for simultaneous image compression and encryption based on wavelet packet transform and multi-chaotic systems,” *Multimed Tools Appl*, vol. 77, pp. 28633–28663, 2018.

[34] M. K. Khairullah, A. A. Alkahtani, M. Z. Bin Baharuddin, and A. M. Al-Jubari, “Designing 1D chaotic maps for fast chaotic image encryption,” *Electronics (Basel)*, vol. 10, no. 17, p. 2116, 2021.

[35] R. Lan, J. He, S. Wang, T. Gu, and X. Luo, “Integrated chaotic systems for image encryption,” *Signal Processing*, vol. 147, pp. 133–145, 2018.

[36] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dyn*, vol. 87, pp. 127–133, 2017.

[37] Y. Su, Y. Wo, and G. Han, "Reversible cellular automata image encryption for similarity search," *Signal Process Image Commun*, vol. 72, pp. 134–147, 2019.

[38] Y.-G. Yang, J. Tian, H. Lei, Y.-H. Zhou, and W.-M. Shi, "Novel quantum image encryption using one-dimensional quantum cellular automata," *Inf Sci (N Y)*, vol. 345, pp. 257–270, 2016.

[39] Y. Wang, Y. Zhao, Q. Zhou, and Z. Lin, "Image encryption using partitioned cellular automata," *Neurocomputing*, vol. 275, pp. 1318–1332, 2018.

[40] Y. Hui, H. Liu, and P. Fang, "A DNA image encryption based on a new hyperchaotic system," *Multimed Tools Appl*, pp. 1–25, 2021.

[41] S. Zhou, P. He, and N. Kasabov, "A dynamic DNA color image encryption method based on SHA-512," *Entropy*, vol. 22, no. 10, p. 1091, 2020.

[42] W. Xingyuan, G. Suo, Y. Xiaolin, Z. Shuang, and W. Mingxu, "A new image encryption algorithm with cantor diagonal scrambling based on the PUMCML system," *International Journal of Bifurcation and Chaos*, vol. 31, no. 01, p. 2150003, 2021.

[43] H. Lin, C. Wang, L. Cui, Y. Sun, C. Xu, and F. Yu, "Brain-like initial-boosted hyperchaos and application in biomedical image encryption," *IEEE Trans Industr Inform*, vol. 18, no. 12, pp. 8839–8850, 2022.

[44] P. Fang, H. Liu, and C. Wu, "A novel chaotic block image encryption algorithm based on deep convolutional generative adversarial networks," *IEEE Access*, vol. 9, pp. 18497–18517, 2020.

[45] A. Yaghouti Niyat and M. H. Moattar, "Color image encryption based on hybrid chaotic system and DNA sequences," *Multimed Tools Appl*, vol. 79, no. 1–2, pp. 1497–1518, 2020.

[46] X. Wang, Y. Su, C. Luo, and C. Wang, "A novel image encryption algorithm based on fractional order 5D cellular neural network and Fisher-Yates scrambling," *PLoS One*, vol. 15, no. 7, p. e0236015, 2020.

[47] R. Matthews, "On the derivation of a 'chaotic' encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[48] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Phys Lett A*, vol. 372, no. 4, pp. 394–400, 2008.

[49] R. Rhouma and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper-chaos," *Phys Lett A*, vol. 372, no. 38, pp. 5973–5978, 2008.

[50] F.-G. Jeng, W.-L. Huang, and T.-H. Chen, "Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes," *Signal Process Image Commun*, vol. 34, pp. 45–51, 2015.

[51] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Computers & Mathematics with Applications*, vol. 59, no. 10, pp. 3320–3327, 2010.

[52] X. Wang and Y. Li, "Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence," *Opt Lasers Eng*, vol. 137, p. 106393, 2021.

[53] Z. Hao, Z. Wang, D. Bai, B. Tao, X. Tong, and B. Chen, "Intelligent detection of steel defects based on improved split attention networks," *Front Bioeng Biotechnol*, vol. 9, p. 810876, 2022.

[54] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn*, vol. 62, pp. 615–621, 2010.

[55] J. Wang, X. Song, and A. A. A. El-Latif, "Single-objective particle swarm optimization-based chaotic image encryption scheme," *Electronics (Basel)*, vol. 11, no. 16, p. 2628, 2022.

[56] J. A. Lazzús, M. Rivera, and C. H. López-Caraballo, "Parameter estimation of Lorenz chaotic system using a hybrid swarm intelligence algorithm," *Phys Lett A*, vol. 380, no. 11–12, pp. 1164–1171, 2016.

[57] I. Naruei, F. Keynia, and A. Sabbagh Molahosseini, “Hunter–prey optimization: Algorithm and applications,” *Soft comput*, vol. 26, no. 3, pp. 1279–1314, 2022.

[58] Waleed Ameen Mahmoud “A Smart Single Matrix Realization of Fast Walidlet Transform” Journal International Journal of Research and Reviews in Computer Science, Volume 2, Issue, 1, Pages 144-151, 2011.

[59] Hamid M Hasan, Waleed A. Mahmoud Al- Jawher, Majid A Alwan “3-d face recognition using improved 3d mixed transform” Journal International Journal of Biometrics and Bioinformatics (IJBB), Volume 6, Issue 1, Pages 278-290, 2012.

[60] Abbas H Kattoush, Waleed A Mahmoud, Ali Shaheen, Ahed Ghodayyah “The performance of proposed one dimensional serial Radon based OFDM system under different channel conditions” The International Journal of Computers, Systems and Signals, Volume 9, Issue 2, Pages 412-422, 2008.

[61] Abbas Hasan Kattoush, Waleed Ameen Mahmoud Al-Jawher, Sulaiman M Abbas, Ali Tweij Shaheen “A N-Radon Based OFDM Trasceivers Design and Performance Simulation Over Different Channel Models” Journal of Wireless Personal Communications, Volume 58, Pages 695-711, 2011.

[62] Waleed A Mahmoud, Ali A Ali, & Saad N Abdul Majed “Wavelet Based Multi Carrier Code Division Multiple Access” proceeding of 5th International Multi-Conference on Systems, Signals and Devices, pages 1-6, 2008

[63] . Hadeel Al-Taai Walid Mahmoud, Mutaz Abdulwahab “New fast method for computing multiwavelet coefficients from 1D up to 3D” Proc. 1st Int. Conference on Digital Comm. & Comp. App., Jordan, Pages 412-422

[64] Waleed A. Mahmoud, MS Abdulwahab, HN Al-Taai “The Determination of 3D Multiwavelet Transform” IJCCCE, Volume 2, Issue 4, pages 28-46 2005.

[65] Waleed A Mahmoud, Majed E Alneby, Wael H Zayer “2D-multiwavelet transform 2D-two activation function wavelet network-based face recognition” J. Appl. Sci. Res, vol. 6, issue 8, 1019-1028, 2010.