Date of publication DEC-31, 2023, date of current version DEC-12, 2023.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.22.4.3357

An Efficient Image Encryption Method Based on Enhanced Josephus Problem and a Non-Invertible Economic Map

AHMED KAREEM SHIBEEB[1], MOHAMMED HUSSEIN AHMED[2], SALAH ALBERMANY[3]

[1]Department of Computer Systems, Technical Institute – Suwaira, Middle Technical University, Baghdad, Iraq. (E-mail: ahmed.kareem@mtu.edu.iq)
2Department of Computer Science, Faculty of Education, Mustansiriyah University, Baghdad, Iraq. (E-mail: mohammedalbawi@uomustansiriyah.edu.iq)
Department of Computer Science, Faculty of Computer Science and Maths, University of Kufa, Najaf, Iraq. (E-mail: salah.albermany@uokufa.edu.iq)

Corresponding author: Ahmed Kareem Shibeeb (e-mail: ahmed.kareem@mtu.edu.iq).

ABSTRACT As an increasing number of digital images are created and transmitted over the internet, there is growing concern over their unauthorized use, which has a big impact on both security and privacy concerns. In this research, we provide a fast and secure image encryption scheme by using an enhanced Josephus problem and two-dimensional non-invertible economic chaotic map (2D-ECM) to safely and covertly protect digital image information throughout public channel transmission. First, the initial values of the 2D-ECM map are generated based on Secure Hash Algorithm (SHA-256) and the input secret key. Then, the Josephus problem is enhanced by substituting the extract operation with location exchange and dynamic start location and step size is employed to scramble the image pixels. In order to integrate the confusion process and diffusion process, the enhanced Josephus problem is utilized indirectly to choose two random columns from the scrambled image and random image to XOR them with the current column. The evaluation results prove that the proposed image cryptosystem is more efficient compared to existing cryptosystems.

KEYWORDS Josephus problem; Image encryption; Two-dimensional chaotic map; Chaos-based cryptography

I. INTRODUCTION

DUE to the development of multimedia technology and the rapid expansion of the Internet, widespread digital multimedia data have gained popularity. A trusted and strong security system is necessary for a variety of applications, including the transmission of sensitive military data, medical data, the Internet of things, confidential video conferencing, and even the sharing of private images [1, 2]. Because there are numerous multimedia technologies available, multimedia material is susceptible to unauthorized access. Using a classical encryption scheme like AES [3], DES [4], IDEA, or RSA [5] is a typical solution to the problem of securing image data. But difficult mathematical calculations and high computing overheads across enormous volumes of multimedia data made these schemes ineffective for real-time image encryption [3]. The most popular methods for securing digital images are permutation and substitution [6, 7], which aim to disrupt the association between the image pixels. In [8], Shannon put up the idea that a strong cryptosystem might be any encryption scheme that contains both confusion (referring to permutation) and diffusion (referring to replacement or any other process that can affect the pixel value). Any encryption algorithm has a source of randomness at its core; this source gives the algorithm its strength and varies from algorithm to algorithm. Chaos-based algorithms attracted a lot of attention because of their randomness due to their sensitivity to initial values and control parameters [9]. High-dimensional chaotic systems typically have a more complicated architecture and offer greater chaotic performance as compared to low-dimensional chaotic systems [10]. Chaos image encryption method based on confusion and diffusion was first introduced by Fridrich in 1998 [11]. Additionally, this approach significantly increases efficiency while still maintaining security [12]. Chaos theory is therefore frequently utilized in the design of image cryptosystems. In [13], the researchers proposed a fast image cryptosystem based on bit-level shuffling, circular rotating, and modified XOR to encrypt grayscale and medical images. They achieved this by using the output sequence of SHA-256 as initial values for the modified Logistic-Tent system. The proposed cryptosystem in [14] employed the input key, but there was no connection to the original image. As a result, it was decrypted using chosen-plaintext cryptanalysis and enhanced to be secure from potential attacks as detailed in [15]. In [16], the secret key connected with the plaintext image was generated using a 5D multi-wing hyper-chaotic system. To increase the security of

the cryptographic system, bit-level permutation is utilized during the confusion process in addition to pixel-level permutation. Many methods attempt to introduce an image cryptosystem by avoiding confusion-diffusion architecture, A fast chaotic image cryptosystem was introduced by Wang et al. [17] based on shuffling the columns and rows of the original image while using the secret key to encrypt the pixels of the rows or columns at the same time. Also, Talhaoui et al. [18] proposed a fast chaotic image cryptosystem based on permutation-less structure and a new1D-chaotic map. A specific counting-out game is related to a mathematical theoretical problem known as the Josephus problem. On the other hand, since each game element is traversed once, Josephus traversal can be achieved if the counting-out order is saved in a sequence [19]. The Josephus problem has been utilized for years in the field of image encryption algorithms. Although the Josephus traversal is easy to understand and rapid to compute, earlier approaches tended to be more permutation-focused [20]. However, because permutation-based encryption never modifies pixel values, it is susceptible to statistical cryptanalysis, ciphertext-only cryptanalysis, and known plaintext cryptanalysis [21, 22]. In [23], Niu and Zhang presented a dynamic step size Josephus problem permutation technique based on the plaintext's pixel value. This method significantly enhances the permutation effect and original image sensitivity, but it encrypts data slowly. However, the scholars in [24] modified the Josephus problem by using an additional chaotic-based parameter to change the distance between the element in the previous round and the element that started the following round. Their proposed cryptosystem separated the confusion and diffusion process, where the modified Josephus problem is used to confuse the image pixels; during the image diffusion stage, the cyclic shift mechanism and the dynamic XOR operation are primarily employed to diffuse images. In addition to that, some researchers apply the improved Josephus problem to design a special image cryptosystem that only employs it in the confusion process, such as Naim et al [25] proposed a novel satellite image cryptosystem based on the standard Josephus problem, LFSR generator, SHA-512, and six dimensional-systems. Despite having a high level of security, the system's speed is slow. Whereas the scheme in [26] encrypts the medical image by using the dynamic Josephus problem for the bit-level permutation. Also, this scheme has good security properties, but it requires higher encryption time.

Based on this discussion, an enhanced Josephus problem based on a two-dimensional noninvertible economic chaotic map is proposed in this paper for the secure transmission of images. The main novelties and contributions of this study, which differ from the previous cryptosystems, are outlined below:

1) To provide an excellent confusion effect and a low computation time substitute the extract operation used in the standard Josephus problem with the location exchange operation and uses dynamic start location and step size instead of fixed.
2) Used the two-dimensional noninvertible economic chaotic map, a game of competition that presents a variety of intriguing phenomena, including the coexistence of complex attractors and wide chaotic ranges. The two-dimensional map is utilized to generate random arrays, which are then utilized in the confusion and diffusion processes.
3) The proposed cryptosystem implements plaintext image content-based initial value generation to resist known and chosen plain text cryptanalysis.
4) The confusion process and diffusion process are merely dependent on the enhanced Josephus problem which makes the proposed algorithm able to resist separate attacks.
5) Through simulations, performance and security analyses are carried out, and it is demonstrated that the proposed method is highly secure against various attacks and reduces the computation time.

The remainder of this paper is organized as follows. After briefly describing the mathematical basics of the Josephus problem in Section 2, Section 3 presents the two-dimensional economic chaotic map (2D-ECM). Details of our proposed cryptosystem are shown in Section 4. Following this, in Section 5, we evaluate the performance and security of the proposed method and is concluded in Section 6.

II. STANDARD JOSEPHUS PROBLEM

Josephus, a well-known Jewish historian, is claimed to have experienced what follows: After the Romans took control of Chetopat, 39 Jews hid in a cave beside Josephus and his companion. Instead of being apprehended by their adversaries, these 39 Jews decided to take their own lives. The third individual in a circle of forty-one had to take their own life after being placed at the front of the queue. The cycle continued until everyone had taken their own lives. However, Josephus and his companion did not want to obey. Where should they stand, given the total number of persons and the step size, to prevent being executed in the first place? Josephus first requested his companion to act as though he was obeying. He set up himself and his friend in places 16 and 31 and managed to win the killing game [27]. To represent this problem, we number the m locations in the ring by 1,2, 3,4, ..., m, and counting is started at the selected number i. Then, every nth element is extracted from the ring. The mathematical formula in equation (1) is used to describe the Josephus sequence [19]:

$$S = fn(m, n, i), \tag{1}$$

where S is the Josephus sequence, *fn* represents the Josephus function, and $m \geq 1$; $n \geq 1$; $1 \leq i \leq m$. In order to further explain the Josephus sequence, we provide a numerical example using the values $m = 9$, $n = 4$, and $i = 1$ in equation (1). The Josephus sequence's generation process is illustrated in Fig. 1. The starting position is $i = 1$, the first element to be extracted is the fourth, the next starting position is i = 5, and the next element to be extracted is the eighth following the ninth. Up till one element is left, this process is repeated.

III. TWO-DIMENSIONAL ECONOMIC CHAOTIC MAP (2D-ECM)

Askar and Elsadany suggested a nonlinear two-dimensional economic map (2D-ECM) in [28], which is used to describe the dynamics behavior of the Cournot Duopoly game by a two-dimensional discrete map. Due to their dynamic features, Cournot Duopoly games are popular among researchers in the field of economics. Two competing companies compete in the Cournot Duopoly game, and the interactions between those enterprises result in complex dynamic behaviors that give important expectations for economic markets. 2D-ECM is used to explore the dynamic properties of such games, and it serves

as a definition for these types of games. The fixed points on the map were calculated by the authors. Furthermore, they studied their stability states, which achieved chaotic attitude because the map under study has complicated dynamics. They concluded that the map of the game is non-invertible of patterns Z4 − Z2. Mathematically, the map is defined as:

$$\begin{cases} y_{n+1} = y_n + v1y_n[a - (2 + c)y_n - dz_n] \\ z_{n+1} = z_n + v2z_n[a - (1 + \omega + c)z_n - dy_n]' \end{cases} \quad (2)$$

where a, c, d, ω, v1, and v2 represent system parameters; y and z refer to the quantities of two companies. The six parameters of the map are important from an economic perspective; the upper price is denoted by a > 0, while the product differentiation is denoted by d ∈ [−0.5, 1].

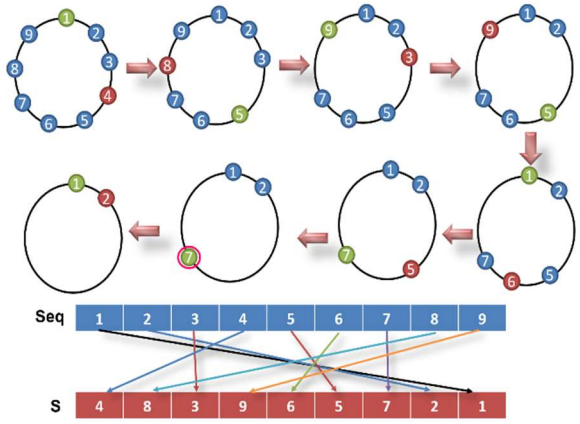

Figure 1. A numerical example of Josephus ring problem.

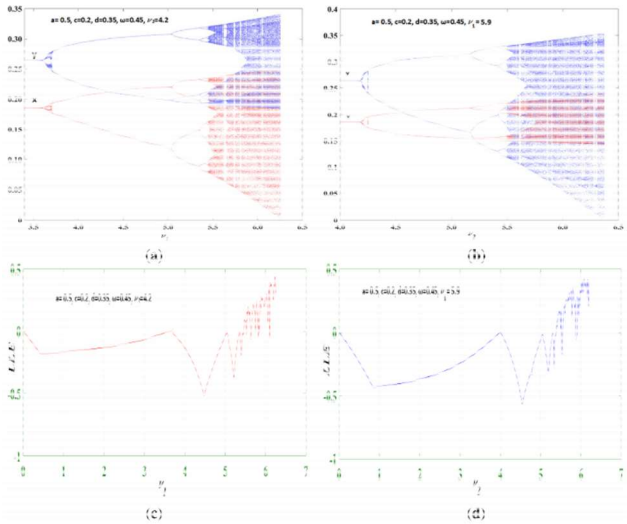

Figure 2. (a), (b) Chaotic attractors of 2D-ECM with different v1 and v2. (c), (d) The Lyapunov spectrums of the 2D-ECM map.

If c > 0, the marginal cost parameter is fixed. The parameter for public ownership is symbolized by ω ∈ [0, 1] and the modification velocity for the ith company is indicated by vi where i = 1, 2. The chaotic attractor of 2D-ECM map for the effects of the system parameters v1 and v2 on the quantities y and z is shown in Figs. 2(a) and 2(b) at the parameter values a = 0.5, c = 0.2, d = 0.35. This selection ensures that the 2D-ECM map has large Lyapunov exponents ash illustrated in Figs. 2(c) and 2(d).

IV. THE PROPOSED IMAGE CRYPTOSYSTEM

Henon map is a two-dimensional discrete-time dynamical system, which is described as follows:

In this proposed system, efforts are devoted to designing an efficient image cryptosystem to improve speed and encryption security. The suggested method uses a collection of enhanced Josephus problem, SHA-256 hash function, and 2D- Economic chaotic map.

A. INITIAL VALUES GENERATION

A type of cryptographic hash function called SHA-256 may transform input data of any size into a binary sequence of 256 bits [29]. Since the SHA-256 function is irreversible, the key cannot be used to deduce any plaintext data. In this proposed cryptosystem, the SHA-256 function is utilized to generate the initial states of the 2D-ECM map. It is possible to mix the hash value of the plaintext image and the input keys by using Equations (3) and (4) as the initial values. The key changes dramatically as the plaintext image modifies slightly, thus improving the plaintext sensitivity. There are two initial values for the two-dimensional economic chaotic map y and z. We suppose that the 256-bit output sequence is produced by the SHA-256 function is H and that H is separated into 32 parts, h1,h2 . . . , h32. The procedure for generating the two initial values of the 2D-ECM map can be specified as follows:

$$\begin{cases} f_1 = c_1 + \frac{1}{256}(h_1 \oplus h_2 \oplus \ldots . \oplus h_8) \\ f_2 = c_2 + \frac{1}{256}(h_9 \oplus h_{10} \oplus \ldots . \oplus h_{16}) \\ f_3 = c_3 + \frac{1}{256}(h_{17} \oplus h_{18} \oplus \ldots . \oplus h_{24}) \\ f_4 = c_4 + \frac{1}{256}(h_{25} \oplus h_{26} \oplus \ldots . \oplus h_{32}) \end{cases}, \quad (3)$$

where c_1, c_2, c_3, and c_4 are user-defined parameters that can be treated as security keys. Secondly, influences the two initial values of economic chaotic map y_0, z_0 by f_1, f_2, f_3, and f_4 as follows:

$$\begin{cases} y_0 = \frac{mod((f_1 + f_3) \times 10^{14}, 256)}{256} \\ z_0 = \frac{mod((f_2 + f_4) \times 10^{14}, 256)}{256} \end{cases}. \quad (4)$$

Then, the initial values y_0 and z_0 will be modified concerning various plaintext images.

B. ENHANCED JOSEPHUS-BASED PERMUTATION

To increase the reliability of the traditional Josephus problem for image encryption, perturbations must be applied because it generates relatively few sequence changes. By adjusting the starting location (i), step size (n), and replacing the extract operation with the locations exchange operation, we can increase the variety of Josephus sequences, provide an additional dislocation effect, and decrease the time complexity. For example, we first give the control parameters of a 2D-ECM map and generate the initial states of y_0, z_0 as described in subsection 4.1, and utilize Equation (2) to iterate for m times.

The two obtained chaotic sequences are represented by yn and zn respectively. Each Josephus start location and step size are indirectly controlled by y and z so that they change the pixel locations randomly and dynamically. Fig. 3 depicts our enhanced Josephus permutation.

C. ENHANCED JOSEPHUS-BASED DIFFUSION

In the conventional image encryption approaches, diffusion and permutation are two mutually independent processes. As a result, it has been discovered that the two processes mentioned above can be attacked independently [30]. Thus, we integrate the diffusion and permutation processes by using the enhanced Josephus problem. In another meaning, we do not directly perform the enhanced Josephus problem to pixel position permutation in this subsection, but indirectly achieve the goal of pixel diffusion by selecting the random column and Xor it with a current column and column in another image that is generated based on 2D-ECM. The integrated confusion-diffusion processes can be described by the following equation:

$$CI(i,j) = SI(i,j) \oplus SI(i,s) \oplus M(i,s), \qquad (5)$$

where CI represents the ciphertext image, SI is the permutated image, M is a random image generated based on a 2D-ECM map, i and j are the index of the current row and column, respectively. However, s represents the index of the column which selected by using the Josephus sequence.

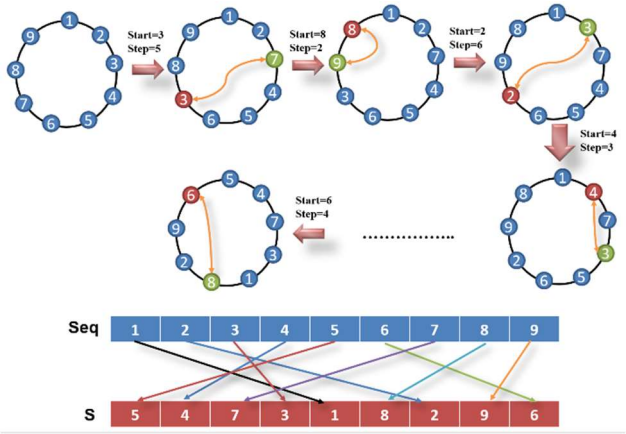

Figure 3. An Enhanced Josephus ring problem basedon random start location, random step size, and locations exchange operation.

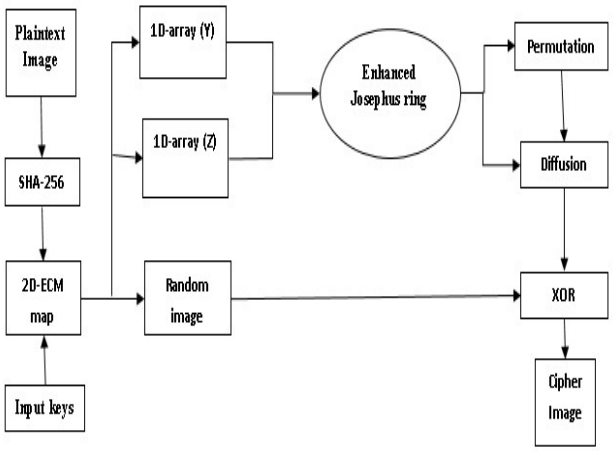

Figure 4. The flow diagram of the image cryptosystem.

D. ENCRYPTION PROCESS

Fig. 4 shows the proposed image cryptosystem. The encryption process includes various steps as follows:

Step 1: Read the plaintext image P (i,j), and convert it to a one-dimensional array P1 (i) with size M × N.

Step 2: Generate the initial values of 2D-ECM based on SHA-256 of the plaintext image and input keys as described in Equations (3) and (4).

Step 3: In order to prevent the transient effect of chaotic function, a 2D-ECM map is idly iterated for Nr times at the start of each round. Nr can have any number between 300 and 600 to increase the key space of the proposed algorithm and prevent the transient effect at the same time.

Step 4: Continue iterating **the** 2D-ECM map to generate two one-dimensional integer arrays (Y, Z) and a two-dimensional random image (RI), They are all size M × N. Mathematically, the aforementioned arrays are obtained as follows:

$$Y(i) = Mod\ (\mathrm{Floor}(\mathrm{y}(i) \times 10^{14}), \mathrm{M} \times \mathrm{N}) + 1, \qquad (6)$$
$$Z(i) = Mod\ (\mathrm{Floor}(\mathrm{z}(i) \times 10^{14}), \mathrm{M} \times \mathrm{N}) + 1, \qquad (7)$$
$$RI(i,j) = Mod\ (Floor((\mathrm{y}(i) + \mathrm{z}(i)) \times 10^{14}), 256). \qquad (8)$$

Step 5: Permute the pixel's positions of the plaintext image based on the enhanced Josephus problem, which is used the chaotic array (Y, Z) and locations exchange operation as described in Subsection 4.2 to reduce the correlation between the adjacent pixels.

Step 6: In order to avoid a spread attack and mix the image columns, the enhanced Josephus problem is applied again to select the random column from the scrambled image and random image to mix them with the current column to produce the ciphertext image (CI) as introduced in Subsection 4.3.

The decryption operation is the opposite step of the encryption operation. First, the random arrays (Y, Z) and random image (RI) produced by the 2D-ECM map should be acquired. Then, the inverse of the diffusion procedure is applied. Finally, the plaintext image (PI) is obtained by the inversion operation of enhanced Josephus ring-based permutation.

V. EXPERIMENTAL RESULTS

Several analytical tests are carried out to verify the security attributes of the image encryption algorithm that is provided in this section. Multiple images are subjected to numerical simulations in order to evaluate the performance of the suggested method. To implement the encryption and decryption program, C#.net 2016 programming language was used. The Microsoft Surface Pro (2017) configuration included a 2.71 GHz CPU, 8 GB of RAM, and Microsoft Windows 10. In this experiment, some known color images with size 512× 512 like “Lena”, “Peppers”, “Sailboat”, “Baboon”, and “Airplane” are considered as tested images. The secret keys are a = 0.5, c = 0.2, d = 0.35, v1=5.9, ω =0.45, v2=4.2, c_1=1, c_2=2, c_3=3, c_4=4, and Nr=430.

A. HISTOGRAM TEST

The distribution of pixel values is commonly described by an image histogram. The ciphertext image should have a flat histogram to resist statistical cryptanalysis. As seen in Fig. 5, the ciphertext image is noise-like and has a uniformly distributed histogram, which is radically different from the plaintext image. Nobody will likely be able to get any useful

statistical data about the encrypted images, if not impossible. Additionally, we utilized the Chi-square (X^2) to quantitatively assess the reliability of the cipher-image histogram as follows:

$$X^2 = \sum_{k=1}^{256} \frac{(C_k - D)}{D}, \quad (9)$$

where $\boldsymbol{C_k}$ is the k gray recurrence value and D is the frequency determined from each gray value ($\boldsymbol{D} = \frac{\boldsymbol{C}}{\boldsymbol{256}}$). The $\boldsymbol{X^2 < 293.2478}$ if the ciphertext-image histogram is totally flat. Therefore, the value of Chi-square for a security encryption technique should generally be as low as possible. The Chi-square of encrypted image results presented in Table 1 shows that the suggested approach is more secure than several schemes.

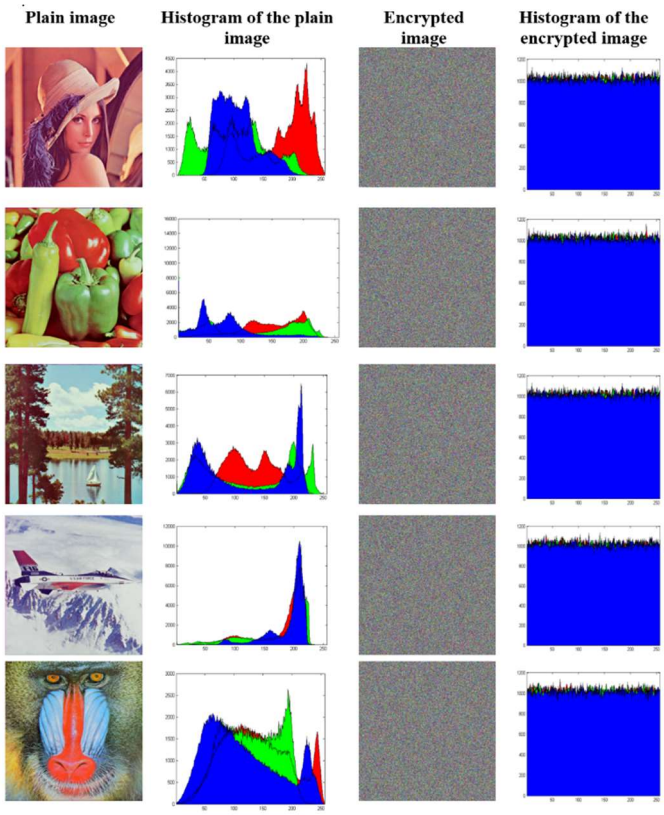

Figure 5. RGB histogram analysis.

B. CORRELATION COEFFICIENT TEST

The correlation between the original image and its ciphertext image must be very low for the encryption algorithm to be extremely secure. The encryption process from the input image to its ciphered image is difficult to predict if there is any correlation at all. A score closer to 1 indicates a significant similarity between plaintext and ciphertext images, whereas a value of 0 indicates less similarity [31]. The correlation coefficient is defined as follows:

$$CC_{xy} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{S(x)S(y)}}, \quad (10)$$

where E(x) and S(x) are denoted as the x gray level expectation and variance. Fig. 6 illustrates the correlation between two neighboring pixels for the plaintext and ciphertext versions of Lena's image encrypted using the suggested approach. On the other hand, Table 2 presents the findings together with a comparison to previous methods. For the ciphertext image, the correlation coefficient is near to 0, while for the plaintext image, it is close to 1. The adjacent pixels of the ciphertext image exhibit a very low correlation, as seen in Table 2. Our method can therefore successfully resist statistical cryptanalysis.

C. LOCAL ENTROPY TEST

The pixels in a ciphertext image should be evenly distributed over the complete image and in any non-overlapping blocks as well. The image should be uniformly distributed throughout, with each randomly chosen blocks exhibiting this distribution. Based on this idea, it is possible to estimate the distribution and randomness of an input image using the local entropy test. Global entropy for a complete image C can be computed with the following formula:

$$GE(z) = \sum_{i=0}^{M-1} \mathrm{P}\,(C_i) \log_2 \mathrm{P}(C_i), \quad (11)$$

where C_i is the i -th gray value in an M-level gray, and $P(C_i)$ is the probability of the C_i. On randomly chosen, uniformly sized, non-overlapping image partitions, Wu et al utilized Local entropy to calculate the entropy value [32]. As a result, Local entropy can be determined by taking the average entropy values of all randomly chosen partitions as follows:

Table 1. Chi-square test.

Image	Plaintext image	Ciphertext image
Peppers	340999.441	271.795
Sailboat	223807.854	251.448
Baboon	101863.462	253.086
Airplane	822925.96	254.718
Lena	237534.114	268.097

Table 1. Correlation coefficients test.

Image	Plaintext image			Ciphertext image		
	H	V	D	H	V	D
Peppers	0.9841	0. 9691	0. 9725	0.0002	-0.0006	-0.0014
Sailboat	0.9817	0. 9723	0. 9574	0.0004	-0.0013	0.0006
Baboon	0.9624	0.9627	0.9381	-0.0023	0.0003	0.0001
Airplane	0.9511	0.9816	0.9665	-0.0009	-0.0007	0.0024
Lena	0.9832	0.9634	0.9485	-0.0002	0.0013	0.0006

Table 3. Local entropy of the testing images at l = 30, T_b= 1936.

Image	Plain image	Cipher image
Peppers	5.741	7.9073
Sailboat	6.8133	7.9061
Baboon	5.7242	7.9035
Airplane	4.9915	7.9028
Lena	5.8749	7.9046

Table 4. NPCR test results.

Images	NPCR%	Critical value		
		NPCR*0.05 = 99.5893%	NPCR*0.01 = 99.581%	NPCR*0.001 = 99.5717%
Peppers	99.7252	Accepted	Accepted	Accepted
Sailboat	99.6241	Accepted	Accepted	Accepted
Baboon	99.6018	Accepted	Accepted	Accepted
Airplane	99.752	Accepted	Accepted	Accepted
Lena	99.7311	Accepted	Accepted	Accepted

Table 5. UACI test results.

Images	UACI	Critical value		
		UACI -0.05 =33.373 UACI +0.05 =33.5541	UACI -0.01 =33.3445 UACI +0.01 =33.5826	UACI -0.001 =33.3115 UACI +0.001 =33.6156
Peppers	33.4521	Accepted	Accepted	Accepted
Sailboat	33.5662	Accepted	Accepted	Accepted
Baboon	33.4835	Accepted	Accepted	Accepted
Airplane	33.5271	Accepted	Accepted	Accepted
Lena	33.5177	Accepted	Accepted	Accepted

Table 6. CDR test of "Lena" image for various cipher keys CK with ΔCK = 10^{-14}

CK	Value	CDR%
a	0.5	99.6068
c	0.2	99.6014
d	0.35	99.571
v1	5.9	99.6029
v2	0.45	99.6118
ω	4.2	99.529
c_1	1	99.6011
c_2	2	99.6224
c_3	3	99.5805
c_4	4	99.6109

$$\overline{E_{l,T_b}}(z) = \frac{1}{l}\sum_{i=0}^{l-1} E(z_i), \tag{12}$$

where T_b is the block size, $E(z_i)$ is the block's typical entropy, and z_i, i= 1, 2,..., l are l randomly different blocks. The allowed range of local entropy for the recommended parameter values in [32] is $[7.9015, 7.9034]$. The local entropy values of ciphertext images encrypted using various encryption techniques are displayed in Table 3. We can see that for most of the ciphertext images, the suggested method has a respectable local entropy value.

D. DIFFERENTIAL CRYPTANALYSIS

To prevent differential cryptanalysis, in which an attacker modifies the plaintext image and analyzes the changes in the ciphertext image as a result, a good cryptosystem should be extremely sensitive to the plaintext images. The number of pixels changes rate (NPCR) and the unified average changing intensity (UACI) are typically utilized to determine the plaintext image sensibility. These tests provide a quantitative assessment of the differences between the ciphertext images CI1 and CI2 produced from two nearly identical plaintext images [33]. These measurements are computed using equations (13), (14), and (15).

$$V(i,j) = \begin{cases} 0 & IF\ CI_1(i,j) = CI_2(i,j) \\ 1 & IF\ CI_1(i,j) \neq CI_2(i,j) \end{cases}, \tag{13}$$

$$NPCR = \sum_{ij} \frac{V(i,j)}{H \times W} \times 100\%, \tag{14}$$

$$UACI = \sum_{ij} \frac{|CI_1(i,j) - CI_2(i,j)|}{255 \times H \times W}, \tag{15}$$

where CI1 (i, j) and CI2 (i, j) are two encrypted images that are produced from 1-bit distinct pixels in the plaintext image. Based on the results from [34], the optimal NPCR and UACI values concern the size of an image and significance level. For example, a 512x512 grayscale image passes all theoretical NPCR critical values at any significance level if the NPCR result is >99.5893%, and it succeed in the UACI measure if the obtained result falls within the critical ranges of (33.3730%, 33.5541%), (33.3445%, 33.5826%), and (33.3115%, 33.6156%) at significance level (α = 0.05), (α = 0.01) and (α = 0.001), respectively. Tables 4 and 5 contain the critical values and measure values of NPCR and UACI for various ciphertext images. The suggested cryptosystem has a higher passing rate for various NPCR and UACI critical values. That is to say, even a small modification to the plaintext image will have a large impact on the ciphertext version. Our cryptosystem is extremely dependent on the plaintext image and can effectively withstand differential cryptanalysis.

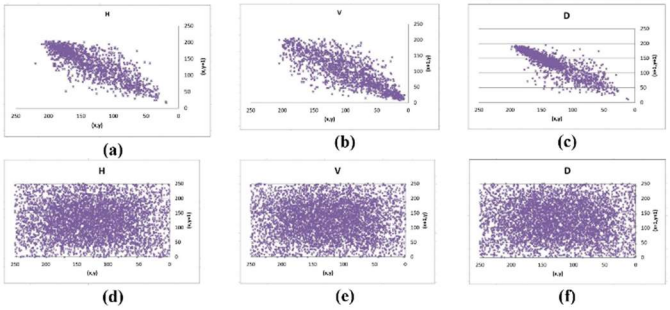

Figure 6. Adjacent pixels Correlation analysis of "Lena" image: (a) horizontally, (b) vertically, and (c) diagonally plot of plaintext image; (d) horizontally, (e) vertically, and (f) diagonally plot of ciphertext image.

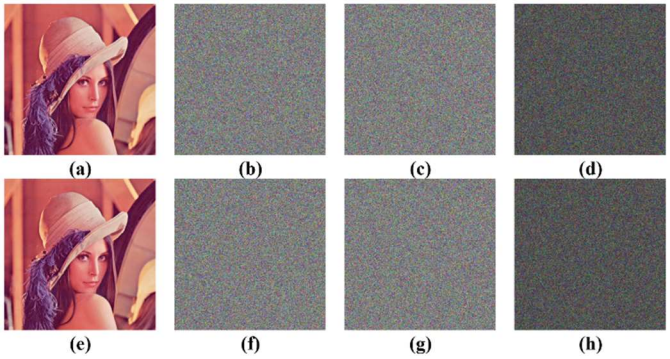

Figure 7. Cipher key sensibility analysis: (a) Plaintext image; (b) ciphertext image with c1 (c) Ciphertext image with c1+ ΔCK; (d) Difference image between (b) and (c); (e) Deciphered image from (b) with c1; (f) Deciphered image from (b) with c1+ ΔCK; (g) Deciphered image from (c) with c1; (h) Difference image between (f) and (g).

E. KEYSPACE AND KEY SENSITIVITY

Keyspace analysis is utilized to calculate the potential number of decryption keys that could be tried. To prevent brute force attacks, the key space shouldn't be smaller than 2^{100} [35]. In our cryptosystem, the control and user-defined parameters of a, c, d, w, v1, v2, c_1, c_2, c_3, and c_4 can be regarded as security keys. The key space would be 100 times larger if the precision of each floating-point number was 10^{-14}. We deduce from the analysis above that the proposed method's key space is around $(10^{14})^{10} \approx 2^{465}$. Moreover, considering the SHA-256 algorithm, which outputs 256 bits in hexadecimal form, the overall key space is $>2^{465}$. The key space of the cryptographic technique is therefore very large. Therefore, using the brute-force method to attack this cryptosystem is hard.

The key also must be highly sensitive to bit changes. A similar key may also be able to decipher the cipher image if the key is not subtle enough. Thus, we examined the cipher-text difference rate (CDR) to evaluate the critical sensitivity [36]. The CDR of three encrypted images CI1, CI2, and CI3 with different cipher keys CK, CK + ΔCK, and CK −ΔCK, respectively are described as follows:

$$Dif(Z_1(i,j),Z_2(i,j)) = \begin{cases} 0 & IF\ Z_1(i,j) = Z_2(i,j) \\ 1 & IF\ Z_1(i,j) \neq Z_2(i,j) \end{cases}, \quad (16)$$

$$DifZ(Z_1,Z_2) = \sum_{ij} Dif\big(Z_1(i,j),Z_2(i,j)\big), \quad (17)$$

$$CDR = \sum_{ij} \frac{DifZ(CI_1,CI_2) + DifZ(CI_1,CI_3)}{2 \times M \times N} \times 100\%. \quad (18)$$

In particular, the reliability of the cipher system is increased by the CDR of the cryptosystem approaching 100%. For the proposed method, we alter the input key with the tiny changes + ΔCK and – ΔCK as shown in Table 6. Furthermore, Fig. 7 shows the results of the secret key sensitivity investigation for the Lena image. The figure shows us that any change in the secret key will cause us to obtain two encrypted images during the encryption process and two completely distinct decrypted outputs during the decryption process. This means that the cipher keys of the proposed system are extremely sensitive.

F. CHOSEN-PLAINTEXT AND KNOWN-PLAINTEXT CRYPTANALYSIS

Other common attacks in the field of cryptanalysis include the chosen- plaintext and known-plaintext attacks. There are two things to think about in order to make the image encryption algorithm immune to such attacks. The cryptosystem must, first and foremost, be connected to the original image. The diffusion process and the permutation process ought to be tightly related [30]. In the suggested image cryptosystem, the original image is encrypted using a one-time cipher key. This cipher key is produced based on the hash value of the original image and user-defined parameters. Therefore, the one-time cipher key will likewise be changed if the original image is changed. The one-time cipher key will differ even for the same plaintext image. Besides, the proposed cryptosystem uses the enhanced Josephus problem to shuffle the image pixels and to select a random column from a scrambled image and a random column from a random image to XOR those with a current column. Consequently, the suggested cryptosystem can resist known and chosen plaintext cryptanalysis since it heavily rely the plain image.

G. NOISE AND OCCLUSION ATTACK

In general, a ciphertext image is susceptible to noise during transmission and processing and may experience data loss. An image cryptosystem must therefore be strong and able to tolerate noise and data loss. To test the robustness of the proposed method, we simulate the noise and various levels of data loss on a Lena cipher image. Figs. 8 and 9 depict the simulation findings. As we can see, the deciphered images still include the majority of the original image's information. This indicates that the suggested algorithm is suitable for use in real-world circumstances and has efficient robustness.

Figure 8. Deciphering results of noise attacks: (a) deciphered "Lena" image after adding Gaussian noise with noise density 0.01; (b) deciphered "Lena" image after inserting Gaussian noise with noise density 0.1; (c) deciphered "Lena" image after inserting Pepper & Salt noise with noise density 0.01; (d) deciphered "Lena" image after adding Pepper & Salt noise with noise density 0.05.

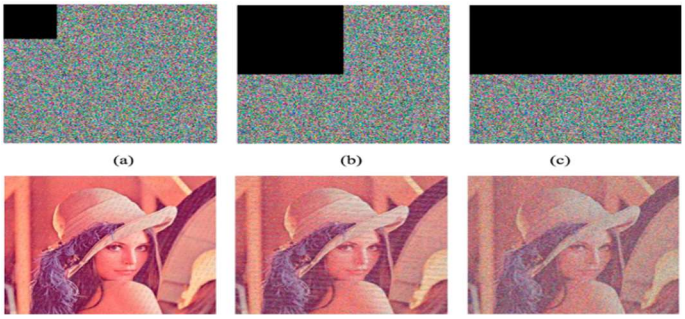

Figure 9. Occlusion attack: (a) 1/16 data loss of ciphertext "Lena"; (b) 1/4 data loss of ciphertext "Lena"; (c) 1/2 data loss of ciphertext "Lena"; (d) deciphered "Lena" from (a); (e) deciphered "Lena" from (b); (f) deciphered "Lena" from (c).

H. PERFORMANCE AND SPEED ANALYSIS

The level of security that a cryptosystem offers is its main concern, and the execution time is its second-most critical performance indicator. The decryption procedure is exactly the opposite of encryption because the suggested algorithm is a type of symmetric key algorithm. As a result, both the encryption and decryption processes take the same amount of time to complete. In this section, we only evaluate and test the

encryption speed. Several systems have been used for speed analysis, which results in ambiguity when comparing various techniques. This issue is solved by using the Number of Cycles Per Byte (NCPB) and Encryption Throughput (ET) [37, 38], which are described as follows:

$$ET = \frac{Image\ size(B)}{Encryptio\ time\ (sec)}, \quad (19)$$

$$\text{NCPB} = \frac{CPU\ speed(GHz)}{ET}. \quad (20)$$

The number of encryption bytes produced in a unit of time increases with the value of the ET. However, a lower NCPB measure is preferable because it means less processing is needed for the encryption process. Table 7 lists the performances of many cryptosystems that have been published in the literature. Table 7 makes it clear that the suggested method outperforms its rivals [13, 15, 17, 18, 20, 23, 24] in terms of both security and speed.

Table 7. Performance analysis of our method and some other methods using Lena image.

Schemes	Image type	Encryption time	Key size	X^2	NPCR	UACI	CPU speed	ET	NCPB
[13]	Gray	> 0.139	$\approx 2^{384}$	240.91	99.6279	33.4816	3	1.7986	1591
[15]	Gray	-	$\approx 2^{138}$	207	99.6159	33.4326	-	-	-
[17]	Gray	>0.0720	$\approx 2^{90}$ **(Failed)**	-	99.27 **(Failed)**	33.28 **(Failed)**	2.20	3.4722	604
[18]	Gray	0.0234>	$\approx 2^{446}$	-	99.6295	33.4851	3.80	10.7672	337
[20]	Gray	-	$\approx 2^{419}$	-	99.6338	33.4040	2.6	-	-
[23]	Gray	> 1.268	-		99.6262	33.4578	3.4	0.1972	16446
[24]	RGB	> 4.972	$\approx 2^{186}$		99.5894	33.4629	2.80	0.0377	70809
Ours	RGB	> 0.0931	$\approx 2^{465}$		99.7311	33.5177	2.71	8.0559	321

VI. CONCLUSIONS

In this paper, an enhanced Josephus problem-based chaotic image cryptosystem is proposed. The main focus is to provide a secure and high-speed scheme. From the experimental results, it is explicit that the suggested cryptosystem, in general, provides better encryption performance in comparison to modern image cryptosystems. Security empirical findings show that the suggested technique is faster and has a higher key space and sensibility. Occlusion and noise assaults produce clearer images, and the data in the anti-differential cryptanalysis test are more closely aligned with theoretical values. Moreover, the proposed method exhibits a higher pass rate in the local entropy test and reduces the autocorrelation between the image pixels. On the other hand, the fair speed tests proved the high speed of the proposed cryptosystem compared to the previous systems. These properties make the proposed cryptosystem a better candidate for real-time image security. In the future, we will investigate leveraging GPUs to speed up the proposed cryptosystem.

References

[1] M. T. Elkandoz and W. Alexan, "Image encryption based on a combination of multiple chaotic maps," *Multimed. Tools Appl*., pp. 1–22, 2022, https://doi.org/10.1007/s11042-022-12595-8.

[2] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Inf. Sci. (Ny)*., vol. 547, pp. 1154–1169, https://doi.org/10.1016/j.ins.2020.09.055.

[3] M. Shariatzadeh, M. J. Rostami, and M. Eftekhari, "Proposing a novel dynamic AES for image encryption using a chaotic map key management approach," *Optik (Stuttg)*., vol. 246, no. August, p. 167779, 2021, https://doi.org/10.1016/j.ijleo.2021.167779.

[4] G. Spasova and M. Karova, "A new secure image encryption model based on symmetric key," P*roceedings of the 2021 International Conference on Biomedical Innovations and Applications (BIA)*, 2022, vol. 1, pp. 107–110. https://doi.org/10.1109/BIA52594.2022.9831258.

[5] Z. Chen and G. Ye, "An asymmetric image encryption scheme based on hash SHA-3, RSA and compressive sensing," *Optik (Stuttg)*., vol. 267, p. 169676, 2022, https://doi.org/10.1016/j.ijleo.2022.169676.

[6] T. S. Ali and R. Ali, "A new chaos based color image encryption algorithm using permutation substitution and Boolean operation," *Multimed. Tools Appl*., vol. 79, no. 27, pp. 19853–19873, 2020, https://doi.org/10.1007/s11042-020-08850-5.

[7] M. H. Ahmed, A. K. Shibeeb, and F. H. Abbood, "An efficient confusion-diffusion structure for image encryption using plain image related Henon map," *Int. J. Comput*., vol. 19, issue 3, pp. 464–473, 2020, https://doi.org/10.47839/ijc.19.3.1895.

[8] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949, https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.

[9] B. Zolfaghari and T. Koshiba, "Chaotic image encryption: State-of-the-art, ecosystem, and future roadmap," *Appl. Syst. Innov*., vol. 5, no. 3, p. 57, 2022, https://doi.org/10.3390/asi5030057.

[10] J. Yu, W. Xie, Z. Zhong, and H. Wang, "Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation," *Chaos, Solitons & Fractals*, vol. 162, p. 112456, 2022, https://doi.org/10.1016/j.chaos.2022.112456.

[11] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurc. Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998. https://doi.org/10.1142/S021812749800098X.

[12] E. Solak, C. Çokal, O. T. Yildiz, and T. Biyikoğlu, "Cryptanalysis of Fridrich's chaotic image encryption," *Int. J. Bifurc. Chaos*, vol. 20, no. 5, pp. 1405–1413, 2010. https://doi.org/10.1142/S0218127410026563.

[13] S. Amina and F. K. Mohamed, "An efficient and secure chaotic cipher algorithm for image content preservation," *Commun. Nonlinear Sci. Numer. Simul*., vol. 60, pp. 12–32, 2018, https://doi.org/10.1016/j.cnsns.2017.12.017..

[14] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, pp. 129–137, 2017, https://doi.org/10.1016/j.sigpro.2017.03.011.

[15] J. Chen, F. Han, W. Qian, Y.-D. Yao, and Z.-L. Zhu, "Cryptanalysis and improvement in an image encryption scheme using combination of the 1D chaotic map," *Nonlinear Dyn*., vol. 93, no. 4, pp. 2399–2413, 2018, https://doi.org/10.1007/s11071-018-4332-9.

[16] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng*., vol. 90, pp. 238–246, 2017, https://doi.org/10.1016/j.optlaseng.2016.10.020.

[17] X. Wang, Q. Wang, and Y. Zhang, "A fast image algorithm based on rows and columns switch," *Nonlinear Dyn*., vol. 79, no. 2, pp. 1141–1149, 2015, https://doi.org/10.1007/s11071-014-1729-y.

[18] M. Z. Talhaoui, X. Wang, and A. Talhaoui, "A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme," *Vis. Comput*., vol. 37, no. 7, pp. 1757–1768, 2021, https://doi.org/10.1007/s00371-020-01936-z.

[19] X. Wang and L. Liu, "Application of chaotic Josephus scrambling and RNA computing in image encryption," *Multimed. Tools Appl*., vol. 80, no. 15, 2021, https://doi.org/10.1007/s11042-020-10209-9.

[20] G. Yang, H. Jin, and N. Bai, "Image encryption using the chaotic Josephus matrix," *Math. Probl. Eng*., vol. 2014, pp. 1–13, 2014, https://doi.org/10.1155/2014/632060.

[21] A. K. Singh and A. Mohan, *Handbook of Multimedia Information Security: Techniques and Applications*, 1st ed. Switzerland: Springer, 2019. https://doi.org/10.1007/978-3-030-15887-3.

[22] W. Feng, J. Zhang, Q. Zhentao, and H. Yigang, "Cryptanalysis of image encryption algorithm based on variable step length Josephus traversing and DNA dynamic encoding," *Journal of Electronics and Information Technology*, vol. 44, pp. 1–8, 2022, https://doi.org/10.11999/JEIT210791.

[23] Y. Niu and X. Zhang, "A novel plaintext-related image encryption scheme based on chaotic system and pixel permutation," *IEEE Access*, vol. 8, pp. 22082–22093, 2020, https://doi.org/10.1109/ACCESS.2020.2970103.

[24] X. Wang and H. Sun, "A chaotic image encryption algorithm based on improved Joseph traversal and cyclic shift function," *Opt. Laser Technol.*, vol. 122, p. 105854, 2020, https://doi.org/10.1016/j.optlastec.2019.105854.

[25] M. Naim, A. Ali Pacha, and C. Serief, "A novel satellite image encryption algorithm based on hyperchaotic systems and Josephus problem," *Adv. Sp. Res.*, vol. 67, no. 7, pp. 2077–2103, 2021, https://doi.org/10.1016/j.asr.2021.01.018.

[26] D. R. I. M. Setiadi, E. H. Rachmawanto, and R. Zulfiningrum, "Medical image cryptosystem using dynamic Josephus sequence and chaotic-hash scrambling," *J. King Saud Univ. – Comput. Inf. Sci.*, vol. 34, issue 9, pp. 6818-6828, 2022, https://doi.org/10.1016/j.jksuci.2022.04.002.

[27] A. Alkhayyat, M. Ahmad, N. Tsafack, M. Tanveer, D. Jiang, and A. A. Abd El-Latif, "A novel 4D hyperchaotic system assisted Josephus permutation for secure substitution-box generation," *J. Signal Process. Syst.*, vol. 94, no. 3, pp. 315-328, 2022, https://doi.org/10.1007/s11265-022-01744-9.

[28] S. S. Askar and A. A. Elsadany, "Nonlinear dynamics of Cournot duopoly game: When one firm considers social welfare," *Discret. Dyn. Nat. Soc.*, vol. 2021, pp. 1–11, 2021, https://doi.org/10.1155/2021/6697341.

[29] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 4th ed. India: Pearson Upper Saddle River, 2006.

[30] W. Feng, Y.-G. He, H.-M. Li, and C.-L. Li, "Cryptanalysis of the integrated chaotic systems based image encryption algorithm," *Optik (Stuttg).*, vol. 186, pp. 449–457, 2019. https://doi.org/10.1016/j.ijleo.2018.12.103

[31] B. Arpacı, E. Kurt, K. Çelik, and B. Ciylan, "Colored image encryption and decryption with a new algorithm and a hyperchaotic electrical circuit," *J. Electr. Eng. Technol.*, pp. 1–17, 2020, https://doi.org/10.1007/s42835-020-00393-x.

[32] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci. (Ny).*, vol. 222, pp. 323–342, 2013, https://doi.org/10.1016/j.ins.2012.07.049.

[33] S. Dhall, S. K. Pal, and K. Sharma, "A chaos-based probabilistic block cipher for image encryption," *J. King Saud Univ. – Comput. Inf. Sci.*, vol. 34, no. 1, pp. 1533–1543, 2022, https://doi.org/10.1016/j.jksuci.2018.09.015.

[34] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber Journals Multidiscip. Journals Sci. Technol. J. Sel. Areas Telecommun.*, vol. 1, no. 2, pp. 31–38, 2011.

[35] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map," vol. 121, pp. 203–214, 2019, https://doi.org/10.1016/j.optlaseng.2019.04.011.

[36] S. A. Jassim and A. K. Farhan, "Combined Chebyshev and logistic maps to generate pseudorandom number generator for internet of things," *Int. J. Electr. Comput. Eng.*, vol. 12, no. 3, pp. 3287–3297, 2022, https://doi.org/10.11591/ijece.v12i3.pp3287-3297.

[37] A. K. Shibeeb, M. H. Ahmed, and A. H. Mohammed, "A new chaotic image cryptosystem based on plaintext-associated mechanism and integrated confusion-diffusion operation," *Karbala Int. J. Mod. Sci.*, vol. 7, no. 3, 2021, https://doi.org/10.33640/2405-609X.3117.

[38] Z. Qiao, S. El Assad, and I. Taralova, "Design of secure cryptosystem based on chaotic components and AES S-Box," *AEU – Int. J. Electron. Commun.*, vol. 121, p. 153205, 2020, https://doi.org/10.1016/j.aeue.2020.153205.

***AHMED KAREEM SHIBEEB**, Received computer Science degree and M.Sc. degree from Al- Mustansiriyah University, Baghdad, Iraq, in 2013 and 2016, respectively. He is Currently a lecturer at Middle Technical University and PhD student at Kufa University. His research interests include multimedia security, chaos-based cryptography, and cryptanalysis of a classical cipher.*

***MOHAMMED HUSSEIN AHMED,** received computer Science degree and M.Sc. degree from Al- Mustansiriyah University, Baghdad, Iraq, in 2010 and 2016, respectively. He is Currently an assistant lecturer at Al- Mustansiriyah University. His research interests include cryptology science, artificial intelligent systems and cryptanalysis of a classical cipher.*

***SALAH ALBERMANY**, a Professor of Computer Science at Kufa University. His research interests include Computer Networks Security, Applied Cryptography, Algorithm Analysis, Authentication, and Algebraic Number Theory.*