Integrated Dual Hyperchaotic and Josephus Traversing based 3D Confusion-Diffusion Pattern for Image Encryption

by De Rosal Ignatius Moses Setiadi

Submission date: 02-Oct-2023 12:02AM (UTC+0700)

Submission ID: 2182099345

File name: Manuscript_rev2.docx (2.74M)

Word count: 8494

Character count: 47939

Integrated Dual Hyperchaotic and Josephus Traversing based 3D Confusion-Diffusion Pattern for Image Encryption

Abstract

This paper introduces an enhanced image encryption technique that relies on 3D confusion and diffusion patterns, aiming to achieve maximum performance in terms of confusion and diffusion. The proposed encryption method combines four phases: dual hyperchaotic, improved logistic map (ILM), Josephus traversing, and a hash function. The first and second phases utilize improved Chen and Lorentz systems-based 3D patterns to enhance confusion and diffusion. In the third phase, bit-plane permutations are performed through Josephus traversing in three directions: x, y, and z. Lastly, the fourth phase implements diffusion based on ILM to optimize encryption performance. The integration of a hash function in this method serves to heighten key sensitivity. The test results demonstrate the method's exceptional performance across various analyses, including statistical, differential, brute-force, and NIST test suite assessments. Additionally, the proposed method outperforms previous approaches significantly, as indicated by the majority assessment.

Keywords: 3D confusion-diffusion, Improved Chen System, Improved Lorentz System, 3D bit-plane permutation, 3D pattern encryption

1. Introduction

The internet is a technology that humans increasingly need. The International Telecommunication Union (ITU) reports that internet users globally reached 66%. This development is also accompanied by crime in cyberspace continuing to increase. Cybersecurity Ventures stated in (Waseso and Setiyanto, 2023) research that it is estimated to cause losses of up to $10.5 trillion annually by 2025. Security is very important in the internet, and cryptography is a vital digital technology extensively employed to secure data during internet transmission. According to the fundamental principles of diffusion and confusion, initially proposed by Claude Shannon (Shannon, 1949). According to Shannon's theory, diffusion entails dispersing the statistical structure of plaintext throughout the entirety of ciphertext. On the other hand, confusion involves establishing a sophisticated and intricate link between the ciphertext and the symmetric key. This complexity arises from a well-defined and repetitive process that includes permutations and replacements. Permutation alters the sequence of bits based on a specific algorithm, while substitution replaces particular components, usually bits, following precise criteria (Andono and Setiadi, 2022). In brief, cryptography functions as an encryption technique, transforming the meaning of data or media to thwart unauthorized access to its contents. The complementary decryption process is employed to restore the data to its original form (Ghadirli et al., 2019; Kaur and Kumar, 2020; Setiadi et al., 2023). By employing these principles of diffusion and confusion, modern image encryption techniques aim to ensure the confidentiality and integrity of sensitive visual data. The encrypted image appears as a seemingly random and indistinguishable arrangement of pixels, making it incomprehensible to unauthorized parties. However, proper decryption using the appropriate symmetric key can recover the original image precisely, allowing authorized users to access its intended content. This ensures secure communication and storage of visual data, preventing unauthorized access and data breaches.

Encryption can be done on various digital media; image encryption is the most frequently used object (Erkan et al., 2023). Images are formed from pixels arranged in a matrix, whereas color images processed by computers generally have three matrix layers, namely red, green, and blue(RGB)(Demirtaş, 2022). Encryption of the image can be done by carrying out the process of diffusion and confusion on the pixels and bits of the image (Andono and Setiadi, 2022; Gan et al., 2019; Hasheminejad and Rostami, 2019; K.U. and Mohamed, 2021; Setiadi and Rijati, 2023; Q. Wang et al., 2022; Wang et al., 2021; Wei et al., 2023), where the level of randomness can determine the quality of the image encryption. However, the image has several intrinsic elements that differ from the text, namely redundancy and high volume, as well as a strong correlation between adjacent pixels.(Feng et al., 2019; Lai et al., 2023; Setiadi et al., 2022).

Encryption of images has been carried out by various studies such as the block shuffle method (Li et al., 2019), Serpent(Shah et al., 2020), DNA (Elmanfaloty et al., 2021; Feng et al., 2019), S-Box(Abduljabbar et al., 2022; Jun and Fun, 2021; Zhu et al., 2023), and chaos-based (Liu et al., 2020; Neamah, 2023; Qian et al., 2021; Wang et al., 2021). Chaos-based methods are relatively more popular and have been developed for image encryption, such as Logistic maps, Tent maps, Barker maps, Arnold cat maps, and Henon maps. The chaos-based method has the advantage of a high level of security because encryption depends on nonlinear dynamics, has extreme sensitivity to initial conditions, and has an uncertain pattern(Jasra and Hassan Moon, 2022). However, currently, the chaos method is also modified or combined with various other methods to increase security as in research (Luo et al., 2019; Qian et al., 2021; Setiadi et al., 2022; L. Wang et al., 2023; Wang et al., 2021; Winarno et al., 2023; Zhu et al., 2023).

The chaotic method has been developed into hyperchaotic like the Lorentz system. In general, the chaotic method has similarities with the hyperchaotic. The difference is in complexity, dimensions, and utilization of discrete dynamical systems. Apart from the Lorentz system, there are also the Chen and Lu systems. Recent research has witnessed the modification and integration of the hyperchaotic method with other approaches, as evidenced by studies conducted by (Abduljabbar et al., 2022; Benaissi et al., 2023; Liu et al., 2020; Naim et al., 2021; Qin et al., 2022; M. Wang et al., 2023; Wang et al., 2019; Ye et al., 2022). The complexity of the hyperchaotic method offers safety advantages, one of which is reflected in the Lyapunov exponent value. The Lyapunov exponent serves as a metric for quantifying the degree of chaos in dynamical systems, including Lorentz systems. This exponent value determines the extent of divergence between two trajectories originating from points in very close proximity at the initial time. Consequently, a higher Lyapunov exponent value implies a faster separation of the two trajectories, leading to the production of a more chaotic sequence(Ye et al., 2022).

Chaotic sequences are generally applied as keystreams for confusion and diffusion processes in image encryption. The keystream is one of the most important components determining the quality of encryption security(Zhang et al., 2023). An increasingly random and unique keystream can increase the randomness of pixels and image bits. With hyperchaotic complexity, the keystream generated from the chaotic sequence has high security. Encryption security can also be improved by creating unique confusion and diffusion patterns(Andono and Setiadi, 2022; K.U. and Mohamed, 2021; Zhang and Liu, 2011) and the use of hash operations to increase keyspace, key sensitivity (Liu et al., 2022; Wei et al., 2023), as well as resistance to various attacks, especially brute force and statistical. Patterns that are widely applied, such as cyclic or rotation scrambling (Cao et al., 2018; Kandar et al., 2019; Wang et al., 2018a; Wang and Sun, 2020), combine column and row scrambling(Andono and Setiadi, 2022; Kumar Patro and Acharya, 2019; Teng et al., 2021; Yu et al., 2022), zigzag(Kamal et al., 2021; Qin et al., 2022; Q. Wang et al., 2022), Josephus traversing(Setiadi et al., 2022; L. Wang et al., 2023; M. Wang et al., 2023; Wang et al., 2021, 2018b; Wang and Sun, 2020). While hash operations have been widely implemented in research (Liu et al., 2022; Setiadi et al., 2022; M. Wang et al., 2023; Y. Wang et al., 2022; Wei et al., 2023) and have proven to increase resistance from differential attacks.

Based on the abovementioned literature, this paper proposes a 3D pattern confusion-diffusion to improve image encryption security based on hyperchaotic and chaotic systems, Josephus traversing and hash functions. In detail, the contribution of this paper is:

1. Design a 3D encryption pattern to increase the security and complexity of encryption.
2. Combines the improved chaotic and dual hyperchaotic system for multi-level and direction permutation and substitution pixels to improve diffusion and confusion encryption.
3. Using Josephus traversing to process bit-level confusion with 3D direction.
4. Utilizing the hash function to increase key sensitivity and keyspace.

Furthermore, the remainder of this paper describes the preliminaries in section 2, which contain various permutation techniques, Josephus traversing, Chen system, Lorentz system, and improved logistics map that inspired the proposed method. The proposed method, which explains in detail the encryption and decryption stages and their flowcharts, is in section 3. A discussion of the results and analysis is presented in section 4. Finally, the conclusion is presented in section 5.

2. Preliminaries

2.1 Permutation Technique

2.1.1 Column and Row Permutation

Some of the permutation techniques used in various image encryption methods are row and column permutations (Babaei et al., 2020; Demirtaş, 2022; Kandar et al., 2019; Kumar Patro and Acharya, 2019; Xu et al., 2020; Yu et al., 2022) to reduce the correlation of neighbouring pixel values. You do this by scrambling the row and column positions at both the pixel level (pixel level permutation) and the bit level (bit level permutation) of the image. Permutations of column and row pixels can be done in an interleaving fashion with multiple iterations(Kandar et al., 2019), cyclic shifting, or rotation-based chaotic map(Babaei et al., 2020; Kumar Patro and Acharya, 2019; Xu et al., 2020), order or swap by sorting chaotic sequence(Demirtaş, 2022; Liu et al., 2020; Yu et al., 2022). Permutations at the bit level are generally simpler, however, they require large computations because they have to be performed on each pixel. In permutation, color images can be done by cross scrambling on pixels(Demirtaş, 2022) or 3D bit-plane on pixel bits to mix bit-planes on all three layers(Gan et al., 2019).

2.1.2 Josephus Traversing

The Josephus algorithm is an algorithm inspired by the puzzle game algorithm that determines who is the last survivor. A number of people sit in a circle, and one starts by removing one person each time his turn comes. This process continues until one person remains the winner. Josephus' algorithm can be found in discrete math problems that require processing a sequence of elements in the correct order. In the permutation process, this algorithm can be used to permutate the image pixel order or to do bit scrambling. Some research using the Josephus sequence algorithm is (Setiadi et al., 2022; L. Wang et al., 2023; M. Wang et al., 2023; Wang et al., 2021; Wang and Sun, 2020). In general, the Josephus traversing algorithm for determining sequence can be calculated by Eq. (1).

$$J(n,k,m) = (J(n-1,k,m) + m - 1)\, mod\, n + 1 \qquad (1)$$

Where $J(n,k,m)$ indicates the last sequence, k is the starting period, m is the reduction frequency, and n is the number of elements sorted. For example, if $n = 8$, $k = 5$, and $m = 3$, then we get the order $5, 2, 7, 4, 1, 6, 3, 8$.

2.2 Chaos System

2.2.1 Improved Lorentz System

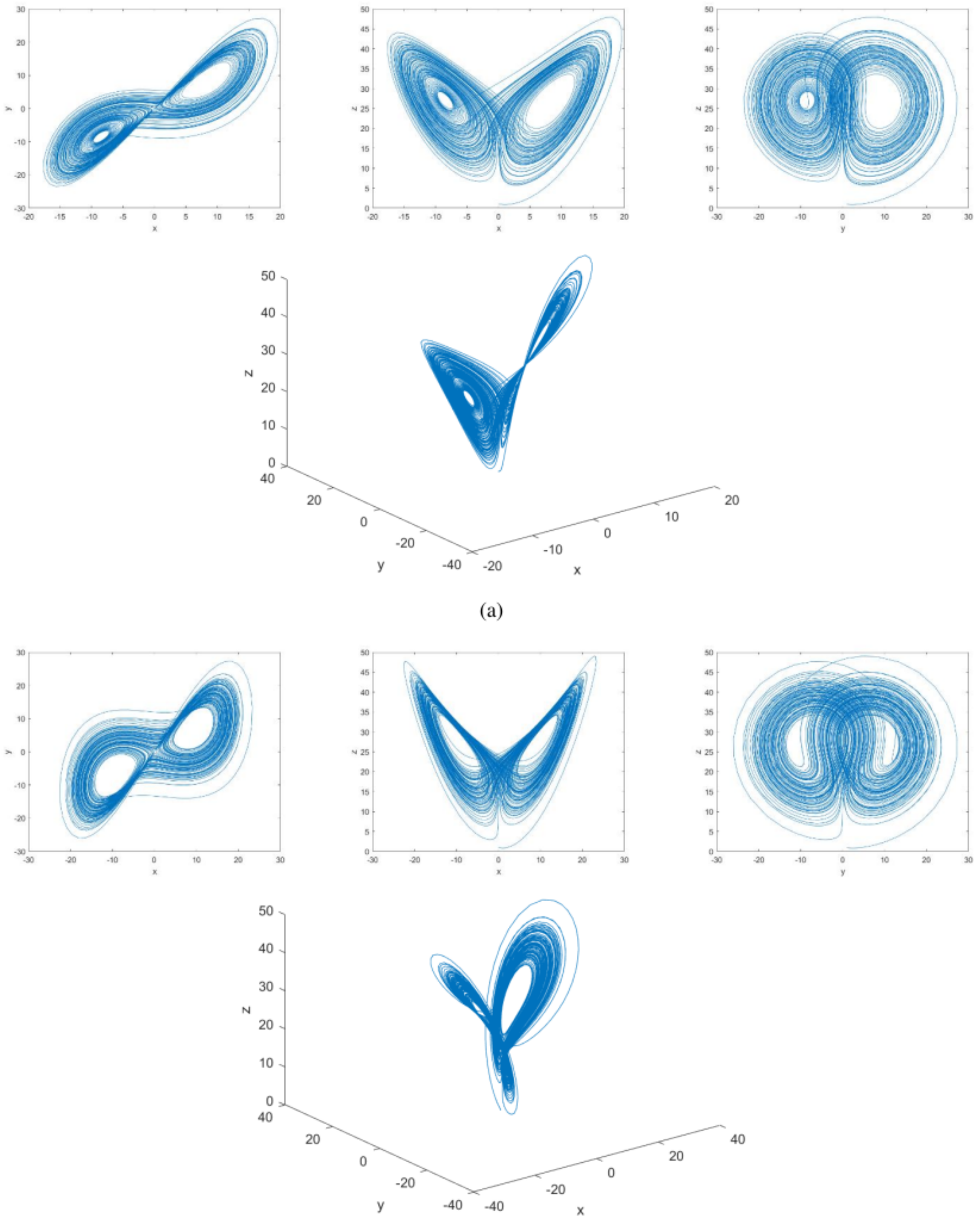
Lorentz system is a hyperchaotic system widely applied for image encryption. Lorentz systems generally have three nonlinear chaotic dimensions and three hyperparameters. The traditional Lorentz system will generate chaotic phenomena using the formula in Eq. (2) (Ye et al., 2022).

$$\begin{aligned} a' &= -\alpha(a-b) \\ b' &= -ac + \gamma a - b \\ c' &= ay - \beta c \end{aligned} \qquad (2)$$

Where α, β, γ is a hyperparameter with a default value $\alpha = 10, \beta = \frac{8}{3}$, and $\gamma = 28$,

Along with developments, the Lorentz system has increased its complexity by adding the hyperparameter δ and is referred to as the Improved Lorenzt system (ImproLS). If the value of $\delta = 0$, the result will be the same as the traditional Lorenzt system. The function of the hyperparameter δ is to produce a larger positive Lyapunov exponent (LE) value. With a value of $\delta = 0.4$, LE=2.0932 can be produced. ImproLS can be calculated by Eq. (3)(Ye et al., 2022). Fig. 1 presents samples of Lorentz chaotic attractor and ImproLS chaotic attractor with 22172677 number of iterations applied.

$$\begin{aligned} a' &= -\alpha(a-b) + \delta bc \\ b' &= -ac + \gamma a - b \\ c' &= ay - \beta c \end{aligned} \qquad (3)$$



(a)

(b)

Figure 1. Lorentz Chaotic Attractor {(a) row standard Lorentz, (b) Improved Lorentz}

2.2.2 Chen System

Chen's chaotic system is a three-dimensional differential nonlinear system that can produce complex and chaotic dynamics. One characteristic of this system is the existence of a strange attractor which can attract the system's motion to certain regions in a typical phase space with an irregular pattern. Chen's chaotic system can be calculated by Eq. (4)(Gan et al., 2019).

$$\begin{aligned} a' &= \alpha(b-a) \\ b' &= (\gamma-\alpha)a - ac + \gamma b \\ c' &= ab - \beta c \end{aligned} \tag{4}$$

Where by default $\alpha = 35, \beta = 3$, and $\gamma = 28$ with 200 iterations, a Chen attractor plot can be produced as in row 1 Fig. 2.

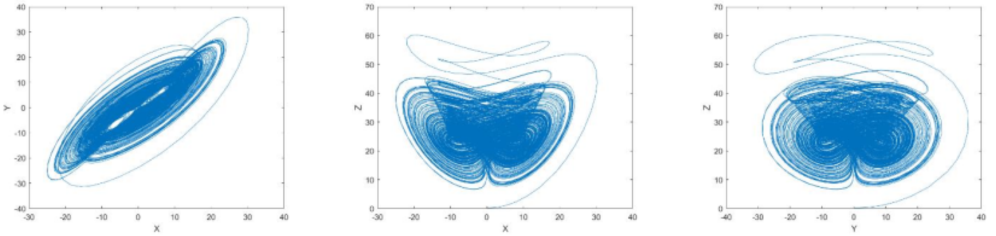


Figure 2. Sample Chen chaotic attractor

2.2.3 Improved Logistic map (ILM)

ILM was first proposed in research (Han, 2019), aiming to generate a likely tend key space and mapping range using a constant chaotic signal generator based on ILM applied in secure communications. ILM has been implemented in several other image encryption research (Benaissi et al., 2023; Moysis et al., 2020), to improve the encryption quality. ILM can be calculated by Eq. (5), whereby the ILM phenomena of constant chaos and constant Lyapunov exponent are obtained with appropriate constant full mapping, as shown in Fig. 3 (left) for bifurcation diagram and Fig. 3(right) Lyapunov exponent spectrum.

$$p_{n+1} = 2\alpha - \alpha_n^2/\alpha \tag{5}$$

Where p_n is initial, and α is the parameter for iteration, the full mapping range of $p_n \in [-2\alpha, 2\alpha]$.

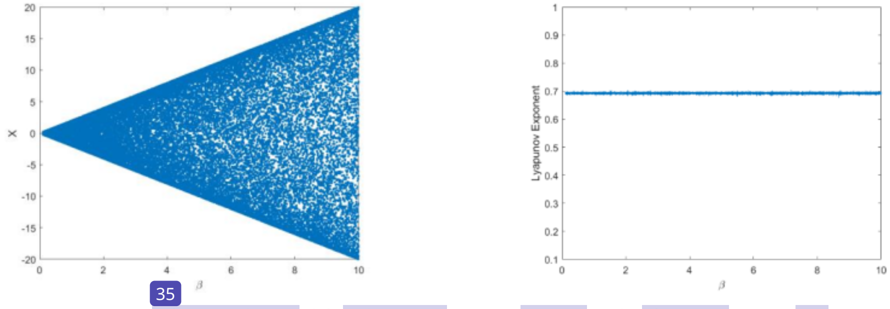


Figure 3. Bifurcation diagram (left) and Lyapunov exponent spectrum (right) of Improved Logistic Map

3. Proposed Method

Inspired by the previously described literature, this study proposes a combination of several permutation techniques, chaos systems, and hash operations to increase the security of image encryption. Patterns of 3D pixel permutation-substitution, bit-plane permutation, and 1D substitution are based on hyperchaotic, Josephus traversing, and improved logistic maps to improve the quality of diffusion and confusion. We use a 3D matrix pattern by reshaping the 2D matrix. Figure 4 provides details illustration of all encryption phases in the proposed method along with an example of a 5×5 matrix as in the research (Erkan et al., 2023, 2022; Toktas and Erkan, 2022). For more detail, the discussion of each phase is explained in sections 3.1 to 3.4.

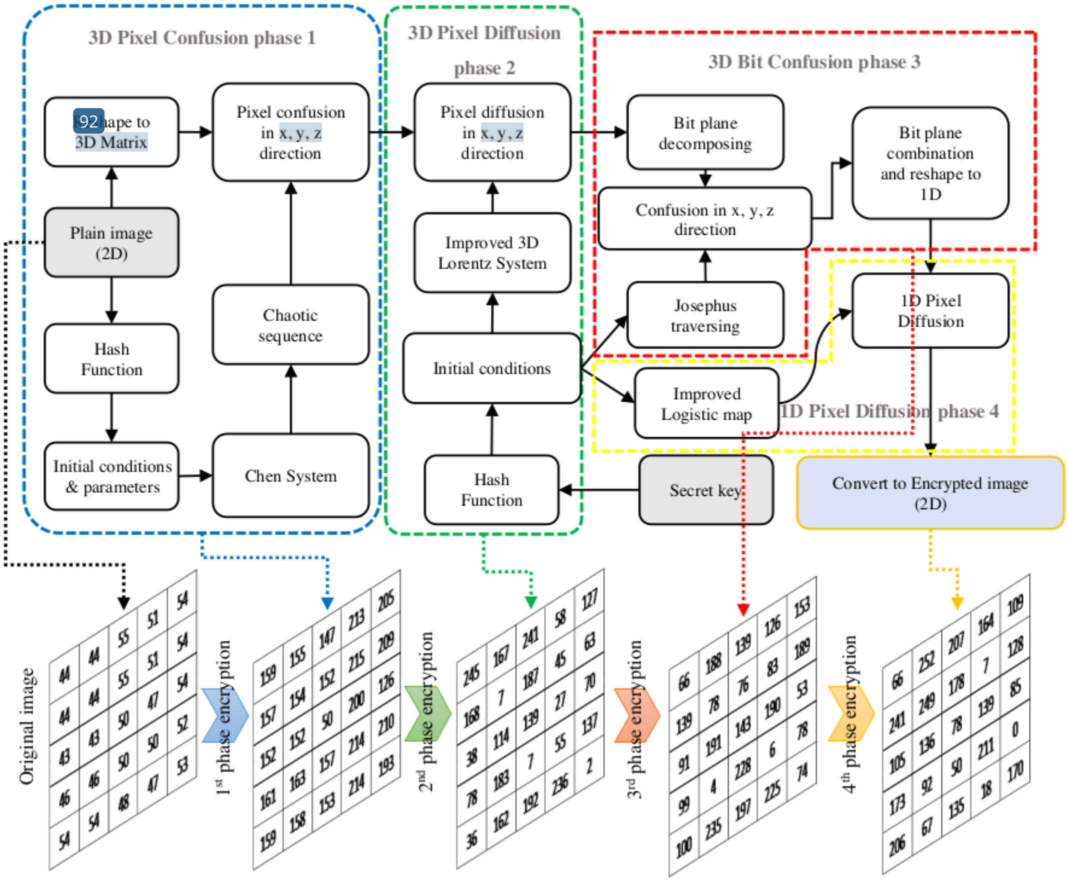


Figure 4. Illustration of the stage detail of the proposed method with sample 5×5matrix

3.1 3D Confusion

The first phase is one of the parts with several contributions, such as 3D encryption patterns and modifications to the Chen system. The 3D encryption pattern makes the permutation process occur three times for each pixel, where the pixel position will change from x, y, and z directions. The detailed steps are as follows:

1. In the first stage, the plain image as input is reshaped into a 3D matrix by calculating the cube root value of the total image pixels (width × height). In this case, it is limited to images with an integer cube root. After obtaining the cube root (cr), reshape the 2D image matrix into a 3D matrix with dimensions ($cr \times cr \times cr$). Then, on each side of cr there are a number of cr 2D matrix layers.
2. On the other hand, the SHA-512 function is performed on the original image, 64 unique characters ($hash$) will be generated, and then each character will be converted into an ASCII number. To determine the initial values a, b, and c is done by calculating the standard deviation (σ) of every 12 numbers and dividing by 10, do the same thing to get additional parameters for the Chen system, i.e., δ and ε, but done at 14 numbers and dividing by 100, see Eq. (6).

$$
\begin{aligned}
a &= (\sigma(hash(1{:}12)))/10 \\
b &= (\sigma(hash(13{:}24)))/10 \\
c &= (\sigma(hash(25{:}36)))/10 \\
\delta &= (\sigma(hash(37{:}50)))/100 \\
\varepsilon &= (\sigma(hash(51{:}64)))/100
\end{aligned}
\qquad (6)
$$

At Eq. (6), ten divisions are carried out for a, b, and c, as well as 100 divisions for δ and ε to prevent the value of the effect of significant changes to the Chen system, producing many duplicate values.

3. Perform an improved Chen system using Eq. (7). As a note, modifications are made by creating dynamic initial conditions and adding parameters δ and ε. This modification aims to make Chen's system more complex and dynamic so that it can increase the chaos effect in generated chaotic sequences.

$$
\begin{aligned}
a' &= \alpha(b-a) \\
b' &= (\gamma-\alpha)a - ac + \gamma b + \delta \\
c' &= ab - \beta c + \varepsilon
\end{aligned}
\qquad (7)
$$

4. Take a number of cr numbers (ncr) in each a', b', and c'. Sort the index in ascending order for each ncr so that an $order\_cr$ is generated as a reference for permutations in a number of 2D matrix cr layers on each of the x, y, and z axes.
5. Get confused 3D matrix in phase 1 ($3Dp1$), and then encryption is continued in phase 2.

3.2 3D Diffusion

In the second phase, the diffusion process is still carried out with a 3D pattern based on the improved Lorentz system so that three modulus operations occur on each pixel in the x, y, and z directions. The proposed 3D diffusion pattern is the third contribution of the proposed method. In detail, the stages of confusion in phase two are as follows:

1. Input the secret key from the user and perform the SHA-512 hash operation to get 64 unique characters ($hash$), then convert the characters to ASCII numbers.
2. Determine the three initial values (a, b, c) and the value of the parameter δ dynamically by calculating the σ of each of the 16 hash characters, as shown by Eq. (8)

$$
\begin{aligned}
a &= (\sigma(hash(1{:}16)))/10 \\
b &= (\sigma(hash(17{:}32)))/10 \\
c &= (\sigma(hash(33{:}48)))/10 \\
\delta &= \begin{cases}
\dfrac{(\sigma(hash(49{:}64)))}{10}, \sigma < 1.3 \\
\dfrac{(\sigma(hash(49{:}64)))}{100}, \sigma < 13 \\
\dfrac{(\sigma(hash(49{:}64)))}{1000} \ \sigma < 130 \\
\dfrac{(\sigma(hash(49{:}64)))/2}{1000} \ \sigma \geq 130
\end{cases}
\end{aligned}
\qquad (8)
$$

Notes for the division operation on Eq. 8 serves the same purpose as Eq. 6.

3. Get the chaotic sequence from a', b', and c', then do the conversion operation to string, take the last three characters, and convert again to double.
4. Take a chaotic sequence of $cr \times cr \times cr$ from a', then convert it into a 3D matrix. Then do the modulus operation as a $3Dp1$ confusion operation for the x axis as in Eq. (9).
5. Repeat step 4, and do the same for b' and c' for the y and z axes, respectively, like Eq. (9).

$$\begin{aligned} 3Dp1_{\ xyz} &= mod((3Dp1_{\ xyz} + a'_{ijk}), 256) \\ 3Dp1_{\ xyz} &= mod((3Dp1_{\ xyz} + b'_{ijk}), 256) \\ 3Dp1_{\ xyz} &= mod((3Dp1_{\ xyz} + c'_{ijk}), 256) \end{aligned} \tag{9}$$

   Where ijk is the coordinates of the chaotic sequence.
6. Get the encrypted $3Dp2$ matrix in phase 2.

3.3 3D Bit Confusion

At this stage, the 3D matrix is confused at the bit-plane level with 3D pattern permutations on the x, y, and z axes. The permutation sequence is generated by Josephus traversing with dynamic parameters based on the hash key. In more detail, the stages in phase 3 are explained as follows:

1. Using the same hash in phase 2, create an initial parameter by calculating the standard deviation of each of the ten hash characters that have been converted to ASCII numbers.
2. Get the initial values of parameters k and m using Eq. (10), while the parameter value n is equal to $8 \times cr$. First of all, the initial parameters k_x and m_x are used for the x-axis. For the y and z axes, use each of the following ten characters of $hash$.

$$\begin{aligned} k_x &= \lfloor \sigma(hash(1{:}10)) \rfloor \\ m_x &= \lfloor \sigma(hash(11{:}20)) \rfloor \\ k_y &= \lfloor \sigma(hash(21{:}30)) \rfloor \\ m_y &= \lfloor \sigma(hash(31{:}40)) \rfloor \\ k_z &= \lfloor \sigma(hash(41{:}50)) \rfloor \\ m_z &= \lfloor \sigma(hash(51{:}60)) \rfloor \end{aligned} \tag{10}$$

3. Generate Josephus sequence using Eq. (1).
4. Convert the numbers in the $3Dp2$ matrix to binary numbers, then reshape the matrix so that the dimensions are $(8 \times cr) \times cr \times cr$.
5. The result of step 4 is to make the x-axis a bit-plane, using the Josephus sequence as a reference for the permutation process on the x-axis.
6. Combine each 8-bit plane, then convert back to integer and reshape so that the dimensions are $cr \times cr \times cr$.
7. Repeat steps 4 to 6 for the y and z axes, and at the end of this phase, a $3Dp3$ matrix will be generated that has been permutated on the x, y, z axes.

3.4 1D Bit Diffusion

Finally, in phase 4, a diffusion process based on ILM was carried out. The purpose of this phase is to optimize the quality of diffusion, in detail, the stages are as follows:

1. Reshape the $3Dp3$ matrix into a 1D shape so that the dimensions are $1 \times (cr \times cr \times cr)$, then save it in the $1Dp4$ variable.
2. Determine the ILM initial condition value using the standard deviation of the hash that has been converted to ASCII form, where this $hash$ is the same as phases 2 and 3. Determine the dynamic initial condition with Eq. (11).

$$p_n = \begin{cases} \sigma\big(hash(1{:}64)\big), & \sigma < 7.99 \\ \dfrac{\big(\sigma\big(hash(1{:}64)\big)\big)}{10}, & \sigma < 79.9 \\ \dfrac{\big(\sigma\big(hash(1{:}64)\big)\big)}{100}, & \sigma \geq 79.9 \end{cases} \tag{11}$$

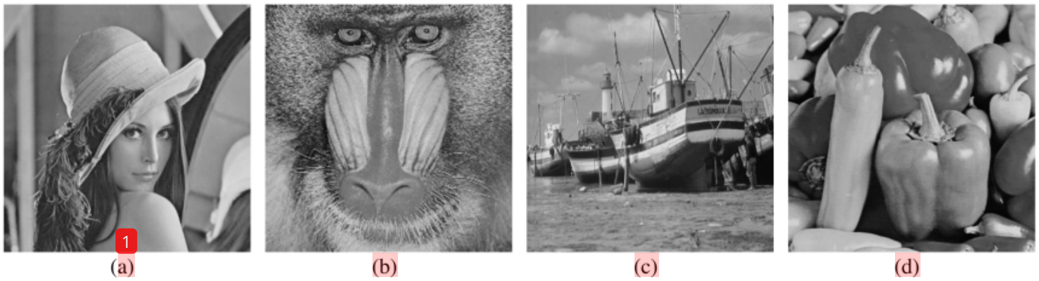
   The purpose of the division operation on Eq. (11) is to prevent the occurrence of inf values in a generated chaotic sequence.
3. Get the chaotic sequence from p, convert it to a string, then take the last three characters and convert them again to a number.
4. Perform modulus operations such as Eq. (12).

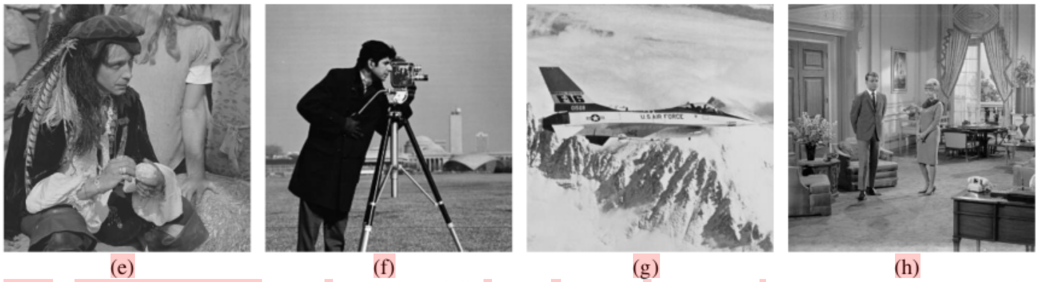
$$1Dp4_i = mod((1Dp4\ _i + p_i), 256) \tag{12}$$

   Where i is the pixel index.
5. Get the final encrypted image by reshaping it to a 2D matrix with the same dimensions as the original image.

4. Results and Analysis

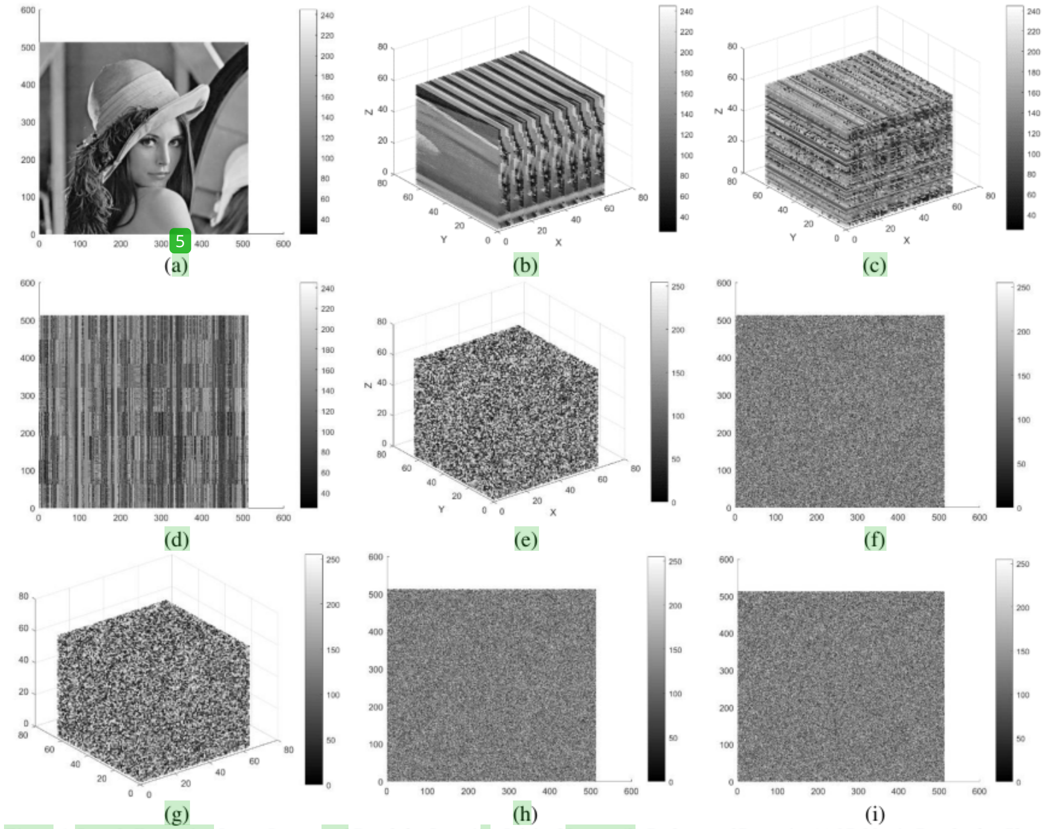
In this section, the proposed method is tested using standard images downloaded from the database (USC Viterbi School of Engineering, n.d.), where the image samples used are presented in Fig. 5. The image used is a grayscale image with dimensions of 512×512 pixels. The hardware used to experiment is a computer with an i7 processor Gen 11th with RAM 16GB. All images are tested with the proposed method, where the encrypted samples from each test are presented in Fig. 6 using scatter plots. This section also presents analysis tests and comparisons with several previous studies, which are explained in more detail in sections 4.1 to 4.7, where comparisons are made with the same dataset.


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



(e) (f) (g) (h)

Figure 5. Sample Image Dataset {(a) Lena; (b) Baboon/Mandrill; (c) Boat; (d) Peppers; (e) Pirate/Man; (f) Cameraman; (g) Airplane/F16; (h) Couple/Livingroom}



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Figure 6. Sample Encryption Input, Stages, and Result for Lena {(a) Original Image; (b) Reshape to 3D matrix; (c) 3D Matrix Result after Phase 1; (d) Result after Phase 1 after Reshape to 2D matrix; (e) 3D Matrix Result after Phase 2; (f) 3D Matrix Result after Phase 2 after Reshape to 2D matrix; (g) 3D Matrix Result after Phase 3; (h) 3D Matrix Result after Phase 3 after Reshape to 2D matrix; (j) Final Encryption Results}

4.1 Histogram and Chi-square Analysis

Histogram analysis is a method for visualizing the distribution of pixel intensities in an image. The image histogram shows how often certain intensity values appear in the image. The histogram can be used to evaluate the quality of image encryption, as good encryption should produce an image with a uniform histogram(Kamal et al., 2021; Setiadi et al., 2022). Based on the plot results presented in Fig. 6(c,d) and Fig. 6 (e,f), there are different pixel intensity distributions. Next can be seen in Fig. 7, there is also a significant histogram change in the cipher image. In the histogram of the original image (Fig. 7 (a,b)), the pixel intensity distribution is uneven, several pixel values have intensities of more than 2500, and other pixel values have zero intensity.

After encryption (Fig. 7 (c,d)) all pixel values from 0 to 255 have the same intensity of ≈ 1000. Visually this is a good indication. To ensure the uniformity of the pixel intensity distribution, chi-square (X^2) analysis is necessary. X^2 can be calculated by Eq. (13).

$$X^2 = \sum_{idx=1}^{256} \frac{(P_{idx} - f)^2}{f} \tag{13}$$

The grey recurrence value (P_{idx}) is defined as the value for each occurrence of the idx-th grey value, while f is the frequency that is calculated from each grey value using the formula ($f = \frac{P}{255}$). It should be noted that idx ranges from 1 to 256 in Matlab due to its indexing starting at 1. By setting a significant level (ς) of 0.05 and a degree of freedom (df) of 255, the resulting chi-square value $X^2_{\varsigma,df}$ = is 293.2478. A value lower than this confirms that the histogram is uniform.

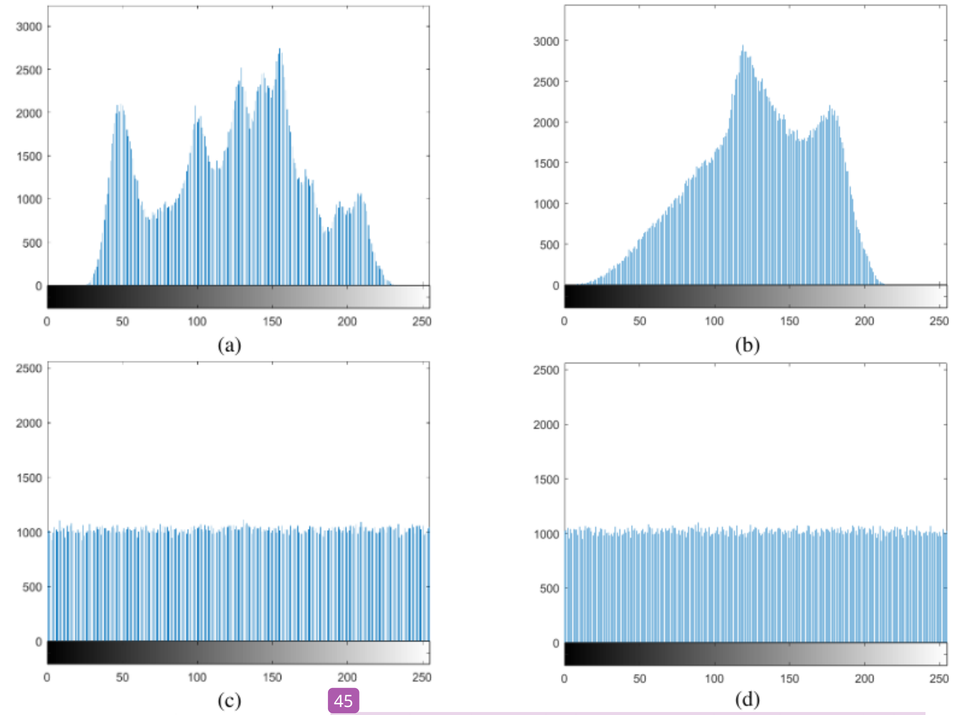


Figure 7. Sample Image Histogram {(a) Original Lena; (b) Original Baboon; (c) Encrypted Lena; (d) Encrypted Baboon}

Table 1. Chi-square Results and Comparison with Previous Method

Image	**Method**			
	(Liu et al., 2020)	**(Jun and Fun, 2021)**	**(Neamah, 2023)**	**Proposed**
Lena	253.4844	274.7188	-	251.8374
Baboon	244.5859	275.7813	259.7125	245.3873
Boat	-	266.0469	255.1092	253.8773
Peppers	265.2813	261.1406	243.2378	239.4873
Pirate	230.0011	-	-	241.8734

Cameraman	251.8281	-	-	249.3286
Airplane	-	-	260.5436	252.8924
Couple	261.0938	-	-	238.8733
Average	251.0458	269.4219	254.6508	246.6946
Pass Rate	6/6	4/4	4/4	8/8

The presentation of the chi-square test results in Table 1 shows that all histograms are validated uniformly. In addition, based on the average chi-square value, the proposed method has a better value than the previous method.

4.2 Information Entropy (IE) Analysis

The IE analysis serves as an important assessment to evaluate the encryption method's ability to resist statistical attacks in image encryption. IE also allows us to measure the level of randomness in the ciphered image. The IE values range from 0 to 8, where values closer to 8 indicate a higher level of randomness, while values closer to zero suggest a lower level of randomness. To calculate IE, we use Eq. (13), which involves variables such as n representing the total number of symbols, c_i denoting the information source, and $p(c_i)$ representing the probability of occurrence of the source c_i.

$$IE(c) = \sum_{i=1}^{n} p(c_i) log_2 \left(\frac{1}{p(c_i)}\right) \tag{13}$$

An encryption technique that yields an entropy value close to 8 implies better encryption quality, as it indicates a high level of randomness in the ciphered image. In Table 2, the entropy measurements for all encrypted images are approximately eight, confirming the effectiveness of encryption quality based on entropy. Furthermore, the proposed encryption method demonstrates superior performance compared to previous methods, making it a promising approach for image encryption tasks. This is evident from its ability to maintain a high level of randomness in the ciphered images, making it more robust against statistical attacks and enhancing the security of the encrypted data.

Table 2. Information Entropy Results and Comparison with Previous Method

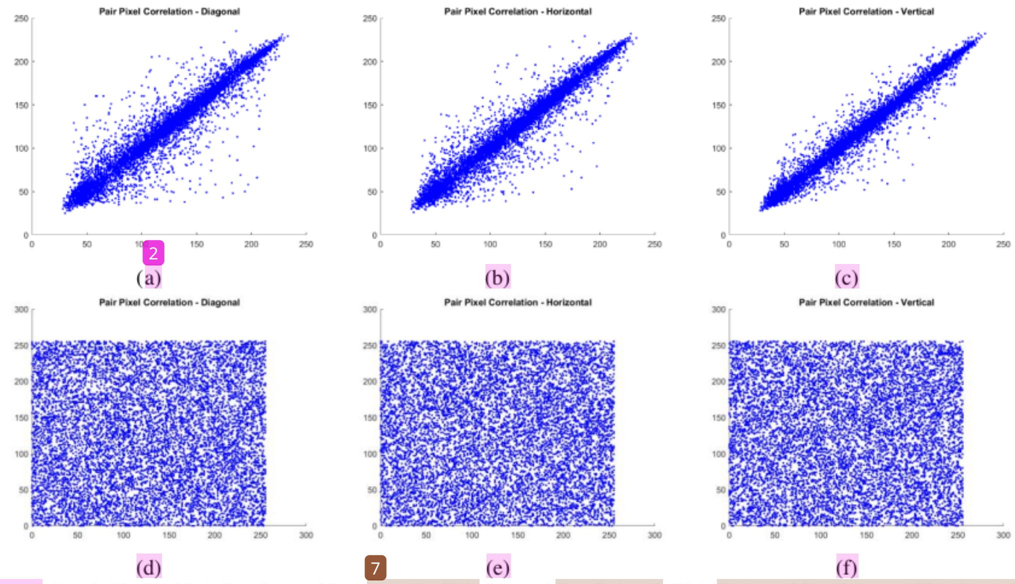
Image	**Methods**				
	(Liu et al., 2020)	**(Benaissi et al., 2023)**	**(Jun and Fun, 2021)**	**(Neamah, 2023)**	**Proposed**
Lena	7.9972	7.9993	7.9971	-	7.9994
Baboon	7.9967	7.9971	7.9969	7.9993	7.9994
Boat	-	7.9972	7.9970	7.9994	7.9993
Peppers	7.9971	7.9993	7.9975	7.9993	7.9994
Pirate	7.9974	-	-	-	7.9994
Cameraman	7.9972	7.9971	-	-	7.9993
Airplane	-	-	-	7.9993	7.9994
Couple	7.9971	-	-	-	7.9993
Average	7.9971	7.9980	7.9971	7.9993	7.9994

4.3 Correlation Coefficient Analysis

Correlation coefficient analysis is valuable for evaluating the correlation between neighboring pixels in image encryption. The correlation coefficient values, ranging from -1 to 1, indicate the degree of correlation between adjacent pixels. A value of 1 signifies a perfect positive correlation, -1 indicates a perfect negative correlation, and 0 suggests no correlation. By employing correlation coefficient analysis, the effectiveness of an encryption algorithm can be assessed, especially in its resistance against statistical attacks (Benaissi et al., 2023). To calculate this, see Eq. (14). In this study, the total number of pixels in the images is represented by $\mathcal{N}$. The variables x and y refer to two adjacent image pixels in the diagonal, horizontal, and vertical directions. Additionally, $E(x)$ and $E(y)$ represent the expectations of x and y, respectively, while r denotes the correlation coefficient of the adjacent pixels.

$$r_{x,y} = \frac{\frac{1}{\mathcal{N}}\sum_{i=1}^{\mathcal{N}}[x_i - E(x)][y_i - E(y)]}{\sqrt{\frac{1}{\mathcal{N}}\sum_{i=1}^{\mathcal{N}}[x_i - E(x)]^2}\sqrt{\frac{1}{\mathcal{N}}\sum_{i=1}^{\mathcal{N}}[y_i - E(y)]^2}} \qquad (14)$$

To delve deeper into the analysis, Figure 8 illustrates the correlation coefficient plot based on 10,000 pairs of pixels for each direction (diagonal, horizontal, and vertical) in both plain and ciphered images. Meanwhile, Table 3 presents the measurement results of r for each diagonal, horizontal, and vertical direction. The outcomes confirm that the proposed method has remarkably reduced the value of r to nearly zero, showcasing its superior performance compared to the previous method. This reduction in correlation indicates a higher level of randomness and an improvement in the encryption quality.



(a) (b) (c)

(d) (e) (f)

Figure 8. Sample Plot Pixel Pair Correlation of Lena image{(a) Plain Diagonal Correlation; (b) Plain Horizontal Correlation; (c) Plain Vertical Correlation; (d) Cipher Diagonal Correlation; (e) Cipher Horizontal Correlation; (f) Cipher Vertical Correlation}

Table 3. Correlation Coefficient Results and Comparison with Previous Method

Image	Direction	Method				
		(Liu et al., 2020)	(Benaissi et al., 2023)	(Jun and Fun, 2021)	(Neamah, 2023)	Proposed
Lena	D	0.0009	−0.0041	-0.0044	-	0.0003
	H	0.01016	−0.0036	-0.0020	-	-0.0004
	V	-0.0012	−0.0045	-0.0046	-	0.0009
Baboon	D	-0.0168	−0.0065	-0.0069	0.0030	0.0013
	H	0.0230	−0.0036	-0.0040	-0.0006	-0.0005
	V	0.0054	−0.0014	-0.0012	0.0035	0.0007
Boat	D	-	0.0003	-0.0018	0.0001	-0.0002
	H	-	0.0012	-0.0020	-0.0011	0.0006
	V	-	0.0012	-0.0047	0.0034	0.0003
Peppers	D	-0.0050	−0.0007	-0.0050	0.0036	0.0004
	H	-0.0024	0.0004	-0.0026	0.0001	0.0011
	V	0.0142	0.0013	-0.0012	-0.0013	-0.0005
Pirate	D	-0.0326	-	-	-	-0.0006
	H	-0.0251	-	-	-	0.0003
	V	-0.0108	-	-	-	-0.0004
Cameraman	D	0.0034	−0.0001	-	-	0.0002
	H	0.0113	0.0001	-	-	0.0001
	V	0.0169	−0.0058	-	-	-0.0006
Airplane	D	-	-	-	-0. 0020	0.0007
	H	-	-	-	-0.0004	0.0012
	V	-	-	-	- 0.0013	0.0004
Couple	D	-0.0025	-	-	-	0.0009
	H	0.0100	-	-	-	-0.0013
	V	-0.0025	-	-	-	0.0005

4.4 Normalized Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) Analysis

NPCR and UACI are statistical metrics utilized to assess the security of image encryption algorithms against differential attacks(Wei et al., 2023). These two assessments gauge the extent to which the difference between two encrypted images is influenced by the same image encryption but with a 1-bit difference in plaintext. NPCR quantifies the percentage change in pixels between the two encrypted images by comparing their respective pixel values. The desirable NPCR value is approximately 99.6094%, corresponding to a 1-bit difference in every 256 encrypted image pixels. On the other hand, UACI measures the average intensity of changes in two encrypted images by calculating the average difference in pixel intensity between them. The optimal UACI value is approximately 33.4635%, indicating a 1-bit difference in every three encrypted image pixels (Zhang, 2021). The formulas to calculate UACI and NPCR are provided in Eq. 15 and 16, respectively.

$$NPCR = \left[\frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H} D(i,j)\right], D(i,j)\begin{cases}0 \; if \; C1(i,j) = C2(i,j)\\ 1 \; if \; C1(i,j) \neq C2(i,j)\end{cases} \quad (15)$$

$$UACI = \left[\frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H}\frac{|C1(i,j) - C2(i,j)|}{255}\right] \quad (16)$$

To compute UACI and NPCR, the default cipher denoted as $C1$and the modified cipher denoted as $C2$ are utilized, with W and H representing the width and height image dimensions, respectively. i and j are the pixel coordinates. In this test, plaintext modification is carried out on pixels at position (256, 256), with a 1-bit change. The outcomes of NPCR and UACI are presented in Table 4 and Table 5, respectively. Observing the results in these tables, it becomes evident that most NPCR and UACI values are closer to the ideal value than previous works. This observation validates the encryption performance of the proposed method against differential attacks, showcasing its effectiveness in securing the encrypted data.

Table 4. NPCR Results and Comparison with Previous Method

Image	**Method**					
	(Liu et al., 2020)	**(Benaissi et al., 2023)**	**(Jun and Fun, 2021)**	**(Neamah, 2023)**	**(Wei et al., 2023)**	**Proposed**
Lena	99.6216	99.6223	99.6269	-	99.5968	99.6130
Baboon	99.6368	99.5667	99.6212	99.6000	99.6338	99.6032
Boat	-	99.6080	99.6254	99.6200	99.6098	99.6208
Peppers	99.5865	99.6403	99.6235	99.6000	99.6063	99.6162
Pirate	99.5773	-	-	-	99.5907	99.6025
Cameraman	99.6353	99.6201	-	-	-	99.6112
Airplane	-	-	-	99.6000	-	99.6067
Couple	99.6414	-	-	-	99.6204	99.6167

Table 5. UACI Results and Comparison with Previous Method

Image	**Method**					
	(Liu et al., 2020)	**(Benaissi et al., 2023)**	**(Jun and Fun, 2021)**	**(Neamah, 2023)**	**(Wei et al., 2023)**	**Proposed**
Lena	33.4994	33.3823	32.6540	-	33.4747	33.4723
Baboon	33.4702	33.5354	32.2105	33.4500	33.4265	33.4589
Boat	-	33.4643	32.5399	33.5000	33.5308	33.4823
Peppers	33.4815	33.5468	33.2394	33.4500	33.4754	33.4798
Pirate	33.5008	-	-	-	33.4541	33.4512
Cameraman	33.4810	33.4591	-	-	-	33.4734
Airplane	-	-	-	33.4100	-	33.4489
Couple	33.4871	-	-	-	33.4666	33.4593

4.5 Visual Analysis

Visual analysis is useful for visually assessing the quality of encryption and decryption. The results of encryption can be evaluated by several measurement tools, such as peak-signal-to-noise ratio (PSNR) and structural similarity index (SSIM). PSNR is used to determine how big the effect of encryption noise is, while SSIM functions to assess image structural changes. The smaller the SSIM value, the bigger the image structural change. In the case of the encryption test, it is different from other image processing tests such as compression and steganography, the smaller the PSNR and SSIM, the better the quality of the encryption produced.(Benaissi et al., 2023; Setiadi, 2021). PSNR and SSIM can be calculated by Eq. (17) and (18), respectively.

$$PSNR_{OC} = 10\log 10\left(\frac{max^2}{\frac{1}{WH}\sum_{i=1}^{W}\sum_{j=1}^{H}\left(O_{ij}-C_{ij}\right)^2}\right) \qquad (17)$$

$$SSIM_{OC} = \frac{(2\mu_O\mu_C + C_1)(2\sigma_{OC} + C_2)}{(\mu_O^2 + \mu_C^2 + C_1)(\sigma_O^2 + \sigma_C^2 + C_2)}$$
$$C_1 = (sc_1 D)^2 \qquad (18)$$
$$C_2 = (sc_2 D)^2$$

Where O, C are original and ciphered images respectively, W, H are the width and height of image dimension respectively, i, j are pixel coordinates, max is the maximum pixel value of O and C, μ is the luminance mean intensity, σ is signal contrast standard deviation of, sc_1 and sc_2 are two stabilizing parameters, by default sc_1 ,sc_2 are 0.01 and 0.03 respectively, and D is the dynamic range of pixel value, i.e. 255, because it is a grayscale image. Based on the PSNR and SSIM measurement results presented in Table 6 shows, the PSNR and SSIM values. They have very low values. This indicates that encryption provides very large noise and changes the image structure significantly.

Table 6. Visual Analysis Results

Image	**Encryption**		**Decryption**		
	PSNR	**SSIM**	**PSNR**	**CC**	**BER**
Lena	7.7238	0.0101	∞	1	0
Baboon	8.1378	0.0116	∞	1	0
Boat	7.9236	0.0093	∞	1	0
Peppers	7.6378	0.0098	∞	1	0
Pirate	7.8328	0.0103	∞	1	0
Cameraman	8.0639	0.0099	∞	1	0
Airplane	7.8378	0.0111	∞	1	0
Couple	7.9967	0.0105	∞	1	0
Average	7.8943	0.0103	∞	1	0

Decryption can be done with the inverse of the encryption step. Not correctly decrypted images sometimes create noise effects or errors in parts of the image. So, to confirm that the decryption process can run well, the decrypted image needs to be compared with the original image. This study used three assessment tools: PSNR, correlation coefficient (CC), and bit error ratio (BER). PSNR can be measured using Eq. (17), but measurements were made on the decrypted and original images. The PSNR value, which indicates that the decryption process is perfect, is ∞. CC determines the correlation level between the original and decrypted image pixels.

Meanwhile, BER is used to determine whether there is an error in the image pixel bits. The CC value must equal 1 and BER equal 0 to prove the decryption is perfect. CC and BER can be measured by Eq. (19) and (20), respectively. While the results of the decryption measurements are also presented in Table 6, these results confirm that the decryption process was carried out perfectly.

$$CC = \frac{\sum_i \sum_j (O_{xy} - \bar{O})(O'_{ij} - \bar{O'})}{\sqrt{\left(\sum_i \sum_j (O_{ij} - \bar{O})^2\right)\left(\sum_i \sum_j (O'_{ij} - \bar{O'})^2\right)}} \tag{19}$$

$$BER = \frac{\sum_{i=1}^{L_O} O_i \veebar O'_i}{L_O} \times 100\% \tag{20}$$

Where O is the original image, O' is the decrypted image, $\bar{O}$ and $\bar{O}'$ are mean of the original and decrypted image, respectively, L_O is bit length.

4.6 Keyspace and Key Sensitivity Analysis

Keyspace is the number of possible encryption keys used in an encryption algorithm. The bigger the keyspace, the more difficult it is for an attacker to guess the right key to decrypt the image. This is very important for encryption algorithms to survive brute-force attacks. The proposed method has many dynamic parameters and depends on the key. Table 7 is a description of the keyspace calculation of the proposed method.

Table 7. Keyspace approximation for all phase

Phase 1	**Phase 2**	**Phase 3**	**Phase 4**
$a, b, c \approx 3 \times 2.5 \times 10^{15}$ $\delta, \varepsilon \approx 2 \times 2.5 \times 10^{14}$	$a, b, c \approx 3 \times 2.5 \times 10^{15}$ $\delta \approx 1.299 \times 10^{10}$	$3 \times (k, m) \approx 2.2012 \times 10^{6}$	$p \approx 6.384016 \text{ x } 10^{19}$
$a, b, c \approx 1.5625 \times 10^{46}$ $\delta, \varepsilon \approx 6.25 \times 10^{28}$	$a, b, c \approx 1.5625 \times 10^{46}$ $\delta \approx 1.299 \times 10^{10}$		
Total key space $\approx 3.6875 \times 10^{46} + 6.384067 \times 10^{19} + 6.25 \times 10^{28}$			

The four columns in Table 7 explain the keyspace calculation for each phase, calculated based on the keyspace of each parameter. Then, each keyspace is calculated in the next row, and the total is in the last row. There are at least 12 parameters with a total keyspace $\approx 3.6875 \times 10^{46} + 6.384067 \times 10^{19} + 6.25 \times 10^{28}$. Minimum standard keyspace to be resistant to brute force attacks, i.e. 2^{100} (Liu and Zhang, 2020; Wu et al., 2017). While the keyspace shown in Table 7 proves to be very large, which is approximately 6.43×10^{29} times the standard, this should confirm that the proposed method resists brute-force attacks.

Key sensitivity analysis tests how sensitive the encryption key is to changes in input data or images. In this case, the secret key is modified by 1-bit in the middle of the key for the decryption process. If changes to the key cause significant changes to the decrypted image, then the key is considered sensitive. This is important in testing the strength of encryption keys and preventing attacks using techniques such as differential or linear cryptanalysis. For example, one of the test results samples in this research was encrypted with a secret key:

"password" then in the decryption process, the secret key: "passvord" was used, which means there was a modification of the 1-bit secret key. The results of the decrypted image are very different compared to decryption using the correct key, as presented in Figure 9. This result also occurs in all experiments with various images and 1-bit secret key modifications, so it proves that the generated key is very sensitive. This is due to the SHA-512 hash function because this will result in changes to the initial parameters for 3D pattern encryption, giving a 'snowball' effect to changes in the chaotic sequence.

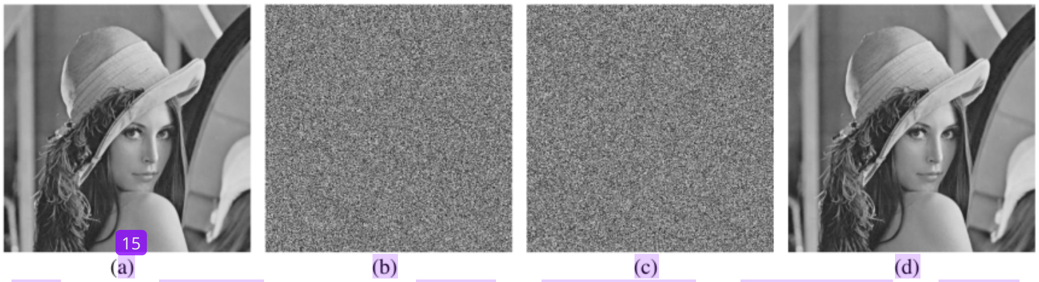


Figure 9. Sample of Key Sensitivity Decryption Results{(a) Original Lena Image; (b) Encrypted Lena Image; (c) Decrypted Lena Image with slight key modification; (d) Decrypted Lena Image with correct key}

4.7 NIST Statistical Test

The test assesses the encrypted image to ascertain its random properties and its ability to appear indistinguishable from an unexpected source, ensuring security against potential attackers. The initial introduction of the National Institute of Standards and Technology (NIST) statistical test suite was documented by (Rukhin et al., 2001). This test suite, known as SP 800–22, encompasses 15 different tests specifically tailored to examine random behavior and bit sequences. This test suite (SP 800–22) can be downloaded at https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software. The outcome of each test is represented by a p-value within the range of [0…1] (Nesa et al., 2019; Setiadi and Rijati, 2023). To validate the encryption and pass the test, each test necessitates a minimum of 106-bit sequences with a resulting p-value greater than 0.01 (Benaissi et al., 2023). The NIST test assessment was done by converting the encrypted image into a binary file and then saving it with the .dat extension. The data file is used as input to perform the NIST test. In this research, we conducted ten experiments on each image with different password variations, as follows: "password", "passvord", "secret", "qwerty", "abc123", "3DHyperchaoticImageEncryption", "Break_Me_If_You_Can", "Pa$$$_w0rd", "Sc!3nDir3ct", and "!t-I$_v312Y_$tR0nG_p@SsW()rD". Table 8 displays the average p-value of all encrypted images (a total of 80 tests). Based on the results presented, it can be seen that the standard deviation value is very minimal, even though the passwords used are very different, from simple to complex. The hash function plays a role in the initial processing of the password before it is used to determine the initial value of the chaotic sequence and other parameters. This proves that the algorithm has high sensitivity and stable encryption performance. All p-values pass and have an average value of more than 0.56, and this shows that the encryption performance is very satisfactory, random and secure based on the NIST test assessment.

Table 8. NIST Statistical Test Suite Results

No	Test Name	p-Value	Pass (Yes/No)
1	Frequency	0.378266±0.00328	Yes
2	Block Frequency	0.744542±0.01621	Yes
3 a	Cumulative Sums (Forward)	0.315179±0.00542	Yes
3 b	Cumulative Sums (Reverse)	0.564376±0.02344	Yes
4	Runs	0.134666±0.00843	Yes
5	Longest Run of Ones	0.296169±0.01363	Yes
6	Rank	0.579314±0.00839	Yes
7	Discrete Fourier Transform	0.764059±0.00793	Yes
8	Nonperiodic Template Matchings	0.776108±0.00562	Yes
9	Overlapping Template Matchings	0.233213±0.00932	Yes
10	Universal Statistical	0.464972±0.00863	Yes
11	Approximate Entropy	0.835195±0.00723	Yes
12	Random Excursions	0.648121±0.00236	Yes
13	Random Excursions Variant	0.786356±0.00621	Yes
14	Serial	0.947372±0.00449	Yes
15	Linear Complexity	0.533217±0.00821	Yes
Average		0.562570	Yes

5. Conclusion

This research proposes 3D encryption patterns for confusion and diffusion can improve security performance. Two hyperchaotic systems are proposed in this research, namely based on the Lorentz and Chen systems and combining them with ILM, Josephus traversing and hash functions. Using 3D patterns can increase the complexity of encryption. This method consists of four phases with permutation and substitution processes at the pixel and bit levels. This combination makes the diffusion and diffusion quality improve significantly. The use of hash functions also plays an important role in improving performance, especially in key sensitivity and key space, so that resistance to brute force attacks increases. The proposed method successfully passes various excellent quality tests, including histogram analysis, chi-square, information entropy, NCPCR, UACI, correlation coefficient, key space, key sensitivity, and NIST test suite. In addition, comparison results with related methods prove that most results show the superiority of the proposed method. Thus, combining two hyperchaotic systems, a chaotic system, Josephus transversing, and a hash function implemented in a 3D pattern has successfully created image encryption with a high level of security. This research makes an important contribution to developing stronger and more reliable image encryption techniques. This is crucial to protect privacy and information integrity amidst the increasing need for data and digital image security. The results of this research can be a basis for developing further image encryption methods with a higher level of security.

References

Abduljabbar, Z.A., Abduljaleel, I.Q., Ma, J., Sibahee, M.A. Al, Nyangaresi, V.O., Honi, D.G., Abdulsada, A.I., Jiao, X., 2022. Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map. IEEE Access 10, 26257–26270. https://doi.org/10.1109/ACCESS.2022.3151174

Andono, P.N., Setiadi, D.R.I.M., 2022. Improved Pixel and Bit Confusion-Diffusion Based on Mixed Chaos and Hash Operation for Image Encryption. IEEE Access 10, 115143–115156. https://doi.org/10.1109/ACCESS.2022.3218886

Babaei, A., Motameni, H., Enayatifar, R., 2020. A new permutation-diffusion-based image encryption technique using cellular automata and DNA sequence. Optik (Stuttg). 203, 164000. https://doi.org/10.1016/j.ijleo.2019.164000

Benaissi, S., Chikouche, N., Hamza, R., 2023. A novel image encryption algorithm based on hybrid chaotic maps using a key image. Optik (Stuttg). 272, 170316. https://doi.org/10.1016/j.ijleo.2022.170316

Cao, C., Sun, K., Liu, W., 2018. A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map. Signal Processing 143, 122–133. https://doi.org/10.1016/j.sigpro.2017.08.020

Demirtaş, M., 2022. A new RGB color image encryption scheme based on cross-channel pixel and bit scrambling using chaos. Optik (Stuttg). 265, 0–2. https://doi.org/10.1016/j.ijleo.2022.169430

Elmanfaloty, R.A., Alnajim, A.M., Abou-Bakr, E., 2021. A Finite Precision Implementation of an Image Encryption Scheme Based on DNA Encoding and Binarized Chaotic Cores. IEEE Access 9, 136905–136916. https://doi.org/10.1109/ACCESS.2021.3118050

Erkan, U., Toktas, A., Lai, Q., 2023. 2D hyperchaotic system based on Schaffer function for image encryption. Expert Syst. Appl. 213, 119076. https://doi.org/10.1016/j.eswa.2022.119076

Erkan, U., Toktas, A., Toktas, F., Alenezi, F., 2022. 2D eπ-map for image encryption. Inf. Sci. (Ny). 589, 770–789. https://doi.org/10.1016/j.ins.2021.12.126

Feng, W., He, Y., Li, H., Li, C., 2019. A Plain-Image-Related Chaotic Image Encryption Algorithm Based on DNA Sequence Operation and Discrete Logarithm. IEEE Access 7, 181589–181609. https://doi.org/10.1109/ACCESS.2019.2959137

Gan, Z., Chai, X., Han, D., Chen, Y., 2019. A chaotic image encryption algorithm based on 3-D bit-plane permutation. Neural Comput. Appl. 31, 7111–7130. https://doi.org/10.1007/s00521-018-3541-y

Ghadirli, H.M., Nodehi, A., Enayatifar, R., 2019. An overview of encryption algorithms in color images. Signal Processing 164, 163–185. https://doi.org/10.1016/j.sigpro.2019.06.010

Han, C., 2019. An image encryption algorithm based on modified logistic chaotic map. Optik (Stuttg). 181, 779–785. https://doi.org/10.1016/j.ijleo.2018.12.178

Hasheminejad, A., Rostami, M.J., 2019. A novel bit level multiphase algorithm for image encryption based on PWLCM chaotic map. Optik (Stuttg). 184, 205–213. https://doi.org/10.1016/j.ijleo.2019.03.065

Jasra, B., Hassan Moon, A., 2022. Color image encryption and authentication using dynamic DNA encoding and hyper chaotic system. Expert Syst. Appl. 206, 117861. https://doi.org/10.1016/j.eswa.2022.117861

Jun, W.J., Fun, T.S., 2021. A New Image Encryption Algorithm Based on Single S-Box and Dynamic Encryption Step. IEEE Access 9, 120596–120612. https://doi.org/10.1109/ACCESS.2021.3108789

K.U., S., Mohamed, A., 2021. Novel hyper chaotic color image encryption based on pixel and bit level scrambling with diffusion. Signal Process. Image Commun. 99, 116495. https://doi.org/10.1016/j.image.2021.116495

Kamal, S.T., Hosny, K.M., Elgindy, T.M., Darwish, M.M., Fouda, M.M., 2021. A New Image Encryption Algorithm for Grey and Color Medical Images. IEEE Access 9, 37855–37865. https://doi.org/10.1109/ACCESS.2021.3063237

Kandar, S., Chaudhuri, D., Bhattacharjee, A., Dhara, B.C., 2019. Image encryption using sequence generated by cyclic group. J. Inf. Secur. Appl. 44, 117–129. https://doi.org/10.1016/j.jisa.2018.12.003

Kaur, M., Kumar, V., 2020. A Comprehensive Review on Image Encryption Techniques. Arch. Comput. Methods Eng. 27, 15–43. https://doi.org/10.1007/s11831-018-9298-8

Kumar Patro, K.A., Acharya, B., 2019. An efficient colour image encryption scheme based on 1-D chaotic maps. J. Inf. Secur. Appl. 46, 23–41. https://doi.org/10.1016/j.jisa.2019.02.006

Lai, Q., Hu, G., Erkan, U., Toktas, A., 2023. A novel pixel-split image encryption scheme based on 2D Salomon map. Expert Syst. Appl. 213, 118845. https://doi.org/10.1016/j.eswa.2022.118845

Li, S., Ma, R., Zhang, H., 2019. Enhancing Security for JPEG Image Against Mosaic Attack Using Inter-Block Shuffle Encryption. IEEE Access 7, 72696–72702. https://doi.org/10.1109/ACCESS.2019.2918860

Liu, L., Lei, Y., Wang, D., 2020. A Fast Chaotic Image Encryption Scheme With Simultaneous Permutation-Diffusion Operation. IEEE Access 8, 27361–27374. https://doi.org/10.1109/ACCESS.2020.2971759

Liu, X., Tong, X., Wang, Z., Zhang, M., 2022. A novel hyperchaotic encryption algorithm for color image utilizing DNA dynamic encoding and self-adapting permutation. Multimed. Tools Appl. 81, 21779–21810. https://doi.org/10.1007/s11042-022-12472-4

Liu, Y., Zhang, J., 2020. A Multidimensional Chaotic Image Encryption Algorithm based on DNA Coding. Multimed. Tools Appl. 79, 21579–21601. https://doi.org/10.1007/s11042-020-08880-z

Luo, Y., Ouyang, X., Liu, J., Cao, L., 2019. An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems. IEEE Access 7, 38507–38522. https://doi.org/10.1109/ACCESS.2019.2906052

Moysis, L., Tutueva, A., Volos, C., Butusov, D., Munoz-Pacheco, J.M., Nistazakis, H., 2020. A Two-Parameter Modified Logistic Map and Its Application to Random Bit Generation. Symmetry (Basel). 12, 829. https://doi.org/10.3390/sym12050829

Naim, M., Ali Pacha, A., Serief, C., 2021. A novel satellite image encryption algorithm based on hyperchaotic systems and Josephus problem. Adv. Sp. Res. 67, 2077–2103. https://doi.org/10.1016/j.asr.2021.01.018

Neamah, A.A., 2023. An image encryption scheme based on a seven-dimensional hyperchaotic system and Pascal's matrix. J. King Saud Univ. - Comput. Inf. Sci. 35, 238–248. https://doi.org/10.1016/j.jksuci.2023.02.014

Nesa, N., Ghosh, T., Banerjee, I., 2019. Design of a chaos-based encryption scheme for sensor data using a novel logarithmic chaotic map. J. Inf. Secur. Appl. 47, 320–328. https://doi.org/10.1016/j.jisa.2019.05.017

Qian, X., Yang, Q., Li, Q., Liu, Q., Wu, Y., Wang, W., 2021. A Novel Color Image Encryption Algorithm Based on Three-Dimensional Chaotic Maps and Reconstruction Techniques. IEEE Access 9, 61334–61345. https://doi.org/10.1109/ACCESS.2021.3073514

Qin, Q., Liang, Z., Liu, S., Wang, X., Zhou, C., 2022. A Dual-Domain Image Encryption Algorithm Based on Hyperchaos and Dynamic Wavelet Decomposition. IEEE Access 10, 122726–122744. https://doi.org/10.1109/ACCESS.2022.3212145

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S., 2001. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Fort Belvoir.

Setiadi, D.R.I.M., 2021. PSNR vs SSIM: imperceptibility quality assessment for image steganography. Multimed. Tools Appl. 80, 8423–8444. https://doi.org/10.1007/s11042-020-10035-z

Setiadi, D.R.I.M., Rachmawanto, E.H., Zulfiningrum, R., 2022. Medical Image Cryptosystem using Dynamic Josephus Sequence and Chaotic-hash Scrambling. J. King Saud Univ. - Comput. Inf. Sci. 34, 6818–6828. https://doi.org/10.1016/j.jksuci.2022.04.002

Setiadi, D.R.I.M., Rijati, N., 2023. An Image Encryption Scheme Combining 2D Cascaded Logistic Map and Permutation-Substitution Operations. Computation 11, 178. https://doi.org/10.3390/computation11090178

Setiadi, D.R.I.M., Rustad, S., Andono, P.N., Shidik, G.F., 2023. Digital image steganography survey and investigation (goal, assessment, method, development, and dataset). Signal Processing 206, 108908. https://doi.org/10.1016/j.sigpro.2022.108908

Shah, T., Haq, T.U., Farooq, G., 2020. Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation. IEEE Access 8, 52609–52621. https://doi.org/10.1109/ACCESS.2020.2978083

Shannon, C.E., 1949. Communication Theory of Secrecy Systems*. Bell Syst. Tech. J. 28, 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

Teng, L., Wang, X., Yang, F., Xian, Y., 2021. Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion. Nonlinear Dyn. 105, 1859–1876. https://doi.org/10.1007/s11071-021-06663-1

Toktas, A., Erkan, U., 2022. 2D fully chaotic map for image encryption constructed through a quadruple-objective optimization via artificial bee colony algorithm. Neural Comput. Appl. 34, 4295–4319. https://doi.org/10.1007/s00521-021-06552-z

USC Viterbi School of Engineering, n.d. SIPI Image Database [WWW Document]. URL http://sipi.usc.edu/database/ (accessed 3.27.19).

Wang, L., Cao, Y., Jahanshahi, H., Wang, Z., Mou, J., 2023. Color image encryption algorithm based on Double layer Josephus scramble and laser chaotic system. Optik (Stuttg). 275, 170590. https://doi.org/10.1016/j.ijleo.2023.170590

Wang, M., Wang, X., Wang, C., Zhou, S., Xia, Z., Li, Q., 2023. Color image encryption based on 2D enhanced hyperchaotic logistic-sine map and two-way Josephus traversing. Digit. Signal Process. 132, 103818. https://doi.org/10.1016/j.dsp.2022.103818

Wang, N., Di, G., Lv, X., Hou, M., Liu, D., Zhang, J., Duan, X., 2019. Galois Field-Based Image Encryption for Remote Transmission of Tumor Ultrasound Images. IEEE Access 7, 49945–49950. https://doi.org/10.1109/ACCESS.2019.2910563

Wang, Q., Zhang, X., Zhao, X., 2022. Image encryption algorithm based on improved Zigzag transformation and quaternary DNA coding. J. Inf. Secur. Appl. 70, 103340. https://doi.org/10.1016/j.jisa.2022.103340

Wang, R., Deng, G.-Q., Duan, X.-F., 2021. An image encryption scheme based on double chaotic cyclic shift and Josephus problem. J. Inf. Secur. Appl. 58, 102699. https://doi.org/10.1016/j.jisa.2020.102699

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

Wang, X., Zhu, X., Wu, X., Zhang, Y., 2018a. Image encryption algorithm based on multiple mixed hash functions and cyclic shift. Opt. Lasers Eng. 107, 370–379. https://doi.org/10.1016/j.optlaseng.2017.06.015

Wang, X., Zhu, X., Zhang, Y., 2018b. An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map. IEEE Access 6, 23733–23746. https://doi.org/10.1109/ACCESS.2018.2805847

Wang, Y., Chen, L., Yu, K., Lu, T., 2022. Image encryption algorithm based on lattice hash function and privacy protection. Multimed. Tools Appl. 81, 18251–18277. https://doi.org/10.1007/s11042-022-12714-5

Waseso, B.M.P., Setiyanto, N.A., 2023. Web Phishing Classification using Combined Machine Learning Methods. J. Comput. Theor. Appl. 1, 11–18. https://doi.org/10.33633/jcta.v1i1.8898

Wei, D., Jiang, M., Deng, Y., 2023. A secure image encryption algorithm based on hyper-chaotic and bit-level permutation. Expert Syst. Appl. 213, 119074. https://doi.org/10.1016/j.eswa.2022.119074

Winarno, E., Nugroho, K., Adi, P.W., Setiadi, D.R.I.M., 2023. Combined Interleaved Pattern to Improve Confusion-Diffusion Image Encryption Based on Hyperchaotic System. IEEE Access 11, 69005–69021. https://doi.org/10.1109/ACCESS.2023.3285481

Wu, J., Liao, X., Yang, B., 2017. Color image encryption based on chaotic systems and elliptic curve ElGamal scheme. Signal Processing 141, 109–124. https://doi.org/10.1016/j.sigpro.2017.04.006

Xu, Q., Sun, K., He, S., Zhu, C., 2020. An effective image encryption algorithm based on compressive sensing and 2D-SLIM. Opt. Lasers Eng. 134, 106178. https://doi.org/10.1016/j.optlaseng.2020.106178

Ye, G., Wu, H., Liu, M., Shi, Y., 2022. Image encryption scheme based on blind signature and an improved Lorenz system. Expert Syst. Appl. 205, 117709. https://doi.org/10.1016/j.eswa.2022.117709

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

Zhang, G., Liu, Q., 2011. A novel image encryption method based on total shuffling scheme. Opt. Commun. 284, 2775–2780. https://doi.org/10.1016/j.optcom.2011.02.039

Zhang, Y., 2021. Statistical test criteria for sensitivity indexes of image cryptosystems. Inf. Sci. (Ny). 550, 313–328. https://doi.org/10.1016/j.ins.2020.10.026

Zhang, Y., Chen, A., Chen, W., 2023. The unified image cryptography algorithm based on finite group. Expert

Syst. Appl. 212, 118655. https://doi.org/10.1016/j.eswa.2022.118655

Zhu, S., Deng, X., Zhang, W., Zhu, C., 2023. Secure image encryption scheme based on a new robust chaotic map and strong S-box. Math. Comput. Simul. 207, 322–346. https://doi.org/10.1016/j.matcom.2022.12.025

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors do not have permission to share data.

Integrated Dual Hyperchaotic and Josephus Traversing based 3D Confusion-Diffusion Pattern for Image Encryption

ORIGINALITY REPORT

20%	12%	18%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	De Rosal Ignatius Moses Setiadi, Nova Rijati. "An Image Encryption Scheme Combining 2D Cascaded Logistic Map and Permutation-Substitution Operations", Computation, 2023 Publication	1%
2	mdpi-res.com Internet Source	1%
3	Mujeeb Ur Rehman, Arslan Shafique, Aminu Bello Usman. "Securing medical information transmission between IoT devices: An innovative hybrid encryption scheme based on quantum walk, DNA encoding, and chaos", Internet of Things, 2023 Publication	1%
4	www.eurchembull.com Internet Source	1%
5	inass.org Internet Source	<1%

6	Mohammed Es-Sabry, Nabil El Akkad, Mostafa Merras, Khalid Satori, Walid El-Shafai, Torki Altameem, Mostafa M. Fouda. "Securing Images Using High Dimensional Chaotic Maps and DNA Encoding Techniques", IEEE Access, 2023 Publication	<1 %
7	Changping Li, Lidan Wang, Dengwei Yan, Hang Shi. "Research on a New Type of Chaotic Image Encryption Algorithm Combining DNA Operation and S-box", 2021 International Conference on Neuromorphic Computing (ICNC), 2021 Publication	<1 %
8	Nova Rijati, De Rosal Ignatius Moses Setiadi. "Nested Block based Double Self-embedding Fragile Image Watermarking with Super-resolution Recovery", IEEE Access, 2023 Publication	<1 %
9	Xiaoyu Zhou, Wien Hong, Guangsong Yang, Tung-Shou Chen, Jeanne Chen. "An Unsolvable Pixel Reduced Authentication Method for Color Images with Grayscale Invariance", Journal of King Saud University - Computer and Information Sciences, 2023 Publication	<1 %
10	oaji.net Internet Source	<1 %

11	Shahna K.U., Anuj Mohamed. "Novel hyper chaotic color image encryption based on pixel and bit level scrambling with diffusion", Signal Processing: Image Communication, 2021 Publication	<1 %
12	beei.org Internet Source	<1 %
13	Mua’ad Abu-Faraj, Abeer Al-Hyari, Charlie Obimbo, Khaled Aldebei, Ismail Altaharwa, Ziad Alqadi, Orabe Almanaseer. "Protecting Digital Images Using Keys Enhanced by 2D Chaotic Logistic Maps", Cryptography, 2023 Publication	<1 %
14	Qiang Lai, Yuan Liu, Liang Yang. "Image encryption using memristive hyperchaos", Applied Intelligence, 2023 Publication	<1 %
15	ijece.iaescore.com Internet Source	<1 %
16	www.journaltocs.ac.uk Internet Source	<1 %
17	www.researchgate.net Internet Source	<1 %
18	Ammar Ali Neamah, Ali A. Shukur. "A Novel Conservative Chaotic System Involved in Hyperbolic Functions and Its Application to	<1 %

	Design an Efficient Colour Image Encryption Scheme", Symmetry, 2023 Publication	
19	"Communications, Signal Processing, and Systems", Springer Science and Business Media LLC, 2020 Publication	<1 %
20	Behzad Yosefnezhad Irani, Peyman Ayubi, Fardin Amani Jabalkandi, Milad Yousefi Valandar, Milad Jafari Barani. "Digital image scrambling based on a new one-dimensional coupled Sine map", Nonlinear Dynamics, 2019 Publication	<1 %
21	B. Rahul, K. Kuppusamy, A. Senthilrajan. "Bio-Metric Based Colour-Image-Encryption using Multi-Chaotic Dynamical Systems and SHA-256 Hash Algorithm", Information Security Journal: A Global Perspective, 2023 Publication	<1 %
22	Submitted to Monash University Student Paper	<1 %
23	Sellami Benaissi, Noureddine Chikouche, Rafik Hamza. "A novel image encryption algorithm based on hybrid chaotic maps using a key image", Optik, 2023 Publication	<1 %

24 De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, Rahmawati Zulfiningrum, Md Kamruzzaman Sarker. "Text Encryption using Transform Dimension, Bit Plane Slicing, and Chaos System", 2022 International Seminar on Application for Technology of Information and Communication (iSemantic), 2022 <1%

Publication

---

25 Jun Peng. "Image Encryption and Chaotic Cellular Neural Network", Machine Learning in Cyber Trust, 2009 <1%

Publication

---

26 Dani Elias Mfungo, Xianping Fu, Yongjin Xian, Xingyuan Wang. "A Novel Image Encryption Scheme Using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information", Applied Sciences, 2023 <1%

Publication

---

27 Junhua Chen, Gu Shi, Chong Yan. "Portable biosensor for on-site detection of kanamycin in water samples based on CRISPR-Cas12a and an off-the-shelf glucometer", Science of The Total Environment, 2023 <1%

Publication

---

28 Amina Souyah. "Multimedia contents confidentiality preservation in constrained environments: a dynamic approach", Multimedia Tools and Applications, 2023 <1%

Publication

29	Dhruvendra Kumar Chourishi, Anil Rajput, Sanjeev Gour. "Chapter 13 Drought Monitoring and Assessment Through Remote Sensing Data in Bundelkhand Area of Madhya Pradesh", Springer Science and Business Media LLC, 2023 Publication	<1 %
30	Punam Kumari, Bhaskar Mondal. "Lightweight image encryption algorithm using NLFSR and CBC mode", The Journal of Supercomputing, 2023 Publication	<1 %
31	Yuling Luo, Yuting Liang, Shunsheng Zhang, Junxiu Liu, Fangxiao Wang. "An image encryption scheme based on block compressed sensing and Chen's system", Nonlinear Dynamics, 2022 Publication	<1 %
32	univ-usto.dz Internet Source	<1 %
33	Submitted to University of Surrey Student Paper	<1 %
34	eprints.utar.edu.my Internet Source	<1 %
35	iopscience.iop.org Internet Source	<1 %

36	Kumar D, Sudha V K, Ranjithkumar R. "A one-round medical image encryption algorithm based on a combined chaotic key generator", Medical & Biological Engineering & Computing, 2022 Publication	<1 %
37	Mohamed Maazouz, Abdelmoughni Toubal, Billel Bengherbia, Oussama Houhou, Noureddine Batel. "FPGA implementation of a chaos-based image encryption algorithm", Journal of King Saud University - Computer and Information Sciences, 2022 Publication	<1 %
38	Submitted to (school name not available) Student Paper	<1 %
39	AASTHA BAJAJ. "Unleashing Economic Potential: Decoding the Fdi-economic Growth Nexus in G-15 Economies Amidst Unique Host Country Traits", Research Square Platform LLC, 2023 Publication	<1 %
40	Febina Ikbal, Rajamma Gopikakumari. "Image block generation from block-based SMRT in colour image encryption and its performance analysis", Journal of King Saud University - Computer and Information Sciences, 2021 Publication	<1 %

41	Submitted to Nottingham Trent University Student Paper	<1%
42	"Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering 2018 (ISMAC-CVB)", Springer Science and Business Media LLC, 2019 Publication	<1%
43	Hao Li, Lianbing Deng, Zhaoquan Gu. "A Robust Image Encryption Algorithm based on a 32-bit Chaotic System", IEEE Access, 2020 Publication	<1%
44	Submitted to International Islamic University Malaysia Student Paper	<1%
45	Ling Wang, Qiwen Ran, Jing Ma. "Double quantum color images encryption scheme based on DQRCI", Multimedia Tools and Applications, 2019 Publication	<1%
46	Rahmat, Zahir Zainuddin, Andani Achmad. "Classification Of Fertile And Infertile Eggs Using Thermal Camera Image And Histogram Analysis: Technology Application In Poultry Farming Industry", 2023 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), 2023 Publication	<1%

47	api.deepai.org Internet Source	<1 %
48	arxiv.org Internet Source	<1 %
49	Chunyan Han. "An image encryption algorithm based on modified logistic chaotic map", Optik, 2019 Publication	<1 %
50	Maria Elisa Esteves Lopes Galvão. "O teorema de toponogov", Universidade de Sao Paulo, Agencia USP de Gestao da Informacao Academica (AGUIA), 1974 Publication	<1 %
51	Qiuyu Zhang, Jitian Han, Yutong Ye. "Image encryption algorithm based on image hashing, improved chaotic mapping and DNA coding", IET Image Processing, 2019 Publication	<1 %
52	Sajid Khan, Han Lansheng, Yekui Qian, Hongwei Lu, Shi Meng Jiao. "Security of multimedia communication with game trick based fast, efficient, and robust color-/gray-scale image encryption algorithm", Transactions on Emerging Telecommunications Technologies, 2020 Publication	<1 %

53	Yu Zhang, Junlin Wang, Xin Wang, Haonan Jing, Zhanshuo Sun, Yu Cai. "Static hand gesture recognition method based on the Vision Transformer", Multimedia Tools and Applications, 2023 Publication	<1 %
54	es.scribd.com Internet Source	<1 %
55	www.ijcse.com Internet Source	<1 %
56	"The International Conference on Advanced Machine Learning Technologies and Applications (AMLTA2019)", Springer Science and Business Media LLC, 2020 Publication	<1 %
57	A. Hadj Brahim, A. Ali Pacha, N. Hadj Said. "An image encryption scheme based on a modified AES algorithm by using a variable S-box", Journal of Optics, 2023 Publication	<1 %
58	Anand B. Joshi, Abdul Gaffar, Sonali Singh. "Security of medical images based on special orthogonal group and Galois field", Multimedia Tools and Applications, 2023 Publication	<1 %
59	Bassem Abd-El-Atty, Ahmed A. Abd EL-Latif. "Applicable image cryptosystem using bit-	<1 %

	level permutation, particle swarm optimisation, and quantum walks", Neural Computing and Applications, 2023 Publication	
60	Deepti Dhingra, Mohit Dua. "A chaos-based novel approach to video encryption using dynamic S-box", Multimedia Tools and Applications, 2023 Publication	<1 %
61	Lamri Laouamer. "New Informed Non-Blind Medical Image Watermarking Based on Local Binary Pattern", Traitement du Signal, 2022 Publication	<1 %
62	Yang Lu, Mengxin Gong, Lvchen Cao, Zhihua Gan, Xiuli Chai, Ang Li. "Exploiting 3D fractal cube and chaos for effective multi-image compression and encryption", Journal of King Saud University - Computer and Information Sciences, 2023 Publication	<1 %
63	journals.plos.org Internet Source	<1 %
64	pse.agriculturejournals.cz Internet Source	<1 %
65	Ammar Ali Neamah. "An image encryption scheme based on a seven-dimensional hyperchaotic system and Pascal's matrix",	<1 %

Journal of King Saud University - Computer and Information Sciences, 2023
Publication

66 Djamel Herbadji, Aissa Belmeguenai, Nadir Derouiche, Hongjung Liu. "Colour image encryption scheme based on enhanced quadratic chaotic map", IET Image Processing, 2020
Publication
<1%

67 Erdem Yavuz. "A new parallel processing architecture for accelerating image encryption based on chaos", Journal of Information Security and Applications, 2021
Publication
<1%

68 Melih Yildirim. "A color image encryption scheme reducing the correlations between R, G, B components", Optik, 2021
Publication
<1%

69 Shuqin Zhu, Congxu Zhu, Hanyu Yan. "Cryptanalyzing and Improving an Image Encryption Algorithm Based on Chaotic Dual Scrambling of Pixel Position and Bit", Entropy, 2023
Publication
<1%

70 Submitted to University of Technology
Student Paper
<1%

71	Wuyan Liang, Limin Zhang, Zhongbao Yang, Tingting Yu, Jingjing Li, Xianli Li. "Image encryption algorithm based on hyperchaotic system and dynamic DNA encoding", Physica Scripta, 2023 Publication	<1 %
72	Zhongyue Liang, Qiuxia Qin, Changjun Zhou. "An image encryption algorithm based on Fibonacci Q-matrix and genetic algorithm", Neural Computing and Applications, 2022 Publication	<1 %
73	fdocumenti.com Internet Source	<1 %
74	www.inass.org Internet Source	<1 %
75	www.researchsquare.com Internet Source	<1 %
76	"Green Energy and Networking", Springer Science and Business Media LLC, 2019 Publication	<1 %
77	"Machine Learning for Cyber Security", Springer Science and Business Media LLC, 2020 Publication	<1 %
78	A. Hadj Brahim, A. Ali Pacha, N. Hadj Said. "A new fast image compression–encryption	<1 %

scheme based on compressive sensing and parallel blocks", The Journal of Supercomputing, 2022

Publication

79 Boriga, Radu, Ana Cristina Dăscălescu, and Iustin Priescu. "A new hyperchaotic map and its application in an image encryption scheme", Signal Processing Image Communication, 2014. <1%

Publication

80 Daniel Murillo-Escobar, Miguel Ángel Murillo-Escobar, César Cruz-Hernández, Adrian Arellano-Delgado et al. "Pseudorandom number generator based on novel 2D Hénon-Sine hyperchaotic map with microcontroller implementation", Nonlinear Dynamics, 2022 <1%

Publication

81 Jakub Oravec, Lubos Ovsenik, Jan Papaj. "An Image Encryption Algorithm Using Logistic Map with Plaintext-Related Parameter Values", Entropy, 2021 <1%

Publication

82 Jingfei He, Chenghu Mi, Xiaotong Liu, Yuanqing Zhao. "Accelerated dynamic MR imaging with joint balanced low-rank tensor and sparsity constraints", Medical Physics, 2023 <1%

Publication

83	Kanaad Deshpande, Junaid Girkar, Ramchandra Mangrulkar. "Security enhancement and analysis of images using a novel Sudoku-based encryption algorithm", Journal of Information and Telecommunication, 2023 Publication	<1 %
84	P. Mathivanan, Ponnambalam Maran. "Color image encryption based on novel kolam scrambling and modified 2D logistic cascade map (2D LCM)", The Journal of Supercomputing, 2023 Publication	<1 %
85	Parveiz Nazir Lone, Deep Singh. "Application of algebra and chaos theory in security of color images", Optik, 2020 Publication	<1 %
86	Submitted to Universitas Dian Nuswantoro Student Paper	<1 %
87	Xingyuan Wang, Nana Guan. "A novel chaotic image encryption algorithm based on extended Zigzag confusion and RNA operation", Optics & Laser Technology, 2020 Publication	<1 %
88	Yongsheng Hu, Han Wu, Luoyu Zhou. "Color image encryption base on a 2D hyperchaotic	<1 %

	enhanced Henon map and cross diffusion", Alexandria Engineering Journal, 2023 Publication	
89	cris.vub.be Internet Source	<1 %
90	dokumen.pub Internet Source	<1 %
91	pure.sruc.ac.uk Internet Source	<1 %
92	www.efda-itm.eu Internet Source	<1 %
93	www.ncbi.nlm.nih.gov Internet Source	<1 %
94	www.tnsroindia.org.in Internet Source	<1 %
95	Ömer Koçak, Uğur Erkan, Abdurrahim Toktas, Suo Gao. "PSO-based image encryption scheme using modular integrated logistic exponential map", Expert Systems with Applications, 2023 Publication	<1 %
96	Ahmed Kamil Hasan Al-Ali, Jafaar Mohammed Daif Alkhasraji. "Colour image encryption based on hybrid bit-level scrambling, ciphering, and public key cryptography",	<1 %

	Bulletin of Electrical Engineering and Informatics, 2023 Publication	
97	De Rosal Igantius Moses Setiadi. "PSNR vs SSIM: imperceptibility quality assessment for image steganography", Multimedia Tools and Applications, 2020 Publication	<1 %
98	Mohammad Abdul Mujeeb Khan, Naveed Ahmed Azam, Umar Hayat, Hailiza Kamarulhaili. "A novel deterministic substitution box generator over elliptic curves for real-time applications", Journal of King Saud University - Computer and Information Sciences, 2022 Publication	<1 %
99	Mostafa MokhtariArdakan, Reza Ramezani, AliMohammad Latif. "Visual Secret Sharing of Gray and Color Images using Fuzzy Random Grids", Applied Soft Computing, 2023 Publication	<1 %
100	Ruisong Ye, Wenhua Guo. "An Image Encryption Scheme Based on Chaotic Systems with Changeable Parameters", International Journal of Computer Network and Information Security, 2014 Publication	<1 %

101	Shuting Cai, Linqing Huang, Xuesong Chen, Xiaoming Xiong. "A Symmetric Plaintext-Related Color Image Encryption System Based on Bit Permutation", Entropy, 2018 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		