Enhanced Hyperchaotic Image Encryption with CAW Transform and Sea-Lion Optimizer

Qutaiba Kadhim Abed[1,*] and Waleed Ameen Mahmoud Al-Jawher[2]

[1] *Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatics, Baghdad, Iraq*
[2] *Uruk University, Baghdad, Iraq*
E-mail: phd202130682@iips.edu.iq; profwaleed54@gmail.com
[*] *Corresponding Author*

Received 15 January 2024; Accepted 23 July 2024

Abstract

One of the most effective methods for ensuring data security in the communication and information fields is encryption. There is an important role for multi-chaotic systems in the field of data encryption, due to its wide advantages and its sensitivity to the values of the coefficients and ergodicity. However, some multi-chaotic systems possess low complexity and randomness, which results in unacceptable security behaviour of the current data encryption systems. In this study, we introduce a novel hyperchaotic encryption scheme that enhances image security using a three-phase approach. First, SHA512 is combined with URUK chaos to generate plain-related random sequences. Next, a hybrid CAW transform (Cosine, Arnold, and Wavelet) improves randomness. Finally, the Sea Lion optimization algorithm shuffles

Journal of Cyber Security and Mobility, Vol. 13_5, 1207–1238.
doi: 10.13052/jcsm2245-1439.13517

pixels to achieve robust encryption. Our experimental results demonstrate that the proposed scheme effectively resists statistical attacks, with superior performance in NPCR, UACI, correlation coefficient, and information entropy tests

Keywords: URUK chaotic system, sea lion optimization, DWT, SHA512, CAW transform, FAN transform.

1 Introduction

The development of several shooting devices over the last few decades has been called these years the era of big data. A modern camera, for example, can take millions of images every day, whereas a conventional camera with a single lens can take numerous pictures every second. Digital images have become an integral part of our lives, capturing precious moments and serving as a visual record of our experiences [1–3]. However, the growing popularity of cloud-based storage platforms has raised concerns about the privacy of data embedded in these images. In today's digital age, robust encryption solutions are essential due to the rapid increase in data transmission over the internet [4–7]. Images constitute a significant portion of data traffic, making the protection of digital media critically important. As access to computers and the internet expands, exposing data to heightened vulnerability, the significance of encryption cannot be overstated. However, standard encryption techniques, such as AES (Advanced Encryption Standard) and DES (Data Encryption Standard), are unsuitable for image encryption because they do not address the high correlation, redundancy, and large volume of image data effectively [8, 9]. These techniques were designed for text data and do not effectively address the high correlation, redundancy, and large volume of image data. As a result, specialized image encryption techniques have been developed to address these limitations. These techniques typically employ a combination of confusion and diffusion to make the encrypted image appear random and unpredictable. Confusion techniques scramble the image data to make it difficult to analyse, while diffusion techniques spread the statistical properties of the image throughout the ciphertext [10–13].

In image encryption, chaotic maps have emerged as a cornerstone of secure data protection. Their inherent complexity and randomness make them ideal for generating encryption keys, bolstering the security of encryption algorithms [14–17]. By leveraging the unpredictable dynamics of chaotic maps, image data is transformed into seemingly unbreakable ciphertext, resistant to even the most sophisticated attacks [18–20]. To further fortify the encryption process, chaos cards enter the scene. These cards harness the erratic behaviour of physical systems, such as chaotic circuits or random number generators, to produce highly secure and random encryption keys. This physical approach to randomness adds an extra layer of protection, safeguarding the integrity and confidentiality of encrypted image data [21–27].

Talhaoui et al. introduced a new chaotic system based on the one-dimensional cosine fraction (1-DCT) [28]. This system exhibits desirable cryptographic properties, a wide range of control parameters, and superior dynamic behaviour. Employing a permutation-less design, the chaotic system's keystream is utilized to diffuse and encrypt the pixel values of image rows and columns, resulting in the encrypted ciphertext image. The proposed method demonstrates exceptional encryption speed, capable of encrypting a 256x256 pixel image in merely 6.7 seconds. However, the algorithm solely performs diffusion, necessitating further security enhancements. Xu et al. proposed a new image encryption method based on a third-order fractional chaotic system [29]. This method is implemented using a hardware circuit of a digital signal processor and encrypts the image by combining block feedback diffusion structure and compressed sensing according to the sequence generated by the system. The authors also suggested that this approach can be used for text encryption. The method has a mean structural similarity (MSSIM) score of greater than 0.9 and encrypts data relatively quickly; however, its resilience to attacks is fairly low. Talhaoui et al. proposed a novel image encryption technique based on a one-dimensional cosine polynomial chaotic system [30]. The proposed method utilizes a chaotic system in conjunction with a traditional architecture that employs parallel diffusion and scrambling to encrypt images. The experimental results demonstrate that the method achieves a fast encryption speed of 11.1 seconds for encrypting a 256x256 pixel image. However, the security performance of the algorithm is deemed unsatisfactory due to its reliance on a shifted scrambling diffusion structure, which renders it vulnerable to certain attacks [31]. Aparna et al. proposed a novel medical image encryption technique that leverages quantum cryptography to generate random sequences for keystream generation and combines it with an adaptive optimization protocol strategy [32]. This approach successfully encrypts medical images using quantum cryptography. It is noteworthy that while the method demonstrates impressive encryption effectiveness and parallel data encryption capabilities, the ciphertext image's information entropy can reach a value of 7.9974, significantly enhancing security. However, it is worth mentioning that the algorithm's keystream generation efficiency could be improved. Muthu and Murali proposed a new one-dimensional chaotic system with a large key space for medical image encryption [33]. They combined this chaotic system with the shuffle approach to encrypt medical images and obtain the ciphertext image. The proposed method achieves fast keystream generation, but its diffusion performance throughout the encryption process is not optimal. Mondal and Singh proposed a medical image encryption method that utilizes a chaotic system to generate a pseudo-random sequence for keystream generation and employs bit-level operations for efficient diffusion and scrambling [34]. This method achieves strong encryption with reduced computational complexity.

This method introduces a groundbreaking image encryption method that combines dual confusion and diffusion in the frequency domain to achieve enhanced security and robustness. The FAN transform is employed to introduce confusion, while the URUK chaotic map is utilized to increase the complexity and unpredictability of the encryption process. To optimize the scrambling operation, the Sea Lion optimization algorithm is employed. The effectiveness of the proposed method is thoroughly evaluated through comprehensive encryption analysis, assessing its computational efficiency and resistance against common attacks. This research contribution significantly advances the field of image encryption by addressing the limitations of existing methods and providing a novel approach that ensures the protection of sensitive visual information.

1. The proposed encryption system is robust, confidential and a secure mechanism method utilizes URUK discrete four-dimensional chaotic maps for the key generation. URUK effectiveness depends on the careful selection and implementation of these keys. URUK keys possess a high-quality and long-range chaotic sequence and are able to provide better protection against statistical, differential, and brute force attacks. The specific choices of URUK map will offer varying degrees of complexity and sensitivity to initial conditions.
2. Application of CAW hybrid transform improves the chaos randomness since it consists of three transforms, namely, Cosine, Arnold and Wavelet transforms. It is proven to have strong procedures and can overcome common weaknesses found in encryption algorithms based on other single transforms.

3. The Sea Lion Optimization algorithm scrambles the pixels with a minimum correlation between adjacent pixels and hence it results in a strong and robust key management strategy. The main purpose is to improve the capability of exploitation in Sea Lion Optimization algorithm with the capability of exploration in the encryption process to produce variants' strengths.
4. This novel encryption possesses wide advantages due to its sensitivity to initial coefficient values and ergodicity. The performance metrics such as Unified Average Change Intensity (UACI) and Number of Pixel Change Rate (NPCR) tests showed quantify the algorithm's ability to withstand modifications in the plaintext image, ensuring that even small alterations in the original data result in significant changes in the encrypted image.
5. Statistical tests are used to evaluate the randomness and resistance to differential attacks of the encrypted image.

The remainder of this paper is structured as follows. Section 2: gives the description of Sea Lion Optimization Algorithm. The hybrid CAW transform theory is briefly discussed in Section 3. Section 4: describes the URUK Chaotic Map. Section 5: shows the process of the Encryption Method. Section 6: demonstrates the decryption Processes. The experimental result and practical analysis are shown in Section 7. Finally, Section 8 is the concludes of this paper.

2 Sea Lion Optimization Algorithm

The Sea Lion Optimization (SLO) algorithm emulates sea lions' hunting strategies, involving detection, tracking, and encirclement. The algorithm begins with random solutions, updating each search agent's position based on the best or a randomly selected agent. Over iterations, a parameter (C) decreases from 2 to 0, balancing exploration and exploitation. The SLO process includes:

1. Detection and Tracking: Simulating sea lions' whisker-based prey detection.
2. Vocalization: Mimicking sea lions' communication during hunting.
3. Attack (Exploitation): Optimizing the solution by encircling the prey

The algorithm mimics the tracking, encirclement, and attack of prey by using mathematical models to mimic the social hierarchy. In the phase of detection and tracking the Sea Lions use their whiskers to sense prey by detecting the size, shape, and position of nearby objects. When the whiskers are oriented against the water flow, they vibrate less than when they are aligned with the current orientation. This difference in vibration helps Sea Lions to detect the presence and location of prey. Sea Lions are able to locate prey and signal to other members of their subgroups to join them in pursuing and hunting the prey. Within this hunting mechanism, the Sea Lion is considered the leader, and the other animals rearrange their positions to the target prey. The target prey is thought to be the best answer available right now, or nearly so, according to the SLO algorithm.

Firstly, Equation (1) provides a mathematical representation of this phenomenon.

$$\overrightarrow{Dlst} = |\overrightarrow{2B} \cdot \overrightarrow{P(t)} - \overrightarrow{SL(t)}| \tag{1}$$

where $\overrightarrow{P(t)}$ and $\overrightarrow{SL(t)}$ stand for the target prey's and Sea Lion's position vectors, respectively, and $\overrightarrow{Dlst}$ stands for the distance between the Sea Lion and the target. t indicates the current iteration, B is the random vector in [0, 1] that is multiplied by two to increase the search space and aid search agents in finding an optimal or nearly optimal solution.

Sea Lions approach their intended prey to position themselves strategically for the next hunting cycle. Equation (2) mathematically represents this behaviour.

$$\overrightarrow{SL(t+1)} = \overrightarrow{P(t)} - \overrightarrow{Dist}.\overrightarrow{C} \tag{2}$$

The leader is gradually led in the direction of and around the target prey by the Sea Lion Optimization algorithm. To do this, the value of t is progressively decreased throughout the number of iterations from 2 to 0. The leader is forced to go toward and surround the prey inside its range by this gradual decline.

Secondly, phase of vocalization: being amphibious means that Sea Lions can live in both the water and on land. In water, their vocalizations travel at a speed of four times that of air. A range of vocalizations are used by Sea Lions to communicate with one another when hunting in groups. Members who are still on shore are also called back by them using their voices. Sea Lions hunt and capture their prey to bring it as near to the surface as they can. They can detect sounds above and below the water because of their small ears. A Sea Lion that has located its target will signal other Sea Lions to encircle and attack them. This behaviour can be expressed mathematically using Equations (3), (4), and (5).

$$\overrightarrow{SP_{\text{leader}}} = |(\overrightarrow{V_1}(1 + \overrightarrow{V_2}))/\overrightarrow{V_2})| \tag{3}$$

$$\overrightarrow{V}_1 = \sin\theta \tag{4}$$

$$\overrightarrow{V}_2 = \sin\emptyset \tag{5}$$

In the context of Sea Lion vocalizations, and $\overrightarrow{V_2}$ represent the sound speeds in water and air, respectively, while $\overrightarrow{SP_{\text{leader}}}$ indicates to leader's sound speed. The sound emitted by the Sea Lion reflects off the air to reach nearby members and refracts within the same medium to reach underwater members. Hence, (sin θ) is used to represent the air-to-air communication, and (sin $\emptyset$) is used to represent the air-to-water communication.

Thirdly, phase of attack (exploitation phase): Sea Lions can locate and encircle their intended prey. The leader, being the most effective search agent, guides the hunt by identifying the prey and alerting other members to its location. The identified prey is typically considered the best option available at the moment. However, a new search agent can emerge, surpass the leader, and locate better prey. To mathematically model Sea Lion hunting behaviour, two stages are introduced:

1. Dwindling Encircling Technique is an essential part of the Sea Lion Optimization method. Its behaviour is dependent on the value of C in Equation (2), which decreases during the iterations progressively from 2 to 0. The Sea Lion leader is compelled by this linear reduction to go toward and surround the prey. Therefore, a Sea Lion's (search agent's) arrival location could be anywhere in between the agent's starting position and the best agent's location at that moment.
2. Circle updating position: Sea Lions typically start their hunt by chasing a bait ball of fish from the edges. During this process, they update their positions using Equation (6). This equation represents the movement of the Sea Lions as they encircle the fish school.

$$\overrightarrow{SL}(t+1) = |\overrightarrow{P}(t) - \overrightarrow{SL}(t)| \cdot \cos(2\pi m) + \overrightarrow{P}(t) \tag{6}$$

Whereas | | denotes an absolute value and m is a random number in the interval [−1, 1], $\overrightarrow{P}(t) - \overrightarrow{SL}(t)$ represents the distance between the search agent (Sea Lion) and the best optimal solution (target prey). When the Sea Lion spots prey on the edge of the bait ball, it begins swimming around it in a circle-shaped pattern. For this reason, this behavior is mathematically represented as $\cos(2\pi m)$.

Fourthly, prey search (exploration phase): During the exploration phase, Sea Lions use their whiskers and zigzag swimming to randomly search for prey. This behavior is mimicked in the study by employing random values. If the random value is greater than 1 or less than -1, moving away from the target prey and its leader is necessary for the Sea Lion. The Sea Lion is compelled by this to look for alternative supplies of prey.

When Sea Lions are exploiting their environment, they adjust their locations according on whatever search agent is performing the best. Nonetheless, searchers adjust their placements based on a randomly selected Sea Lion during the exploring stage. Said another way, the SLnO algorithm searches globally for the global optimal solution if the random value is bigger than one. This is accomplished by proposing Equations (7) and (8).

$$\overrightarrow{Dlst} = |\overrightarrow{2B} \cdot \overrightarrow{SL}_{rnd}(t) - \overrightarrow{SL(t)}| \tag{7}$$

$$\overrightarrow{SL}(t+1) = \overrightarrow{SL}_{rnd}(t) - \overrightarrow{Dlst} \cdot \overrightarrow{C} \tag{8}$$

where $\overrightarrow{SL}_{rnd}(t)$ denotes a randomly chosen Sea Lion from the existing population.

The SLnO algorithm starts with solutions that are produced at random. The best-found solution or a randomly selected search agent is used to update each search agent's position. Over the course of the iterations, parameter (C) is gradually decreased from 2 to 0 in order to enable the exploration and exploitation phases. In particular, a search agent is chosen at random when the absolute value of |C|is greater than one. On the other hand, search agents adjust their placements in accordance with their counterparts when |C|is smaller than one. Ultimately, when a stopping requirement is satisfied, the SLO algorithm comes to an end [35].

While SLO is a promising optimization algorithm with applications in various fields, its use indirectly optimizing encryption algorithms is not straightforward and comes with certain limitations. It's crucial to consider both the potential advantages and challenges before exploring this approach. The potential advantages of using GWO in encryption can be used in enhancing key generation. SLnO can be used to search for strong and complex encryption keys within a large key space, potentially making brute-force attacks more difficult. As well as it can improve diffusion and scrambling: SLnO's ability to mimic the hunting behaviour of Sea Lion, including encircling, attacking, and searching, might be adapted to design scrambling and diffusion processes in encryption algorithms, leading to a more robust and unpredictable ciphertext.

3 The Hybrid Caw Transform (Cosine, Arnold and Discreet Wavelet Transform)

Hybrid transform are famous signal processing techniques that possess the advantages of the conventional transforms. They have wide applications in different applications of artificial intelligence compared to the conventional transforms. Their implementation show that such transforms combined the advantages of the combined conventional transforms. Recently, several types of research on hybrid and mixed transformation have been conducted [36–42]. As an important contributor, the CAW hybrid transforms, proposed in [33] has taken on the mission of promoting innovation and has developed a roadmap to pioneer this change. The hybrid Transform model, proposed in [43], introduce a novel approach to image processing by combining linear and nonlinear transformation techniques. This combined transformation process, effectively captures both spatial and frequency domain information, improving the performance of image processing tasks like watermarking and encryption [43]. The CAW hybrid transform leverages the strengths of Cosine, Arnold, and Wavelet transforms:

It is worth noting that the cosine transform is considered useful in obtaining important and useful information from periodic data compared to the wavelet transform. At the same time, wavelets are accurate in processing multi-frequency data compared to Fourier transform. The Arnold transform replaces parameter locations, reorganizes pixels, and helps in arranging image pixels and defining their boundaries. Based on the above features, the new CAW hybrid transform combines the advantages of both transforms and shows much higher sensitivity than the cosine and wavelet transforms, but it is computationally more complex than both transforms.

4 URUK Chaotic Map

A discrete chaotic system with complex and unexpected behavior, the URUK system exists in four dimensions [44, 45]. URUK is a high-dimensional map involving multiple state variables, leading to a vast and intricate key space. This significantly increases the difficulty of brute-force attacks, as attackers would need to explore an exponentially larger number of possible keys. The complex dynamics of URUK map creates highly sensitive and unpredictable output sequences, making it challenging to analyze and predict the encrypted data. Small changes in the initial conditions or parameters of URUK map can dramatically alter the resulting sequence. This property

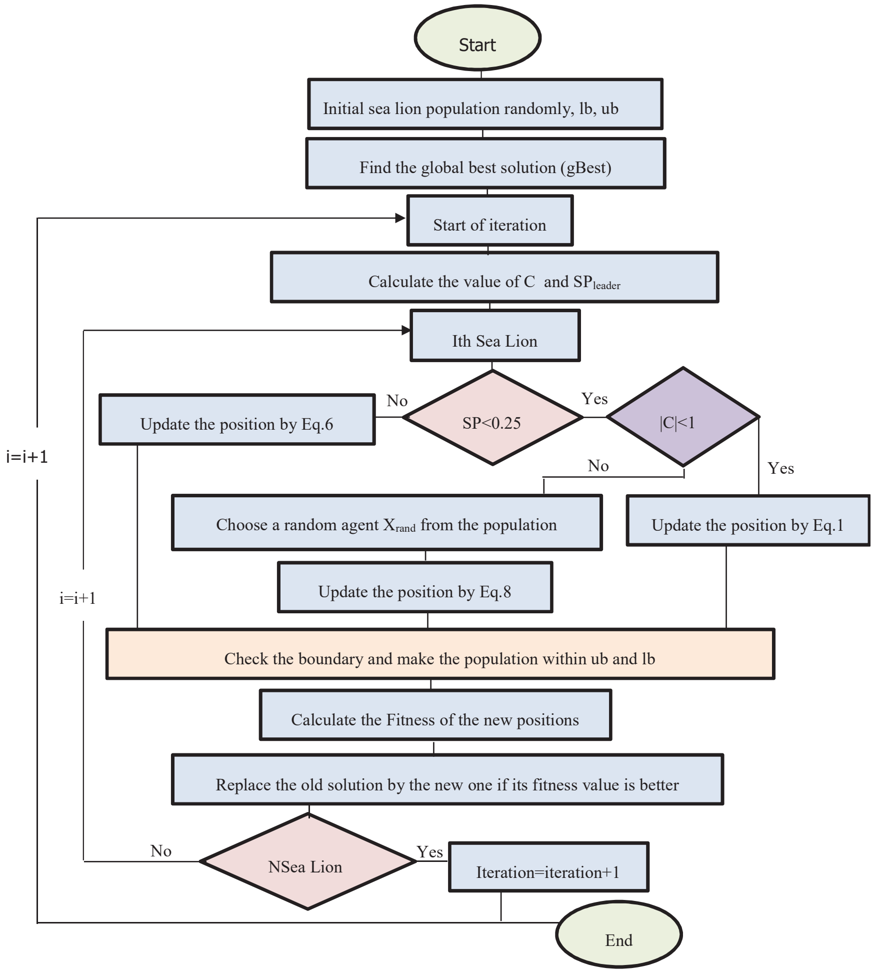

Start
Initial sea lion population randomly, lb, ub
Find the global best solution (gBest)
Start of iteration
Calculate the value of C and SP$_{leader}$
Ith Sea Lion
No
SP<0.25
Yes
|C|<1
Update the position by Eq.6
No
Yes
Choose a random agent X$_{rand}$ from the population
Update the position by Eq.1
Update the position by Eq.8
i=i+1
i=i+1
Check the boundary and make the population within ub and lb
Calculate the Fitness of the new positions
Replace the old solution by the new one if its fitness value is better
No
NSea Lion
Yes
Iteration=iteration+1
End

Figure 1 The flowchart of the Sea Lion Optimization algorithm. 1. 2D Cosine Transform: Captures important periodic data. 2. Arnold Transform: Permutes pixel positions to enhance security. 3. Wavelet Transform: Processes multi-frequency data accurately. The process involves applying the Cosine Transform, then the Arnold Transform, followed by inverse Cosine and Wavelet Transforms, creating a robust encryption mechanism.

makes the encrypted data highly resistant to differential attacks, which exploit relationships between slightly modified plaintexts and their ciphertexts. The intricate interactions between multiple state variables in URUK map leads to more efficient diffusion and scrambling of the plaintext data. This means the information is spread across the entire ciphertext, making it more difficult to extract or recover any meaningful fragments. The flexibility of URUK maps allows for incorporating additional layers of complexity and security features into the encryption scheme. This could include chaotic masking, dynamic key generation, or hybrid cryptosystems combining chaos with traditional cryptographic techniques. 4D URUK map provides even greater complexity and can be combined with other chaotic maps for enhanced security [44, 45].

The URUK chaotic map, defined by four variables (x, y, z, w) and bifurcation parameters (a, b, c, d), introduces trigonometric functions and nonlinear terms, enhancing unpredictability. The equations governing URUK are:

$$\begin{gathered}
\mathrm{X}_{(n+1)} = 1 - (\mathrm{X}_n \times \mathrm{Y}_n \times \mathrm{Z}_n \times \mathrm{W}_n) - \mathrm{X}_n^2 - \mathrm{Y}_n^2 - a \times \tan\left(\mathrm{Z}_n^2\right) - \mathrm{W}_n^2 \\
a \times \tan \\
\mathrm{Y}_{(n+1)} = \mathrm{X}_n - b \times \tan(\mathrm{Z}_n) \\
\mathrm{Z}_{(n+1)} = \mathrm{Y}_n - c \times \tan(\mathrm{Z}_n) \\
\mathrm{W}_{(n+1)} = \mathrm{X}_n - d \times \mathrm{W}_n
\end{gathered} \tag{9}$$

This complexity makes it suitable for generating secure encryption keys, resisting various attacks.

5 The Novel Image Encryption Algorithm

The encryption process comprises three distinct phases:

1. Key Generation: Initial parameters for the chaotic map are derived from the plain image using SHA512, which are then used to generate key sequences through the URUK chaos map.
2. Image Transformation: The image undergoes CAW hybrid transform and DWT, followed by FAN transform-based permutation and sub-band decomposition.
3. Diffusion and Scrambling: The resulting matrices are diffused and shuffled using the Sea Lion Optimization algorithm to produce the final encrypted image.

The procedure of images encryption is given in this section as depicted in Figure 2. In the first phase, the initial parameters of the chaotic map are generated from the pixels of the plain image (P). The parameters are generated by the Secure Hash Algorithm 512 (SHA512) from the plain image. Next, 64 decimal numbers each of them of 8 bits are obtained. From which the control parameters X, Y, Z and W values were calculated. These initial values are then used to iterate URUK chaos map to create key sequences. The CAW hybrid transform is computed subsequently to get matrix C and after that the quantification of the matrix Q will be obtained.

In the second phase, one level decomposition DWT of the plain image (P) will be performed which produces the coefficient's matrix A. The B matrix obtained after permutation of A matrix coefficients applying FAN transform. Next the B matrix will be split into four equal size quarters (Q1, . . . Q4). The FAN transform will be applied to each quarter individually that produced the matrices U1, . . . , U4 respectively. The final matrices masked in one matrix and intern Quantified to produce the matrix U.

In the third phase, the diffusion processed on the matrices Q and U to produce matrix R. Next, the permutation key sequence is obtained by iterative the Sea Loin Optimization algorithm. Next, using the key sequence to perform the permutation operation on the matrix R to obtain the matrix E. Finaly, a shuffle of the pixels is made through the Sea Lion Optimization to obtain the encrypted image F. The detail of these phases is given by the following procedure.

Phase I

1. Preprocessing: Input natural image of size 512×512 pixels and convert it to a matrix of pixels suitable for forthcoming extraction of useful information for encryption.
2. Key generation: Generate the chaos sequence number, the initial conditions of the URUK map. These keys are obtained from the input natural image values to make this method more sensitive to plain images and resilient to known plain attacks and determine the randomness and sensitivity of the encryption process. The initial values of X, Y, Z and W are extracted by the following steps:
   a. Generate a secret key or initial condition for the chaotic map, Apply SHA512 to the input image to obtain 512-bit hash values
   b. Convert the 512 bits into 64 decimal numbers (h) each of them 8bits
   c. Obtain X, Y, Z and W values using the following equations on the 64 decimal values:

$$k_1 = \sum_{1}^{16} h_i, \quad X = \frac{mode(k_1 \times 2^6, 99)}{100} \tag{10}$$

$$k_2 = \sum_{17}^{32} h_i, \quad Y = \frac{mode(k_2 \times 2^6, 99)}{100} \tag{11}$$

$$k_3 = \sum_{33}^{48} h_i, \quad Z = \frac{mode(k_3 \times 2^6, 99)}{100} \tag{12}$$

$$k_4 = \sum_{49}^{64} h_i, \quad W = \frac{mode(k_4 \times 2^6, 99)}{100} \tag{13}$$

3. Chaotic scrambling: By applying the URUK chaotic map repeatedly to each pixel's value or its position in the image, generating a seemingly random sequence based on the initial key generated in step 2 above.
4. Appy CAW transform to the generated matrix from step 3 above to get the sparse numbers
5. Quantification: Apply normalization to adjust the encrypted pixel values to ensure they fall within a desired range for representation and transmission. The purpose of this quantification of the image is to facilitate the diffusion process by the following normalized equation:

$$Q = round(255 \times \frac{C - min}{max - min}) \tag{14}$$

Phase II:

6. For the same nature image in phase I apply Wavelet transform to get the sparse image to obtain matrix A.
7. Permutation: Rearrange the parameters of Wavelet version of the image of step-6 above based on the outer application of FAN transform in order of disrupting their original Wavelet coefficients relationships to obtain matrix B.
8. Decompose the image into four separated equally sub-bands of Q_1, Q_2, Q_3 and Q_4.
9. Apply FAN transform to scramble each of the above four sub-band individually.
10. Mask all four sub-bands to form only one combined template.
11. Quantify the image to facilitate the diffusion process by the normalized Equation (14) to obtain U

Phase III

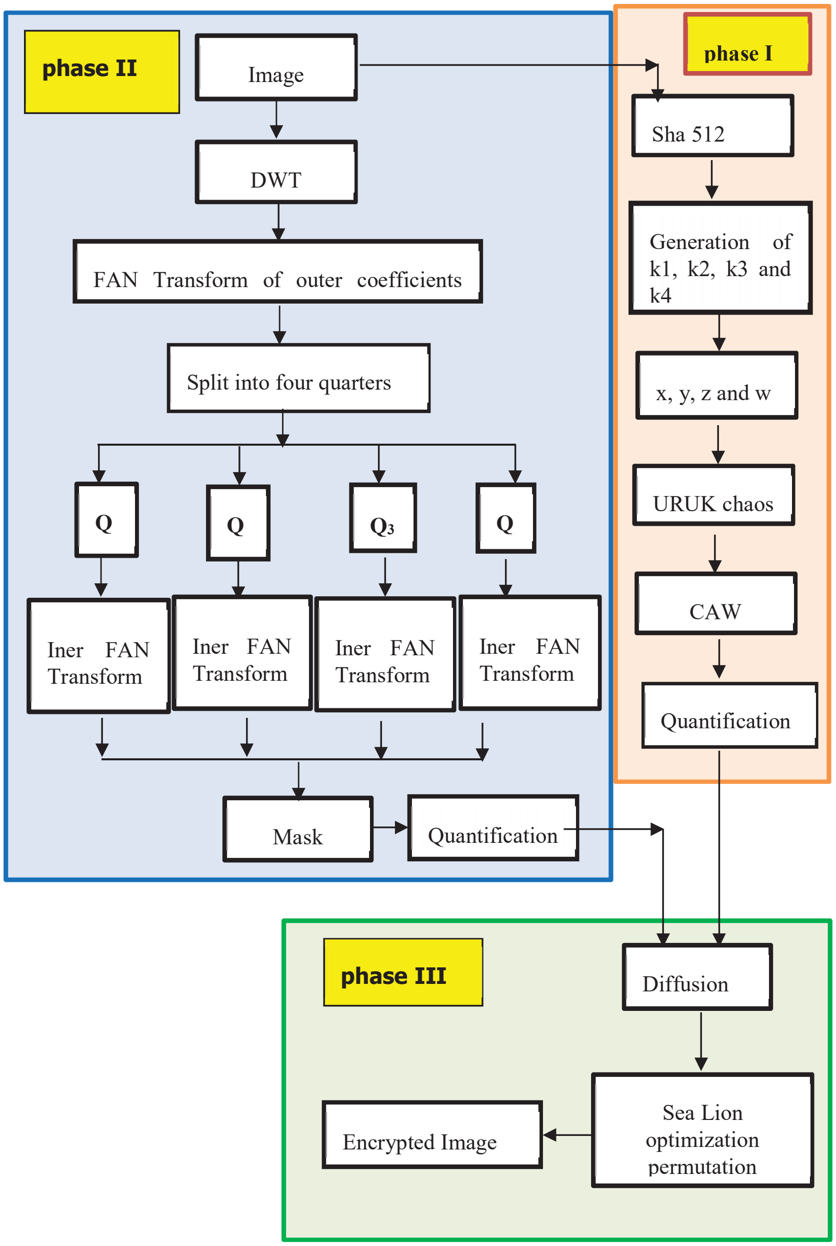


Figure 2 The main block diagram of the proposed encryption system.

12. Diffuse between the generated matrices from step-5 and step-11 using URUK map using the following Equation:

$$R = XOR(U, Q) \tag{15}$$

13. Shuffle all image pixels using the Sea Lion Optimization algorithm to get the minimum correlation between adjacent pixels through the following procedure:

    a. Generate the initial population of the Sea Lion Optimization algorithm
    b. Use the value of each member as an initial value for the URUK map to generate a sequence of chaos number
    c. Sort the sequence of chaos numbers and obtain the index values
    d. Scramble the image by using the index values of the chaos sequence number

    $$E = R(index(:)) \tag{16}$$

    e. Compute the fitness of scrambled image by using the following objective function.

    $$\textit{Min Fitness} = \textit{Correlation}(E) \tag{17}$$

    f. Update the position of the population to enhance the results.
    g. Repeat until all iteration is done and use the final URUK chaos sequence to shuffle the image to form the encrypted image F.

6 The Decryption Processes

The decryption process is carried out by using the same encryption steps, but in reverse, as it requires sending the key parameters of the URUK chaos map to the counterparty in order to use them to generate the same key to be able to decrypt the encryption. The shuffle process that was applied by the Uruk chaos map and the Sea Lion optimization algorithm is reversed. the diffusion process is reversed. Then reversing the quantization process so that the values return to their normal state. The image is divided into four parts (Q1, Q2, Q3 and Q4) and the scrambling that was applied to each part using the FAN transform is reversed. Mask (Q1, Q2, Q3 and Q4) parts into one image part and the scrambling is also reversed using the FAN transform. Finally, the inverse DWT is applied to obtain the original image as demonstrated in Figure 3.

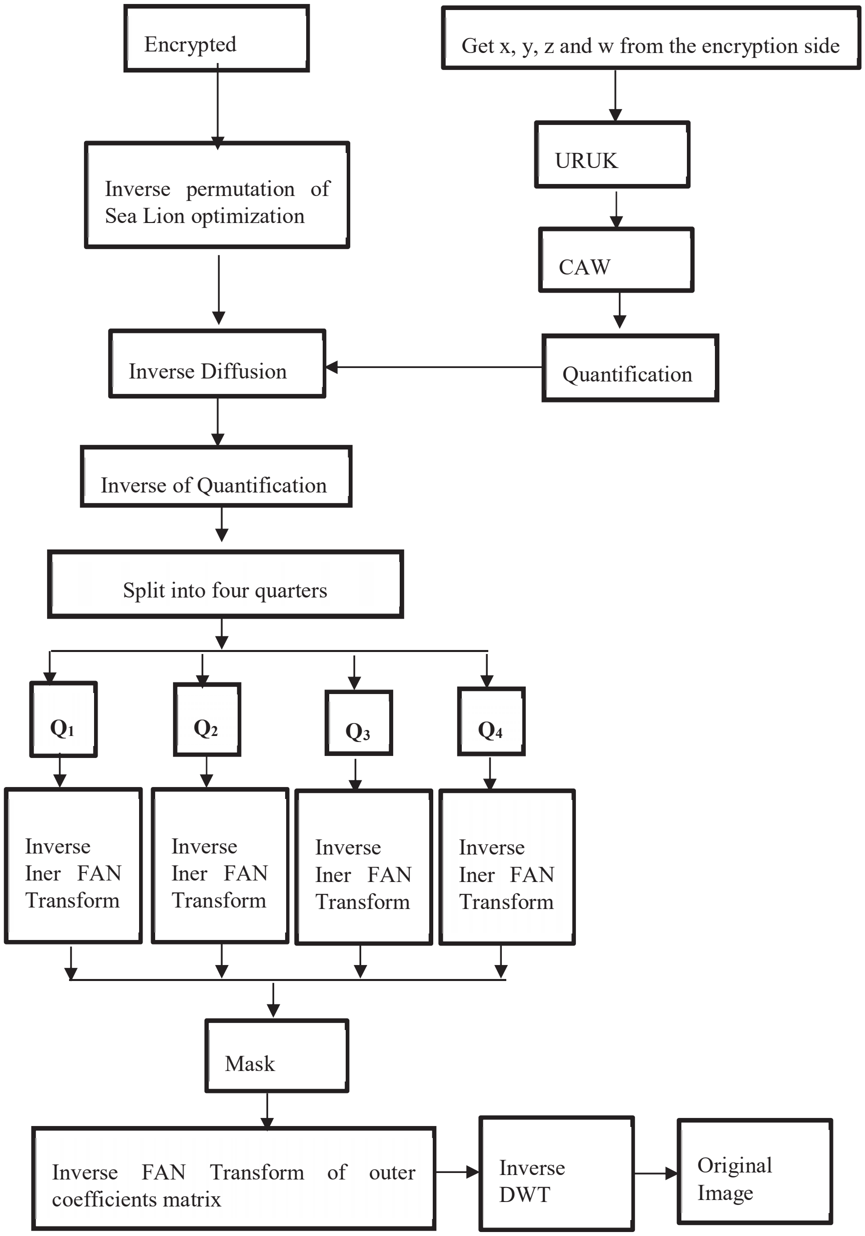

Encrypted
Get x, y, z and w from the encryption side
URUK
Inverse permutation of Sea Lion optimization
CAW
Inverse Diffusion
Quantification
Inverse of Quantification
Split into four quarters
Q1
Q2
Q3
Q4
Inverse Iner FAN Transform
Inverse Iner FAN Transform
Inverse Iner FAN Transform
Inverse Iner FAN Transform
Mask
Inverse FAN Transform of outer coefficients matrix
Inverse DWT
Original Image

Figure 3 The main block diagram of the decryption processes.

7 The Experimental Result and Practical Analysis

The results demonstrate the efficacy of the proposed method. The plain image is encrypted through a series of encryption processes, including confusion and diffusion. A visual representation of the image outputs sheds light on how the security is affected by these processes and the appearance of the image. The process of encryption is effective since the part that decrypts an image can only fully decode it if the correct key parameters are known and how they should be arranged. A slight alteration in the secret parameter could affect the decrypted result. To make sure the encryption method is stable, let's make a few minor adjustments to the aforementioned secret settings.

7.1 Key Space Analysis

The total number of keys used in the encryption process determines the size of the key space. For any encryption method to successfully withstand a brute-force attack, the key space must be vast. A brute force attack cannot be successfully executed on a key space whose size is more than $2^{100} \approx 10^{30}$. In the proposed method, SHA-512 is used to generate initial values X, Y, Z, and W for URUK chaos map. The proposed method's key space, assuming a precision of 10^{-14} is $2^{512} \times 10^{14} \times 10 = 2^{512} \times 10^{140}$. This vast key space ensures robustness against brute-force attacks, providing a high degree of protection [44].

7.2 Key Sensitivity Analysis

The encryption and decryption keys needed. the proposed method must be extremely confidential. The initial secret keys for the URUK chaos map and

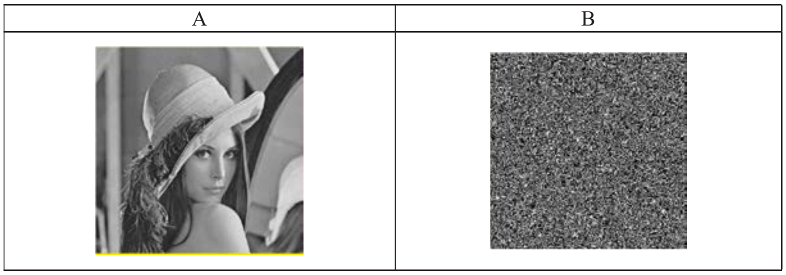


Figure 4 Depicts the failure to decrypt a standard Lena image (256x256) using an incorrect decryption key (DK) generated with modified control parameters (a) Standard Lena Image, (b) Decryption Result with Modified Control Parameters.

one pixel from original image have been altered. the four secret keys X, Y, W, and Z put in the wrong order. The decryption process did not give the original image. This high sensitivity is crucial for strong encryption, as shown in Figure 4. The figure demonstrates how attempts to decrypt an image (the Lena image) that fail when keys derived with slightly changed starting values are used. the Sensitivity analysis demonstrates that altering a single bit in the secret key produces significantly different decrypted images. This high sensitivity underscores the robustness of the encryption scheme against known-plaintext attacks, ensuring that minor changes in the key or plaintext result in substantial variations in the ciphertext.

7.3 Analysing the Correlation Values

The correlation coefficient between neighbouring pixels in an image measures their resemblance to one another. A high correlation coefficient implies that the intensity values of two adjacent pixels are highly similar, while a low correlation coefficient indicates that their intensities are considerably different. This correlation can be computed using the following formula:

$$r_{x,y} = \frac{E\{[x - E(x)][y - E(y)]\}}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, D(x) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)]^2 \tag{18}$$

where N is the number of samples. Any image has a correlation coefficient between -1 and 1. The value -1 indicates a negative correlation between picture pixels, while the value 1 indicates a significant positive connection. There is no association between the neighbouring pixels when the value is 0. Each component of the encrypted image has a correlation coefficient that is almost 0, proving that the pixels are unrelated to one another. Table 1 provides the correlation coefficients for the encrypted images in the diagonal (D), vertical (V), and horizontal (H) axes. Figure 5 shows the distribution of neighbouring images before and after applying the encryption method. The correlation coefficients between adjacent pixels in encrypted images are near zero, confirming the method's effectiveness in disrupting pixel relationships. Table 2 presents these coefficients, highlighting the superiority of our approach compared to traditional methods, which often exhibit higher correlation values.

Table 1 Provides the correlation values between adjacent pixels in the cipher image

Image	Diagonal (D)	Vertical (V)	Horizontal (H)
Lena	0.0005	0.0006	0.0001
Tree	0.0007	−0.0002	0.0006
Pepper	0.0003	−0.0000	0.0001
Baboon	−0.0005	0.0003	−0.0002
Aircraft	0.0008	0.0003	0.0002

Table 2 Compares the correlation values obtained using the proposed method with those from other encryption techniques

Method	Diagonal (D)	Vertical (V)	Horizontal (H)
Ref. [34]	0.0014162	0.000029777	0.10468
Ref. [27]	0.001843	0.002319	−0.001327
Ref. [20]	0.00163	0.00053	0.00273
Ref. [12]	−0.0029	0.0006	−0.0005
Ref. [11]	0.010518	0.089618	0.0080415
Proposed method	0.0005	0.0006	0.0001

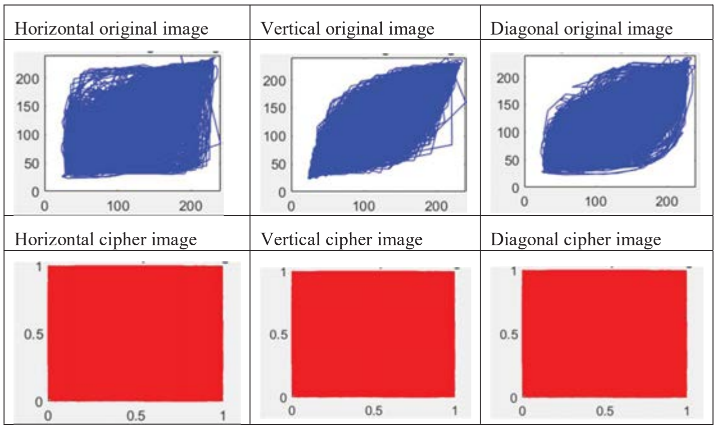


Figure 5 Shows the distribution of neighbouring of Lena image before and after applying the encryption method.

7.4 Mean Square Error (MSE)

The following formula is used to determine the MSE value between the original and encrypted images.

$$MSE(I,E) = \frac{1}{N \times M} \sum_{a=1}^{N} \sum_{b=1}^{M} [I(a,b) - E(a,b)]^2 \tag{19}$$

Table 3 MSE, PSNR, and SSIM values for proposed method

Image	MSE	PSNR	SSIM
Lena	7765.4336	27.5874	0.0067
Tree	9739.9774	27.5517	0.0102
Pepper	8419.5951	27.7219	0.0088
Baboon	7270.6165	27.3783	0.0075
Aircraft	10287.4225	25.8676	0.0080

where M and N represent the image's pixels, I (a, b) is input image, E(a, b) is encrypted image. Table 3 displays the MSE values matching the original and encrypted images. A higher MSE score indicates that no information about the original image is provided by the encrypted image.

7.5 Peak Signal to Noise Ratio (PSNR)

The equation is used to determine the PSNR between the input and output images.

$$PSNR = 20 \times \log_{10}\left(\frac{255}{MSE}\right) \tag{20}$$

where the highest value of a pixel in an image is 255. Table 3 showed the PSNR values of the encrypted images. The extremely low PSNR values indicate a full alteration of the input image.

7.6 Histogram Analysis

Histogram analysis is used to analyze the statistical characteristics of both the original and the encrypted images. An image's number of pixels with varying intensities can be seen by histogram analysis. The original and encrypted images have considerably different histograms. The encryption algorithm can withstand a range of statistical attacks, as shown by the histogram analysis presented in Figure 6.

7.7 Structural Similarity Index Measure

The Structural Similarity Index Measurement (SSIM) assesses the degree of degradation in an encrypted image throughout the encryption process. The SSIM can be computed using the following mathematical formula:

$$\mathrm{SSIM}(I, J) = \frac{(2\mu_I\mu_J + L_1)(2\sigma_{IJ} + L_2)}{\left(\mu_I^2 + \mu_J^2 + L_1\right)\left(\sigma_I^2 + \sigma_J^2 + L_2\right)} \tag{21}$$

Table 4 Compared the encryption time with other methods

Ref. [9]	93.9
Ref. [6]	315.6
Ref. [2]	1677.4
Ref. [17]	162.6
Ref. [30]	36.0
The proposed method	16.908804

The symbol σIJ represents the covariance between the image intensities of I and J, while μI and σJ denote the mean intensities of I and J images, respectively. $L_1 = (0.01 \times H)^2$, $L_2 = (0.03 \times H)^2$ and $H = 2^8 - 1$. The range of SSIM is between $[-1, 1]$. Values that are close to 0 are preferred for encryption in a secure system, while values that are close to 1 are required for decryption. The SSIM values for encrypted images are presented in Table 3.

7.8 Resistance to Chosen-plaintext Attacks

The most significant attack is the chosen-plaintext one. After selecting the desired image for their plaintext, the attackers generate the relevant encrypted image and try to obtain data relating to encryption. For system security, the arrangement and confidentiality of the keys determine the encryption technique employed in this research. The proposed solution's comparatively large key size makes it harder for potential hackers to figure out the correct secret keys and how to arrange them.

7.9 Examining the Complexity of Time

The speed at which an encryption algorithm executes is one of the key criteria used to evaluate its effectiveness. Considering the 512×512 image's encryption process, in Table 4 the time calculation for the encrypted images is compared with other methods.

7.10 Attack by Noise

The efficiency of the proposed method in countering noise attacks is assessed. Salt and pepper noise (SPN) is added to the encrypted image. Decrypted images were successfully retrieved. Figure 7 depicts the encrypted image with noise of 0.05 and 0.005.

Table 5 The entropy values for the encrypted images

Image	Entropy
Lena	7.9994
Tree	7.9993
Pepper	7.9993
Baboon	7.9992
Aircraft	7.9993

Table 6 Entropy comparison with other methods

Ref. [34]	7.9989
Ref. [27]	7.997418
Ref. [20]	7.998461
Ref. [12]	7.9998
Ref. [11]	7.9646
Proposed method	7.9994

7.11 Entropy Analysis

The randomness of a set of data is measured by the entropy.

$$H(s) = -\sum_{k=0}^{M} p(s_k)\log_2 p(s_k) \tag{22}$$

The entropy of data s, represented by H(s), and the probability of occurrence $\mathrm{S_k}$, represented by $\mathrm{p(S_k)}$. The maximum entropy value for an image is 8 With 256 different grey levels. An entropy rating of approximately 8 indicates that an image is very unexpected. The original image and the encrypted image entropy values are displayed in Table 5. This indicates that the proposed encryption approach is immune to entropy-based assaults because the entropy values high. Table 6 shows the entropy comparison with other methods.

7.12 Occlusion Attack Analysis

When sending images over a public network, criminal activity or network congestion may cause data loss. An image can be recovered using occlusion attack analysis in the event of data losing. We looked at the encrypted image in Figure 8 with occlusions of 32 × 32, 64 × 64, and 128 × 128 in order to assess how resilient the suggested encryption approach is against occlusion attacks. The outcomes show that even with these occlusions present, it is still possible to correctly decrypt the encrypted image. The robustness of the suggested approach against cropping attacks is confirmed by this analysis.

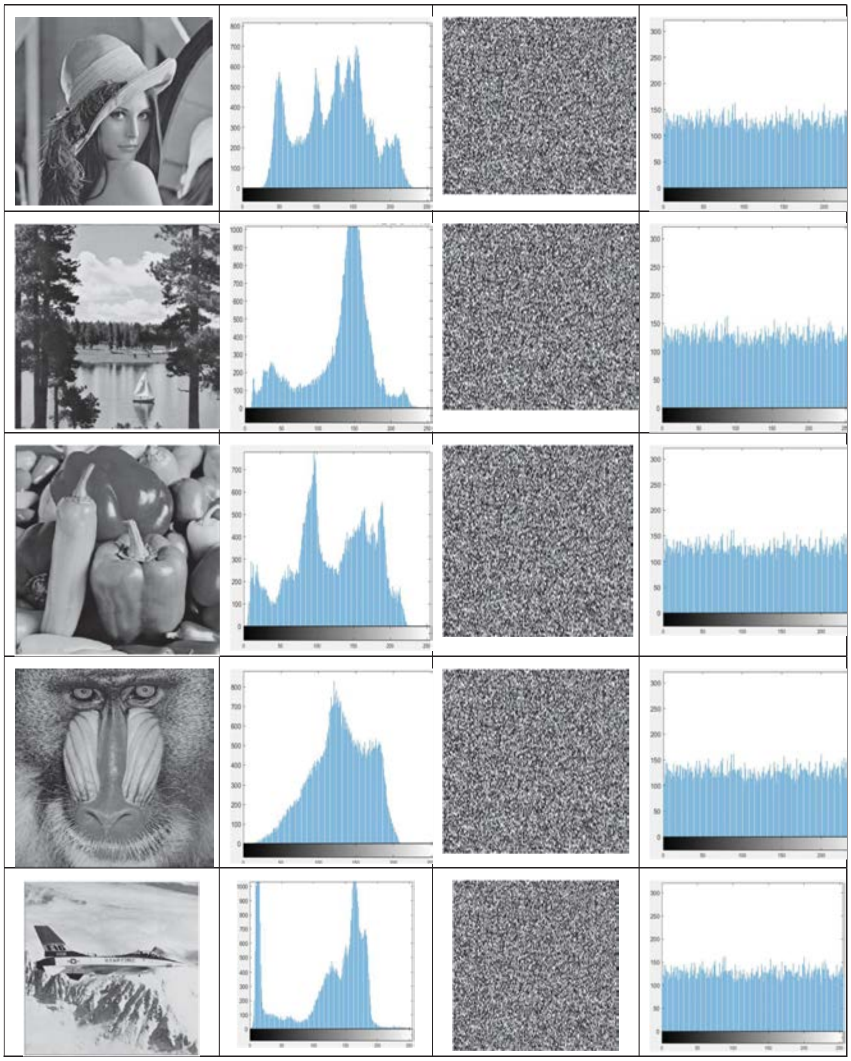
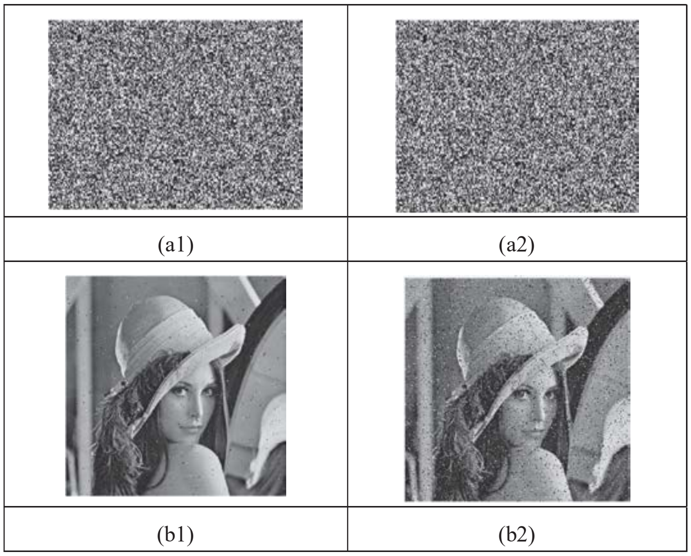


Figure 6 The histogram of the original and encrypted images.

7.13 Analysis Using NPCR and UACI

The statistic known as NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity) evaluates how resilient an image encryption method is to different types of attacks. Differential attacks take advantage of how sensitive the encryption method is to even small changes in



(a1) (a2)

(b1) (b2)

Figure 7 Illustrates how resistant images are to noise attack the decrypted images are (b1) and (b2), and (a1) SPN with noise density = 0.005; (a2) SPN with noise density = 0.05.

the input image. An attacker will find it more challenging to distinguish the encrypted image from the original due to the significant visual difference.it can be calculated as follows:

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} Q(C1_{i,j}, C2_{i,j}) \tag{23}$$

$$UACI = \frac{1}{M \times N \times 255} \sum_{i=1}^{M} \sum_{j=1}^{N} |C1_{i,j} - C2_{i,j}| \tag{24}$$

Where C1 and C2 stand for two encrypted images, M and N is the image size. Here, $Q(C1_{i,j}, C2_{i,j})$ is computed as

$$Q(C1_{i,j}, C2_{i,j}) = \begin{cases} 0, & \text{if } C1_{i,j} = C2_{i,j}, \\ 1, & \text{otherwise.} \end{cases} \tag{25}$$

Table 7 shows the NPCR and UACI values for the input image. The proposed method is significantly resistant to virous types of attacks. the UACI and NPCR values In Table 8 compared the proposed and current methods.

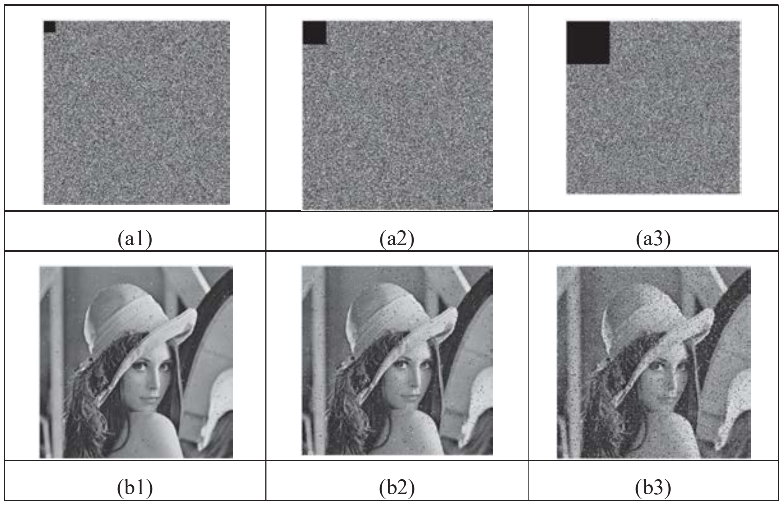


Figure 8 Illustrate how resistant images are to cut attacks The images (a1), (b1), and (b3) have been encrypted. (a1) cuts a patch size of 32 x 32 pixels; (a2) cuts a patch size of 64 x 64 pixels; (a3) cuts a patch size of 128 x 128 pixels; and (a4).

Table 7 The UACI and NPCR values for proposed method

Image	UACI	NPCR
Lena	33.5773	99.6304
Tree	30.1515	99.6292
Pepper	33.4099	99.6090
Baboon	33.4724	99.6281
Aircraft	33.4860	99.6002

Table 8 Compared NPCR and UACI values for the proposed and current methods

	NPCR	UACI
Ref. [34]	99.587	30.701
Ref. [27]	0.995998	0.33391
Ref. [20]	99.620901	33.365006
Ref. [12]	99.6453	33.4733
Ref. [11]	99.78342	33.84126
Proposed method	33.5773	99.6304

8 Conclusion

The proposed hyperchaotic system effectively conceals the wavelet-permuted sub-band coefficients (Q1, Q2, Q3, and Q4), enhancing security. It also offers benefits such as wide key sensitivity, large key space, and straightforward implementation. The URUK Hyperchaotic system makes attackers hard to synthesize and predicts which resulting into higher security and system complexity. Furthermore, the hybrid CAW transform breaks the correlation between the neighboring pixels and makes the algorithm possess strong expansibility. Using FAN transform enhance more safety of the proposed hyperchaotic system. SHA512 is applied to the original image to extract URUK initial values. Using Sea Lion optimization automatically adjusting the key length according to the parameter adjustment. As well as it is helpful to broaden usability of the proposed hyperchaotic system and useful to network security and secure communications applications. According to sensitivity analysis, a single bit change in the secret key produces distinct decrypted images. The effectiveness of the proposed method for image encryption was evaluated, and a variety of characteristics were used for analysis and implementation, including PSNR, entropy, UACI, NPCR, examination of the calculation time and histogram analysis. The proposed hyperchaotic encryption system significantly enhances security by integrating the CAW hybrid transform and Sea Lion Optimization algorithm. The system demonstrates high sensitivity, extensive key space, and strong resistance to statistical and differential attacks. Future research could explore the application of this encryption method to different data types and optimize the algorithm for real-time performance. Additionally, investigating the integration of other chaotic maps and optimization algorithms could further improve the robustness and efficiency of the encryption process

References

[1] S. P. Praveen, V. S. Suntharam, S. Ravi, U. Harita, V. N. Thatha, and D. Swapna, “A Novel Dual Confusion and Diffusion Approach for Grey Image Encryption using Multiple Chaotic Maps,” *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 8, 2023.

[2] Z. Hua, Y. Zhou, and H. Huang, “Cosine-transform-based chaotic system for image encryption,” *Inf Sci (N Y)*, vol. 480, pp. 403–419, 2019.

[3] A. A. Abdul-Kareem and W. A. M. Al-Jawher, “Image Encryption Algorithm Based on Arnold Transform and Chaos Theory in the Multi-wavelet Domain,” *International Journal of Computers and Applications*, vol. 45, no. 4, pp. 306–322, 2023.

[4] M. Muthumari, V. Akash, K. P. Charan, P. Akhil, V. Deepak, and S. P. Praveen, “Smart and multi-way attendance tracking system using

an image-processing technique," *in 2022 4th International conference on smart systems and inventive technology (ICSSIT), IEEE*, 2022, pp. 1805–1812.

[5] Q. K. Abed and W. A. M. Al-Jawher, "A Robust Image Encryption Scheme Based on Block Compressive Sensing and Wavelet Transform," *International Journal of Innovative Computing*, vol. 13, no. 1–2, pp. 7–13, 2022.

[6] L. Liu and S. Miao, "A new simple one-dimensional chaotic map and its application for image encryption," *Multimed Tools Appl*, vol. 77, pp. 21445–21462, 2018.

[7] A. A. Abdul-Kareem and W. A. Mahmoud Al-Jawher, "Hybrid image encryption algorithm based on compressive sensing, gray wolf optimization, and chaos," *J Electron Imaging*, vol. 32, no. 4, p. 43038, 2023.

[8] A. S. Reddy, S. P. Praveen, G. B. Ramudu, A. B. Anish, A. Mahadev, and D. Swapna, "A Network Monitoring Model based on Convolutional Neural Networks for Unbalanced Network Activity," *in 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), IEEE*, 2023, pp. 1267–1274.

[9] J. Tang, Z. Yu, and L. Liu, "A delay coupling method to reduce the dynamical degradation of digital chaotic maps and its application for image encryption," *Multimed Tools Appl*, vol. 78, pp. 24765–24788, 2019.

[10] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, "Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys," *Neural Comput Appl*, vol. 31, pp. 2395–2405, 2019.

[11] S. Roy, U. Rawat, H. A. Sareen, and S. K. Nayak, "IECA: an efficient IoT friendly image encryption technique using programmable cellular automata," *J Ambient Intell Humaniz Comput*, vol. 11, pp. 5083–5102, 2020.

[12] M. Essaid, I. Akharraz, and A. Saaidi, "Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps," *Journal of Information Security and Applications*, vol. 47, pp. 173–187, 2019.

[13] A. A. Abdul-Kareem and W. A. M. Al-Jawher, "WAM 3D discrete chaotic map for secure communication applications," *International Journal of Innovative Computing*, vol. 13, no. 1–2, pp. 45–54, 2022.

[14] M. Ghazvini, M. Mirzadi, and N. Parvar, "A modified method for image encryption based on chaotic map and genetic algorithm," *Multimed Tools Appl*, vol. 79, pp. 26927–26950, 2020.

[15] U. Sirisha and B. S. Chandana, "Privacy preserving image encryption with optimal deep transfer learning based accident severity classification model," *Sensors*, vol. 23, no. 1, p. 519, 2023.

[16] A. A. Shah, S. A. Parah, M. Rashid, and M. Elhoseny, "Efficient image encryption scheme based on generalized logistic map for real time image processing," *J Real Time Image Process*, vol. 17, no. 6, pp. 2139–2151, 2020.

[17] X. Wang, L. Feng, R. Li, and F. Zhang, "A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model," *Nonlinear Dyn*, vol. 95, pp. 2797–2824, 2019.

[18] Q. K. Abed and W. A. M. Al-Jawher, "Anew Architecture of Key Generation Using DWT for Image Encryption with Three Levels Arnold Transform Permutation," *Journal Port Science Research*, vol. 5, no. 3, pp. 166–177, 2022.

[19] U. Sirisha and S. C. Bolem, "Aspect based sentiment & emotion analysis with ROBERTa, LSTM," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 11, 2022.

[20] P. K. Naskar, S. Bhattacharyya, D. Nandy, and A. Chaudhuri, "A robust image encryption scheme using chaotic tent map and cellular automata," *Nonlinear Dyn*, vol. 100, pp. 2877–2898, 2020.

[21] L. Zhu et al., "A stable meaningful image encryption scheme using the newly-designed 2D discrete fractional-order chaotic map and Bayesian compressive sensing," *Signal Processing*, vol. 195, p. 108489, 2022.

[22] U. Sirisha, S. P. Praveen, P. N. Srinivasu, P. Barsocchi, and A. K. Bhoi, "Statistical analysis of design aspects of various YOLO-based deep learning models for object detection," *International Journal of Computational Intelligence Systems*, vol. 16, no. 1, p. 126, 2023.

[23] K. A. K. Patro, B. Acharya, and V. Nath, "Secure multilevel permutation-diffusion based image encryption using chaotic and hyperchaotic maps," *Microsystem Technologies*, vol. 25, pp. 4593–4607, 2019.

[24] S. P. Praveen, S. Sindhura, A. Madhuri, and D. A. Karras, "A novel effective framework for medical images secure storage using advanced cipher text algorithm in cloud computing," *in 2021 IEEE International Conference on Imaging Systems and Techniques (IST), IEEE*, 2021, pp. 1–4.

[25] Q. K. Abed and W. A. M. Al-Jawher, “An Image Encryption Method Based on Lorenz Chaotic Map and Hunter-Prey Optimization,” *Journal Port Science Research*, vol. 6, no. 4, pp. 332–343, 2023.

[26] K. A. K. Patro, M. Prasanth Jagapathi Babu, K. Pavan Kumar, and B. Acharya, “Dual-layer DNA-encoding–decoding operation based image encryption using one-dimensional chaotic map,” *in Advances in Data and Information Sciences: Proceedings of ICDIS 2019, Springer*, 2020, pp. 67–80.

[27] X. Wang, Y. Wang, X. Zhu, and S. Unar, “Image encryption scheme based on Chaos and DNA plane operations,” *Multimed Tools Appl*, vol. 78, pp. 26111–26128, 2019.

[28] 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, pp. 1757–1768, 2021.

[29] J. Xu, J. Mou, J. Liu, and J. Hao, “The image compression–encryption algorithm based on the compression sensing and fractional-order chaotic system,” *Vis Comput*, pp. 1–18, 2022.

[30] M. Z. Talhaoui, X. Wang, and M. A. Midoun, “A new one-dimensional cosine polynomial chaotic map and its use in image encryption,” *Vis Comput*, vol. 37, pp. 541–551, 2021.

[31] T. Krishna, S. P. Praveen, S. Ahmed, and P. N. Srinivasu, “Software-driven secure framework for mobile healthcare applications in IoMT,” *Intelligent Decision Technologies, no. Preprint*, pp. 1–14, 2022.

[32] H. Aparna et al., “Double layered Fridrich structure to conserve medical data privacy using quantum cryptosystem,” *Journal of Information Security and Applications*, vol. 63, p. 102972, 2021.

[33] J. S. Muthu and P. Murali, “A novel DICOM image encryption with JSMP map,” *Optik (Stuttg)*, vol. 251, p. 168416, 2022.

[34] B. Mondal and J. P. Singh, “A lightweight image encryption scheme based on chaos and diffusion circuit,” *Multimed Tools Appl*, vol. 81, no. 24, pp. 34547–34571, 2022.

[35] R. Masadeh, B. A. Mahafzah, and A. Sharieh, “Sea lion optimization algorithm,” *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 5, 2019.

[36] W. A. Mahmoud, “A Smart Single Matrix Realization of Fast Walidlet Transform,” *International Journal of Research and Reviews in Computer Science,* vol. 2, no. 1, p. 144, 2011.

[37] M. H. M. Hasan, W. A. A. Jouhar, and M. A. Alwan, "3-d face recognition using improved 3d mixed transform," *Int J Biom Bioinformatics*, vol. 6, no. 1, p. 278, 2012.

[38] W. A. Al-Jowher, N. N. Al-Ramahi, and M. Alfaouri, "Image identification and labeling using hybrid transformation and neural network," *Neural Network World*, vol. 17, no. 4, p. 377, 2007.

[39] W. A. Mahmoud and R. A. Jassim, "Image Denoising Using Hybrid Transforms," *Engineering and Technology Journal*, vol. 25, no. 5, 2007.

[40] W. A. Mahmoud, J. J. Stephan, and A. A. W. Razzak, "Facial Expression Recognition Using Fast Walidlet Hybrid Transform," *Journal Port Science Research*, vol. 3, no. 1, pp. 59–69, 2020.

[41] E. Candes, L. Demanet, D. Donoho, and L. Ying, "Fast discrete curvelet transforms," *multiscale modeling & simulation*, vol. 5, no. 3, pp. 861–899, 2006.

[42] M. N. Do and M. Vetterli, "Orthonormal finite ridgelet transform for image compression," *in Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101), IEEE*, 2000, pp. 367–370.

[43] M. I. M. Al-Khuzaay and W. A. M. Al-Jawher, "New Proposed Mixed Transforms: CAW and FAW and Their Application in Medical Image Classification," *International Journal of Innovative Computing*, vol. 13, no. 1–2, pp. 15–21, 2022.

[44] A. A. Abdul-Kareem and W. A. M. Al-Jawher, "URUK 4D Discrete Chaotic Map for Secure Communication Applications," *Journal Port Science Research*, vol. 5, no. 3, pp. 131–142, 2022.

[45] A. A. Abdul-Kareem and W. A. M. Al-Jawher, "A Hybrid Domain Medical Image Encryption Scheme Using URUK and WAM Chaotic Maps with Wavelet–Fourier Transforms," *Journal of Cyber Security and Mobility*, pp. 435–464, 2023.

Biographies

Qutaiba Kadhim Abed earned a Bachelor from Diyala University in Diyala, Iraq, in 2014 and a Master of Science in Computer Science from Diyala University in Diyala, Iraq, in 2019. Currently, he is a Ph.D. candidate at the Iraqi Commission for Computers and Informatics, Information Institute for Postgraduate Studies in Baghdad, Iraq. His research interests are image encryption, chaos, compressive sensing, and optimization algorithms.

Waleed Ameen Mahmoud Al-Jawher President Assistance for Scientific Affairs, University of Uruk, Iraq. He received a School of Research in Digital Signal Processing (2005). He received his Ph.D. in Digital Signal Processing from the University of Wales, United Kingdom (1986). He has a teaching experience in Computer Science and Communication engineering for 44 years. A total of (15) National Awards. He published over (290) papers and supervised more than (210) MSc and PhD Students. He was the First Professor Award at the University of Baghdad, Iraq. His present areas of research interest are the field of Digital Signal Processing and its applications.