





Lorenz, Rossler, and Chan systems for key generation and pixel selection in chaotic image encryption

Raghad Abed Sahun ¹, Aws Hamed Hamad ^{2*}, Lamis Hamood Al-saadi ³, Ameer K. Jawad ⁴

¹Physics Department, College of Sciences, Mustansiriyah University, Baghdad, Iraq

²Biotechnology Research Center, Al-Nahrain University, Baghdad, Iraq

³Department of Mathematical, College of Education for Pure Science, University of Babylon, Iraq

⁴Faculty of Engineering and Information Technology, Al-Zahraa University for Women, Karbala, Iraq

ARTICLE INFO

Received: 12/06/2025

Accepted: 25/08/2025

Available online: 19/11/2025

December Issue

[10.37652/juaps.2025.161423.1435](https://doi.org/10.37652/juaps.2025.161423.1435)

 CITE @ JUAPS

ABSTRACT

The increasing need for secure multimedia communication has driven the development of more robust encryption schemes. This paper introduces a novel chaotic image encryption algorithm that uniquely integrates three different chaotic systems, including Lorenz, Rossler, and Chan, to generate a highly unpredictable, non-sequential encryption process. Unlike prior dual-system approaches, the proposed method assigns distinct roles to each chaotic system for key generation, pixel selection, and indexing, thereby enhancing both confusion and diffusion properties while maintaining low computational overhead. The three proposed chaotic systems, Lorenz, Rossler, and Chan, introduce a high level of randomness in the encryption process. Lorenz system generates chaotic random integer numbers (CRINs) as encryption keys to ensure unpredictability. Rossler system randomly selects nonsequential pixel indices to enhance diffusion. Chan system applies an XOR operation between the selected image pixels and the generated chaotic keys and encrypt image with highly resistant to decryption attempts. The Diffie-Hellman key exchange protocol was also incorporated to share encryption keys between parties securely. Multiple image quality assessment metrics were used to evaluate the proposed algorithm's effectiveness. The results indicated that the encrypted images exhibited significant distortion with a Mean Squared Error (MSE) of 9254.5 and a Peak Signal-to-Noise Ratio (PSNR) of 8.4673 dB, indicating strong encryption. The Structural Similarity Index Measure (SSIM) was very low (0.000604), reflecting high image scrambling. The encrypted image's entropy was 7.9997, nearing the ideal value of 8, ensuring maximum randomness. The decryption process accurately reconstructed the original image with an SSIM of 1 and zero MSE, with encryption and decryption times of 0.409s and 0.369s, respectively. The proposed encryption algorithm offers an effective solution for protecting digital images in public communication channels. Integrating chaotic systems with a structured encryption framework shows strong resistance to modern cryptographic threats. This approach is particularly valuable in high-security areas such as military operations, medical data transfer, and confidential communications.

Corresponding author

Aws Hamed Hamad

aws.hamed@rdd.edu.iq

Keywords: *Chaos, Correlation, Cryptography, Key space, Real-time encryption*

1 INTRODUCTION

The risk of losing sensitive information online has escalated with increased multimedia data exchange, particularly for digital images used in fields like health-

care, military, and finance [1, 2]. Images are more susceptible to statistical and differential attacks due to their high redundancy, strong spatial correlations, and complex data structure [3, 4]. Traditional encryption

methods are inefficient for image data, leading to slow processing speeds [5]. These have escalated the need for secure and low-complexity encryption techniques that can withstand cryptographic attacks and meet real-time requirements.

Chaotic systems have brought much more attention as one of the ideal image encryption methods. The nature of chaos theory provides ideal properties, such as extreme sensitivity to initial conditions, pseudo-randomness, and ergodicity. These properties make it a highly suitable option for cryptographic purposes [6–9]. Chaotic-based encryption provides maximum unpredictability because it is less susceptible to brute-force, statistical, and differential attacks than conventional encryption techniques [10, 11]. Image encryption has been well studied, involving several chaotic maps, such as the Lorenz, Logistic, Henon, and Rossler systems. [12, 13] On the other hand, most existing schemes have some limitations, such as poor key sensitivity, low entropy, or insufficient security against Chosen-Plaintext Attacks (CPA). Therefore, a better and faster chaos-based image encryption algorithm is trying to tackle these challenges [14].

The novelty of this work lies in its architectural design. It assigns separate roles to three chaotic systems in a non-sequential fashion, including CRIN generation via Lorenz, key indexing via Rossler, and pixel selection via Chan. This structure significantly improves resistance to statistical analysis and brute-force attacks compared to previous dual-chaotic or hybrid designs.

In this work, three types of chaotic systems (Lorenz, Rossler, and Chan) are combined as an innovative image encryption algorithm to improve the security and efficiency of the encryption process. The method deployed by the LRC encryption algorithm uses chaotic dynamics and gains high randomization in choosing keys and pixels. Thus, attaining good diffusion and confusion properties. The study makes the following key contributions:

- Chaotic key generation — Generating chaotic random integer numbers (CRIN) used as encryption keys by working with Lorenz, Rossler, and Chan chaotic systems.
- Random Pixel Selection – Using chaotic sequences to randomly or obliviously select non-sequential pixel positions, thus increasing randomness.
- XOR Ciphering – XORing the chaotic key values with the pixel values to strengthen security.

- Extensive Security Analysis—The accuracy of encryption measurement is evaluated via performance metrics, including MSE, PSNR, SSIM, Entropy, UACI, NPCR, Histogram, and Correlation measurements.

The main goal of this study is to design a robust and computationally efficient image encryption algorithm that can keep digital images safe from cryptanalytic attacks. Our approach is intended for a large key space, good randomness, high attack resistance, and low time complexity to be practical in real-time applications. This research advances media security in several fields, including medical imaging, confidential picture transfer, and military communications. An integrated, high-dimensional combination of chaotic systems generates encryption complexity and unpredictability in the suggested method. Results demonstrated that the proposed approach outperforms other chaotic encryption algorithms in security, efficiency, and robustness, advancing the field of chaotic cryptography.

2 LITERATURE REVIEW

Numerous approaches have been proposed in chaotic image encryption. These can be grouped into the following categories:

2.1 Single-system chaos-based methods

Several studies have employed a single chaotic map, such as Logistic or Lorenz, for generating key streams or performing direct pixel transformations. For instance, in [15], a random sequence and XOR operation were used to obscure images based on a single chaotic source. Although these techniques are simple and computationally light, they typically suffer from limited key space, poor diffusion, and lower resistance to statistical attacks.

2.2 Dual-system chaotic encryption

Some works used two chaotic systems to improve confusion and diffusion. In [16], a two-layer image encryption algorithm was proposed using Lorenz and Rossler systems in a direct XOR-based structure. While such combinations slightly enhance randomness, they often lack flexible architecture and do not offer clear separation of roles between the systems involved.

2.3 Hybrid chaos-based techniques

Several researchers have combined chaotic maps with classical encryption schemes to form hybrid systems.

In [17], chaotic maps were integrated with an enhanced AES algorithm. In [18], an intelligent codebook method was combined with RSA for smart encryption. Similarly, [19] proposed a TIC system merging zigzag scanning, RSA, and Duffing/Lu chaotic systems. While in [20], discrete orthogonal moments and a modified logistic chaotic map were employed along with Charlier polynomials. These hybrid schemes often yield high complexity and resource requirements, limiting their practicality in real-time scenarios.

2.4 Advanced multi-stage chaotic architectures

Some studies presented multi-phase chaotic frameworks. In [21], a triple-stage encryption process was introduced. Reference [22] employed a hybrid parallel DES, Present algorithm using a 2D chaotic map. In [23], a sine-cosine chaotic map was used for a bit-plane-based medical image cryptosystem. In [24], a dual-domain approach was proposed for secure communication. These methods offer layered security but often suffer from sequential processing and limited adaptability.

2.5 Chaos with bio-inspired or mathematical transforms

A number of techniques incorporate chaotic systems with bio-inspired or mathematical encoding. For example, [25] proposed a DNA-based encryption scheme to secure medical images. In [26], a 24×24 nonlinear transformation was integrated with DNA to form a symmetric encryption structure. While these methods increase the encoding complexity, their real-time feasibility and general applicability are still under exploration.

2.6 Research gap and motivation

Despite the diversity of existing encryption schemes, many studies fall short in terms of fully utilizing chaotic dynamics. Most either rely on a single or dual chaotic map with direct XOR operations, lack a modular structure with well-defined roles for each chaotic system, or sacrifice speed and flexibility for layered security.

This paper addresses these limitations by proposing a lightweight yet fully chaotic encryption system using three distinct chaotic maps (Lorenz for CRIN generation, Rossler for dynamic indexing of CRIN keys, and Chan for chaotic pixel selection), each with a unique and non-overlapping role in the encryption process. This architecture achieves high key sensitivity, strong confusion and diffusion, and real-time performance without relying on

classical cryptographic primitives.

3 DEFINITION AND TYPES OF CHAOS

Chaotic signals are dynamical and non-periodic signals that look random. An interactive system has a fixed number of independent state variables governed by ODEs that involve all state variables [10, 27–29]. Chaotic state variables in dynamical systems fluctuate in a limited, non-periodic, random manner [30]. In addition, they possess a sensitive dependency trait in the parameters and initial values, meaning that any two same initial values will result in the same result. The slight difference in initial values leads to radically different results. This characteristic enables the creation of an endless number of chaotic signals from the same system with various initial values [31]. The types of chaos are chaotic maps and chaotic flows. A chaotic map is an evolution function that behaves in some way. A discrete-time can be used to parameterize chaotic maps. Kth iterated functions are the typical representation of discrete maps. Famous examples of chaotic maps include the logistic map [32], the Duffing map [33], and the Henon map [34]. While the continuous-time system of chaotic flow has obtained a set of differential equations [35], numerous well-known chaotic flow systems exist, including the Lorenz, Rössler, and Chan systems.

3.1 Mathematical modeling of selected chaotic systems

3.1.1 Lorenz system

Edward Lorenz, a meteorologist and mathematician, was the first to investigate the Lorenz system, which consists of a collection of ordinary differential equations (ODEs). The development of a more basic mathematical model of atmospheric convection occurred in 1963. Three ordinary differential equations, known as the Lorenz equations, comprise the model [9, 10, 27].

$$\begin{aligned}\dot{x} &= \sigma(y - x) \\ \dot{y} &= rx - y - xz \\ \dot{z} &= xy - bz\end{aligned}\tag{1}$$

Where \dot{x} , \dot{y} and \dot{z} are the state vectors of the Lorenz system; σ , r , and b are the Lorenz parameters equal to 10, 28, and $8/3$, respectively [11, 36]. All the state vectors and the 3D strange attractors are shown in Figure 1.

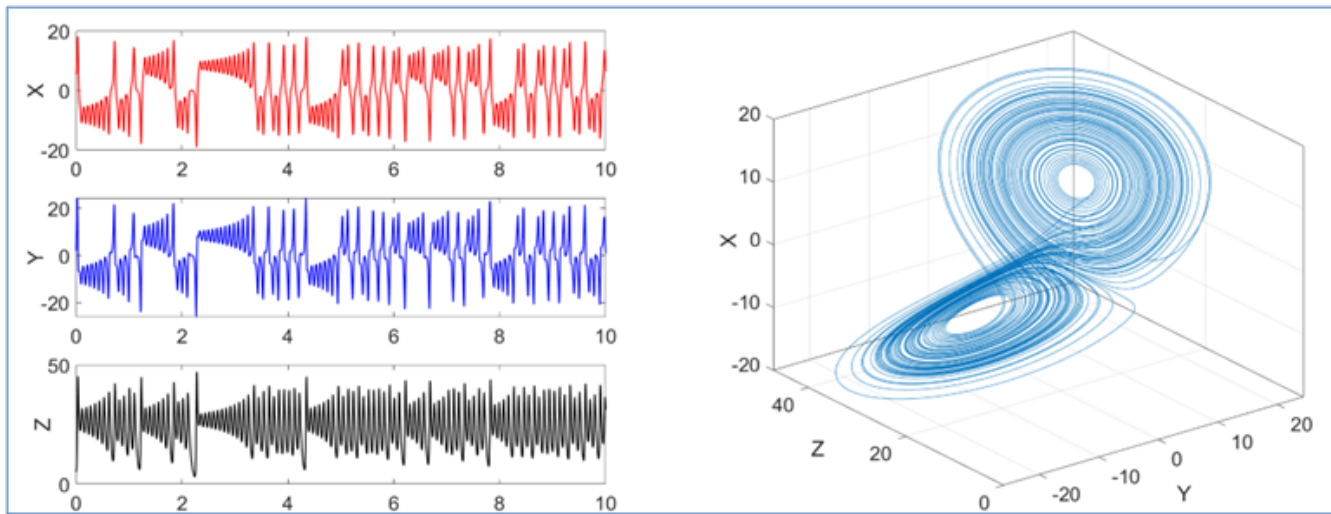


Fig. 1 Time series X, Y, and Z of the Lorenz system and 3D strange attractor [8]

3.1.2 Rossler system

The Rossler system is a three-dimensional (\dot{x} , \dot{y} and \dot{z}) with three-parameter (a , b , and c) chaotic system [29,37]. All state vectors and strange attractors are shown in Figure 2.

The following equations describe the Rossler system:

$$\begin{aligned}\dot{x} &= -(y + z) \\ \dot{y} &= ay + x \\ \dot{z} &= b + z(x - c)\end{aligned}\quad (2)$$

The control parameters a , b , and c are equal to 0.2, 0.2, and 5.7, respectively.

3.1.3 Chan system

A three-dimensional (\dot{x} , \dot{y} and \dot{z}) chaotic system with three parameters (a , b , and c) is the Chan system [38–40]. In Figure 3, every state vector and strange attractor are displayed. The following equations explain the Chan system:

$$\begin{aligned}\dot{x} &= a(y - x) \\ \dot{y} &= (c - a)x + cy - xz \\ \dot{z} &= xy - bz\end{aligned}\quad (3)$$

The parameters a , b , and c are equal to [3, 24, 35], respectively.

3.2 Lyapunov exponent (le)

Lyapunov Exponent (LE), the divergence rate average of near locations along an orbit, measures chaotic functions' sensitive dependency on initial conditions [41,42].

If all LEs are less than zero, the orbit is attracted to a fixed or stable point; if all LEs are zero, there is an ordinary attractor, indicating neutral stability and constant separation; and if at least one LE is positive, the dynamic is chaotic. The LE values of the Lorenz, Rossler, and Chan chaotic systems are shown in Table 1.

$$\lambda = \lim_{k \rightarrow \infty} \frac{1}{k} \sum_{j=1}^k \ln \left| \frac{\Delta D_j}{\Delta D_0} \right| \quad (4)$$

Table 1 Lyapunov exponents of the Lorenz, Rossler, and Chan systems

Chaotic System	λ_1	λ_2	λ_3
Lorenz System	0.8319	0.0059	-14.504
Rossler System	0.0505	0.0093	-5.3934
Chan System	1.9447	0.0024	-15.947

A positive Lyapunov exponent ($\lambda_1 > 0$) means the system is chaotic. This shows that small changes in the starting values grow quickly over time, making the system unpredictable. This property is very important in encryption because it helps create highly sensitive and secure keys.

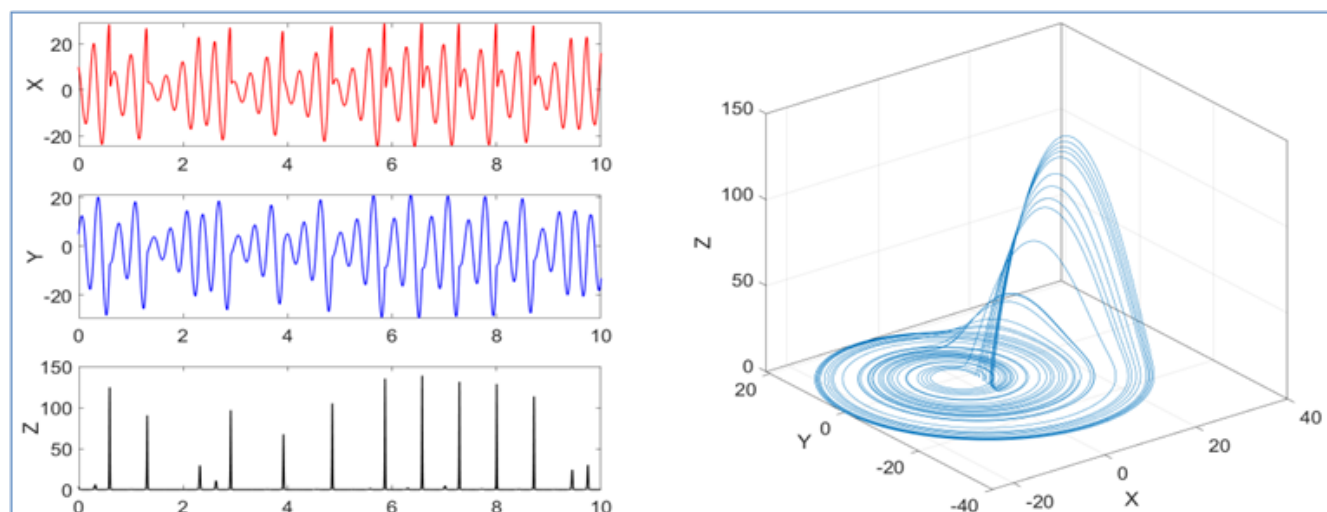


Fig. 2 Rossler system time series X, Y, Z, and 3D strange attractor [8]

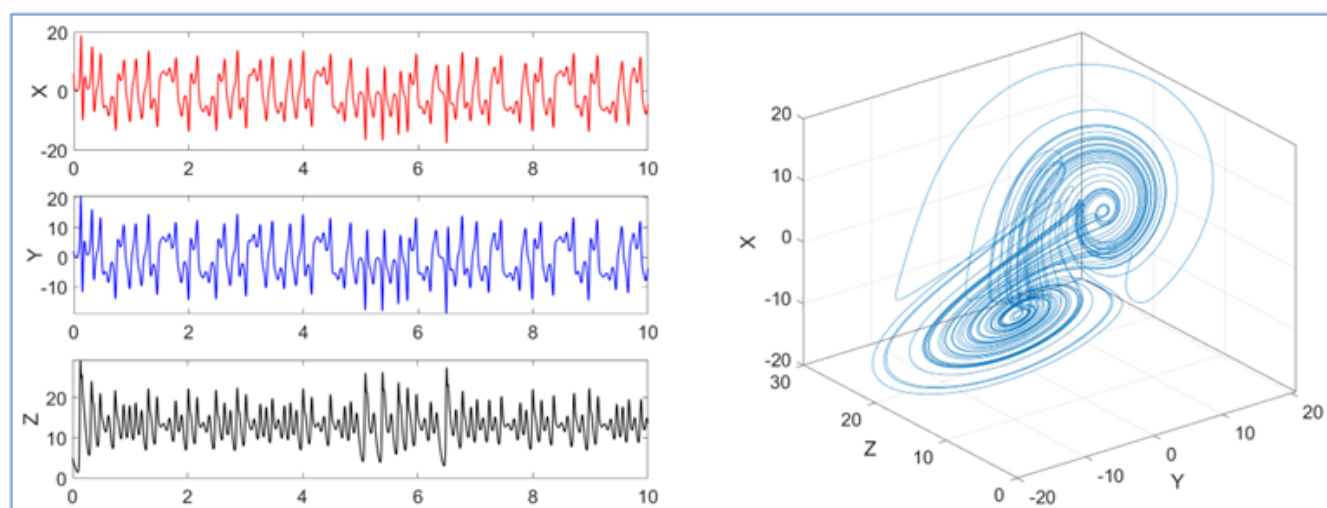


Fig. 3 Time series X, Y, and Z of the Chan system and 3D strange attractor [8]

4 METHODOLOGY OF THE PROPOSED IMAGE ENCRYPTION

This section details the proposed image encryption methodology based on a hybrid chaotic system named LRC, which incorporates three distinct chaotic generators: Lorenz, Rossler, and Chan systems. The architecture is illustrated in Algorithm 1 and Figure 4.

Algorithm 1: Proposed Image Encryption Algorithm using Lorenz-Rössler-Chan (LRC) Systems

Data: Original image I of size $M \times N$, secret initial values and parameters for Three Chaotic Systems (Lorenz, Rössler, and Chan).

Result: Encrypted image E .

- 1-Initialize parameters and initial conditions for Lorenz, Rössler, and Chan systems
- 2-Generate chaotic sequences X_L, Y_L, Z_L from the Lorenz system
- 3-Generate CRIN from X_L using:
 $CRIN(i) = \text{mod}(\text{Fix}(X_L(i) * \text{BigNumber}), 255) + 1$
- 4-Generate chaotic sequences XR from Rossler and XC from Chan
- 5- Convert Rossler and Chan sequences to index selectors (for CRIN and pixels)
- 6- For each pixel index i in the image:
 - a. Select pixel $P(i)$ from I using Chan-based selector
 - b. Select key $K(i)$ from CRIN using Rossler-based selector
 - c. $E(i) = P(i) \text{ XOR } K(i)$

Return Encrypted image E

The LRC system was designed by integrating three chaotic signal generators, each responsible for different phases of the encryption pipeline. These generators create dynamic sequences based on chaotic flows, which were used to select, modify, and shuffle pixel values in the input image. The system consisted of the following core components: First Chaotic Signal Generator (based on the Lorenz chaotic systems), Second Chaotic Signal Generator (typically a different chaotic flow (Rossler system)), and Third Chaotic Signal Generator (the final system, such as Chan, contributing to pixel-level random-

ization). Each chaotic system operates independently with unique initial conditions and parameters to ensure high entropy and complex transformation patterns.

Step 1. Chaotic Random Integer Numbers (CRIN) Generation The first chaotic generator produces a continuous chaotic sequence X_{chaos} , which is then transformed into a discrete integer sequence known as Chaotic Random Integer Numbers (CRIN) using the following formula:

$$CRIN = \text{fix} \left(X_{chaos} * 10^{10} \% 255 \right) + 1 \quad (5)$$

This equation ensures that each chaotic value is scaled, modularly wrapped within the 8-bit pixel intensity range of 0–254, and then incremented by 1. The addition of +1 is essential to guarantee that all CRIN values lie strictly between 1 and 255, avoiding the zero value. This equation has been widely adopted in previous chaos-based encryption schemes. It ensures a proper mapping of continuous chaotic values to 8-bit integer keys. Relevant works that employed a similar CRIN formulation are explained in [7, 15].

Step 2. Chaotic Random Selection from CRIN The second chaotic generator (Rossler system) creates another chaotic sequence, which serves as a selector over the previously generated CRIN values. This step adds a second layer of nonlinearity by chaotically sampling from the CRIN sequence. The resulting output defines a dynamic and unpredictable pattern used to alter the spatial structure of the image, i.e., to shuffle pixel positions or rows/columns.

Step 3. Chaotic Pixel Value Permutation Simultaneously, the third chaotic generator (Chan system) is applied directly to the original image pixels. A chaotic random selector generated from this signal determines which pixels are selected and how their intensities are modified. This operation focuses on pixel-level confusion to ensure that each pixel in the encrypted image differs significantly from its original counterpart.

Step 4. Final Encryption Phase The results from the pixel shuffling (based on the first and second chaotic generators) and pixel value permutation (based on the third chaotic generator) were combined through a mixing operation, typically XOR or modular addition. This step produced the final encrypted image, as shown in Figure 5. The use of three different chaotic flows increases the complexity of the key space and boosts resistance to known cryptographic attacks.

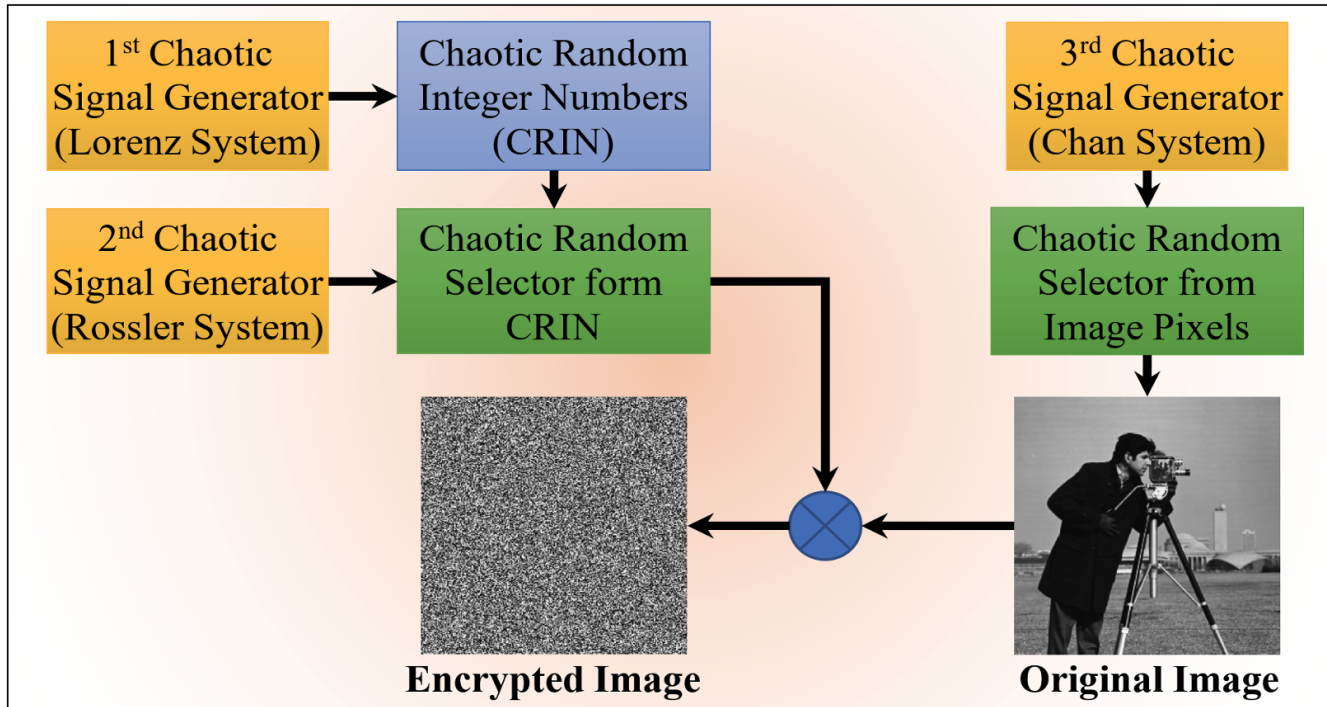


Fig. 4 The proposed system for image encryption

5 IMAGE TESTING QUALITY

In this section, seven different statistical tests were run with three different image sizes to determine the safety and efficiency of the proposed cryptographic system. The Histogram graph, mean squared error (MSE), peak signal to noise ratio (PSNR), correlation (Corr), and entropy are some of the performance tests that were used. Along with the time of the encryption process (delay per second).

5.1 Mean square error (mse)

The MSE is the most commonly used estimate for measuring image quality. It is a comprehensive reference measure, with better results for values closer to zero [43].

$$MSE = \frac{1}{MN} \sum_{n=0}^M \sum_{m=1}^N [O(n, m) - E(n, m)]^2 \quad (6)$$

In this equation, O and E represent the unencrypted and encrypted versions of the picture, respectively. When MSE equals 0, the encryption fails to obscure the original image's features.

5.2 Peak signal-to-noise ratio (psnr)

The peak signal-to-noise ratio (PSNR) can help evaluate the encryption strategy by comparing the original and encrypted images' pixel values, which can be calculated using equation 7.

$$PSNR_{db} = 10 * \log_{10} \left[\frac{M * N * 255^2}{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (O(i_j) - E(i_j))^2} \right] \quad (7)$$

Two images, O and E , and two sizes, M and N , are involved. Low PSNR favors encryption [43].

5.3 Structural similarity index measure (ssim)

SSIM guesses how good digital pictures and videos will be. The software uses a full reference metric on an uncompressed or distortion-free image to find related images. Between two standard-sized $N*M$ windows, the SSIM index was calculated for various image windows.

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1) (2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1) (\sigma_x^2 + \sigma_y^2 + c_2)} \quad (8)$$

- μ_x, μ_y are the average of x and y respectively.
- σ_x^2, σ_y^2 the variance of x and y , σ_{xy} The covariance

of x and y .

- $c_1 = (k_1 L)^2$, $c_2 = (k_2 L)^2$ two variables to stabilize the division with a weak denominator.
- L the dynamic range of the pixel values (typically is $2^{\text{bits per pixel}} - 1$)
- $k_1 = 0.01$, $k_2 = 0.03$ by default [44].

5.4 Entropy

Entropy analysis evaluates encryption and randomness. Compare the plain and cipher images' entropy to assess encryption quality. Calculating image entropy:

$$\text{Entropy} = \sum_{i=0}^{2^n-1} \left[p(i) * \log_2 \left(\frac{1}{p(i)} \right) \right] \quad (9)$$

The bit-valued I probability is $p(i)$. The maximum entropy for images with 256 gray levels (0–255) is 8, which is optimal randomness. Practical image entropy is less than maximal [43].

5.5 The correlation coefficient (cc)

The similarity between two images may be calculated using the correlation coefficient.

$$CC = \frac{\sum_{i=1}^N (x_i - E(x)) (y_i - E(y))}{\sqrt{\sum_{i=1}^N ((x_i - E(x)))^2} \sqrt{\sum_{i=1}^N ((y_i - E(y)))^2}} \quad (10)$$

where $E(x) = \frac{1}{N} \sum_{i=1}^N x(i)$, x and y are the pixel values of the original and encrypted images, respectively. The correlation coefficient in image encryption measures the strength and direction of a linear relationship between two variables. It has a perfect positive correlation of 1 and a perfect negative correlation of -1. A low correlation coefficient, near zero, indicates no correlation between original and encrypted images [7, 8, 43]. The three types of correlation plots are vertical (V), horizontal (H), and diagonal (D).

5.6 Histogram

A histogram shows the distribution of pixel values by plotting the number of pixels at each color intensity level. It quickly and easily evaluates image encryption methods by ensuring pixel value consistency [30, 43].

6 TESTED IMAGES USED TO EVALUATE THE LRC ALGORITHM

Five standard digital images with different sizes, color channels, and entropy values were selected to evaluate the performance of the proposed encryption system, as shown in Figure 5.

Baboon, Peppers, Lena, Rod, and Cameraman images were selected that cover both grayscale (Cameraman) and color images (the others), with various dimensions and entropy levels ranging from 7.0097 to 7.7629, which reflects the degree of information content in each image.

7 ENCRYPTION AND DECRYPTION RESULTS

The effectiveness of the proposed chaotic image encryption system was evaluated through both numerical metrics and visual analysis. Objective results such as MSE, PSNR, SSIM, Entropy, and correlation coefficients were used to quantitatively assess the quality of encryption and decryption. In parallel, visual inspections, including image appearance, histogram distribution, and pixel correlation plots, provide qualitative insights into the system's ability to obscure and recover image content. Together, these results offer a comprehensive validation of the system's security strength, reversibility, and resistance to statistical attacks (Tables 2 and 3) (Figures 6 and 7).

7.1 Encryption and decryption performance

As indicated in Table 2, the Mean Square Error (MSE) values for all images are significantly high, reflecting a large difference between the original and encrypted versions. Consequently, the PSNR values are low (ranging from 7.6 dB to 8.7 dB), which confirms that the encrypted image is highly distorted and visually unrecognizable, a crucial property for secure encryption. Moreover, the Structural Similarity Index (SSIM) values for the encrypted images are all near zero or even negative, indicating the absence of any structural similarity between the original and encrypted images. This is desirable and further verifies the system's ability to prevent attackers from extracting meaningful information through visual inspection or structural analysis. Regarding entropy, all encrypted images recorded values very close to the ideal maximum of 8 for 8-bit images. The values range between 7.9974 and 7.9998, suggesting that the pixel values in the encrypted images are evenly distributed. This uniform distribution hinders any statistical attack based on frequency analysis, as the encrypted data no

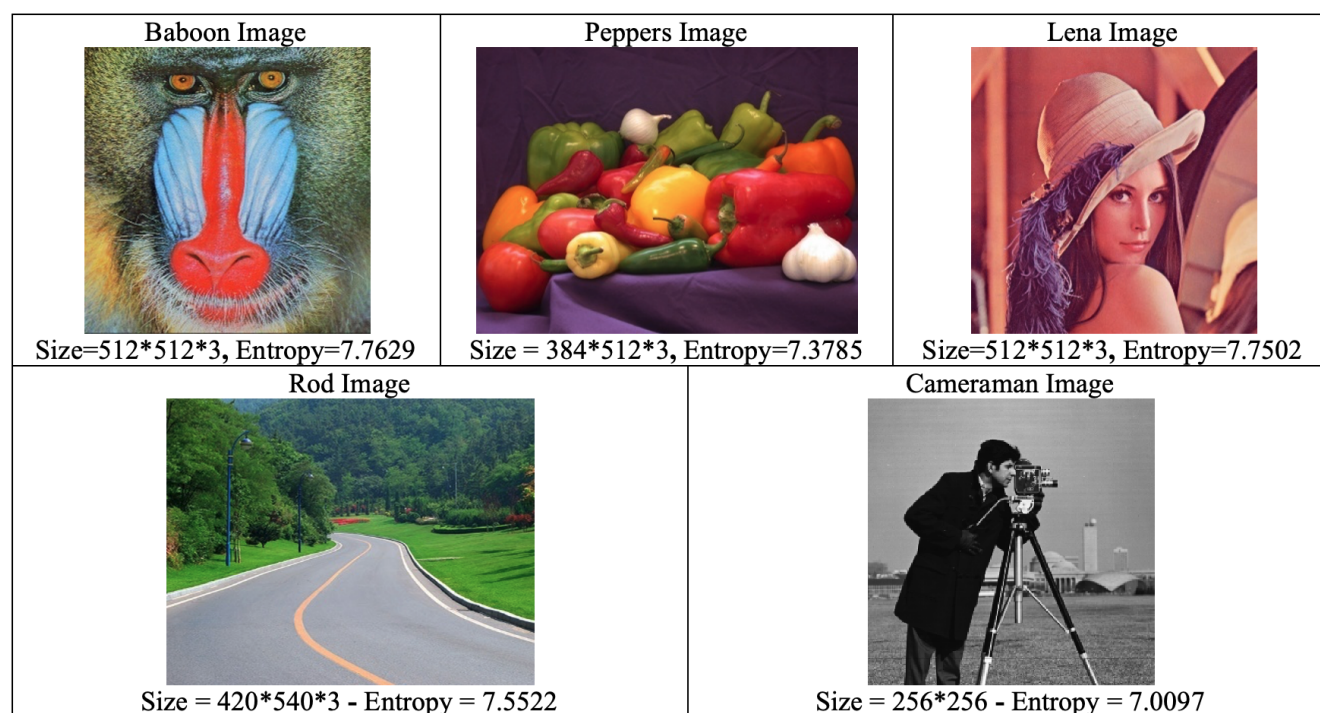


Fig. 5 The Digital Images used for testing the proposed encryption system

longer follows the predictable patterns of the original image. The delay time ranges from approximately 0.02 to 0.14 seconds, depending on image sizes. These values reflect the efficiency of the encryption algorithm, especially considering that the chaotic key generation and encryption steps are computationally intensive. The low processing time demonstrates that the proposed scheme is not only secure but also suitable for real-time or near-real-time applications.

7.2 Decryption accuracy

As shown in Table 3, the proposed system successfully reconstructs the original image without any loss of quality. The MSE values are zero and PSNR values are infinite for all test images, indicating perfect reconstruction. Similarly, the SSIM values are exactly 1, meaning full structural preservation. This result confirms the high reliability of the system and its capacity for lossless recovery. The decryption entropy values also match the original images exactly, proving that no information was lost or altered during the process. The decryption delay remains similar to the encryption time, which is expected due to the symmetric nature of the system.

Table 2 Objective Encryption Results for the Proposed System.

Image	MSE	PSNR (dB)	SSIM	Entropy	Delay (Sec)
Baboon	8637.1	8.7671	0.00025	7.9998	0.1433
Peppers	11240	7.6232	0.000464	7.9997	0.1068
Lena	8935	8.6199	0.000431	7.9998	0.1410
Rod	9286	8.4521	0.000604	7.9997	0.1204
Cameraman	9429.4	8.3860	-0.00079	7.9974	0.0205

Table 3 Objective Decryption Results for the Proposed System.

Image	MSE	PSNR (dB)	SSIM	Entropy	Delay (Sec)
Baboon	0	Inf	1	7.7629	0.1523
Peppers	0	Inf	1	7.3785	0.1290
Lena	0	Inf	1	7.7502	0.1572
Rod	0	Inf	1	7.5522	0.1266
Cameraman	0	Inf	1	7.0097	0.0162

7.3 Histogram analysis

The histogram analysis of the Lena image (Figures 6 and 7) further supports the encryption strength. The histogram of the original image shows clear peaks and valleys, reflecting the non-uniform distribution of pixel intensities. In contrast, the encrypted image exhibits a flat histogram, where pixel values are uniformly distributed across all intensity levels in the R, G, and B channels. This randomness indicates that the encryption algorithm successfully conceals statistical information, making it resistant to histogram-based attacks. After decryption, the histogram is restored identically to the original, which demonstrates the accuracy of the decryption process and confirms the reversibility of the system.

7.4 Pixel correlation analysis

Coordination between nearby pixels indicates image encryption. Smooth transitions and spatial continuity make neighboring pixels in natural images highly correlated. In the Lena image, the original image has vertical correlation values of 0.98503, horizontal correlation values of 0.97193, and diagonal correlation values of 0.95933. These numbers plummet to -0.00022, -0.000652, and 0.00153 after encryption. These near-zero values show that the encrypted image has no substantial association between neighboring pixels in any direction, indicating effective confusion and randomization. This comprehensive decorrelation prevents pixel proximity-based statistical or predictive attacks.

7.5 Decryption accuracy

It is worth noting that some decryption results (e.g., MSE = 0, PSNR = ∞ , SSIM = 1) are identical to those reported in other works such as Ref [16]. This is expected, as these metrics represent perfect reconstruction and are mathematically deterministic when the decryption process is lossless and the original image is standard (e.g., Lena or Peppers). Hence, such similarity is not indicative of redundancy but rather of successful decryption.

8 KEY SENSITIVITY AND KEY SPACE

8.1 The key sensitivity

If there is even the slightest difference in the encryption and decryption keys, the encrypted signal will no longer be reliably decoded. Sensitivity is crucial for all safe cryptosystems. This means the attackers cannot obtain any information by changing even a single element of the key, the starting state of X0, Y0, or Z0,

by a small amount, as shown in Table 4. It shows that the suggested encryption scheme is highly sensitive to chaotic key settings. Changing even a small amount of initial conditions or control parameters can cause image recovery failure, even if all other keys stay identical. The technology is resilient to key-related attacks since even minor modifications prohibit correct decryption. When evaluated under such modest variations, the third chaotic generator (Chan system) yields lower encryption distortion (i.e., greater PSNR values and lower MSE) than the Lorenz and Rossler systems. However, Table 4 shows that the decrypted image's entropy (7.7629) matches that of the encrypted and visually distorted image. Restoring pixel values but not spatial positions explains this. Unreturned values created a jumbled picture. Since pixel value probability distribution remains constant, the entropy metric seems deceptively similar to the original image, while encryption remains visually effective.

Table 4 Hybrid deep learning methods applied to object recognition systems

Chaotic	Value Change	MSE	PSNRdB	Mean CC.	SSIM	Entropy
Lorenz System	$x_0 = x_0 \pm 10^{-15}$	8617.2	8.7771	0.00073	0.00214	7.9996
	$r = r \pm 10^{-15}$	8391.3	8.8922	0.02047	0.00675	7.9995
	$b = b \pm 10^{-15}$	8420.3	8.8775	0.01808	0.00550	7.9997
Rossler System	$y_0 = y_0 \pm 10^{-15}$	8623.5	8.7740	-0.00056	0.00023	7.9998
	$a = a \pm 10^{-15}$	8631.5	8.7700	-0.00146	0.00029	7.9997
	$c = c \pm 10^{-15}$	8604.7	8.7834	0.00120	0.00197	7.9998
Chan System	$z_0 = z_0 \pm 10^{-15}$	6323.4	10.121	-0.00122	0.00184	7.7629
	$b = b \pm 10^{-15}$	6299.1	10.138	0.00264	0.00218	7.7629
	$h = h \pm 10^{-15}$	6319.1	10.124	-0.00053	0.00022	7.7629

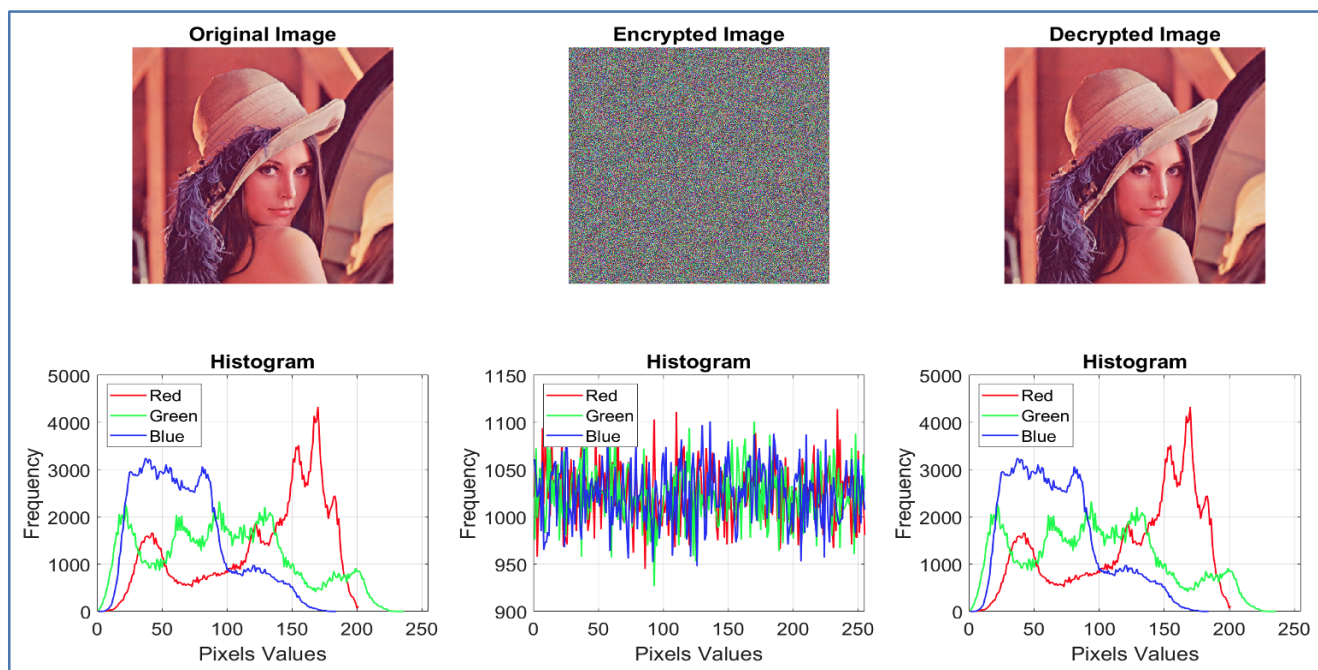
8.2 Key space calculation

A cryptosystem's key space is equal to the number of encrypting keys it has. Large key spaces that can resist brute-force attacks are signs of a good cryptosystem. The accepted key space of an encryption method should usually be bigger than 2100 [45]. These techniques use a full search for keys. People who want to listen need to know the system parameters and starting values in order to use the LRS algorithm to get the original voice from the encrypted signals. For a 10-15 floating point accuracy, each measure has a 1015 range of possible values. It's not possible to know for sure how many keys are in a disordered system, but we can get a good idea of it, as shown by the following equation:

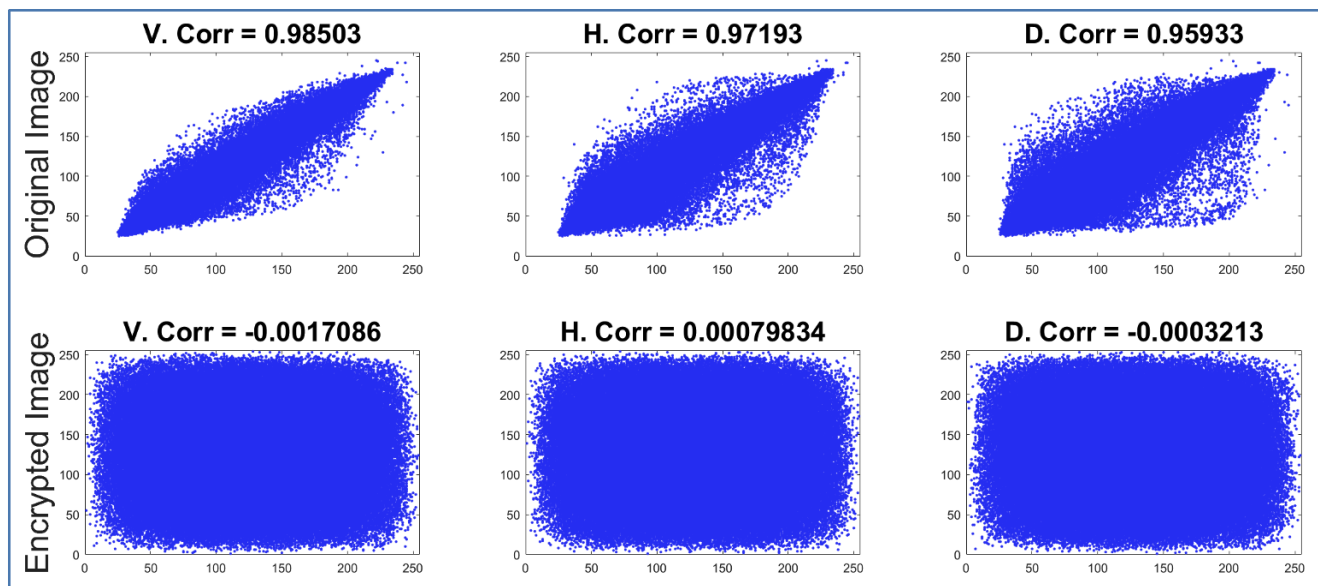
$$\text{Key Space} = \prod_{i=1}^d \frac{1}{s} * \mathbf{R}(i) \quad (11)$$

Where:

- d: Number of Parameters and Initial Values for a chaotic

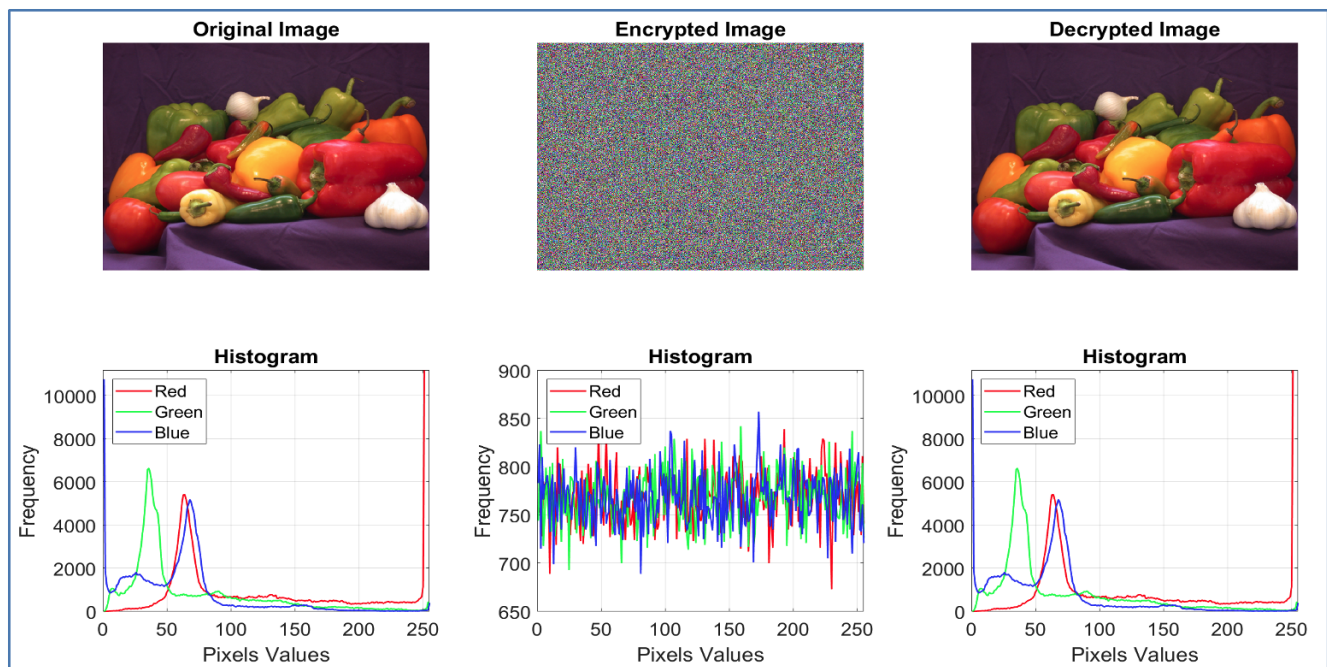


(a) Original encrypted and decrypted Lena images with their histogram

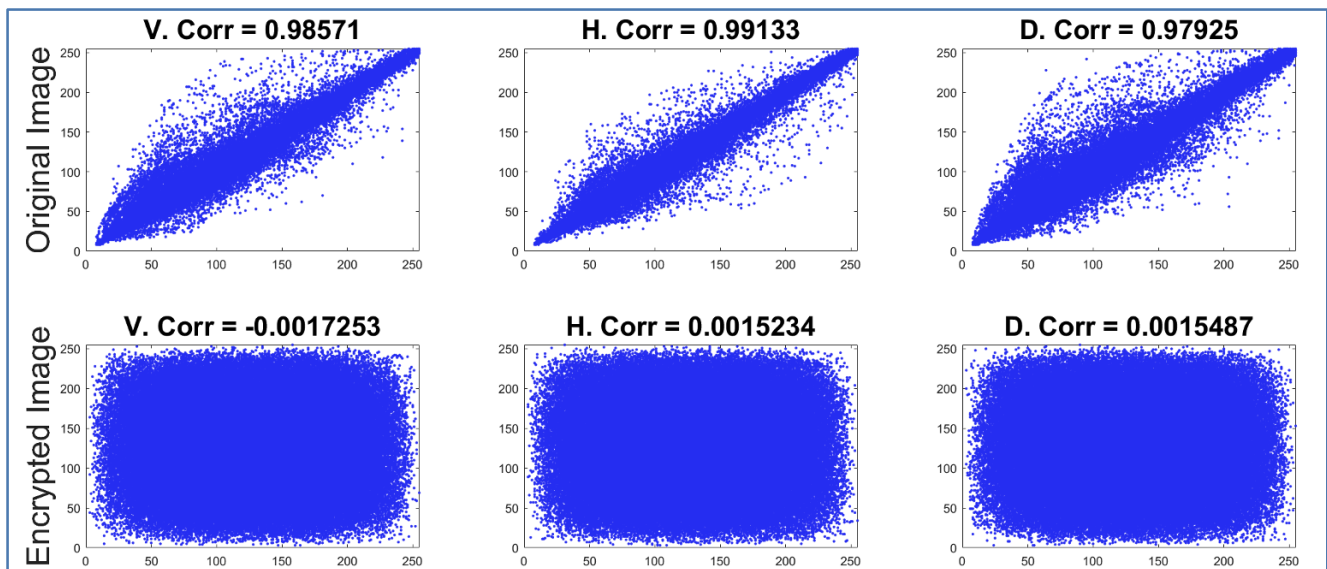


(b) V., H., and D. Sectors and Correlation Values for Lena Original and Encrypted Images

Fig. 6 (a) Original encrypted and decrypted Lena images with their histogram. (b) V., H., and D. Sectors and Correlation Values for Lena Original and Encrypted Images



(a) Original Peppers Images with Their Histogram, Encrypted, and Decrypted



(b) V., H., and D. Sectors and Correlation Values for Peppers Original and Encrypted Pictures

Fig. 7 (a) Original encrypted and decrypted Lena images with their histogram. (b) V., H., and D. Sectors and Correlation Values for Lena Original and Encrypted Images

system.

- *S*: Key Sensitivity for a chaotic system.
- *R*: The system stays within the chaos limits if the difference between the most important and least important values for any initial value or parameter value is large. We assume that *R* is 1, even though it is usually a lot more than 1. This makes the answer easier. If that's the case, there will be more keys than we can count right now.

The proposed system has 3 initial values, 3 parameters, and 2 numbers for step size and big number. All key dimensions equal 8 dimensions. The key for one dimension equal:

$$\text{Key(One System)} \approx (2^{50})^8 = 2^{400} \quad (12)$$

Key space overall system based on Lorenz, Rossler, and Chan systems:

$$\text{All Keys} = (2^{400}_{\text{one system}})^3 = 2^{1200} = 1200 \text{ bits} \quad (13)$$

9 COMPARISON OF THE PROPOSED SYSTEM WITH OTHER RESEARCH

The comparison presented in Table 5 focuses on widely accepted core metrics (MSE, PSNR, Entropy, Correlation, Key Space) that are used consistently in most previous literature. While additional performance aspects such as memory usage and throughput are also important, they are platform-dependent and are often excluded from theoretical or algorithmic comparisons to maintain consistency and fairness.

Although [16] utilizes Lorenz and Rossler systems for image encryption, its structure is fundamentally different from our proposed method. It performs XOR directly between image pixels and chaotic keys, without involving non-sequential indexing or a third chaotic system. Our approach, by contrast, introduces a three-phase system with separated chaotic functions for key and pixel indexing, leading to more complex transformation patterns and improved performance metrics.

10 CONCLUSION

Our proposed chaotic-based image encryption system demonstrates a highly secure, efficient, and robust performance across all evaluation metrics. The encryption process effectively eliminates pixel correlation and achieves high entropy values close to the ideal (≈ 8), indicating a nearly uniform distribution of pixel intensities. The decryption process recovers the original image with

the same accuracy (MSE = 0, PSNR = ∞ , SSIM = 1), confirming the algorithm's reversibility and lossless nature. The system also exhibits strong sensitivity to initial conditions and key parameters. A minor change as small as 10^{-15} in any chaotic system parameter total decryption failure. This high key sensitivity, combined with a vast key space estimated at 1200-bit, ensures exceptional resistance to brute-force attacks. Furthermore, the integration of the three different chaotic systems enhances complexity and unpredictability. Even though the Chan system fails to restore the image visually, however, it preserves the entropy level of the original image. This anomaly is explained by the preservation of pixel values without restoring the correct positions. This emphasizes that entropy alone is not a sufficient measure of success. Additionally, the system executes both encryption and decryption in fractions of a second, supporting real-time feasibility. The structural distortion in encrypted images, as confirmed by low SSIM and high MSE, along with uniform histograms and spectral flattening, further validates the strength of the algorithm. With its modular design and reliance on variable chaotic parameters, the proposed method offers high scalability, making it suitable for a broad range of secure imaging applications. While the proposed encryption scheme was evaluated under ideal transmission conditions, future work will consider analyzing its robustness in noisy channels. This includes simulating scenarios where the encrypted image is partially degraded due to transmission noise and evaluating the ability to reliably recover the original content.

FUNDING SOURCE

No funds received.

DATA AVAILABILITY

N/A

DECLARATIONS

Conflict of interest

The authors declare that no competing of interest.

Consent to publish

All authors consent to the publication of this work.

Ethical approval

N/A

Table 5 Comparing the Proposed Methods with the Other Articles

Ref.	Image	MSE	PSNRdB	Mean CC.	Entropy	Key Space
[16]	Peppers	11262	7.6148	-3.4e-5	7.9997	600 bits
[46]	Peppers	10033	8.1624	0.00175	7.9968	-
	Lena	9199	8.4933	0.0092	7.7396	-
[47]	Peppers	-	-	0.0035	7.9959	-
[30]	Cameraman	-	8.9311	0.6069	7.9973	144 bits
	Peppers	-	8.6262	0.4200	7.9997	
	Lena	-	8.6309	0.4915	-	
[48]	Peppers	-	-	0.0017	7.9976	N/A
	Lena	N/A	-	0.0019	7.9217	
[49]	Cameraman	9445	8.38	-	7.9991	N/A
	Peppers	8413	8.88	-	7.9994	
[24]	Lena	7734.4	9.2465	0.00011	7.9979	148 bits
	Peppers	9255.6	8.4667	0.00015	7.9971	
	Cameraman	9412.1	8.3940	0.00141	7.9972	
[20]	Lena	-	-	0.0912	7.7608	210 bits
Proposed System	Cameraman	9474.5	8.296	-0.0006	7.9997	1200 bits
	Peppers	11259	7.615	0.000201	8	

REFERENCES

- [1] Al-Saadi LHM. Analog Speech Encryption Based On Biorthogonal Transforms. Babylon University/Pure and Applied Sciences. 2013;21(8):2621–2628
- [2] Abbadi. Fast Image Matching in Huge Database. Journal of Computer Science. 2014;10(8):1488–1496. [10.3844/jcssp.2014.1488.1496](https://doi.org/10.3844/jcssp.2014.1488.1496)
- [3] Khalid M, Hussein E, Jawad AK, Jawad A. Digital image encryption based on random sequences and XOR operation. Journal of Engineering and Applied Sciences. 2019;14(8):10331-4
- [4] SHANTHAKUMARI R, MALLIGA S. Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment. Sādhanā. 2019;44(5). [10.1007/s12046-019-1106-0](https://doi.org/10.1007/s12046-019-1106-0)
- [5] Hussein AL-Zahawy BW, Hreshee SS. Encryption Audio Signal with IDEA Technique Enhanced by Chaotic System. In: 2024 3rd International Conference on Advances in Engineering Science and Technology (AEST). IEEE; 2024. p. 96–101. [10.1109/aest63017.2024.10959755](https://doi.org/10.1109/aest63017.2024.10959755)
- [6] Jawad AK, Abdullah HN, Hreshee SS. Secure speech communication system based on scrambling and masking by chaotic maps. In: 2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA). IEEE; 2018. p. 7–12. [10.1109/icasea.2018.8370947](https://doi.org/10.1109/icasea.2018.8370947)
- [7] Jawad AK, Karimi G, Radmelkshahi M. A Novel Digital Audio Encryption Algorithm Using Three Hyperchaotic Rabinovich System Generators. ARO-THE SCIENTIFIC JOURNAL OF KOYA UNIVERSITY. 2024;12(2):234–245. [10.14500/aro.11869](https://doi.org/10.14500/aro.11869)
- [8] Jawad Ak, Karimi G, Radmalekshahi M. A Novel Lorenz-Rossler-Chan (LRC) Algorithm for Efficient Chaos-Based Voice Encryption. In: 2024 3rd International Conference on Advances in Engineering Science and Technology (AEST). IEEE; 2024. p. 114–119. [10.1109/aest63017.2024.10959812](https://doi.org/10.1109/aest63017.2024.10959812)
- [9] Wa'il A, Hussein H, Jawad AK. Enhancement of Image Transmission Using Chaotic Interleaver over Wireless Sensor Network. International Journal of New Technology and Research (IJNTR). 2016;2(7):24-8
- [10] Abdullah HN, Hreshee SS, Jawad AK. Design of Efficient noise reduction scheme for secure speech masked by chaotic signals. Journal of American Science. 2015;11(7):49-55
- [11] Abdullah HN, Hreshee SS, Jawad AK. Noise reduction of chaotic masking system using rep-

- etition method, [unpublished]; 2016. Available: www.researchgate.net/publication/291356303
- [12] Xu D, Li G, Xu W, Wei C. Design of artificial intelligence image encryption algorithm based on hyperchaos. *Ain Shams Engineering Journal*. 2023;14(3):101891. [10.1016/j.asej.2022.101891](https://doi.org/10.1016/j.asej.2022.101891)
- [13] Stoyanov B, Kordov K. Image Encryption Using Chebyshev Map and Rotation Equation. *Entropy*. 2015;17(4):2117–2139. [10.3390/e17042117](https://doi.org/10.3390/e17042117)
- [14] Hamed Hamad A, Yousif Dawod A, Fakhrulddin Abdulqader M, Al_Barazanchi I, Muwafaq Ghani H. A secure sharing control framework supporting elastic mobile cloud computing. *International Journal of Electrical and Computer Engineering (IJECE)*. 2023;13(2):2270. [10.11591/ijece.v13i2.pp2270-2277](https://doi.org/10.11591/ijece.v13i2.pp2270-2277)
- [15] Khalid M, Hussein EA, Jawad AK. Digital Image Encryption Based on Random Sequences and XOR Operation. *Journal of Engineering and Applied Sciences*. 2019;14(8):10331–10334. [10.36478/jeasci.2019.10331.10334](https://doi.org/10.36478/jeasci.2019.10331.10334)
- [16] Albakri AY, Karan O. A Two-Layer For Image Encryption Using Lorenz and Rossler Chaotic Systems. *JMCER*. 2024;2024:9-19
- [17] Chothe RV, Ugale SP, Chandwadkar DM, Shelke SV. Authenticated image encryption using robust chaotic maps and enhanced advanced encryption standard. *Indonesian Journal of Electrical Engineering and Computer Science*. 2025;37(3). [10.11591/ijeecs.v37.i3](https://doi.org/10.11591/ijeecs.v37.i3)
- [18] Sihwail R, Ibrahim D. A New Image Encryption Method Using an Optimized Smart Codebook. *Human Behavior and Emerging Technologies*. 2025;2025(1). [10.1155/hbe2/7807003](https://doi.org/10.1155/hbe2/7807003)
- [19] Al-Kufi MAHJ. Image Encryption Algorithm Using Differential Equations. *Journal of Information Systems Engineering and Management*. 2025;10(7s):276–289. [10.52783/jisem.v10i7s.861](https://doi.org/10.52783/jisem.v10i7s.861)
- [20] A Elanany S, A Karawia A, M Fouda Y. Enhanced Image Encryption Scheme Utilizing Charlier Moments and Modified Chaotic Mapping. *International Journal of Wireless and Microwave Technologies*. 2025;15(1):1–17. [10.5815/ijwmt.2025.01.01](https://doi.org/10.5815/ijwmt.2025.01.01)
- [21] F Yousif S, Salman Hameed A, T Al-Zuhairi D. A Secure Image Cryptographic Algorithm Based on Triple Incorporated Ciphering Stages. *Iraqi Journal for Electrical and Electronic Engineering*. 2024;20(2):1–21. [10.37917/ijece.20.2.1](https://doi.org/10.37917/ijece.20.2.1)
- [22] Jasim SH, Hoomod HK, Hussein KA. Image Encryption Based on Hybrid Parallel Algorithm: DES-Present Using 2D-Chaotic System. *International Journal of Safety and Security Engineering*. 2024;14(2):633–646. [10.18280/ijss.140229](https://doi.org/10.18280/ijss.140229)
- [23] Njitacke ZT, Maghrabi LA, Ahmad M, Althaqafi T. Efficient Bit-Plane Based Medical Image Cryptosystem Using Novel and Robust Sine-Cosine Chaotic Map. *Computers, Materials & Continua*. 2025;83(1):917–933. [10.32604/cmc.2025.059640](https://doi.org/10.32604/cmc.2025.059640)
- [24] Mahalingam H, Veeramalai T, Menon AR, S S, Amirtharajan R. Dual-Domain Image Encryption in Unsecure Medium—A Secure Communication Perspective. *Mathematics*. 2023;11(2):457. [10.3390/math11020457](https://doi.org/10.3390/math11020457)
- [25] Zeenath, DurgaDevi K, Carey M JW. An Efficient Image Encryption Scheme for Medical Image Security. *International Journal of Electrical and Electronics Research*. 2024;12(3):964–976. [10.37391/ijeer.120330](https://doi.org/10.37391/ijeer.120330)
- [26] Shah T, ul Haq T. Construction of 24-by-24 nonlinear layer for symmetric algorithm and its application to data encryption in parallel with DNA transform. *The Journal of Supercomputing*. 2023;80(1):1037–1058. [10.1007/s11227-023-05512-9](https://doi.org/10.1007/s11227-023-05512-9)
- [27] Abdullah HN, Hreshee SS, Karimi G, Jawad AK. Performance Improvement of Chaotic Masking System Using Power Control Method. In: *International Middle Eastern Simulation and Modelling Conference 2022, MESM 2022*; 2022. p. 19-23
- [28] Hreshee SS, Abdullah HN, Jawad AK. A High Security Communication System Based on Chaotic Scrambling and Chaotic Masking. *International Journal on Communications Antenna and Propagation (IRECAP)*. 2018;8(3):257. [10.15866/irecap.v8i3.13541](https://doi.org/10.15866/irecap.v8i3.13541)
- [29] Hussein EA, Khashan MK, Jawad AK. A high security and noise immunity of speech based on double chaotic masking. *International Journal of Electrical and Computer Engineering (IJECE)*. 2020;10(4):4270. [10.11591/ijece.v10i4.pp4270-4278](https://doi.org/10.11591/ijece.v10i4.pp4270-4278)
- [30] Alsaabri HH, Hreshee SS. Robust Image Encryption Based on Double Hyper Chaotic Rabinovich System. In: *2021 7th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*. IEEE; 2021. p. 146–152. [10.1109/iccitm53167.2021.9677722](https://doi.org/10.1109/iccitm53167.2021.9677722)

- [31] Samia R. Solution bounds of the hyper-chaotic Rabinovich system. *Nonlinear studies*. 2017;24(4)
- [32] Rahman Z, Yi X, Billah M, Sumi M, Anwar A. Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home. *Electronics*. 2022;11(7):1083. [10.3390/electronics11071083](https://doi.org/10.3390/electronics11071083)
- [33] Mahdi A, K Jawad A, S Hreshee S. Digital Chaotic Scrambling of Voice Based on Duffing Map. *International Journal of Information and Communication Sciences*. 2016;1(2):16–21. [10.11648/j.ijics.20160102.11](https://doi.org/10.11648/j.ijics.20160102.11)
- [34] Alroubaie ZM, Hashem MA, Hasan FS. FPGA design of encryption speech system using synchronized fixed-point chaotic maps based stream ciphers. *International Journal of Engineering and Advanced Technology*. 2019;8(6):1534–1541. [10.35940/ijeat.f8156.088619](https://doi.org/10.35940/ijeat.f8156.088619)
- [35] Forgia GL, Cavaliere D, Espa S, Falcini F, Latorata G. Numerical and experimental analysis of Lagrangian dispersion in two-dimensional chaotic flows. *Scientific Reports*. 2022;12(1). [10.1038/s41598-022-11350-1](https://doi.org/10.1038/s41598-022-11350-1)
- [36] Li X, Yu H, Zhang H, Jin X, Sun H, Liu J. Video encryption based on hyperchaotic system. *Multimedia Tools and Applications*. 2020;79(33–34):23995–24011. [10.1007/s11042-020-09200-1](https://doi.org/10.1007/s11042-020-09200-1)
- [37] Kaibou R, Azzaz MS. FPGA Implementation of Mixed Robust Chaos-based Digital Color Image Watermarking. In: 2021 International Conference on Networking and Advanced Systems (ICNAS). IEEE; 2021. p. 1–5. [10.1109/icnas53565.2021.9628906](https://doi.org/10.1109/icnas53565.2021.9628906)
- [38] Ahmad M. Chaos Based Mixed Keystream Generation for Voice Data Encryption. *International Journal on Cryptography and Information Security*. 2012;2(1):39–48. [10.5121/ijcis.2012.2104](https://doi.org/10.5121/ijcis.2012.2104)
- [39] Dai W, Xu X, Song X, Li G. Audio Encryption Algorithm Based on Chen Memristor Chaotic System. *Symmetry*. 2021;14(1):17. [10.3390/sym14010017](https://doi.org/10.3390/sym14010017)
- [40] Kaur G, Singh K, Gill HS. Chaos-based joint speech encryption scheme using SHA-1. *Multimedia Tools and Applications*. 2021;80(7):10927–10947. [10.1007/s11042-020-10223-x](https://doi.org/10.1007/s11042-020-10223-x)
- [41] N’Gbo N, Tang J. On the Bounds of Lyapunov Exponents for Fractional Differential Systems with an Exponential Kernel. *International Journal of Bifurcation and Chaos*. 2022;32(12). [10.1142/s0218127422501887](https://doi.org/10.1142/s0218127422501887)
- [42] Jovic B. In: *Chaotic Synchronization, Conditional Lyapunov Exponents and Lyapunov’s Direct Method*. Springer Berlin Heidelberg; 2011. p. 49–78. [10.1007/978-3-642-21849-1_3](https://doi.org/10.1007/978-3-642-21849-1_3)
- [43] Witwit NH, Al-Sultan AY. A High-Security Image Utilizing Triple Generators for the Rabinovitch System. *International Journal of Intelligent Engineering and Systems*. 2023;16(4):682–689. [10.22266/ijies2023.0831.55](https://doi.org/10.22266/ijies2023.0831.55)
- [44] Bakurov I, Buzzelli M, Schettini R, Castelli M, Vanneschi L. Structural similarity index (SSIM) revisited: A data-driven approach. *Expert Systems with Applications*. 2022;189:116087. [10.1016/j.eswa.2021.116087](https://doi.org/10.1016/j.eswa.2021.116087)
- [45] Mokhnache S, Daachi MEH, Bekkouch T, Diffellah N. A Combined Chaotic System for Speech Encryption. *Engineering, Technology & Applied Science Research*. 2022;12(3):8578–8583. [10.48084/etasr.4912](https://doi.org/10.48084/etasr.4912)
- [46] Alexan W, Elkandoz M, Mashaly M, Azab E, Aboshousha A. Color Image Encryption Through Chaos and KAA Map. *IEEE Access*. 2023;11:11541–11554. [10.1109/access.2023.3242311](https://doi.org/10.1109/access.2023.3242311)
- [47] Wang X, Su Y. Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform. *Scientific Reports*. 2020;10(1). [10.1038/s41598-020-75562-z](https://doi.org/10.1038/s41598-020-75562-z)
- [48] Long M, Tan L. A Chaos-Based Data Encryption Algorithm for Image/Video. In: 2010 Second International Conference on Multimedia and Information Technology. IEEE; 2010. p. 172–175. [10.1109/mmit.2010.27](https://doi.org/10.1109/mmit.2010.27)
- [49] Yasser I, Mohamed MA, Samra AS, Khalifa F. A Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications. *Entropy*. 2020;22(11):1253. [10.3390/e22111253](https://doi.org/10.3390/e22111253)

How to cite this article

Sahun RA, Hamad AH, Al-saadi LH, Jawad AK. Lorenz, Rossler, and Chan systems for key generation and pixel selection in chaotic image encryption. *Journal of University of Anbar for Pure Science*. 2025; 19(2):192-207. doi:[10.37652/juaps.2025.161423.1435](https://doi.org/10.37652/juaps.2025.161423.1435)