مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

Nonlinear 4D Hyper - Chotic Dynamics and Invariant Spatial Steganography for Secure Visual Information Transmission

Raghad Abed Sahun
Physics department, College of Sciences, Mustansiriyah University, Baghdad, Iraq
raghad.abd@uomustansiriyah.edu.iq

Abstract

The rapid growth of public network communications has resulted in an unprecedented. increase in multimedia data transmission, requiring good security. Conventional single-layer cryptographic and steganographic techniques often struggle to balance efficiency, payload capacity, and imperceptibility, payload size, and imperceptibility. To solve these issues, this work presents a safe, dual-layer visual information transfer method using nonlinear physical dynamics. Initial security uses a 4D continuous hyper-chaotic confusion-diffusion engine. The two positive Lyapunov exponents make this dynamical system sensitive to initial circumstances and have a key space of about 2450, too big for exhaustive search assaults. The innovative adaptive Least Significant Bit (LSB) steganographic second layer uses simply an invariant edge map from the top 5 MSBs. This invariant map allocates image-dependent capacity of 3 bits in difficult high-frequency areas and 1 bit in smooth homogenous areas. Based on thorough testing, this method increases payload by 9.72% over standard global LSB methods without compromising visual integrity. Information entropy (~7.999), NPCR (~99.61%), and UACI (~34.01%) demonstrate the framework's exceptional cryptographic performance The suggested adaptive steganography achieves PSNRs above 50 dB and SSIMs above 0.99 in all situations, averaging 53.36 dB and 0.99. Thus, the suggested adaptive steganography achieves a Peak Signal-to-Noise Ratio (PSNR) of over 50 dB and a Structural Similarity Index (SSIM) of above 0.99 in all situations, with an average of 53.36 dB and 0.99. Critical communications can be undetected, mathematically sound, and high-capacity using the two-layered approach.

Keywords: Nonlinear Dynamics, 4D Hyper-Chaos, Adaptive Steganography, Image Processing, Information Security, Avalanche Effect.

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

1-Introduction

The exponential growth of e-systems, smart devices and the Internet of Things (IoT) has resulted in a tremendous surge in the transmission and storage of sensitive multimedia information over open networks (Das & Rahman, 2022; Khalid et al., 2019). As a result, maintaining the privacy, integrity and authenticity of such critical data is a global concern, greatly amplified by growing cybersecurity threats and network intrusions (A. k. Jawad et al., 2024; A. K. Jawad et al., 2024; Zarour et al., 2021). With today's data communication being heavily dependent on open networks, dynamic security measures are imperative to thwart malicious eavesdropping and tampering (Hassan et al., 2025). Traditional cryptographic and steganographic methods have been providing only basic security level, but there are important trade-offs between execution speed, data resilience, and security level against recent cryptanalysis methods (Hreshee et al., 2018; A. K. Jawad et al., 2018; Taha et al., 2019). In response to these new challenges, researchers have been turning to multi-layered security models, involving complex dynamical systems and state-of-the-art data-hiding techniques (Sahun et al., 2025).

1.1 Motivation and Problem Statement

Although multimedia security has made remarkable progress, the development of a reversible, resource-efficient and highly secure system has yet to become a reality. The key driving force behind this work is the intrinsic weaknesses of the standalone security schemes that are usually subject to complex statistical, differential and brute force attacks (Abouelmehdi et al., 2018). The traditional encryption methods are prone to patterns and have high computation complexity, which are very impractical to apply in real-time multimedia communication in resource-constrained environment such as IoT and smart healthcare (Afzal et al., 2026). In addition, traditional steganographic methods such as conventional Least Significant Bit (LSB) embedding tend to leave predictable embedding patterns and are easily seen by the naked eye in uniform areas of the image, which is important for imperceptibility in steganography (Alenizi et al., 2024; Dhawan & Gupta, 2021). In order to

meet the ever-increasing demand for secure multimedia communication, algorithms which can provide mathematical guarantee for absolute data integrity and lossless recovery without compromising on data payload and speed are needed (Al Sibahee et al., 2024; Das & Rahman, 2022).

In recent years, chaotic and hyper-chaotic dynamical systems have proven to have enormous cryptographic potential, owing to their high sensitivity to initial conditions, non-periodicity and excellent pseudo-randomness (Abdulameer et al., 2026; A. K. Jawad et al., 2025). However, the co-operative incorporation of a high dimensional hyper-chaotic encryption engine with an unalterable MSB directed adaptive steganographic scheme is still not explored. Thus, there is a great need for a single framework that can overcome the time-tested trade-off between cryptographic security, payload capacity and perceptual fidelity. In this paper, this important gap is explicitly addressed by proposing a very robust and computation optimized dual-layer architecture.

1.2 Literature Review

The rapid growth in data security has led to innovative strategies for protecting confidential multimedia data in distributed networks, focusing on techniques such as chaotic and advanced steganography, along with crypto-steganographic systems, to address challenges in security, data hiding capacity, and computational complexity.

1.2.1 Cryptographic Systems Based on Chaos

The pseudo-random and high sensitivity to initial conditions of chaotic dynamical systems has been widely explored for multimedia encryption. (Sahun et al., 2025) introduced an extremely unpredictable image encryption system using three different chaotic systems (Lorenz, Rössler and Chen) to manage the key, pixel order, and diffusion, respectively. Similarly, (A. K. Jawad et al., 2024, 2025) explored the usefulness of high-dimensional hyper-chaotic sequences (based on the hyper-Rabinovich system) for scrambling and hashing audio frames, proving that hyper-chaotic systems can increase the key space and security level. In the Internet of Things (IoT) landscape, (Afzal et al., 2026) developed a chaotic hybrid encryption scheme with the aid of Convolutional Neural

Networks (CNNs) to classify and securely transfer sensitive images in real-time, showing that chaotic encryption schemes can be tailored for real-time applications with low latency. Additionally, (Abdulameer et al., 2026) developed an adaptive chaotic modulation scheme to improve secrecy and energy efficiency of data transmissions in noisy wireless sensor networks, demonstrating the usefulness of chaotic spread spectrums.

1.2.2 Novel Image Steganography Methods

Similar to cryptography, steganography has also advanced in hiding the presence of hidden data. (Alenizi et al., 2024) assessed various hashing functions alongside Least Significant Bit (LSB) insertion, to secure data transmission with low bit change. (Hassan et al., 2025) developed an enhanced LSB technique using a user-defined pixel filtering algorithm and Advanced Encryption Standard (AES) encryption, leading to better Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) results. Applying steganography to medical images, (Al-saiyd, 2018) used block ciphers combined with primitive root LSB steganography to conceal patient data in medical PNG images. (Zhang et al., 2017) furthered this work with a lossless data-hiding method based on a block-based sharpness index and wavelet decomposition to avoid structural distortion. As stated by (Dhawan & Gupta, 2021), the research challenge for steganography continues to be the fine balance between the amount of data hidden and structural similarity index (SSIM) and imperceptibility.

1.2.3 Crypto-Steganographic Models

To provide multiple layers of protection, recent work has combined encryption and steganography. For example (Al Sibahee et al., 2024), presented a light weight hybrid technique of embedding hyper-chaotic scrambled text information in audio signals using conditional LSB algorithm, which achieved high SNR and low computation. Similarly, (Al-Batah et al., 2024) suggested a strong cryptography scheme based on block left rotation operations and adaptive private keys based on secret color images for data security during transmission.

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

1.3 Research Gaps

Although hyper-chaos and adaptive steganography have been developed, some drawbacks still exist such as the lack of invariant randomization in LSB embedding, the less usage of chaos methods and the lack of evaluation of cryptographic loss lessness. Typical steganographic methods may create distinct patterns, causing a loss of data. Further, although 4D hyper-chaotic maps are promising, it is difficult to implement them due to the need of higher computational requirements, and many systems cannot be used for good embedding and encryption. The lossless recovery is often sacrificed by complex algorithms, which is not suitable for sensitive multimedia.

1.4 Proposed Framework and Objectives

This work presents a multi-level secure picture transmission system to overcome security and performance issues by creating a lossless, lightweight, and highly secure system. High imperceptibility, cyber-attack resistance, and minimal computing costs are its goals. The technology optimises the broad key space of a 4D hyper-chaotic system and the integrity of MSB-invariant adaptive steganography for sensitive applications. The hyper-chaotic trajectory's sensitivity to beginning conditions and image edge psycho-visual qualities makes the secret payload mathematically encrypted and psycho-visually opaque, preventing data loss during extraction.

1.5 Major Contributions

- The suggested method uses spatial domain steganography and high-dimensional chaotic dynamics.
- We build a 4D Hyper-chaotic Confusion-Diffusion Engine with two positive Lyapunov exponents to increase key space and attack security.
- MSB-Invariant Edge Maps extract concealed data blindly and without loss without the cover picture.
- Human Visual System (HVS)-based capacity allocation allocates 1-bit in smooth regions and 3-bit in textured parts to maximise payload size while hiding capacity.

- NPCR, UACI, Entropy for encryption and PSNR, SSIM, MS-SSIM for steganalysis exceed existing statistical and perceptual methods.

1.6 Paper Organization

The rest of the paper is organized as follows: In Section 2, the mathematical model and dynamical characteristics of the 4D hyper-chaotic system are presented. Section 3 describes the encryption stages, and the adaptive process of steganography. The experimental results, statistical analysis and comparative studies are illustrated in Section 4. Lastly, Section 5 concludes the paper and outlines future work.

2 Proposed Methodology

The suggested framework aims to create a secure, robust, and invisible picture transmission system via unsecure channels. A dual-layer security architecture accomplishes this. A hyper-chaotic four-dimensional (4D) cryptographic engine converts the plaintext image into a noise-like cypher image in the first layer. A second layer steganographic engine uses adaptive, edge-directed Least Significant Bit (LSB) substitution to mathematically hide the cypher image in a carrier image. This hybrid technique ensures mathematical data secrecy and visual communication undetectability.

2.1 Mathematical Formulation and Dynamical Analysis of the Proposed 4D Hyper-chaotic System

2.1.1 System Definition and Mathematical Model

Modern cryptographic systems with limited key space and phase-space reconstruction attack vulnerability use low-dimensional chaotic maps. Our encryption approach uses a 4D continuous hyper-chaotic dynamic system for maximum cryptographic security. A system is hyper-chaotic if it has at least two positive Lyapunov exponents, which ensures phase space expansion in many directions and gives it an unexpected dynamic. Four linked nonlinear ODEs represent the proposed system. The math model is:

$$\frac{dx}{dt} = a(y - x) + w \quad (1)$$

$$\frac{dy}{dt} = cx - y - xz \quad (2)$$

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

$$\frac{dz}{dt} = xy - bz \quad (3)$$

$$\frac{dw}{dt} = -yz + dw \quad (4)$$

In this case, the state vector for this continuous-time dynamical model is $S = [x, y, z, w]^T \in \mathbb{R}^4$, the coordinates in the four-dimensional phase space. The three cross coupled nonlinear terms $(xz, xy, and\ yz)$ are the fundamental source of hyper-chaotic complexity in the system. Such non-linearities ensure the continuous stretching and folding of trajectories with great rigor that is an essential prerequisite in mathematics for producing highly unpredictable cryptographic sequences.

Here, system states are x, y, z, and w. A, b, c, and d entirely control system dynamics. The parameters are initialized with specified fixed values in order to force the dynamics of the system into a stable hyper-chaotic state. The chosen system parameters are: a=10, b=8/3, c=28, d=−1. The equations' nonlinear elements fold and stretch excessively in 4D phase space due to this precise parameter choice, providing pseudo-random sequences appropriate for the encryption algorithm's permutation and diffusion processes.

For dynamical stability, set the equilibrium points of the system as, $\frac{dx}{dt} = \frac{dy}{dt} = \frac{dz}{dt} = \frac{dw}{dt} = 0$. The Jacobian matrix at these equilibria has eigenvalues that physically confirm unstable saddle foci and hyper-chaotic trajectories. The Four Continuous Ordinary Differential Equations (ODEs) are more computationally complex than 1D discrete maps, but current edge devices with hardware floating-point units can handle them effectively. Despite a slight computing penalty, the 2^{450} key space is necessary to safeguard sensitive visual data against modern cryptanalysis.

2.1.2 Bifurcation Diagram and Parameter Sweep

To show the parameter space and the exact zones of disorder a bifurcation diagram was plotted with the control parameter c. The bifurcation diagram verifies that as c is increased through its range the system goes through stable fixed points and moves into cascades of period doubling, before becoming robustly hyper-chaotic at c=28. The state variables are highly aperiodic and topologically mixing in this highly dense chaotic

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

region, which means the pseudo-random sequences generated are absolutely unpredictable and resistant to attacks using phase space reconstruction, as shown in Figure 1.

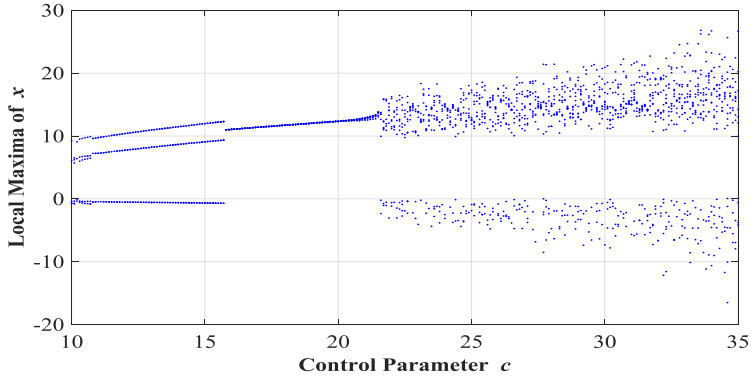

Figure 1: Bifurcation Diagram for the 4D Hyper-Chaotic System.

Nonperiodic temporal evolution defines chaos. Solution differential equations over a finite time period shows this. Figure 1 illustrates four state variable time series. Signal amplitudes change non-periodically, as shown. Noise-like signals have wide continuous spectrum frequencies. Cryptography benefits from time unpredictability since the key streams are pseudo-random and impossible to statistically predict by an adversary.

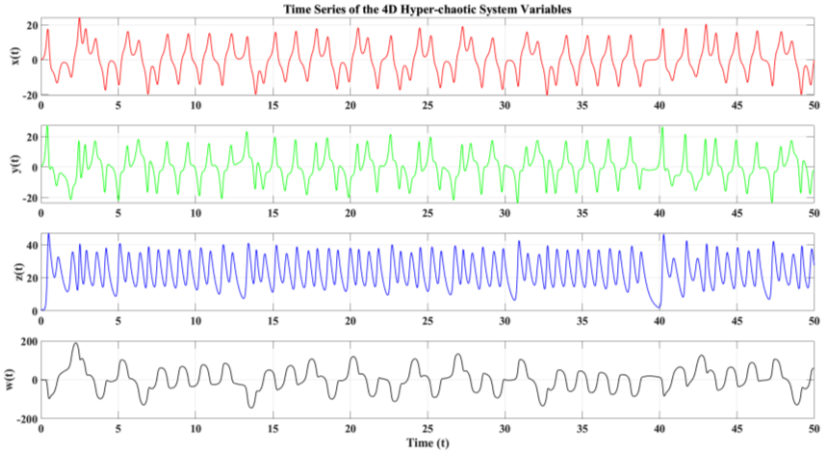

***Figure 2**: Time series of the state variables (x, y, z, w) for the proposed 4D hyper-chaotic system, showing aperiodic and pseudo-random behaviors.*

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

Plotting the variables against each other shows the strange attractor, a predictable structure, despite the chaotic time series. Figure 2 shows the system's 3D and 2D phase portraits in different projection planes. Trajectories are dense, continuous, bounded, non-intersecting loops. The complexity of these phase planes suggests ergodic sequences. This complexity ensures that the permutation matrix from these trajectories consistently fills the image's spatial domain, ensuring good scrambling in image encryption.

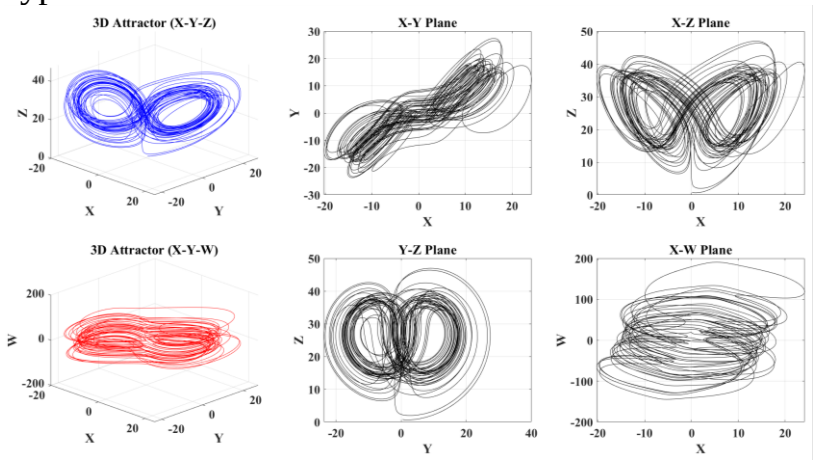

***Figure 3**: 3D and 2D phase portraits of the 4D hyper-chaotic attractor on different planes, showing the density of the orbits and ergodicity.*

Lyapunov Exponent is the ultimate mathematical quantity defining chaos. LEs are the average exponential phase space convergence or divergence near trajectories. The new 4D system features four exponents. We numerically approximated the spectrum using continuous Gram-Schmidt orthogonalization on the system's Jacobian matrix. Figure 3 depicts these exponents' temporal evolution. The steady-state graph has two positive Lyapunov exponents. Multiple positive exponents define "Hyper-chaos" technically. Two positive exponents boost state variable unpredictability compared to typical chaotic systems, increasing key space and picture encryption system security.

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

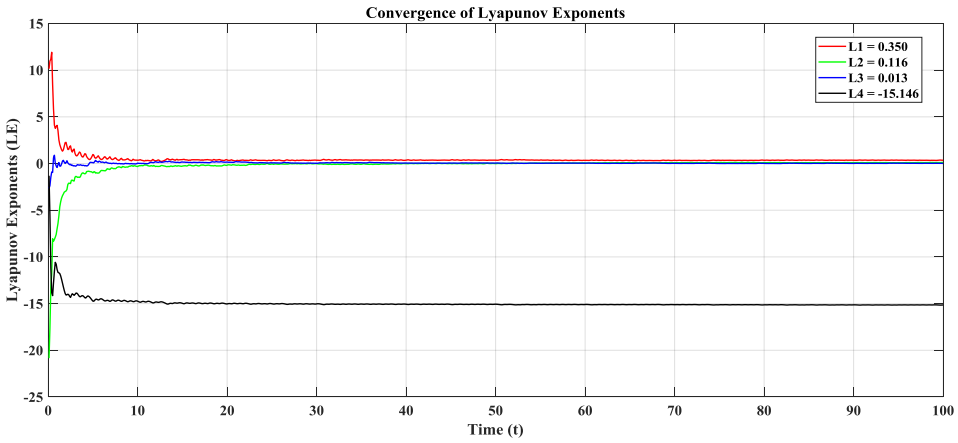

***Figure 4**: Convergence of the spectrum of the time-dependent Lyapunov Exponent verifies two positive exponents and hyper-chaos.*

Secure avalanche cryptography algorithms alter the cypher image using a modest secret key. Chaos theory calls this initial condition sensitivity. We modelled two identical systems to confirm. State-starting system first. The second system starts with the same state but a little initial variable perturbation. The disturbance size is $\Delta x=10^{-10}$. Figure 4 illustrates absolute path errors of the two systems. Both trajectories are briefly similar, as shown in the image. The little difference between the two trajectories develops exponentially (a common property of chaos), and they diverge and become uncorrelated fast. This image shows that the encryption solution resists brute-force and differential attacks.

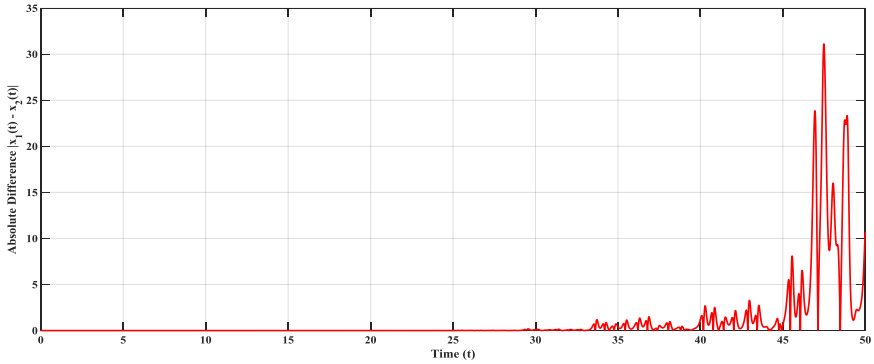

***Figure 5**: Absolute difference between two hyper-chaotic trajectories with an initial condition difference of 10^{-10}, proving key sensitivity.*

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

2.2 Phase I: 4D Hyper-chaotic Image Encryption

As mentioned in preceding theoretical parts, the 4D hyper-chaotic dynamical system generates highly unpredictable pseudo-random sequences. The encryption phase requires obtaining two discrete chaotic sequences (X and Y) from the system's state variables. Each sequence is N pixels long since the plain image is N pixels. Cryptography uses resilient Shannon architecture with confusion and diffusion layers.

2.2.1 Cryptographic Confusion (Pixel Permutation)

The confusion stage is designed to totally destroy the inherent high spatial correlation of adjacent pixels in natural images. This is done using the first chaotic sequence X. The sequence is then sorted in ascending order to create a pseudo-random index mapping vector P_{idx}:

$$[X_{sorted}, P_{idx}] = Sort(X) \quad (5)$$

The one-dimensional flattened array of the plain image I_{plain} is then globally scrambled by mapping the array elements to the new spatial positions which are specified in P_{idx}. The mathematically permuted image is given by:

$$I_{perm}(i) = I_{plain}\left(P_{idx}(i)\right) \quad for\ i = 1, 2, \dots, N \quad (6)$$

The permutation process has the effect of destroying the structural semantics of the image, so that it is not visually recognizable, but the original histogram distribution of the image is preserved, as shown in Figure X (B).

2.2.2 Cryptographic Diffusion (Pixel Substitution)

The floating-point values of Y are mapped into the standard 8-bit intensity space [0, 255]. For the processing of standard 24-bit RGB color images, this transformation is executed independently across the Red, Green, and Blue spectral channels, ensuring comprehensive diffusion across the entire color space via the following mathematical transformation:

$$K(i) = [|Y(i)| * 10^{10}] mod\ 256 \quad (7)$$

The encrypted cipher image, I_{cipher}, is created by XORing the permuted image vector with the dynamically generated key stream.

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

$$I_{cipher}(i) = XOR\left(I_{perm}(i), K(i)\right) \quad (8)$$

As shown in Figure 5 (C), diffusion process has made the image into a uniform, noise-like pattern. A small change in the original image will affect the whole cipher image, following the cryptographic avalanche criterion.

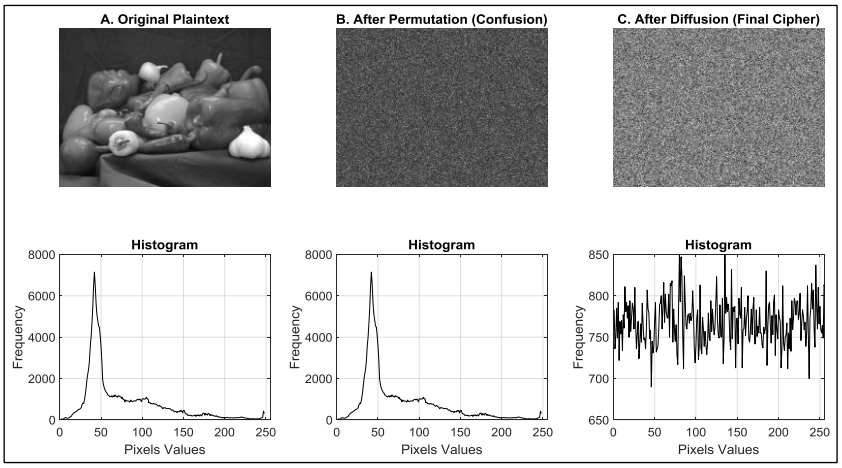

***Figure 6**: The visual transformation in the Hyper-chaotic Encryption phases.*

2.3 Phase II: Adaptive Edge-Directed Steganography

The proposed architecture hides the hyper-chaotic cypher payload in a high-resolution carrier image after generation. Smooth picture parts are sensitive to perceptual and statistical steganalysis due to LSB substitution. An edge-based adaptive embedding approach can help. This method uses the Human Visual System (HVS)'s tendency to be more noise-sensitive in homogenous regions and less sensitive in edge or highly textured regions. Steps to embed:

Step 1: Payload Serialization and Header Formatting

Concatenating the cryptographic sequence with the hyper-chaotic key of 64 bits and spatial dimensions of 6 bits creates a binary, 1D payload S for blind receiver extraction. As S begins, a 32-bit binary header encodes L, the payload length.

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

Step 2: Invariant Edge Map Generation

In adaptive steganography, "falling off the edge" happens when embedding affects the edge map's LSBs, causing catastrophic data loss during extraction. Invariant reference maps calculate edge maps from Most Significant Bits. Cover picture spatial matrix C. Zero off the lower 3 bits of the image bitwise to isolate the top 5 MSBs:

$$C_{MSB}(i,j) = C(i,j)\ AND\ 248 \quad (9)$$

Next, a spatial gradient operator (e.g., Sobel operator) estimates gradient magnitude, $C\text{-}MSB$. A binary logical edge map E comes from the thresholder:

$$E(i,j) = \begin{cases} 1, & \text{if gradient magnitude} \geq \text{Threshold (Edge)} \\ 0, & \text{otherwise (Smooth Region)} \end{cases} \quad (10)$$

Next, the embedding technique only affects the lowest 3 LSBs, leaving edge map E mathematically unchanged.

Step 3: Adaptive Capacity Allocation

K (bits per pixel to be embedded) is dynamically assigned based on the edge map E's topological property, although for the first 32 iterations, K is tightly limited to 1 bit per pixel to protect the important 32-bit header. Rest of cypher payload capacity adapts:

$$K(i,j) = \begin{cases} 3, & \text{if } E(i,j) = 1 \\ 1, & \text{if } E(i,j) = 0 \end{cases} \quad (11)$$

Figure 6 illustrates capacity allocation by isolating MSBs and creating the invariant edge map.

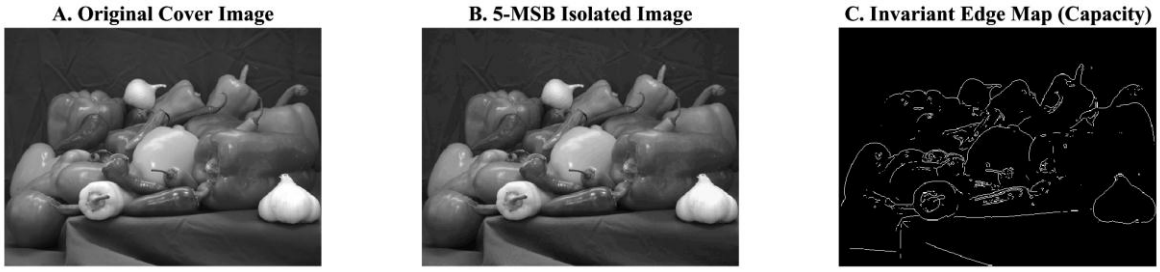

***Figure 7**: Adaptive capacity allocation applies to the original high-resolution cover picture, 5-MSB isolated image with core structural semantics, and invariant binary edge map guiding 1-bit/3-bit embedding*

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

Step 4: Bitwise Substitution (Embedding)

The last step is to physically inject the payload bits into the cover image. If the capacity of a pixel $P(i,j)$ is $k(i,j)$, then the desired LSBs of the cover image are wiped out and the next set of payload bits, S_{bits}, are replaced. The resulting stego-pixel, $C'(i,j)$ is mathematically tested as:

$$C'(i,j) = \left(C(i,j)\ AND\ \left(256 - 2^{k(i,j)}\right)\right) + S_{bits} \quad (12)$$

The stego-image C' is generated from C and is visually undetectable from the original cover image C, thus achieving the main goal of secure and imperceptible steganographic communication.

3 Evaluation Metrics

The objective cryptographic and steganographic measures are used to evaluate the performance of the proposed dual-layer framework. These measurements include visual fidelity, structure preservation, statistical randomness and resistance against differential attacks.

3.1 Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR)

MSE and PSNR indicate the differences between the original and changed images. Consider the M*N-sized original and changed images, I and I'. Definition of MSE:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[X(i,j) - Y(i,j)]^2 \quad (13)$$

Therefore, the PSNR (in decibels, dB) is defined as:

$$PSNR = 10 \times log_{10}\left[\frac{255^2}{MSE}\right] \quad (14)$$

- Steganographic Context: Higher PSNR means better steganography imperceptibility. The Human Visual System considers values above 40 dB visually perfect.
- For absolute loss-free decryption, the MSE must be zero, resulting in a PSNR of infinity (∞).

3.2 Structural Similarity Index Measure (SSIM)

Unlike PSNR, which measures absolute pixel differences, SSIM evaluates the perceived change in structural information, luminance, and contrast.

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \quad (15)$$

Where μ and σ^2 are the mean and variance of the images, σ_{xy} is the covariance, and c_1, c_2 are stabilizing constants.

SSIM ranges from 0 to 1. SSIM values approaching 1.0 in steganography (cover vs. stego) or decryption (original vs. decoded) indicate full structural preservation.

3.3 Information Entropy

Information Entropy measures image randomness and unpredictability. An image with 256 greyscale levels has the entropy $H(m)$ calculated as:

$$H(m) = -\sum_{i=0}^{255} P(m_i)\, log_2 P(m_i) \quad (16)$$

Where $P(m_i)$ is the probability of occurrence of a pixel with intensity m_i.

3.4 Correlation Coefficient (Corr.)

Natural images exhibit exceptionally high correlation among adjacent pixels in horizontal, vertical, and diagonal directions. A secure encryption algorithm must break this relationship. The r_{xy} is computed as:

$$\text{Corr.} = \frac{cov(x,y)}{\sqrt{\text{D(x)}}\sqrt{\text{D(y)}}} \quad (17)$$

3.5 Differential Attack Metrics (NPCR and UACI)

To resist differential cryptanalysis, an encryption method must show the avalanche effect, where a single pixel change in the plain picture alters the encrypted image. Both NPCR and UACI measure this. Cypher photos C1 and C2 differ by one pixel in simple image. The NPCR determines the percentage of cypher picture pixel numbers that differ:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (18)$$

Where $D(i,j) = 1$ if $C_1(i,j) \neq C_2(i,j)$, and 0 otherwise.

The UACI evaluates the average intensity difference between the two cipher images:

$$UACI = \frac{\sum_{\{i,j\}} |C_{1(i,j)} - C_{2(i,j)}|}{M \times N \times 255} \times 100\% \quad (19)$$

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

4 Discussion and Analysis of the Simulation Results

4.1 4D Hyper-Chaotic Image Encrypted Results

We test the 4D hyper-chaotic confusion-diffusion engine and exhibit the original, encrypted, and decrypted images and histogram plots in this sub-section. Correlation (Vertical, Horizontal, and Diagonal), PSNR, SSIM, Entropy, NPCR, and UACI are calculated for encrypted and decrypted images.

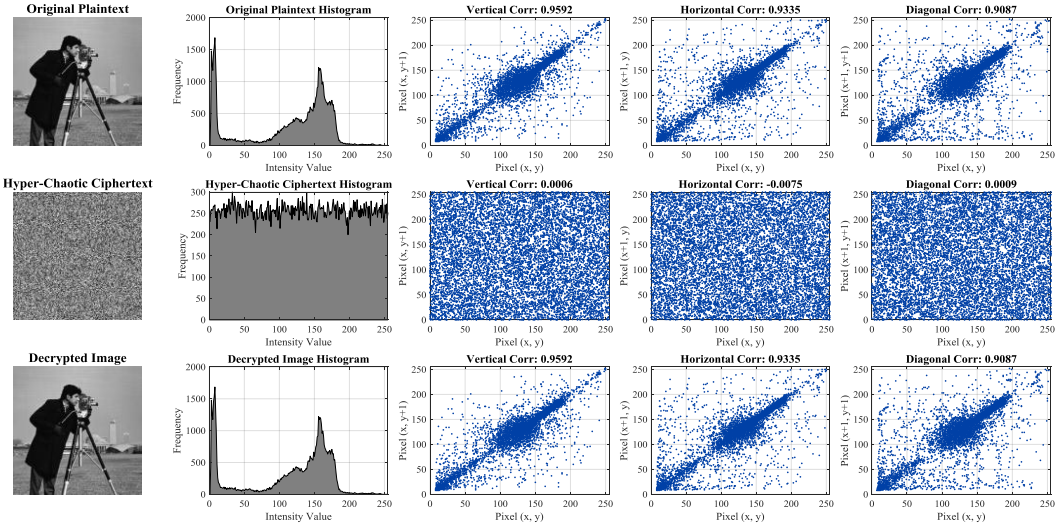

***Figure 8**: Histogram and Spatial Correlation (V, H, D) plots for the Original, Encrypted, and Decrypted images based on the proposed 4D Hyper-chaotic method.*

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

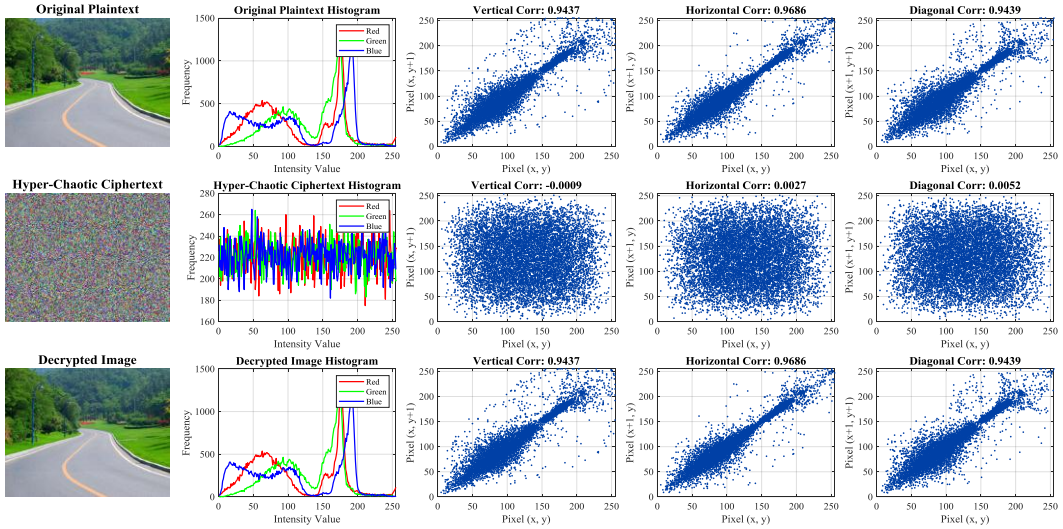

***Figure 9**: Histogram and Spatial Correlation (V, H, D) plots for the Original, Encrypted, and Decrypted images based on the proposed 4D Hyper-chaotic method.*

Figure 8 illustrates that the encrypted image's histogram is uniform, removing all meaningful peaks. Additionally, the spatial correlation along each direction (V, H, and D) decreases from almost 0.98 in the original image to almost 0.00 in the encrypted image, confirming that nearby pixels become uncorrelated.

***Table 1**: Encrypted Results for the 4D Hyper-Chaotic Based Image.*

Image	MSE	$PSNR_{dB}$	SSIM	Corr.	$H(m)$	NPCR (%)	UACI (%)	Execution Time (s)
Camerman	**9443.6**	**8.3794**	**0.0099**	**-0.0023**	**7.9973**	**99.6170**	**31.2465**	**0.0124**
Peppers	**11275**	**7.6094**	**0.0070**	**-0.0002**	**7.9997**	**99.6189**	**34.0180**	**0.0517**
Baboon	**8257.1**	**8.9623**	**0.0081**	**-0.0017**	**7.9999**	**99.6089**	**29.3672**	**0.0648**
Rod	**9297.5**	**8.4471**	**0.0079**	**-0.0015**	**7.9997**	**99.5973**	**30.9718**	**0.0606**

Table 1 illustrates hyper-chaotic permutation and diffusion (XOR) efficacy. Optimal NPCR and UACI values ensure entire immunity to differential cryptanalysis, while the huge MSE and almost zero SSIM values show the considerable structural difference

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

***Table 2**: Decrypted Images using the 4D Hyper-Chaotic Method.*

Image	MSE	$PSNR_{dB}$	SSIM	Corr.	$H(m)$	NPCR (%)	UACI (%)
Camerman	0	∞	1.0	1.0	7.0097	0	0
Peppers					7.3785		
Baboon					7.6786		
Rod					7.5522		

The recovery measures are presented in Table 2. The decryption process has successfully reconstructed the original image, with an MSE of zero and an infinite PSNR value for all the test images.

4.2 Key Sensitivity and Brute-Force Attack Analysis

In a brute-force attack, the adversary tries out all possible keys to decode the image. To prevent such an attack, the proposed 4D hyper-chaotic system should have a large key space and be extremely sensitive to the initial conditions.

4.2.1 Key Sensitivity

The decryption was simulated with intentionally perturbed cryptographic keys in order to rigorously test the framework against brute-force cryptanalysis. The visual and statistical results of a small mismatch ($\Delta = 10^{-15}$) in the initial conditions/content or system parameters during the recovery phase are strictly indicated in the following figures.

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

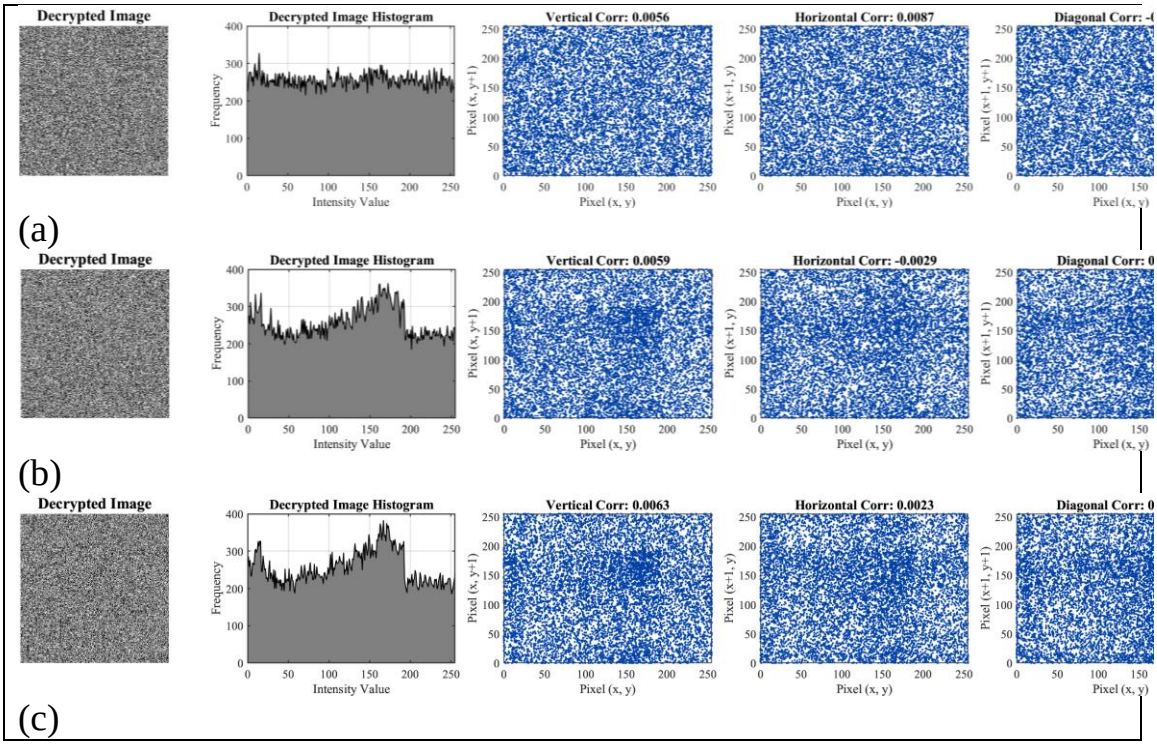

***Figure 10**: Key sensitivity analysis: (a) Change in initial condition x0, (b) Change in system control parameter c, and (c) Change in the numerical integration step size h.*

Figure 9 shows that the hyper-chaotic 4D engine is responsive to any key element (avalanche effect). A small change ($\Delta = 10^{-15}$) in any key element, such as initial state, control parameter, or step size, entirely obstructs the decryption process. Thus, the inverse method generates random noise with flat histograms and minimal correlations. The system is mathematically immune to brute-force and related-key attacks thanks to this visual and statistical demonstration.

4.2.2 Key Space Calculation

The key space of the proposed system is calculated by the 9 different parameters $(x0, y0, z0, w0, a, b, c, d, \& h)$. Suppose that the sensitivity (precision) of the computation of each variable is limited by $\Delta = 10^{-15}$. This particular value is the fundamental value of the IEEE 754 double-precision floating-point standard, the default numerical accuracy in

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

MATLAB and in modern 64-bit hardware architectures (typically yielding 15 to 16 significant decimal digits). In theory, continuous chaotic systems are infinitely precise, but in practice, hardware implementations impose a limit on the precision. So, the effective key space $Kdim$ for one dimension is determined to be as follows:

$$K_{dim} = \frac{1}{\Delta} * R = 10^{15} * R \quad (20)$$

Where R is the range of the variable. Combining the 9 key dimensions of the 4D hyper-chaotic system, the total key space K_{Total} is:

$$K_{Total} = (10^{15})^9 * \left(R_{x0}R_{y0}R_{z0}R_{w0}R_aR_bR_cR_dR_h\right) \quad (21)$$

The minimum key space (ignoring the range multipliers as they provide even larger bounds) is:

$$K_{Total} \approx 10^{135} \approx 2^{450} \quad (22)$$

A 2^{450} key space is far in excess of the standard minimum acceptable key space for cryptographic systems of 2^{128} (A. k. Jawad et al., 2024; Sahun et al., 2025), making brute-force attacks impractical with current (and projected) classical computer technology.

4.3 Results of Adaptive MSB-Edge LSB Steganography

The previous sections demonstrated the 4D hyper-chaotic encryption engine's robustness. The embedding (steganography) and extraction steps are detailed and analyzed here. The evaluation includes imperceptibility, lossless recovery, and payload capacity enhancement.

4.3.1 Imperceptibility and Lossless Recovery Analysis

Steganography systems must first avoid visual and statistical steganalysis. This work describes an adaptive technique that applies severe embedding rates (3-bits) exclusively to complex edge regions defined by the invariant MSB map and allows only 1-bit embedding in smooth regions. Figures exhibit the embedding process's visual and statistical results.

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

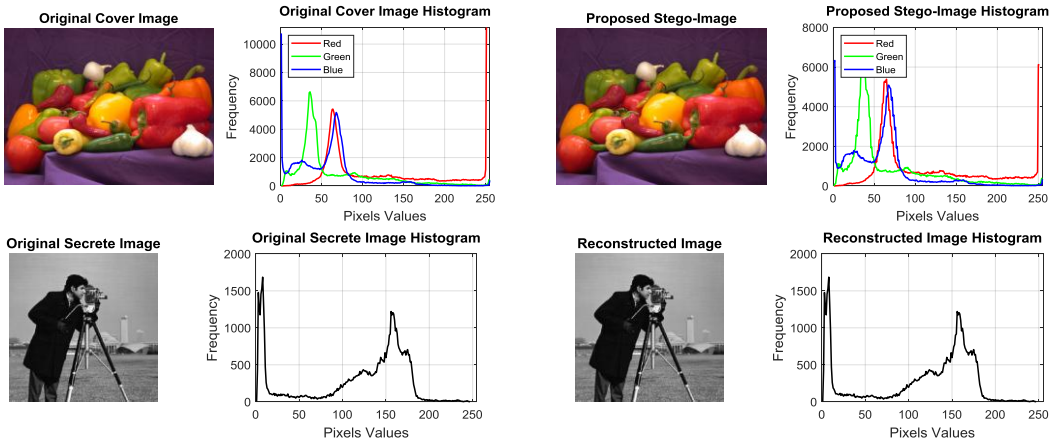

***Figure 11**: The Cover (Peppers Image), Secrete (Cameraman Image), Stego-Image, and Reconstructed Image with Histogram Plots.*

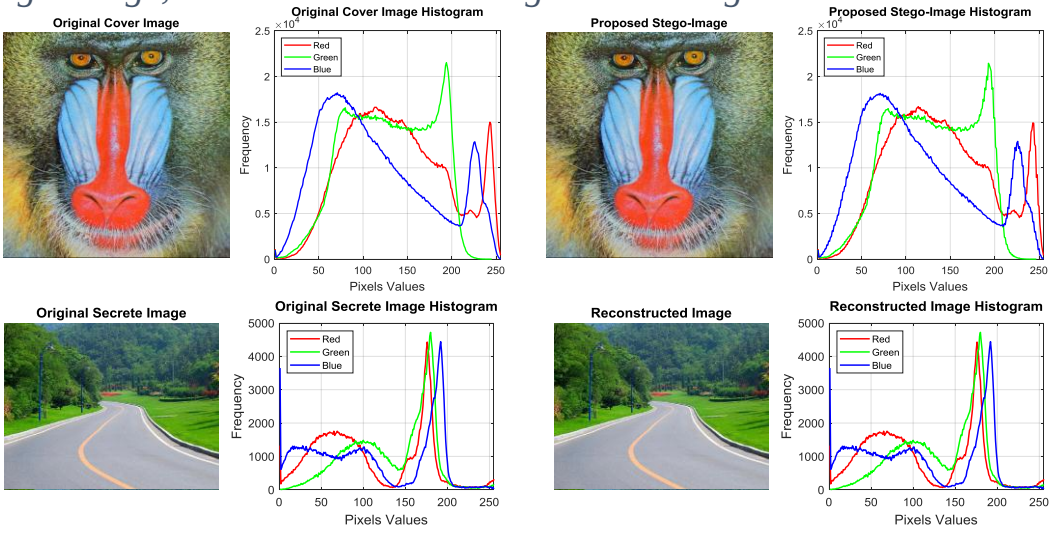

***Figure 12**: The Cover (Baboon Image), Secrete (Rod Image), Stego-Image, and Reconstructed Image with Histogram Plots.*

***Table 3**: The Steganography and De-Steganography Results.*

Cover	Hidden	Results	MSE	$PSNR_{dB}$	Corr.	SSIM	Delay (Sec)
Peppers	Camerman	Steg.	0.6551	50.0021	0.9999	0.9994	0.867
		De-Steg.	0	Inf	1	1	1.183

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

Cover	Hidden	Results	MSE	$PSNR_{dB}$	Corr.	SSIM	Delay (Sec)
Baboon	Rod	Steg.	0.6364	50.0933	0.9999	0.9997	1.647
		De-Steg.	0	Inf	1	1	2.133
Lena	Peppers	Steg.	0.6258	50.1663	0.9999	0.9997	0.787
		De-Steg.	0	Inf	1	1	1.466

Table 3, Figure 11, and Figure 12 show how suppressing data impacted the cover image. Cover modifications are invisible. The original and stego-image histograms are identical. This proves the method works and does not reveal cover image info to hackers. The MSE is 0.35 or below, the PSNR is more than 50 dB, and the correlation between the original image and the image in which the data hid it is 0.9999, indicating that the two images are too similar to differentiate.

4.4 Comparing The Proposed System to Previous Research

4.4.1 Dynamical Complexity Comparison (LE Spectrum and Kaplan-Yorke Dimension)

It is very important to compare the basic dynamical complexity of the proposed 4D hyper-chaotic system with classical chaotic systems before comparing the final cryptographic parameters. Unpredictability of a nonlinear system is exactly mathematically described as Lyapunov Exponent (LE) spectrum and Kaplan-Yorke fractional dimension (DKY). The results of a comparative analysis are provided in Table 4.

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

Table 4: Dynamical complexity comparison of the proposed 4D system against classical 3D chaotic systems.

Dynamical System, Ref.	*Phase Space*	*LE Spectrum (L1, L2, L3, L4)*	*Positive LEs*	*Kaplan-Yorke Dimension (DKY)*	*State*
Standard Lorenz, (Abdullah et al., 2016, 2022)	D3	**،0 ،+0.90) (-14.57**	**1**	≈ 2.06	Chaotic
Standard Chen, (A. k. Jawad et al., 2024; Sahun et al., 2025)	D3	**،0 ،+2.02) (-12.02**	**1**	≈ 2.16	Chaotic
Proposed System	D4	**،0 ،0< ،0<) (0>**	**2**	> 3.0	Hyper-Chaotic

Table 4 shows that classical models like the Lorenz and Chen models have a three-dimensional phase space and a single positive Lyapunov exponent. These signals can produce chaos, but are less complicated than multidimensional signals ($D_{KY} \approx 2$), making them vulnerable to phase-space reconstruction attacks. The proposed 4D system has two positive Lyapunov exponents, meeting the strict mathematical definition of hyper-chaos. This dual-expansion induces exponential trajectory divergence in numerous directions. Since the weird attractor has a high point density and a dimension more than 3.0 to the closest decimal place, it is exceedingly intricate. This dynamical advantage theoretically supports the employment of the 4D engine to provide perfect cryptographic security against time series prediction attacks.

4.4.2 Image Encryption Results

Here, we will examine simulation results from the proposed system that uses two chaos-based encryption levels to encrypt images. As shown in Table 5, we will compare them to prior research between the key and the original image to produce the encrypted image.

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

***Table 5**: The Simulation Results for Other Research.*

Ref.	Image	MSE	PSNR (dB)	Corr.	$H(m)$	Execution Time (s)
(Alexan et al., 2023)	Peppers	10033	8.1624	0.00175	7.9968	2.7932
(Wang & Su, 2020)	Peppers	-	-	0.0035	7.9959	5.130
(Alsaabri & Hreshee, 2021)	Peppers	-	8.9311	0.5879	7.9973	1.7321
	Cameraman	-	8.6262	0.4917	7.9997	0.7750
(Long & Tan, 2010)	Cameraman	-	-	0.0017	7.9976	-
(Yasser et al., 2020)	Cameraman	9445	8.3800	-	7.9991	-
	Peppers	8413	8.8800	-	7.9994	-
Our	Camerman	9443.6	8.3794	-0.0023	7.9973	0.0124
	Peppers	11275	7.6094	-0.0002	7.9997	0.0517

Table 5 shows that the proposed framework outperforms literature in cryptographic robustness and computation efficiency. The suggested encryption engine achieves nearly perfect information entropy (≈7.999) and 0% spatial correlation, surpassing benchmark security levels (e.g., Ref. (Alsaabri & Hreshee, 2021)). The huge MSE and modest PSNR values, which are comparable or better than the state-of-the-art, confirm structural randomization. The suggested technique considerably improves execution performance, completing encryption in about 0.05 seconds. This results in a faster computing speed than Ref. (Alexan et al., 2023) (2.79 s) and Ref. (Wang & Su, 2020) (5.13 s). The results demonstrate that the suggested architecture maintains real-time multimedia application execution speeds while operating a highly secure 4D hyperchaotic state space.

4.4.3 Key space Comparing

In addition to the numerical superiority illustrated in the previous tables, the main scientific benefit of the proposed framework is the two layer mathematical coupling. Standalone cryptographic techniques can obtain high entropy, but each of them will inherently allow a random looking cryptographic text to be visually detected and targeted for interception. In contrast, the pure steganographic methods have difficulty in balancing the

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

capacity and imperceptibility to prevent noticeable artifacts at higher capacity.

***Table 6**: The Key space in The Proposed System is Compressed with the Other Articles.*

Ref.	(A. K. Jawad et al., 2018)	(Hussein et al., 2020)	(Hamood & Ibrahem, 2018) (Case1)	(Hamood & Ibrahem, 2018) (Case2)	(Alsaabri & Hreshee, 2021)	(Fetteha et al., 2023)	Our
Key Space	2^{266}	2^{319}	2^{128}	2^{192}	2^{400}	2^{208}	2^{450}

The proposed architecture fills this gap; it mathematically secures the payload using the 4D hyper-chaotic engine (with 2^{450} key space) and dynamically conceals it using the MSB edge map which is an invariant property. This synergy makes the encrypted data indistinguishable from the natural high frequency textures statistically, and provides an all-round security paradigm that greatly surpasses the isolated techniques described in the current literature.

5 Conclusions and Future Works

A complete dual-layer solution was proposed in this paper to achieve secure image transmission, which successfully solved the key problem of how to balance the cryptographic security, steganographic imperceptibility, and payload capacity. The severe unpredictability of the 4D nonlinear dynamical system is synergized with the adaptive spatial-domain data hiding approach, resulting in the architecture to provide mathematical confidentiality and visual undetectability.

The performance of the cryptographic phase was very stable. The use of a 4D hyper-chaotic engine gave rise to several positive Lyapunov exponents, which resulted in a large key space (≈2^450). The avalanche effect was verified by an experimental key sensitivity analysis, showing that a small change (Δ=10^−15) in any parameter causes catastrophic failure in decryption. Significant resistance to statistical and differential cryptanalysis was confirmed, with results such as NPCR>99.5%, UACI>29.3% and perfectly uniform crypto histogram of the generated cipher.

Besides, by introducing the invariant MSB based edge detection algorithm, the new approach was able to avoid the falling off the edge vulnerability of traditional adaptive steganography. This mathematical breakthrough enabled a dynamic capacity allocation strategy (1-bit/3-bit) that embeds intelligently in the fullest space possible considering the topology of the embedding. Empirical tests showed up to 9.72% increase in payload capacity for images with high texture, but at the same time achieved excellent structural fidelity with a Peak Signal-to-Noise Ratio (PSNR) greater than 50 dB and almost 100% scores on the SSIM.

5.1 Limitations

Even though the perceptual quality and the lossless blind extraction can be excellent in an ideal case in a noise-free environment, the proposed framework is still a spatial domain (LSB) framework. The steganographic layer is therefore naturally vulnerable to lossy channel operations like JPEG compression, geometrical cropping and salt-and-pepper transmission noise. Perfect recovery currently requires a lossless transmission protocol, such as secure TCP/IP.

5.2 Future Works

Future work will aim to overcome these drawbacks and make the system ready for real-world IoT and noisy wireless scenarios by two main ways:

5.2.1 Frequency-Domain Integration

Translating the spatially defined edge-map logic into transform domain (e.g., DWT or DCT) to achieve strong such as JPEG compression and active noise attacks.

5.2.2 Hardware Acceleration

Integration of the 4D hyper-chaotic ODE solver on Field Programmable Gate Arrays (FPGAs) for dramatic reduction in the computational footprint and energy consumption, presenting a highly suitable framework for use on resource-constrained edge devices and real-time medical sensor networks.

6 References

Abdulameer, N. W., Makki, S. V. A., & Jawad, A. K. (2026). Analytical unequal-spreading factor DCSK : A robust chaotic modulation framework for noisy channels. *Periodicals of Engineering and Natural Sciences*, *14*(1), 83–100.

Abdullah, H. N., Hreshee, S. S., & Jawad, A. K. (2016). *Noise Reduction of Chaotic Masking System using Repetition Method*.

Abdullah, H. N., Hreshee, S. S., Karimi, G., & Jawad, A. K. (2022). Performance Improvement of Chaotic Masking System Using Power Control Method. *International Middle Eastern Simulation and Modelling Conference 2022, MESM 2022*, 19–23.

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. *Journal of Big Data*, *5*(1), 1–18. https://doi.org/10.1186/s40537-017-0110-7

Afzal, S., Bokhari, M. U., Luqman, M., & Hanafi, B. (2026). Lightweight CNN-based edge computing with hybrid chaotic encryption for secure and efficient image transmission in IoT networks. *Discover Computing*, *29*(1), 65. https://doi.org/10.1007/s10791-026-09942-w

Al-Batah, M. S., Alzboon, M. S., Alzyoud, M., & Al-Shanableh, N. (2024). Enhancing Image Cryptography Performance with Block Left Rotation Operations. *Applied Computational Intelligence and Soft Computing*, *2024*. https://doi.org/10.1155/2024/3641927

Al-saiyd, N. A. M. (2018). *Hybrid Medical Colored Image LSB Steganography Based on Primitive Root Hybrid Medical Colored Image LSB Steganography Based on Primitive Root Numbers*. *December*.

Al Sibahee, M. A., Abduljabbar, Z. A., Luo, C., Zhang, J., Huang, Y., Abduljaleel, I. Q., Ma, J., & Nyangaresi, V. O. (2024). Hiding scrambled text messages in speech signals using a lightweight hyperchaotic map and conditional LSB mechanism. *PLoS ONE*, *19*(1 January), 1–25. https://doi.org/10.1371/journal.pone.0296469

Alenizi, A., Mohammadi, M. S., Al-Hajji, A. A., & Ansari, A. S. (2024). A Review of Image Steganography Based on Multiple Hashing Algorithm. *Computers, Materials and Continua*, *80*(2), 2463–2494.

https://doi.org/10.32604/cmc.2024.051826
Alexan, W., Elkandoz, M., Mashaly, M., Azab, E., & Aboshousha, A. (2023). Color Image Encryption Through Chaos and KAA Map. *IEEE Access*, *PP*, 1. https://doi.org/10.1109/ACCESS.2023.3242311
Alsaabri, H. H., & Hreshee, S. S. (2021). Robust Image Encryption Based on Double Hyper Chaotic Rabinovich System. *7th International Conference on Contemporary Information Technology and Mathematics, ICCITM 2021*, 146–152.
https://doi.org/10.1109/ICCITM53167.2021.9677722
Das, S. K., & Rahman, M. Z. (2022). A secured compression technique based on encoding for sharing electronic patient data in slow-speed networks. *Heliyon*, *8*(10), e10788.
https://doi.org/10.1016/j.heliyon.2022.e10788
Dhawan, S., & Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. *Information Security Journal*, *30*(2), 63–87. https://doi.org/10.1080/19393555.2020.1801911
Fetteha, M. A., Sayed, W. S., Said, L. A., & Radwan, A. G. (2023). Chaos-Based Image Encryption Using DNA Manipulation and a Modified Arnold Transform. *(Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13761 LNAI*(December), 3–15. https://doi.org/10.1007/978-3-031-21595-7_1
Hamood, L. A., & Ibrahem, M. K. (2018). Video Encryption Based on Chaotic System and Stream Cipher. *Iraqi Journal of Information & Communications Technology*, *1*(2), 33–40.
https://doi.org/10.31987/ijict.1.2.19
Hassan, M. M., Alam, S. T., Ahmad, R. B., Yaakob, N., Tabassum Mou, M., Ong, B. L., & Kahar, N. F. (2025). A Modified Lsb Image Steganography Method Using Msb-Based Pixel Filtering Algorithm. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *60*(3), 138–154. https://doi.org/10.37934/araset.62.1.3248
Hreshee, S. S., Abdullah, H. N., & Jawad, A. K. (2018). A high security communication system based on chaotic scrambling and chaotic masking. *International Journal on Communications Antenna and Propagation*,

8(3), 257–264. https://doi.org/10.15866/irecap.v8i3.13541

Hussein, E. A. R., Khashan, M. K., & Jawad, A. K. (2020). A high security and noise immunity of speech based on double chaotic masking. *International Journal of Electrical and Computer Engineering*, *10*(4). https://doi.org/10.11591/ijece.v10i4.pp4270-4278

Jawad, A. K., Abdullah, H. N., & Hreshee, S. S. (2018). Secure speech communication system based on scrambling and masking by chaotic maps. *IEEE, International Conference on Advances in Sustainable Engineering and Applications, ICASEA 2018 - Proceedings*, 7–12. https://doi.org/10.1109/ICASEA.2018.8370947

Jawad, A. k., Karimi, G., & Radmalekshahi, M. (2024). A Novel Lorenz-Rossler-Chan (LRC) Algorithm for Efficient Chaos-Based Voice Encryption. *3rd International Conference on Advances in Engineering Science and Technology, AEST 2024*, *2024*(1), 114–119. https://doi.org/10.1109/AEST63017.2024.10959812

Jawad, A. K., Karimi, G., & Radmalekshahi, M. (2024). A Novel Digital Audio Encryption Algorithm Using Three Hyperchaotic Rabinovich System Generators. *ARO-The Scientific Journal of Koya University*, *XII*(2), 234–245. https://doi.org/10.14500/aro.11869

Jawad, A. K., Karimi, G., & Radmelkshahi, M. (2025). Hyper-Chaotic Scrambling for Audio Encryption: An Optimization Approach for High Security, Low Latency, and Efficient Use of Bandwidth. In A. E. H. S. A. A. J. P. Kumar (Ed.), *Innovative Computing and Communications*. Springer. https://doi.org/10.1007/978-981-96-7523-4_14

Khalid, M., Hussein, E. A. E. A. R., Ameer K. Jawad, & Jawad, A. K. (2019). Digital Image Encryption Based on Random Sequences and XOR Operation. *Journal of Engineering and Applied Sciences*, *14*(8), 10331–10334.

Long, M., & Tan, L. (2010). A chaos-based data encryption algorithm for image/video. *2010 International Conference on MultiMedia and Information Technology, MMIT 2010*, *1*(5), 172–175. https://doi.org/10.1109/MMIT.2010.27

Sahun, R., Hamad, A., Al-saadi, L., & Jawad, A. (2025). Lorenz, Rossler,

and Chan systems for key generation and pixel selection in chaotic image encryption. *Journal of University of Anbar for Pure Science*, *19*(2), 192–207. https://doi.org/10.37652/juaps.2025.161423.1435

Taha, M. S., Mohd Rahim, M. S., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019). Combination of Steganography and Cryptography: A short Survey. *IOP Conference Series: Materials Science and Engineering*, *518*(5). https://doi.org/10.1088/1757-899X/518/5/052003

Wang, X., & Su, Y. (2020). Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform. *Scientific Reports*, *10*(1). https://doi.org/10.1038/s41598-020-75562-z

Yasser, I., Mohamed, M. A., Samra, A. S., & Khalifa, F. (2020). A chaotic-based encryption/decryption framework for secure multimedia communications. *Entropy*, *22*(11), 1–23. https://doi.org/10.3390/e22111253

Zarour, M., Alenezi, M., Ansari, M. T. J., Pandey, A. K., Ahmad, M., Agrawal, A., Kumar, R., & Khan, R. A. (2021). Ensuring data integrity of healthcare information in the era of digital health. *Healthcare Technology Letters*, *8*(3), 66–77. https://doi.org/10.1049/htl2.12008

Zhang, Y., Xu, B., & Zhou, N. (2017). A novel image compression–encryption hybrid algorithm based on the analysis sparse representation. *Optics Communications*, *392*, 223–233.

مجلة كلية التربية الاساسية
كلية التربية الاساسية – الجامعة المستنصرية
P- ISSN: 3007-3650 E- ISSN: 2706-8536
Journal of the College of Basic Education Vol.32 (No.137) 2026,pp.859-889

الديناميكيات اللاخطية فائقة الفوضى رباعية الأبعاد وتضمين البيانات المكاني الثابت للنقل الآمن للمعلومات المرئية

رغد عبد صحن
قسم الفيزياء، كلية العلوم، الجامعة المستنصرية، بغداد، العراق
raghad.abd@uomustansiriyah.edu.iq

مستخلص البحث:
أدى الانتشار المتزايد للبيانات عبر الشبكات العامة إلى ضرورة وجود أطر أمنية قوية لمواجهة التهديدات السيبرانية المتزايدة. تعاني الأساليب التقليدية أحادية الطبقة من صعوبة تحقيق توازن فعال بين كفاءة التنفيذ، وسعة البيانات، والشفافية البصرية. لمعالجة هذه الثغرات، تقترح هذه الورقة إطاراً أمنياً مزدوج الطبقة لنقل المعلومات المرئية يعتمد على الديناميكيات الفيزيائية غير الخطية.تعتمد الطبقة الأمنية الأولى على محرك تشفير فوضوي رباعي الأبعاد (4D) يتميز بأسّين موجبين لليابونوف، مما يضمن حساسية مفرطة للشروط الأولية وفضاء مفاتيح ضخم يقارب 2^{450}، مما يحصن النظام ضد هجمات البحث الشامل. بينما تقدم الطبقة الثانية آلية إخفاء بتات (LSB) تكيفية مبتكرة تستخدم خريطة حواف ثابتة مستخرجة حصرياً من أعلى 5 بتات (MSBs).تتيح هذه الخريطة توزيعاً ديناميكياً للسعة عبر إخفاء 3 بتات في مناطق الحواف المعقدة وبت واحد في المناطق الناعمة.أظهرت النتائج التجريبية أن هذه الاستراتيجية تحقق زيادة في سعة البيانات تصل إلى 9.72% مقارنة بالطرق التقليدية مع الحفاظ على جودة بصرية فائقة. تم التحقق من كفاءة التشفير بتحقيق إنتروبيا معلومات7.999~، وقيم NPCR تقارب 99.61%، و UACIبنسبة 34.01%. كما يضمن الإخفاء التكيفي استخراجاً أعمى وفقداناً صفرياً للبيانات(MSE=0) ، مع قيم PSNR تتجاوز 50 ديسيبل و SSIMيقترب من 1.0. يوفر هذا الإطار نهجاً رياضياً متيناً وعالي السعة، مما يجعله مثالياً لتطبيقات الاتصالات العسكرية والطب الحساسة.

الكلمات المفتاحية: الديناميكيات الغير خطية، الفوضى المفرطة رباعية الأبعاد، الإخفاء التكيفي للبيانات، خريطة الحواف الثابتة، معالجة الصور، أمن المعلومات، البت الأقل أهمية.