

Highly Secure Image Steganography via 4D Fractional-Order Chaos and MSB-Invariant Adaptive Embedding

Aws Hamed Hamad* 

Biotechnology Research Center, Al-Nahrain University, Iraq.

*Correspondence: aws.hamed@nahrainuniv.edu.iq



Article – Peer Reviewed

Received: July 15, 2026

Accepted: September 13, 2026

Published: September 21, 2026

Copyright: © 2026 RAME Publishers

This is an open access article under the CC BY 4.0 International License.



<https://creativecommons.org/licenses/by/4.0/>

Cite this article: Aws Hamed Hamad, “Highly Secure Image Steganography via 4D Fractional-Order Chaos and MSB-Invariant Adaptive Embedding”, *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 7, issue 4, pp. 450-465, 2026.

<https://doi.org/10.26706/ijceae.7.4.20260811>

Abstract: Steganography in the spatial domain generally faces the challenge of having high capacity, high fidelity and high security. This study presents a channel-agnostic adaptive solution to address the issues of spatial desynchronization and to also increase the cryptographic complexity. This method is based on the use of a 4D fractional order hyper-chaotic system to create the scattered embedding coordinates with initial conditions, fractional orders and continuous coefficients as the three active keys. At the same time, a structural map is being generated which is invariant under MSB and which determines the local capacity. This system separates the concept of capacity estimation from LSB modifications, and dynamically allocates 1-bit payloads to smooth regions and 3 bits to structural boundaries. Under noise free conditions, experimental results are conducted on grayscale and RGB images which shows the exact secret recovery ($MSE=0$). The method can be used to obtain the highest payload gain of 9.65% relative to the standard 1-bit baselines with Peak Signal-to-Noise Ratios ($PSNR$) > 50 dB and Structural Similarity ($SSIM$) > 0.999 . The non-local memory of the fractional dynamics is an expansion of the theoretical key space around 598 bits, enhancing exhaustive parameter search ability. Finally, the framework mathematically separates the scattering of capacity from the embedding of data so that a good tradeoff between scattering security and high-fidelity adaptive embedding is obtained.

Keywords: Fractional-Order Calculus, Hyper-Chaotic Systems, Adaptive Steganography, Pseudo-Random Scattering, Key Sensitivity, MSB-Invariant Edge Map, Blind Extraction, Dimension-Agnostic Processing.

1. Introduction

With the widespread digital communications in today's world, it has become a critical challenge to securely transmit sensitive visual data over public networks. Classical cryptography protects data confidentiality by converting the plaintext data into unreadable data which will be called as cipher, but by itself gives a hint to the existence of the encrypted data to unauthorized interceptors [1], [2]. To overcome this basic weakness, digital image steganography is used to embed the secret payload into innocent-looking cover media in such a way that the communication's presence is not even known. If such a method is applied uniformly over the entire cover image, however, certain statistical anomalies and visual artifacts are inevitable in homogeneous image regions, making the system high susceptible to modern steganalysis [3]. The technique is steganography, which is content adaptive in order to maximize payload capacity without compromising visual fidelity. The adaptive algorithms make use of the psycho-visual masking property of the Human Visual System (HVS) that influences the weightage of the data payloads by directing more data payloads towards topologically complex areas like edges and higher frequency textures while reducing the data payloads in smooth areas [4], [5], [6]. Although theoretically effective, high-capacity adaptive steganography has two major structural issues

that spur this research: While in theory effective, there are two significant structural problems that drive the work in this research with high-capacity adaptive steganography:

The key constraint is the basic issue of spatial desynchronization (also known as the 'falling off the edge' problem). The structural gradient of the cover image is inevitably changed when the secret data is adaptively embedded at the edge pixels. This means that the receiver is unable to recalculate the correct edge map and therefore cannot correctly reconstruct the original cover image without the knowledge of the original image with which the cover image was produced. This makes it impossible to reconstruct the original edge map without knowing the original cover image used to produce the cover image, which results in catastrophic synchronization failure and corrupted extraction of data if there was no original cover image sent along with the stego-image. Recently, efforts have been made to overcome this by incorporating meta-heuristic optimization algorithms [5], [7], but this results in significant computational expense and is problematic for deployment in real-time applications. The second challenge is related to the cryptographic security of the embedding locations in the space. Most traditional chaos-based steganographic schemes are based on low-dimensional chaotic maps of integer order [3], [8]. The elementary dynamical systems have limited key spaces and have predictable short-term phase space trajectories. As a result, the pseudo-random embedding paths created are still susceptible to a wide variety of sophisticated phase space reconstruction methods and brute force predictive attacks, particularly in the context of modern steganalysis methods based on machine learning [9].

The previous Invariant Adaptive (IA) scheme (e.g., [1], [10]) were strictly based on chaotic dynamic with integer order and global embedding [11], [12], [13], while the present framework is based on a combination of MSB-invariant capacity map and fractional-order four-dimensional hyper-chaotic scattering generator. The main contribution is that the non-local fractional dynamics for the spatial permutation are combined with a dynamic capacity-allocation mechanism (1-bit/3-bit) that does not require the original cover image for channel-agnostic blind extraction.

1.1 Research Objectives

In order to address the mentioned drawbacks, the goal of this research is to develop and evaluate a dimension-independent, highly secure scattered adaptive steganographic system. The main objective is to separate capacity-allocation logic from the physical data-embedding process. It does so in order to increase the embedding capacity in topologically complex areas dynamically, while mathematically ensuring that the embedding process is perfect, meaning that there is no need to send the original cover image to the receiver. At the same time, the research is designed to make the cryptographic problem of the path embedding even harder to solve by using an advanced fractional-order hyper-chaotic generator instead of the traditional integer-order map, in order to make it immune to exhaustive brute force attack and phase space reconstruction.

1.2 Scientific Contributions

The proposed framework brings together a new cross section of fractional calculus, chaotic cryptography and adaptive steganography. The key contributions of this paper to the field of science are summarized:

1. **Absolute MSB-Invariant Adaptive Synchronization:** A new capacity allocation mechanism is proposed that is based solely on the top 5 Most Significant Bits (MSBs) of the cover image. The framework defines a dynamic 1-bit (smooth region) and 3-bit (edge region) embedding thresholds, by computing the Sobel edge gradient only from the isolated structural luminance. The MSBs are preserved during the Least Significant Bit (LSB) injection process, ensuring that the reference map is 100% mathematically invariant, and that there is absolute blind and lossless extraction ($MSE = 0$).
2. **Fractional-Order Hyper-Chaotic Stego-Key Generation:** We embed the scattering coordinates to create a four-dimensional continuous fractional-order hyper-chaotic system, which is solved by the Grünwald-Letnikov (GL) approximation. This infinite non-local memory trace introduced by the fractional derivatives ($q=0.98$) doubles the size of the key space to about 10^{180} (598 bits). This mechanism can achieve a high level of cryptographic sensitivity ($\Delta = 10^{-15}$) and ensures that no unauthorized extraction can take place.
3. **Dimension-Agnostic Spatial Architecture:** The proposed architecture is dimension-agnostic and can process both 2D grayscale images and 3D RGB images (as opposed to other adaptive algorithms that were confined to 2D grayscale matrices, such as [14]. The structural edge map is computed spatially and is duplicated in each of the color channels, and thus does not get desynchronized by the usual grayscale conversion blending weights.
4. **Empirical validations** show that the proposed method allows a payload gain of up to 9.65% (which depends on the textural density), and the visual imperceptibility measured by Peak Signal-to-Noise Ratio (PSNR) is > 50 dB and > 0.999 (Structural Similarity).

1.3 Paper Organization

The rest of this paper is structured as follows: In section 2, the related literature pertaining to chaos-based cryptography and adaptive steganography is critically reviewed. In section 3, the methodology is outlined, which involves the mathematical modeling of the fractional-order hyper-chaotic system, generation of the MSB-invariant edge map, scattered embedding and blind extraction algorithms. The experimental results are fully analyzed in this section, covering various aspects like payload capacity evaluation, visual fidelity, and sensitivity testing with stego-key. Finally, the general findings and future directions for research are presented in Section 5.

2. Related Works

With the advancement of secure communication protocols there has been a lot of research into cryptography and steganography. Based on the use of chaotic systems, adaptive edge-directed embedding, optimization algorithms and hybrid integration, the recent literature can be divided into different approaches. This section presents a critical evaluation of the previous studies, considering the theoretical background and highlighting the common shortcomings in the research.

2.1 Chaos-Based Cryptography in Image Security

Because of their pseudo-randomness, ergodicity and sensitivity to initial conditions, chaotic systems have been largely applied to image encryption [11], [15], [16], suggested image encryption technique by using multiple chaotic systems. The method was able to obtain high entropy and resistance to differential attacks on many medical imaging modalities, yet it only considered encryption and did not use steganographic concealment. To further secure the transmission of healthcare data, [17] proposed a hybrid chaotic system with zigzag-based block permutation. Although there is a critical need for lossless recovery for medical diagnosis, the imperceptibility aspect was ignored by the methodology; the presence of the payload is still apparent. Furthermore, the computation complexity of real-time edge healthcare systems was not properly explored. To overcome reversibility, [18] proposed a deep learning recovery network to implement reversible steganography algorithm based on pixel-shift. The method resulted in close-to-perceptual indistinguishability (MSSIM performance of 0.988) and it was also able to withstand both SRM and deep learning steganalysis. But it was very sensitive to JPEG compression (failed below QF = 50), and could only be used to compress grayscale images.

2.2 Edge-Directed Steganography, Adaptive Steganography

To reduce the visual distortion on uniform payload embedding, researchers have turned their attention to content adaptive steganography, which reduces the visual distortion by exploiting Human Visual System's (HVS) lower sensitivity to high-frequency structural boundaries. To restrict LSB embedding to the highly textured region of the image, [4] suggested a Region of Interest (ROI) adaptive method using Canny edge detection. This method has led to a significant increase in the Peak Signal-to-Noise Ratio (PSNR) as compared to the conventional LSB. The technique did introduce a lot of computational complexity and was not algorithmically specific for choosing the threshold, however, this made it hard to reproduce and resistant to the most recent steganalysis. [19] extended the multi-detector methods by adding Canny, LoG and Prewitt detectors with optimal parameters as determined by the Bee Colony Footprint Edge Optimization (BCFEO) algorithm. Remarkably at low bit-rates, the framework achieved the PSNR of 64.96 dB. However, the BCFEO optimization is very computational-intensive, and the validation is only performed on fixed-resolution gray-level images and did not include learning-based steganalysis and lossy channel conditions. In an effort to improve the capacity of the system, [14] have proposed a new method for increasing the capacity by using hybrid edge detection (Canny and Sobel) with adaptive MSB substitution, which resulted in capacities up to 2.97 bpp. The method was tested for execution stability in noise and compression attacks, but was still only grayscale optimized and not tested with Spatial Rich Model (SRM) steganalysis.

In the optimization of the selection process, mathematically, [20] adopted the Genetic Algorithm (GA) to manage the Holistically-Nested Edge Detection (HED) attention maps. This method is able to successfully thwart CNN-based steganalysis (Xu-Net and Ye-Net), and retain a PSNR above 60 dB for low capacities. It showed good performance in ideal channels but the performance of the algorithm was poor in lossy channel operations such as JPEG compression and cropping which caused a bit error rate (BER) close to 0.5. Another approach was taken by [9] which used linear hash function over GF(2) in adaptive partitioning of blocks by gradient distributions. The framework was computationally efficient but was very susceptible to modern SRM-based steganalysis (100% detection at 0.1 bpp) and it was not very effective in reducing the embedding distortion.

2.3 Hybrid Frameworks and Optimization-Driven Steganography

Recent research efforts have been increasing to combine meta-heuristic optimization algorithms with the steganography pipeline and have resulted in hybrid frameworks and optimization-driven steganography. In content-adaptive LSB

framework, [5] presented a method based on Ant Colony Optimization (ACO) for payload dispersion to embed the content information in an adaptive manner and AES-GCM encryption for the content information. Although the method was able to get a PSNR around 60 dB and successfully resist both CNN-based steganalysis (CNN-Xu_Net, CNN-Ye_Net), the ACO algorithm imposed a tremendous computational burden and the system completely failed to recover the data when compressed in JPEG mode (QF=75). Likewise, [7] presented a multi-objective adaptive firefly-based secure steganography framework (MOAFOSS) to adaptively reduce the Mean Squared Error (MSE) at runtime. Although the proposed algorithm successfully surpasses the performance of the conventional algorithms such as PSO and GA in terms of structural preservation, the PSNR obtained by the proposed algorithm did not reach the standard acceptable values for visual imperceptibility as 42.58 dB. The iterative evaluation of the GA, however, limits the practical use of the GA in real systems of communication. In this case, [21] combined LBP, canny edge detection, and AES-256 with Arnold Cat Map scrambling. It was able to attain a 3.00 bpp capacity in their framework, but it was very fragile to normal image processing techniques, and was mainly used for tamper detection rather than for secure and confidential communication.

2.4 Advanced Cryptographic and Hyper-Chaotic Integration

The necessity for expanded key spaces has led to the adoption of multi-dimensional hyper-chaotic systems. [1] suggested a dual-layer secure transmission approach that is based on an adaptive steganography (MSB invariant) and a continuous 4D hyper-chaotic confusion-diffusion engine. For a PSNR > 50 dB and to obtain a perfect lossless recovery (MSE = 0), the system was found to have two positive Lyapunov exponents and a very large key space. Although this method solved the synchronization problem inherent in adaptive LSB, it was only tested under spatial domain attacks and its ability to resist the current deep learning steganalysis remained unchecked. [22] presented a three-stage cascade encryption (chaos-FrFT-Gyrator) scheme, which was capable of embedding text, image and audio information simultaneously. The system showed good numerical separation in known-plaintext attacks, but had no error-correcting capability, resulting in a linear rise in the Bit Error Rate (BER) when subjected to mild noise and occlusion attacks. In order to overcome the problem of robustness in losing channels, [23] proposed a base-3 (ternary) embedding algorithm based on DCT coefficients and Canny edge classification. This frequency domain method proved to be very robust against JPEG recompression and SRNet deep steganalysis but very susceptible to geometric transformations (e.g., rotation), which illustrates the tradeoff between capacity, robustness and complexity that is the subject of ongoing research in modern steganography.

2.5 Scientific Gaps and Motivation

The main objective of this study is to fill some of the gaps mentioned in the above-mentioned literature:

1. Traditional adaptive steganography methods like edge-directed LSB dynamically adjust the reference pixels used to compute the capacity map. This change causes a receiver "falling off the edge" synchronization problem. Optimization algorithms aim to fix this but have too much computational overhead. A mathematically invariant, lossless map without meta-heuristics is needed.
2. Uncomplicated Cryptography: The Logistic, Tent, and Arnold Cat Map are integer-order chaotic maps utilized in several chaotic map steganographic systems. Phase-space reconstruction and deep learning-based predictive assaults are becoming more likely in these systems with limited key space. The coupling of infinite non-local memory traces in a fractional-order hyper-chaotic system with the huge key space enlargement (e.g., 10^{180}) in spatial adaptive steganography has not been properly researched and examined.
3. Capacity-Fidelity Trade-off Limit: Global LSB substitution has low capacity, while increasing the payload (such as a 3-LSB one) decreases visual and statistical imperceptibility (PSNR lowers, detectability higher). A dynamic dimension-agnostic allocation technique that quantitatively identifies structural capacity analysis (MSBs) and data injection is needed to maximize payload gain without visual or statistical anomalies.
4. Insufficient Strict Sensitivity Analysis: Previous research validates chaotic encryption with histogram uniformity or standard correlation. To demonstrate immunity from brute force extraction attempts, the "Avalanche Effect" (trajectory divergence) reaction to microscopic perturbations (10-15) in fractional parameters is theoretically required.

3. Proposed Methodology

The proposed steganography methodology addresses some of the most critical payload capacity-security trade-offs by embedding the payload adaptively, dimension-agnostically, and scattered. The fractional-order hyper-chaotic system used in the cryptographic processing simply generates a random stego-key, unlike older systems that embedded data sequentially or globally. This scattered key determines embedding places, and a structural edge map governs their bit-capacity.

3.1 General Architecture of the Framework

The implementation of the framework is divided and executed systematically as metadata preserving, stego-key generation and adaptive embedding. A 25-bit metadata header is separated at the start of the cover, to allow full extraction of the data without loss. The framework then divides into two parallel processes, as shown in the Figure 1: the fractional-order dynamical mapping, for spatial scattering; and the invariant Most Significant Bit (MSB) edge detection for capacity allocation.

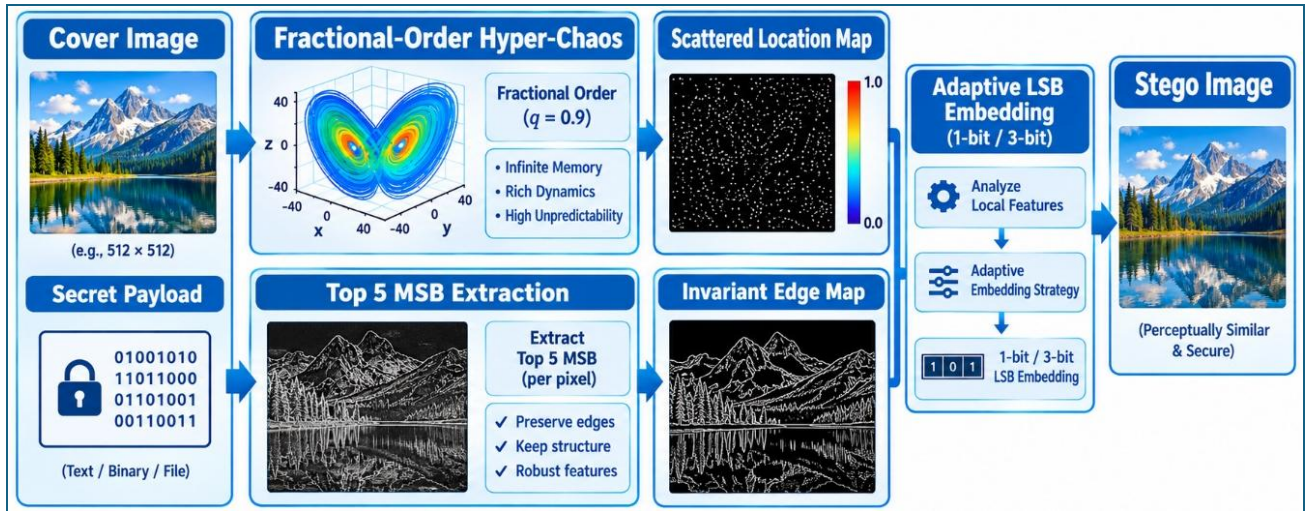


Figure 1. Block diagram of the proposed scattered adaptive steganography framework.

The architectural flow above shows that the system ensures that the spatial selection mechanism (chaotic system) and the payload capacity determination (MSB logic) are physically separated. This physical separation prevents the bit alteration as part of the last step of embedding from "re-entering" the capacity map, thus avoiding all desynchronization errors of conventional adaptive steganography. To ensure perfect reversibility, the exact bit-allocation of the metadata header must be strictly defined, as detailed in Table 1

Table 1. Bit-allocation structure of the 25-bit static metadata header.

Header Field	Allocated Bits	Description
Secret Height	12 bits	Defines the height of the secret image payload.
Secret Width	12 bits	Defines the width of the secret image payload.
Channel Indicator	1 bit	1 for RGB (3 channels), 0 for Grayscale.
Total	25 bits	Embedded in the first 25 pixels.

Fractional-Order Hyper-Chaotic Generator and Stego-Key

The system uses a four-dimensional fractional order hyper-chaotic system to create a cryptographically secure scattering path (the stego-key). Fractional calculus opens the door to non-local infinite memory, and is expected to increase the difficulty of phase-space reconstruction due to its higher-dimensional fractional-order dynamics and non-local memory. The fractional-order system is defined theoretically by using Caputo derivative, and numerically integrated with the help of a Grünwald-Letnikov (GL) approximation of the fractional-order derivative for ease of computation.

$$D_t^q x(t) = \frac{1}{\Gamma(1-q)} \int_0^t (t-\tau)^{-q} x'(\tau) d\tau \quad (1)$$

Where q denotes the fractional order ($0 < q < 1$) and $\Gamma(\cdot)$ represents the Gamma function. The 4D continuous system driving the stego-key is mathematically formulated as:

$$D_t^{q_1} x = a(y - x) + w \quad (2)$$

$$D_t^{q_2} y = cx - y - xz \quad (3)$$

$$D_t^{q_3} z = xy - bz \quad (4)$$

$$D_t^{q_4} w = -yz + dw \quad (5)$$

The first 500 samples were discarded as transient samples to ensure high cryptographic security, and to avoid initial state predictability, the valid embedding permutation was generated. The chaotic stego-key generation parameters and initial conditions are described in detail in Table 2.

Table 2. Initial conditions and system parameters used for fractional stego-key generation.

Parameter Type	Symbol	Value
Initial Conditions	x_0, y_0, z_0, w_0	0.1, 0.2, 0.3, 0.4
Fractional Orders	q_1, q_2, q_3, q_4	0.98, 0.98, 0.98, 0.98
Fixed Coefficients	a, b, c, d	$10, \frac{8}{3}, 28, -1$

3.2 Invariant Structural Edge Map Generation

The main drawback of traditional adaptive steganography is that the reference map gets distorted during the embedding process, causing a loss of synchronization between the sender and receiver. The proposed framework is based only on the Most Significant Bits (MSBs) to control the embedding logic and to ensure the capacity of the map is invariant.

Represent the native color picture by a 3D array C whose size is $M * N * 3$, M and N are the number of spatial pixels, and $C(i, j, k)$ is the value of the color channel k at the spatial pixel (i, j) , with $k \in \{1, 2, 3\}$ representing the red, green, and blue channels respectively and all values in $C(i, j, k)$ being drawn from the range $[0, 255]$. The algorithm first performs a bitwise AND with the decimal mask 248 (binary 11111000_2) with all the channels to clear out the lower three Least Significant Bits (LSBs):

$$C_{MSB}(i, j, k) = C(i, j, k) \text{ AND } 248 \quad (6)$$

A robust 3D matrix C MSB is projected in a 2D luminance plane (Y) using standard psychovisual weighting coefficients:

$$Y(i, j) = 0.2989 \cdot C_{MSB}(i, j, 1) + 0.5870 \cdot C_{MSB}(i, j, 2) + 0.1140 \cdot C_{MSB}(i, j, 3) \quad (7)$$

Subsequently, the spatial gradient is calculated using the Sobel differential operator. The horizontal gradient G_x and vertical gradient G_y are obtained through 2D spatial convolution ($*$) with the respective Sobel kernels S_x and S_y :

$$G_x(i, j) = Y(i, j) * S_x, \quad G_y(i, j) = Y(i, j) * S_y \quad (8)$$

The absolute gradient magnitude $G(i, j)$ is mathematically defined as:

$$G(i, j) = \sqrt{G_x(i, j)^2 + G_y(i, j)^2} \quad (9)$$

Finally, a binary structural edge map $E(i, j)$ is generated by applying a threshold T_{edge} . To ensure dimension-agnostic compatibility with the native color image, this 2D map is replicated across the spatial depth to form E_{3D} , mathematically expressed as:

$$E_{3D}(i, j, k) = \begin{cases} 1, & \text{if } G(i, j) \geq T_{edge} \text{ (Complex Edge)} \\ 0, & \text{if } G(i, j) < T_{edge} \text{ (Smooth Region)} \end{cases} \quad (10)$$

It builds only on the 5 most significant bits (MSBs); the 3 least significant bits (LSBs) are discarded before it generates the edge-map. Thus, changing the LSBs at the transmitter will not affect the E_{3D} at the receiver and the whole process is mathematically reversible. The result of this transformation from the original image to the separated MSB luminance and the final image of the invariant edges is shown in Figure 2.

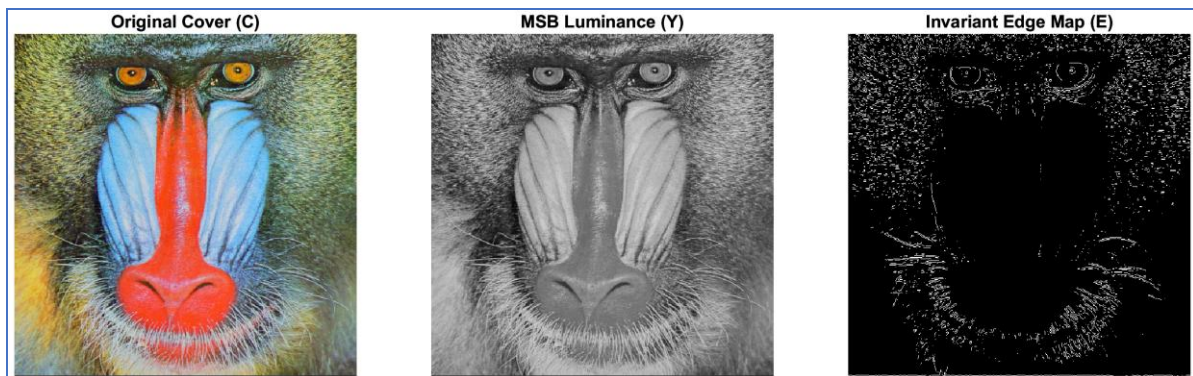


Figure 2. Visual representation of the invariant structural edge map.

The example visual sequence shown above illustrates the effect of converting the original cover (left) to the MSB luminance map (center). Notice that the macro-structural content of the image is not lost but that the microscopic texture details contained in the LSBs are discarded. The result is the invariant edge map which is seen on the right side which clearly shows the high frequency boundaries. Each of these white pixels ($E_{3D} = 1$) represents areas of the HVS where it is least sensitive to noise, and therefore allows for the embedding of a higher payload.

3.3 Scattered Adaptive Capacity and Mathematical Embedding

The scattered embedding coordinates can be identified by the vector of stego-key and the map E_{3D} with the topological complexity can be used to allocate the adaptive payload capacity. The capacity of the bit for each of the $k(i, j, k)$, is dynamically set according to the following step function:

$$k(i, j, k) = \begin{cases} 3 \text{ bits,} & \text{if } E_{3D}(i, j, k) = 1 \\ 1 \text{ bit,} & \text{if } E_{3D}(i, j, k) = 0 \end{cases} \quad (11)$$

Hence, the proposed algorithm C_{prop} (excluding the required 25-bit metadata header) is defined as follows:

$$C_{prop} = \left(\sum_{i=1}^M \sum_{j=1}^N \sum_{c=1}^3 k(i, j, c) \right) - 25 \quad (\text{bits}) \quad (12)$$

The embedding process is done physically using direct mathematical substitution. Let B_{secret} denote the decimal integer value of the secret binary stream chunk (which has a k bit length). The stego-pixel $S(i, j, k)$ is calculated by wiping the lowest k bits with a dynamic masking variable M_{mask} , and adding B_{secret} .

$$M_{mask} = 256 - 2^{k(i, j, k)} \quad (13)$$

$$S(i, j, k) = (C(i, j, k) \text{ AND } M_{mask}) + B_{secret} \quad (14)$$

This adaptive substitution ensures that high density data is only injected at structural boundaries defined by the fractional stego-key, with an optimum balance of cryptographic scattering, payload and visual imperceptibility. This is the sequential transformation of the continuous chaotic trajectories (real-valued) to the discrete and unique integer embedding coordinates as shown in Figure 3.

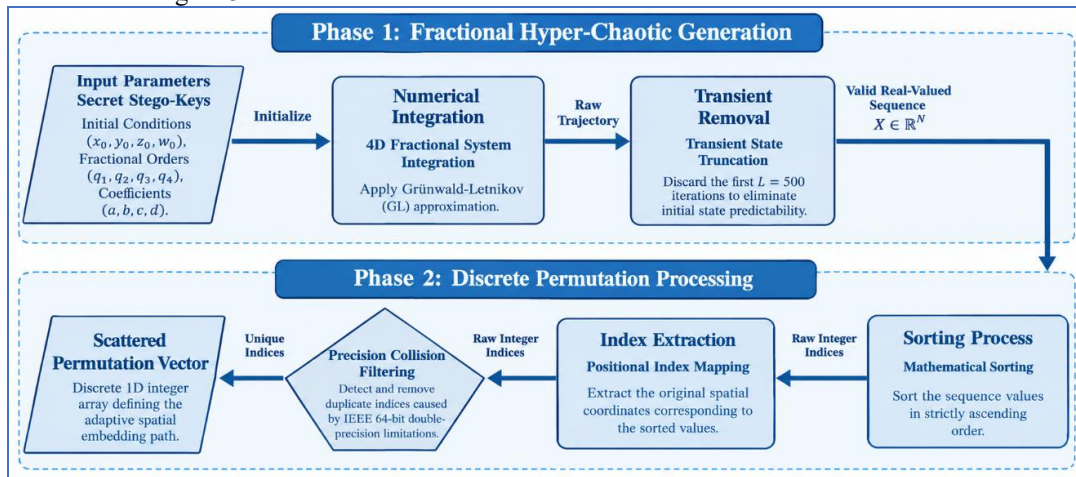


Figure 3. Flowchart of the generation of the scattered index of the fractional order hyper-chaotic system.

The generation process begins by numerically integrating the fractional system as shown in the Figure 3. The first 500 transient iterations are removed to fully remove the initial state predictability. Mathematically sort the remaining valid real valued sequence, and extract the original sequence indices. This resulting integer vector is the pseudo-random spatial permutation path for payload scattering after any possible duplicates due to numerical precision limits are filtered, and is used as the definitive pseudo-random spatial permutation path for embedding secret data in a non-sequential manner across the cover medium.

3.4 Blind Extraction and Perfect Reversibility

One of the most important criteria for an advanced steganographic system is blind extraction, in which the receiver can completely recover the secret message without using the original cover image. The proposed framework is fully reversible by the use of a deterministic extraction sequence. The extraction algorithm starts with reading the 25-bit static metadata header included in the first 25 pixels of the received stego-image S. This header was embedded in the standard way of 1-bit

substitution; thus, the spatial dimension (H_{secret}, W_{secret}) and color depth (C_{secret}) can be easily retrieved by extracting the absolute Least Significant Bit (LSB):

$$Header(i) = S(i) \text{ AND } 1, \quad \text{for } i = 1, 2, \dots, 25 \quad (15)$$

This metadata computes the exact total payload bits ($Total_{Bits} = H_{secret} \times W_{secret} \times C_{secret} \times 8$), which acts as the strict stopping criterion for the algorithm. The receiver has to reconstruct the invariant edge map E_{3D} to find out the embedding capacity of the other pixels. By preserving the top 5 Most Significant Bits (MSBs) during the adaptive embedding, the receiver performs the same masking operation on the stego-image S:

$$S_{MSB}(i, j, k) = S(i, j, k) \text{ AND } 248 \quad (16)$$

This ensures that the structural luminance at the receiver side is exactly the same as that at the sending side, and that the result of the Sobel gradient at the receiving side is the same as at the sending side. After that, the receiver feeds the same secret keys (initial conditions and fractional orders) into the Grünwald-Letnikov fractional generator, thus regenerating the same chaotic stego-key vector. The receiver walks along the scattered permutation path as summarized in the algorithmic flowchart in Figure 4. If edge map $E_{3D}(i, j, k)$ is reconstructed to be 1, then the receiver can take the 3 bits by masking the pixel with 7 (binary 00000111₂). If $E_{3D}(i, j, k) = 0$, only 1 bit is extracted.

$$Extracted_{Bits} = \begin{cases} S(i, j, k) \text{ AND } 7, & \text{if } E_{3D}(i, j, k) = 1 \\ S(i, j, k) \text{ AND } 1, & \text{if } E_{3D}(i, j, k) = 0 \end{cases} \quad (17)$$

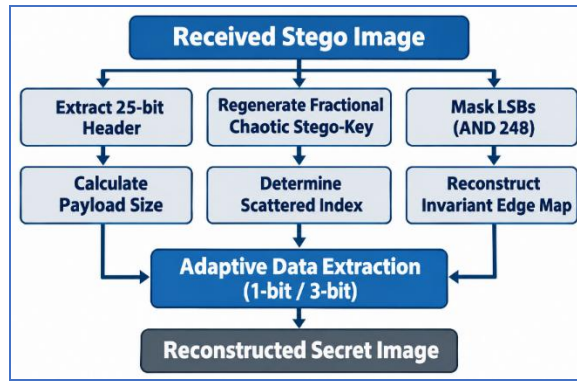


Figure 4. Algorithmic flowchart demonstrating the blind extraction process.

The parallel structure demonstrated in the flowchart, visually verifies the synchrony integrity of the system. The algorithm performs header extraction, regeneration of the stego-key and edge map reconstruction as independent parallel pre-processing operations, which ensures that all dynamic variables are mathematically aligned prior to the extraction of the scattered payload. This structural independence has the ability to completely remove the type of bitstream desynchronization errors that have been common in adaptive steganography models.

4. Evaluation Metrics

Standard mathematical metrics are used to quantify imperceptibility, fidelity and capacity improvement of the proposed framework.

4.1 Peak Signal-to-Noise Ratio (PSNR)

The PSNR is an objective measure of visual distortion between the original cover image C and the stego-image S. It is based upon the Mean Squared Error (MSE). If the image has a size of $M \times N \times 3$, the formulas are:

$$MSE = \frac{1}{M \times N \times 3} \sum_{k=1}^3 \sum_{i=1}^M \sum_{j=1}^N [C(i, j, k) - S(i, j, k)]^2 \quad (18)$$

$$PSNR = 10 \cdot \log_{10} \left(\frac{255^2}{MSE} \right) \quad (\text{dB}) \quad (19)$$

Higher PSNR values (typically above 40 dB) indicate excellent steganographic imperceptibility.

4.2 Structural Similarity Index Measure (SSIM)

It is different from PSNR that measures absolute errors of pixels, the SSIM considers the degradation of perceived structural information, luminance, and contrast. It is given by the formula:

$$SSIM(C, S) = \frac{(2\mu_C\mu_S + c_1)(2\sigma_{CS} + c_2)}{(\mu_C^2 + \mu_S^2 + c_1)(\sigma_C^2 + \sigma_S^2 + c_2)} \quad (20)$$

Where μ and σ^2 are the local means and variances, respectively, σ_{CS} is the covariance, and c_1, c_2 are stabilizing constants. An SSIM value approaching 1.0 indicates near-perfect structural preservation.

4.3 Payload Gain Capacity (G%)

The payload gain percentage is computed for the proposed MSB-invariant adaptive algorithm in comparison to the standard 1-bit global LSB embedding by measuring the number of edge pixels (N_{edge}) in the cover matrix:

$$G\% = \left(\frac{c_{prop} - c_{std}}{c_{std}} \right) \times 100 \quad (21)$$

4.4 Correlation Coefficients

To check statistical linear dependence and structural similarity between original cover image (C) and generated stego-image (S), correlation coefficient (r) is used. Values close to 1.0 mean that the adaptive embedding process does not change the statistical properties of the image and retains the structural pixel relationships. It is mathematically defined as:

$$r = \frac{\sum_{i,j} (c_{i,j} - \mu_C)(s_{i,j} - \mu_S)}{\sqrt{\sum_{i,j} (c_{i,j} - \mu_C)^2 \sum_{i,j} (s_{i,j} - \mu_S)^2}} \quad (22)$$

Where μ_C and μ_S denote the mean pixel values of the cover and stego images, respectively.

5. Results and Discussion

5.1 Fractional-Order Hyper-Chaotic Dynamics and Stego-Key Sensitivity

The pseudo-random index generation is in the heart of the proposed scattered adaptive steganographic framework. A four-dimensional fractional order hyper-chaotic system is used as the stego-key generator, which is capable of resisting the modern attacks such as phase-space reconstruction attacks and brute force key guessing. The non-local infinite memory trace stored in the generation path is mathematically provided by the fractional calculus, significantly increasing the dynamical complexity of the model, which goes far beyond the integer order ones. The time series of the state variables are shown in figure 5.

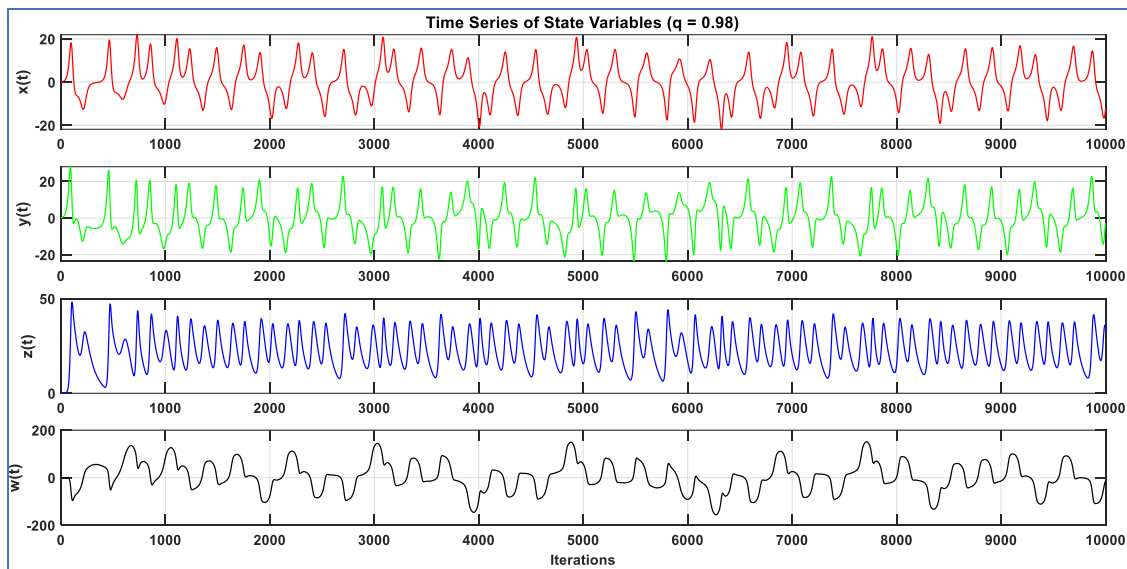


Figure 5. Continuous pseudo random amplitude variations.

Figure 5 shows large temporal variations that are extremely non-periodic. As a result, these sequences produce a uniform and unpredictable spatial permutation vector, which was able to effectively spread the secret bits embedded in the cover image. In order to check the chaotic dynamical behavior of the system, the phase portraits are mapped in Figure 6.

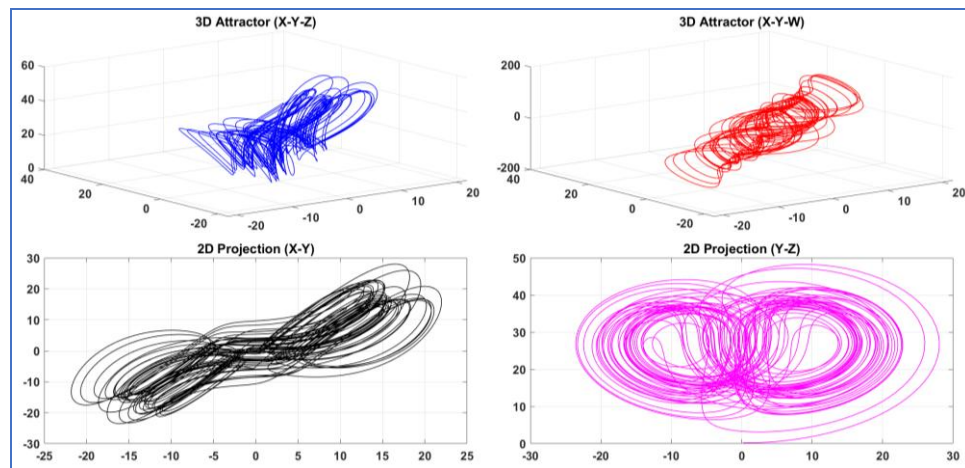


Figure 6. Two and three-dimensional phase portraits.

The trajectory has the appearance of a bounded aperiodic pattern in the plotted phase space which has a butterfly shape. This indicates that it is not stable and it does not diverge to infinity, as seen in Figure 6, and that shows that the system is not stable, nor is it infinite divergent, but that it is strictly confined inside the phase space. But, with only visual representation, it cannot be called hyper-chaos. In the case of the strict mathematical proof, one needs to numerically calculate the spectrum of Lyapunov Exponents (LE) as is shown in Figure 7.

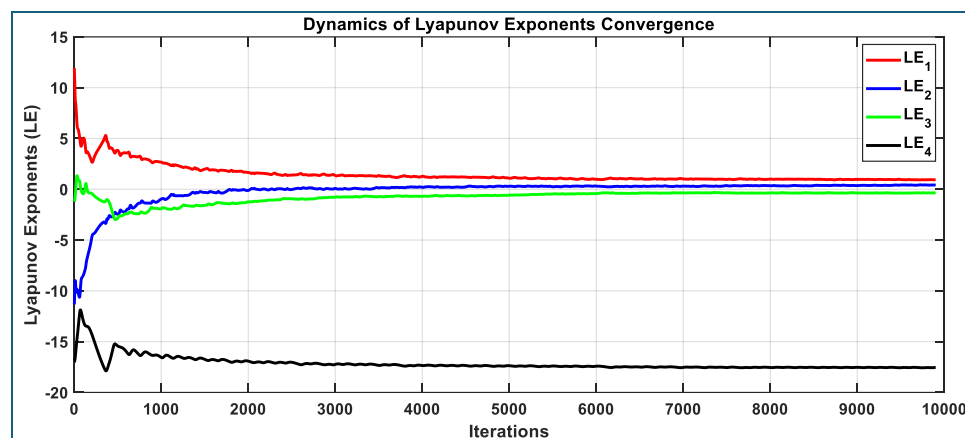


Figure 7. Dynamic Convergence of Lyapunov Exponents.

The spectrum excellently converges over the iterative evaluation showing two clearly positive Lyapunov Exponents ($LE_1 > 0$ and $LE_2 > 0$) as seen in Figure 7. The converged Lyapunov spectrum is numerically reported in Table 3. Two positive exponents are part of the dynamics generated, giving the criterion for categorizing the dynamics as hyper-chaotic in this study. This means that the system grows at the same time in several directions of space.

Table 3. Numerical values of the converged Lyapunov Exponents spectrum.

Exponent	Final Converged Value
LE_1	46.7042475294450
LE_2	20.3465877191712
LE_3	-17.8723373624309
LE_4	-876.972050374003

One of the most important properties of any stego-key generator is that even a very small change in the security key results in complete failure to extract the data in an avalanche effect. In the proposed framework, the secret keys are the initial conditions (x_0, y_0, z_0, w_0) and the fractional orders (q_1, q_2, q_3, q_4) which increase the conventional key space. Figure 12 shows the fractional order perturbed sensitivity of the system.

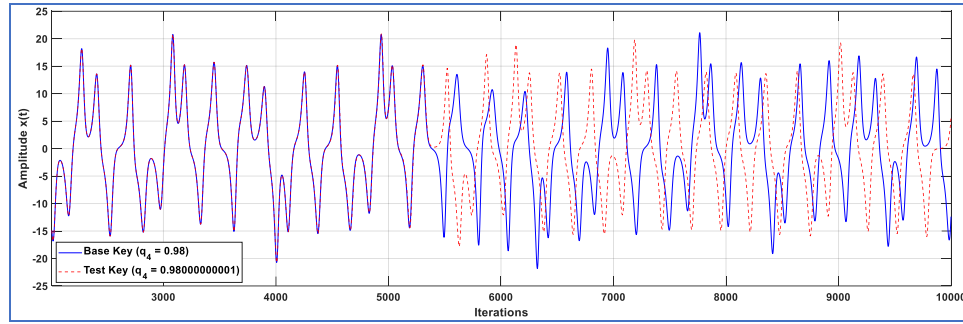


Figure 8. Extreme trajectory divergence resulting from a minimal perturbation in the fractional order parameter ($\Delta q_4 = 10^{-10}$).

In Figure 8, the value of one fractional order parameter is changed from 0.98 to $0.98 + 10^{-10}$, resulting in a trajectory that starts out close to the base sequence but soon and exponentially diverges. This is to validate that the fractional orders work individually as very sensitive cryptographic keys. Moreover, it is shown in figure 9 that the system is absolutely sensitive to initial conditions.

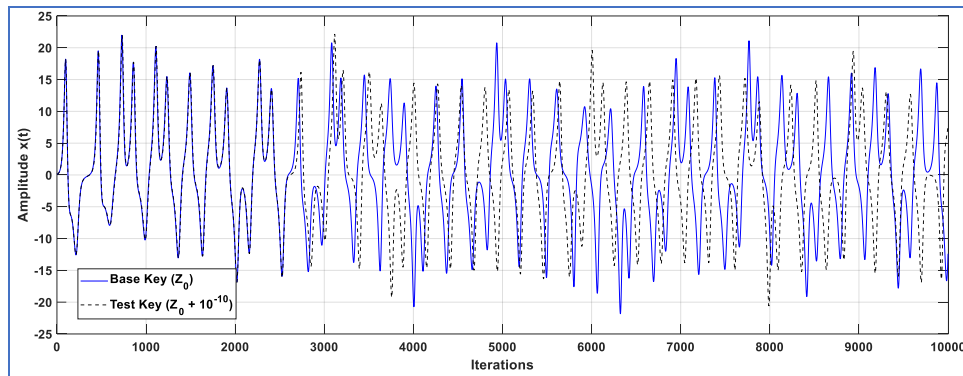


Figure 9. Complete spatial divergence of the pseudo-random sequence when the initial condition variance (Δz_0) is very small (10^{-15}).

5.2 Payload Capacity and Edge-Directed Gain

One of the drawbacks of conventional spatial domain steganography is that the payload size is limited by the embedding rate due to visual degradation. This is addressed by the proposed framework that uses an MSB-invariant structural edge map to dynamically allocate embedding capacity. The embedding capacity is not fixed but differs depending on the complexity of the textural content on the cover image as detailed in Table 4. Homogeneous regions are able to store 1 bit/pixel without being detected by human visual sensitivity and high frequency structural boundaries are able to store 3 bits/pixel while significantly reducing the perceptual impact of the embedding modifications.

Table 4. Quantitative comparison of embedding capacity and payload gain across standard color cover images (512×512×3).

Cover Image	Total Embeddable	Spatial Edge Locations	Proposed Capacity	Payload (bpp)	Payload Gain
Peppers	786,432 Samples	16,968	102,542.88 Bytes	3.129bpp	% 4.32+
Lena	786,432 Samples	24,888	104,522.88 Bytes	3.189bpp	% 6.33+
Baboon	786,432 Samples	37,957	107,790.12 Bytes	3.289bpp	% 9.65+

The empirical results show clearly the intelligent and content-aware properties of the proposed adaptive steganographic algorithm. In a conventional (1-bit Least Significant Bit) embedding scheme the theoretical capacity is strictly determined by the spatial characteristics of the image and is fixed at 98,300.88 Bytes, after subtracting the 25-bit metadata header reduction. The proposed framework overcomes this limitation by using the MSB-invariant edge map. The complexness of the carrier image is directly proportional to the embedding capacity. The "Peppers" image, which has broad homogeneous regions and smooth gradients, has 16,968 structural edge pixels, and a conservatively estimated capacity gain of 4.32%. By comparison, the "Baboon" photo, with its high frequency of fine texture details, such as fur patterns, has a much higher edge count of 37,957 pixels. The textural density enables the algorithm to safely inject a higher amount of 3-bit payload chunks, with a maximum of 107,790.12 Bytes, which corresponds to a maximum payload gain of 9.65% relative to the conventional 1-bit LSB baseline used in this study. The "Lena" image has a medium texture profile, resulting in a middle 6.33% gain. The data shows that the framework has been successful in utilizing the psycho-visual masking effects of the

HVS (Human Visual System). The system pushes data payloads dynamically into heavy points of data structure only at complex boundaries where visual noise is naturally hidden to optimize data throughput while keeping the imperceptibility of the stego-image intact.

5.3 Pixel-Level Fidelity and Statistical Similarity

The basic demand for a good steganographic system is that the cover medium must not contain visible artifacts or statistically significant anomalies, which are perceptible by a human observer, when the secret information is embedded in it. For quantitative assessment of the imperceptibility of the proposed adaptive scattered embedding method, its Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM) and the Correlation Coefficient (Corr.) was calculated for different topological test cases and presented in Table 5. Needless to mention, all the secret images were sized to fit within the “payload” dimensions of their respective cover image. In the case of RGB images, the MSE and PSNR are calculated across all three channels.

Table 5. Quantitative imperceptibility performance and structural fidelity of the generated stego-images.

Cover Image	Secret Image	MSE	PSNRdB	SSIM	Corr.
Peppers	Cameraman	0.6307	50.1327	0.9994	0.9999
Lena	Cameraman	0.5912	50.4133	0.9997	0.9999
Baboon	Cameraman	0.5121	51.0371	0.9998	0.9999
Baboon	Rod	0.6219	50.1938	0.9997	0.9999

As shown in the empirical results in Table 5, the proposed framework shows excellent visual fidelity. In a large number of image processing studies, PSNR values greater than 40 dB are considered to signify low visible distortion but this threshold does not guarantee perceptual undetectability. Interestingly, the proposed approach produces the PSNR values of more than 50 dB (from 50.13 dB to 51.03 dB) for all the image pairs under test. The high performance is directly attributed to a psycho-visual masking property of Human Visual System (HVS): strictly restricting the high capacity 3-bit embedding to complex structural edges and limiting smooth regions to 1-bit alterations. Furthermore, SSIM is always greater than 0.999, i.e., the integrity of the macro-structure, its luminance and contrast are preserved before and after the data is inserted, which shows a very high degree of similarity between the two images. In order to complement the mathematical metrics, the embedding process is also evaluated visually and statistically and is presented in Figures 10-11.

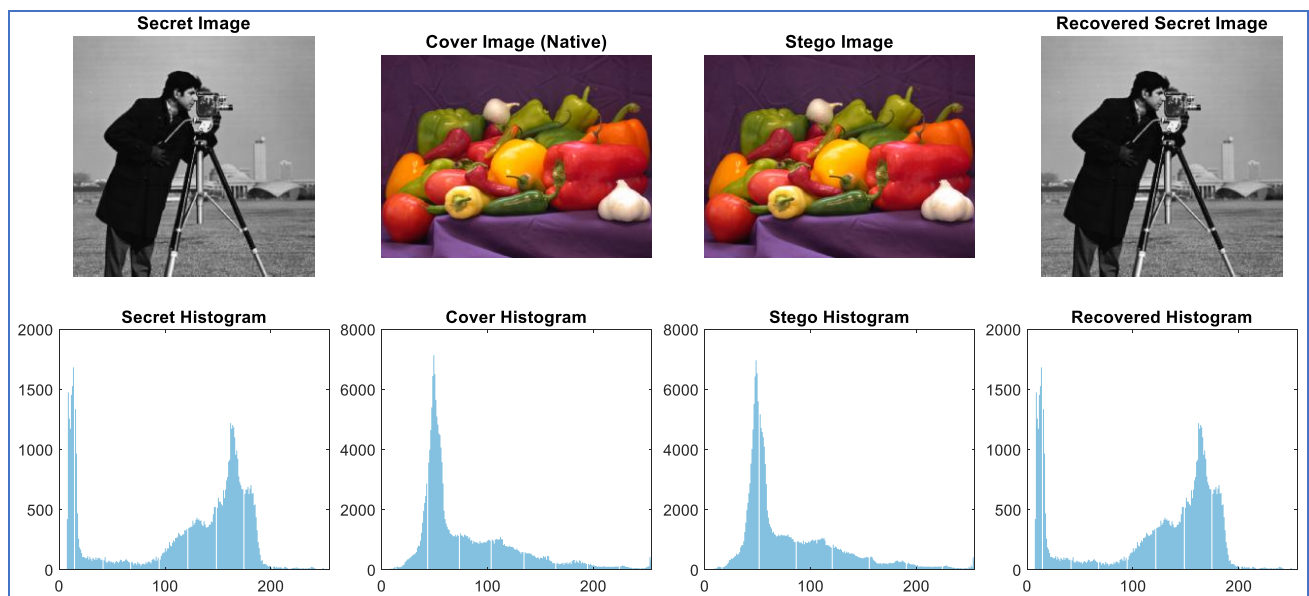


Figure 10. Visual and statistical evaluation of embedding the Cameraman payload into the Peppers cover image.

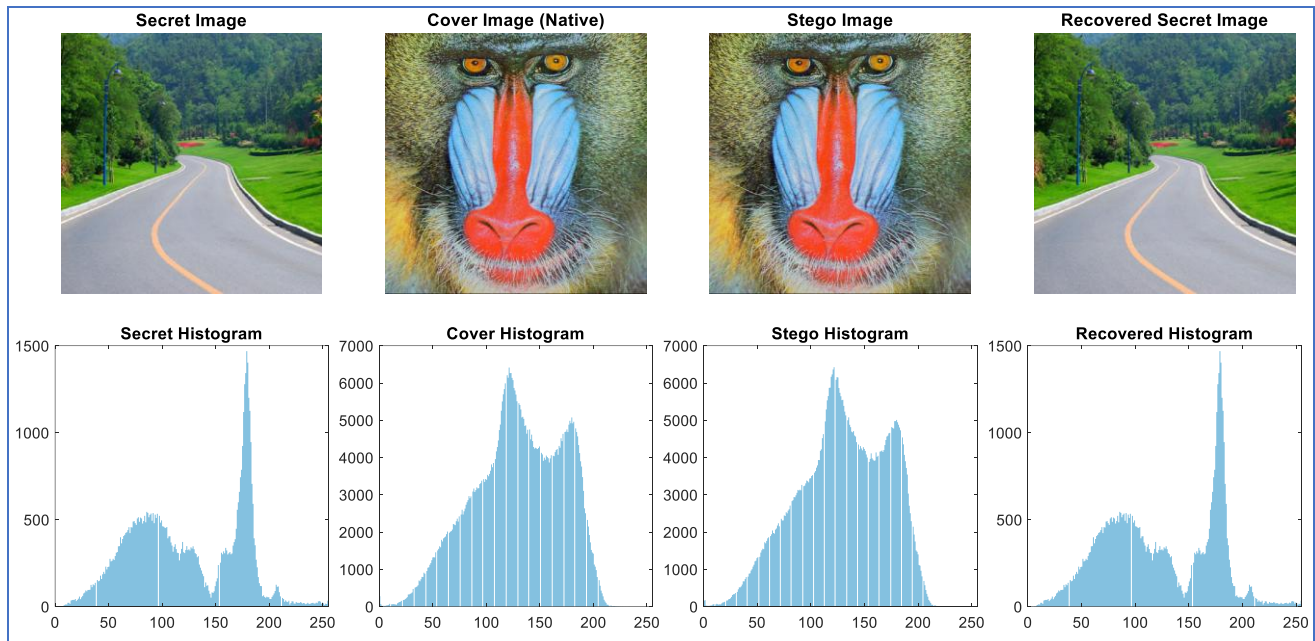


Figure 11. Visual and statistical results of embedding a Rod image payload into the Baboon cover image.

A subjective visual assessment of generated stego-images (Figures 10–11) confirms the quantitative measurements, where no distortion, color bleeding or edge pixelation can be observed when compared to their native cover images. Importantly, the statistical robustness is verified using the histogram analysis. The structures of the frequency distributions of the pixel intensities (Cover Histogram vs Stego Histogram) are the same. The histogram comparison suggests that only small differences should be noted in the first-order pixel-intensity distribution when embedding the proposed method. However, the similarities of the histograms do not give any indication of resistance to contemporary steganalysis (SRM, for instance) is recognized as a valuable avenue for future research.

5.4 Blind Reversibility and Lossless Extraction

One of the key problems in adaptive steganography is keeping the sender-receiver in sync. The conventional method is prone to corruption of the bitstream due to the modification of the reference map used to extract the bitstream. Table 6 shows that the proposed MSB-invariant edge map is effective to solve this desynchronization problem.

Table 6. Quantitative validation of lossless recovery for the extracted secret payload images.

Cover Image	Secret Image	MSE	PSNRdB	SSIM	Corr.
Peppers	Cameraman	0.0000	∞	1.0000	1.000
Lena	Cameraman	0.0000	∞	1.0000	1.000
Baboon	Cameraman	0.0000	∞	1.0000	1.000
Baboon	Rod	0.0000	∞	1.0000	1.000

As mathematically confirmed in Table 6, the proposed framework is exact lossless recovery (noiseless conditions). In all the topological test cases (complex and smooth), the Mean Squared Error (MSE) between the original secret payload and the blindly extracted payload is equal to 0, which gives an infinite PSNR of ∞ and a perfect SSIM of 1.0000. The secret images are recovered without any degradation on the pixels as shown in Figures 10-11, where the "Recovered Secret Image" and "Recovered Histogram" panels show the recovered images. This perfection is possible since only the top 5 MSBs are used to calculate the spatial edge map and are completely not touched in the LSB substitution phase. Therefore, the receiver creates a capacity map that is exactly the same as the sender's map, so that each 1-bit and 3-bit chunk is retrieved from exactly the same location scattered by the fractional chaotic stego-key, without the need to access the original cover image.

5.5 Key Space and Brute-Force Resistance

In order to quantify the theoretical key space, the proposed framework utilizes 12 highly sensitive parameters: the four initial conditions (x_0, y_0, z_0, w_0) , the four fractional orders (q_1, q_2, q_3, q_4) and the four system coefficients (a, b, c, d) . The

coefficients are not constants but dynamic secret ones which are chosen within continuous range that can support the hyper-chaotic dynamics mathematically. Given a typical IEEE 64-bit double-precision format, with an effective computational precision of 10^{-15} per parameter, the total key space SKS can be found as follows.

$$K = (10^{15})^{12} = 10^{180} \quad (23)$$

Converted to bits, this yields:

$$K_{bits} \approx \log_2(10^{180}) = \frac{180 \times \ln(10)}{\ln(2)} \approx 598 \text{ bits} \quad (24)$$

2^{598} is a key space that greatly surpasses the required cryptographic density of 2^{128} [2], [24], [25]. This substantial theoretical capacity increases the computational difficulty of exhaustive key-search attacks under the tested implementation assumptions.

5.6 Comparative Analysis with State-of-the-Art

A comparative analysis with recent state-of-the-art steganographic and cryptographic methods is carried out, in order to place the proposed framework in the context of secure communications. The comparison is made based on embedding capacity, visual imperceptibility (PSNR), extraction reversibility (MSE) and cryptographic key space.

Table 7. Performance comparison between the proposed framework and recent studies.

Author (Year), Ref	Methodology / Domain	Embedding Capacity	PSNR (dB)	Reversibility (Extraction)	Cryptographic Key Space
R. A. Sahun (2026), [1]	Integer 4D Hyper-Chaos (Encrypt-then-Hide) + MSB	Adaptive	> 50.00	Exact lossless (noiseless)	≈ 450 bits
Abadin and Sulaiman (2026), [19]	BCFEO + Multiple Edge Detectors	1.00 bpp	55.91	Lossless	AES-128 standard
Ismail et al. (2026), [14]	Hybrid Edge (Canny/Sobel) + MSB	2.97 bpp	42.27	Lossless	Not specified
Patel and Vekariya (2026), [26]	Block-based Indexing + 3-LSB	3.00 bpp (with index overhead)	49.19	Lossless (noiseless only)	Not specified
Aljughaiman et al. (2025), [5]	ACO + Saliency LSB	Fixed Low Payload	60.16	Lossy under compression	AES-GCM
Noorallahzadeh (2026), [23]	Ternary DCT + Canny	0.64 bpp	62.4	Lossless	Not specified
S. Anu Priya, et al(2026), [4]	ROI Canny-based LSB	Adaptive	44.8	Lossless	Not specified
Proposed Framework	Fractional 4D Chaos (Simultaneous Scatter-Hide)	Adaptive (Up to +9.65% Gain)	> 50.00	Absolute Lossless (MSE = 0)	≈ 598 bits

The proposed framework provides a desirable trade-off between capacity, security and fidelity as shown in Table 7. Optimization based approaches [5], [23] achieve higher PSNR, but introduce tremendous amount of computation, and traditional edge adaptive methods [4], [19] may not have a good encryption or lower PSNR. While both make use of MSB-invariant mapping for exact lossless recovery (MSE=0), the main novelty of our framework compared to [1] is that instead of the two-stage "encrypt-then-hide" approach, our framework implements a highly efficient simultaneous scatter-and-hide approach. Moreover, the higher order chaos in [1] is increased from integer order to fractional order, which utilizes the non-local memory to greatly enlarge the active key space from 450 bits to 598 bits, and consequently enhance the theoretical resistance against exhaustive brute-force parameter search.

5.7 Computational Complexity and Runtime Analysis

The computational parts of the proposed framework are the fractional order numerical integration, Sobel edge map generation part and scattered index generation part. The Sobel filtering and pixel-wise embedding operations have linear relationship with the number of image samples $\mathcal{O}(N)$. The non-local history approximation of the fractional-order generation has an additional computational cost but it is still much faster than iterative meta-heuristic algorithms (e.g., genetic algorithms). The framework was realized on a common personal computer (Intel Core i7, 16 GB RAM) with the

help of MATLAB. The average embedding time is around 2.4 seconds and blind extraction time is about 2.1 seconds per $512 \times 512 \times 3$ RGB image. This shows the viability of the proposed method for secure transmission in practical applications not requiring real-time.

5.8 Limitations of the Current Study

In the present study, the proposed method has been shown to have good imperceptibility parameters, but an exhaustive evaluation has not been carried out in the present study against recent steganalysis detectors including the classifiers based on SRM and CNN. This is an essential weakness and will be looked into in future work. In addition, experiments were not conducted to distinguish the role of the fractional order dynamics, the MSB based edge mapping, adaptive bit allocation and chaotic scattering and are therefore deferred to future research. Additionally, the current evaluation only considers a small number of standard benchmark images and provides only single-run performance data. Future work should involve larger and more varied data sets in order to achieve greater statistical generality, and to provide mean performance with standard deviations.

6. Conclusion

A channel-agnostic scattered adaptive steganography framework to solve the issue of spatial desynchronization was proposed in this paper. The system was able to separate capacity allocation from the physical embedding of data, and thus to obtain a strictly invariant structural edge map from the unaltered Most Significant Bits (MSBs). This isolation avoided a 'falling off the edge' vulnerability, allowing exact lossless blind extraction ($MSE = 0$) in the noiseless case. A 4D fractional order hyper-chaotic system was employed to secure the embedding path of the spatial embedding. The non-local memory of the fractional derivatives led to a very sensitive scattering sequence, which extended the theoretical active key space to about 598 bits and made the exhaustive search of parameters more difficult. The experimental results showed that the framework adapts dynamically to the carrier topologies, with the maximum payload gain being of 9.65% with respect to the standard 1-bit LSB. This capacity enhancement has been achieved while keeping the visual fidelity on the high side with PSNR values greater than 50 dB and SSIM greater than 0.999. The current study is however limited to noiseless spatial domain condition and not extensively evaluated against recent learning-based steganalysis (e.g., SRM) and known-cover attacks. In future, the efforts would be spent on incorporating powerful error correcting codes, invariant fractional logic in frequency domain (DCT/DWT), in order to make the code more robust towards lossy compressions, as well as benchmarking the steganalysis.

References

- [1] R. A. Sahun, "Nonlinear 4D Hyper - Chotic Dynamics and Invariant Spatial Steganography for Secure Visual Information Transmission," *Journal of the College of Basic Education*, vol. 32, no. 137, pp. 859–889, 2026.
- [2] A. K. Jawad, G. Karimi, and M. Radmelkshahi, Hyper-Chaotic Scrambling for Audio Encryption: An Optimization Approach for High Security, Low Latency, and Efficient Use of Bandwidth. Springer, 2025. doi: 10.1007/978-981-96-7523-4_14.
- [3] H. Alwan and Z. Hussain, "A Multiplicative-Additive Chaotic-Address Steganography," *Journal of Kufa for Mathematics and Computer*, vol. 7, no. 2, pp. 16–25, Nov. 2021, doi: 10.31642/JoKMC/2018/070204.
- [4] S. Anu Priya, M. Angelin Rosy, and M. Felix Xavier Muthu, "An Enhanced ROI-Based Image Steganography Method for Secure Data Hiding," *International Explore Journal of Computer Science and Applications*, vol. 4, no. 2, pp. 110–119, Apr. 2026, doi: 10.34293/iejcsa.v4i2.105.
- [5] A. Aljughaiman and R. Alrawashdeh, "Content-adaptive LSB steganography with saliency fusion, ACO dispersion, and hybrid encryption with ablation study," *Scientific Reports*, vol. 16, no. 1, p. 3829, Dec. 2025, doi: 10.1038/s41598-025-33920-9.
- [6] A. K. Singh and J. Singh, "Parameter optimized edge guided image steganography using variable bit LSB embedding for high capacity and visual fidelity," *Discover Applied Sciences*, vol. 8, no. 6, 2026, doi: 10.1007/s42452-026-08602-4.
- [7] A. V Gahan and G. D. Devanagavi, "An Intelligent Multi-Objective Optimization Approach for High-Capacity Secure Image Steganography," *Engineering, Technology & Applied Science Research*, vol. 16, no. 3, pp. 34973–34981, Jun. 2026, doi: 10.48084/etasr.18267.
- [8] H. N. Abdullah, S. S. Hreshee, and A. K. Jawad, "Noise Reduction of Chaotic Masking System using Repetition Method," 2016. [Online]. Available: <https://www.researchgate.net/publication/291356303>
- [9] E. Daiyrbayeva *et al.*, "Application of a Linear Hash Function in Adaptive Image Steganography," *Technologies*, vol. 14, no. 4, p. 243, Apr. 2026, doi: 10.3390/technologies14040243.

- [10] T. Alobaidi, "Blind Content-Adaptive Multi-Image Steganography Using Canonical Sparse Multi-Transform Residual Maps and AES-GCM," *Systems and Computing*, vol. 2, no. 2, pp. 84–94, Jul. 2026, doi: 10.64409/sycom.v2.i2.64.
- [11] M. Khalid, E. A. E. A. R. Hussein, Ameer K. Jawad, and A. K. Jawad, "Digital Image Encryption Based on Random Sequences and XOR Operation," *Journal of Engineering and Applied Sciences*, vol. 14, no. 8, pp. 10331–10334, 2019.
- [12] S. S. Hreshee, H. N. Abdullah, and A. K. Jawad, "A high security communication system based on chaotic scrambling and chaotic masking," *International Journal on Communications Antenna and Propagation*, vol. 8, no. 3, pp. 257–264, 2018, doi: 10.15866/irecap.v8i3.13541.
- [13] A. K. Jawad, H. N. Abdullah, and S. S. Hreshee, "Secure speech communication system based on scrambling and masking by chaotic maps," *International Conference on Advances in Sustainable Engineering and Applications, ICASEA 2018 - Proceedings*, no. March, pp. 7–12, 2018, doi: 10.1109/ICASEA.2018.8370947.
- [14] S. M. Ismail, F. E. AbuAladas, M. Abu Helou, and W. Abu-ulbeh, "Edge-Adaptive High-Capacity Image Steganography Using Hybrid Edge Detection and MSB Embedding," *Computers*, vol. 15, no. 3, p. 141, Feb. 2026, doi: 10.3390/computers15030141.
- [15] R. Sahun, A. Hamad, L. Al-saadi, and A. Jawad, "Lorenz, Rossler, and Chan systems for key generation and pixel selection in chaotic image encryption," *Journal of University of Anbar for Pure Science*, vol. 19, no. 2, pp. 192–207, Dec. 2025, doi: 10.37652/juaps.2025.161423.1435.
- [16] A. K. Jawad, A. S. Lefta, A. H. Hamad, and R. A. Sahun, "Improving image encryption using international data encryption algorithm (IDEA) and henon chaotic map," *AIP Conference Proceedings*, vol. 3408, no. 1, 2026, doi: 10.1063/5.0334160.
- [17] M. Lyle, P. Sarosh, and S. A. Parah, "Adaptive image encryption based on twin chaotic maps," *Multimedia Tools and Applications*, vol. 81, no. 6, pp. 8179–8198, 2022.
- [18] X. Huang, B. Zhang, and X. Zhu, "Pixel shift-based reversible steganography for privacy-preserving medical images," *Frontiers in Medicine*, vol. 13, no. August, Aug. 2026, doi: 10.3389/fmed.2026.1871854.
- [19] A. F. M. Z. Abadin and R. Sulaiman, "A Multilayer Secure Image Steganography Framework Using Edge-Adaptive Embedding and Pre-Encryption," *International Journal of Advanced Computer Science and Applications*, vol. 17, no. 5, pp. 77–87, 2026, doi: 10.14569/IJACSA.2026.0170509.
- [20] R. Alrawashdeh, S. Almuhammadi, M. Niazi, M. Mahmud, and M. M. Rahman, "Secure edge-guided adaptive image steganography using HED-based attention maps and CNN," *Scientific Reports*, vol. 15, no. 1, p. 42984, Dec. 2025, doi: 10.1038/s41598-025-27150-2.
- [21] M. A. W. Putra and A. Rahman, "The Design Of A Hybrid Lsb Steganography Framework With Adaptive Pixel Selection And Chaos Encryption For Social Media Images," *Journal of Computer Networks, Architecture and High Performance Computing*, vol. 8, no. 2, pp. 273–280, May 2026, doi: 10.47709/cnahpc.v8i2.7930.
- [22] Y. Wang, Y. Li, M. Yu, Z. Liu, and H. Chen, "Multimodal Information Steganography with Chaos-Gyrator Cascaded Encryption and Statistical Isolation," *Electronics*, vol. 15, no. 16, p. 3515, Aug. 2026, doi: 10.3390/electronics15163515.
- [23] M. H. Noorallahzadeh, "Novel Adaptive DCT-Based Steganography Algorithm with Coefficient Selection Optimization for JPEG Images," *Journal of Intelligent Communication*, vol. 5, no. 1, pp. 116–139, Feb. 2026, doi: 10.54963/jic.v5i1.1570.
- [24] A. K. Jawad, G. Karimi, and M. Radmalekshahi, "A Novel Digital Audio Encryption Algorithm Using Three Hyperchaotic Rabinovich System Generators," *ARO-The Scientific Journal of Koya University*, vol. XII, no. 2, pp. 234–245, 2024, doi: 10.14500/aro.11869.
- [25] A. k. Jawad, G. Karimi, and M. Radmalekshahi, "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*, vol. 2024, no. 1, pp. 114–119, 2024, doi: 10.1109/AEST63017.2024.10959812.
- [26] A. Patel and D. Vekariya, "An Efficient Image Steganography Method Using Block-Based Indexing and LSB Substitution," *Journal of Innovative Image Processing*, vol. 8, no. 2, pp. 536–557, 2026, doi: 10.36548/jiip.2026.2.006.