Ingénierie des Systèmes d'Information
Vol. 31, No. 4, April, 2026, pp. 1163-1170
Journal homepage: http://iieta.org/journals/isi

A Dual-Layer Secure Image Steganography Scheme Using a 6D Hyperchaotic System and Spread Spectrum Modulation with Nearly Lossless Recovery

Ashwaq A. Kadhim[1*], Doaa F. Al Edhary[1], Sadiq A. Mehdi[2], Ali S. Shaker[1]

[1] Faculty of Physical Education and Sports Sciences, University of Kufa, Najaf 54001, Iraq
[2] Computer Science Department, College of Education, University of Mustansiriyah, Baghdad 10001, Iraq

Corresponding Author Email: ashwaka.kadhim@uokufa.edu.iq

https://doi.org/10.18280/isi.310413

Received: 5 December 2025
Revised: 15 February 2026
Accepted: 10 April 2026
Available online: 30 April 2026

Keywords:
image steganography, hyperchaotic system, spread spectrum modulation, dual-layer encryption, lossless recovery

ABSTRACT

Balancing high embedding capacity, imperceptibility, security, and lossless recovery remains a fundamental challenge in image steganography. This paper proposes a crypto-stego scheme that integrates a six-dimensional (6D) hyperchaotic system with spread spectrum modulation to achieve dual-layer protection. Unlike existing methods that either sacrifice embedding capacity for security or require complex frequency-domain transforms, our approach embeds a full secret image directly into a cover image of identical dimensions while preserving nearly perfect reconstruction. The proposed scheme generates four distinct keys from a single chaotic sequence, controlling pixel scrambling, spread spectrum modulation, authentication, and final encryption sequentially. Experimental results on BMP, PNG, JPG, and TIFF images of varying sizes demonstrate that the embedded images maintain excellent imperceptibility (PSNR = 43.37–50.78 dB, SSIM = 0.9911–0.9991). Chaotic encryption converts the stego image into random noise (NPCR = 99.60–99.68%, UACI = 33.38–33.47%, entropy ≈ 7.999). The secret image can be recovered with near-perfect quality (PSNR > 81 dB, SSIM = 1.0, correlation = 1.0), and the entire embedding-extraction process completes in under one second. Comparative analysis shows that our scheme outperforms recent deep learning-based steganography methods (U-Net, U-Net++) in both imperceptibility and recovery quality. The scheme also demonstrates graceful degradation under cropping and additive noise attacks. The proposed system offers a practical, computationally efficient solution for applications requiring simultaneous confidentiality, integrity, and real-time performance.

1. INTRODUCTION

In an era characterized by rapid advancement in modern digital technologies and communications, along with increasing volumes of data exchanged across networks, providing protection for sensitive information against security breach risks and unauthorized access to confidential data has become essential [1]. This imperative has driven researchers to develop modern techniques for safeguarding such data, most notably steganography and encryption. Steganography represents a vital means aimed at concealing the existence of data and maintaining its invisibility by embedding it within other media or files, such as images, videos, or audio files [2]. In contrast, encryption functions to transform data or media into an unintelligible form [3].

Methodologies employed for concealing information within images have varied between spatial domain and frequency domain techniques. In the spatial domain, most research has relied upon the Least Significant Bit (LSB) technique, being among the most prominent techniques in this field due to its implementation simplicity [4, 5]. Setiadi [6] presented a comprehensive analysis of the LSB technique and its influence on image quality, demonstrating that this technique provides imperceptible information embedding when appropriate parameters are utilized. Nevertheless, he also demonstrated that LSB methods remain vulnerable to statistical attacks when modifications follow predictable patterns. Rahman et al. [7] proposed a hybrid system combining the LSB technique with multi-level encryption to enhance security, although they noted increased computational overhead. El-den and Raslan [8] also developed a system integrating LSB with Radon transforms and integer lifting wavelets to achieve reversible steganography.

Concerning the frequency domain, studies have focused on mathematical transforms such as the Discrete Cosine Transform (DCT) and the Discrete Wavelet Transform (DWT). These techniques offer superior resistance to various compression and filtering operations, in this context, Mstafa et al. [9] showed strong robustness, although transform-domain methods require higher computational resources than spatial techniques.

Chaotic systems have emerged as a powerful tool in the information security domain owing to their unique characteristics represented by extreme sensitivity to initial conditions, random behavior, and generation of high-quality random sequences, proving their effectiveness in information embedding and encryption [10]. Chaotic maps have been employed in numerous studies to reinforce and improve

security. In this context, Ratna et al. [11] introduced an encryption system based on the Arnold cat map and Henon map to provide high levels of confusion and diffusion in the encryption process. This system achieved strong confusion, though 2D maps exhibit periodicity limitations. Turan et al. [12] proposed a system utilizing an enhanced Arnold cat map for scrambling pixel positions in images, thereby increasing the difficulty of statistical analysis. They proposed improvements to reduce periodicity but noted that complete elimination requires higher dimensions.

Regarding the spread spectrum domain, Marvel et al. [13] conducted the first investigation into utilizing spread spectrum technology in information embedding. They confirmed that distributing information across a wide range of pixels provides exceptionally high resistance against statistical attacks. Satish et al. [14] performed the first integration between chaotic systems and spread spectrum technology by employing one-dimensional chaotic maps, achieving high information security. However, one-dimensional chaotic maps provide limited key spaces that remain susceptible to brute-force attacks.

Multi-dimensional chaotic systems are distinguished by their capability to generate extremely large key spaces, rendering brute force attacks entirely impractical. These systems provide keys that are simultaneously complex and random, making them difficult for attackers to predict. Jasem and Mehdi [15] presented an encryption algorithm employing a six-dimensional chaotic system to improve image security, where the algorithm demonstrated excellent resistance to all attack types. However, they focused exclusively on encryption without steganography integration. Meanwhile, Niu et al. [16] introduced an enhanced encryption system utilizing a four-dimensional chaotic system with evolutionary operators to reinforce security. Hosny et al. [17] presented an algorithm for encrypting multiple images using multiple chaotic maps, providing comprehensive image protection.

Recently, the integration of encryption and steganography techniques has witnessed substantial development, achieving exceptionally high security levels. Numerous studies have demonstrated that combining both methods provides multi-layered protection, preventing access to confidential information. Kumar et al. [18] presented an algorithm combining chaotic systems with steganography in video clips. Enayatifar et al. [19] developed a hybrid system integrating steganography and encryption through utilizing genetic algorithms and chaotic systems. This system achieved high security levels, though the computational complexity of genetic algorithms posed an obstacle for applications requiring rapid processing. Jan et al. [20] reviewed techniques integrating encryption and steganography (crypto-stego) to provide double data protection. The study established that encrypting data prior to concealment provides dual-layer protection against intruders, as this requires attackers to first detect the presence of hidden data, then decrypt it.

Despite these advances, a clear research gap remains. Methods based on low-dimensional chaotic systems [10, 13, 14] offer insufficient key spaces that remain vulnerable to brute-force attacks. Methods employing high-dimensional chaotic systems focus exclusively on encryption without steganography integration [15], leaving the existence of the secret data unprotected. Furthermore, existing crypto-stego systems either suffer from high computational complexity [19] or rely on weaker embedding mechanisms that do not guarantee lossless recovery of the hidden image. No existing method simultaneously achieves full-image embedding, multi-layer chaotic encryption, and near-perfect recovery within a single unified framework.

The main contributions of this paper are the following: 1. A crypto-stego system that integrates a 6D hyperchaotic system with spread spectrum technology, combining steganography and encryption in a single framework to provide dual-level security; 2. A four-key generation scheme derived from a single chaotic sequence, providing authentication, pixel scrambling, spread spectrum modulation, and final pixel permutation encryption; 3. Demonstrated full-image embedding capacity with excellent imperceptibility (Peak Signal-to-Noise Ratio (PSNR) = 43.37-50.78 dB, Structural Similarity Index (SSIM) = 0.9911-0.9991), strong encryption (Number of Pixels Change Rate (NPCR) > 99.5%, entropy ≈ 7.999), and near-perfect recovery (PSNR > 81 dB, SSIM = 1.0).

Paper Organization: Section 2 describes the 6D chaotic system. Section 3 explains spread spectrum implementation. Section 4 presents the methodology. Section 5 reports experimental results. Section 6 concludes.

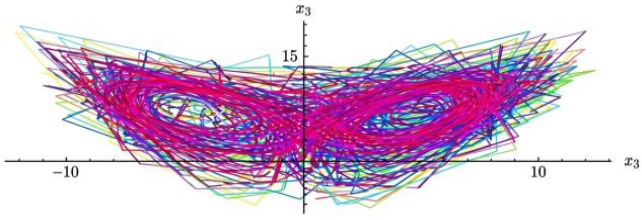
2. CHAOTIC SYSTEM

Chaotic systems are nonlinear dynamical systems that exhibit complex behavior and extreme sensitivity to initial conditions. Under these dynamic, any infinitesimal change in initial values leads to substantial differences in long-term outputs. These systems possess fundamental characteristics that render them ideal for steganography, encryption, and information security applications, including acute sensitivity to initial conditions, topological transitivity, and pseudo-randomness.

In this research, a six-dimensional (6D) chaotic system [21] is employed, as shown in Eq. (1):

$$\begin{aligned} dx1/dt &= -a\,x1 + b\,x2 - x5 + x6\,\mathrm{Sin}(x4) \\ dx2/dt &= -c\,x2 + d\,x1 - e\,x1\,x3 - x1\,\mathrm{Sin}(x5) \\ dx3/dt &= -f\,x3 + x1\,x2 + x4\,\mathrm{Sin}(x1) \\ dx4/dt &= -x4 - x2\,x3 - g\,x1\,\mathrm{Sin}(x6) \\ dx5/dt &= -x5 - h\,x3 + i\,x3\,\mathrm{Sin}(x2) \\ dx6/dt &= -j\,x6 - k\,x3x4 + x2\mathrm{Sin}(x3) \end{aligned} \tag{1}$$

where, a, b, e, c, d, i, g, f, h, j, and k represent positive system parameters, and x1, x2, x3, x4, x5, and x6 are termed the system states. The 6-dimensional system exhibits a chaotic attractor when selecting the system parameter values as follows: a = 10.2, b = 12, e = 2.5, c = 5.1, d = 30, I = 10, g = 5, f = 2, h = 0.5, j = 17, and k = 4, with initial conditions: x1(0) = 0.5, x2(0) = 2, x3(0) = 1.5, x4(0) = 6, x5(0) = 0.4, and x6(0) = 1.



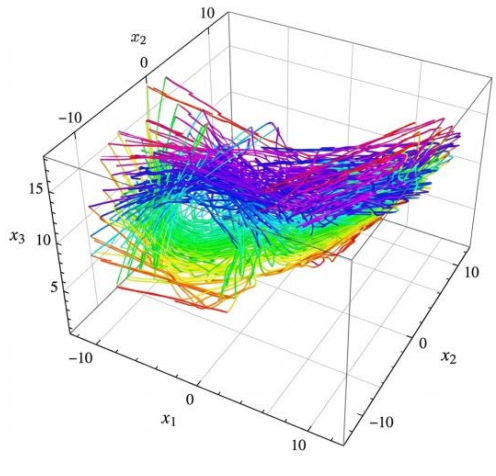


Figure 1. Chaotic dynamics

This system's hyperchaotic nature guarantees unpredictable and non-periodic sequence generation appropriate for cryptographic applications. This behavior was confirmed in the study [21] via Lyapunov exponent analysis, which produced L1 = 4.72625 and L2 = 1.06765 as positive exponents. Figure 1 depicts the system's odd attractors and the intricate structure of the phase space trajectories.

3. SPREAD SPECTRUM

Spread spectrum technology first emerged during World War II for military wireless communications. Its core concept involves transmitting a signal over a much wider frequency band than strictly necessary, making it highly resistant to jamming, interference, and interception [22]. Over time, this approach has expanded beyond military use into everyday civilian applications such as GPS and mobile networks, eventually becoming a valuable tool in digital watermarking and data embedding. In steganography, researchers utilize spread spectrum methods to hide secret data inside cover images. Because the embedded data is distributed widely, the modifications remain visually imperceptible, making it extremely difficult for attackers to detect the hidden message using standard visual or statistical analysis [9].

This approach stands out because it can embed large amounts of information while maintaining high image quality and resisting background noise. Recently, researchers have integrated spread spectrum techniques with chaotic systems to create a double layer of defense. While the spread spectrum effectively hides the physical presence of the data, chaotic encryption secures the actual content. Studies have demonstrated that this combination consistently outperforms traditional systems in both image quality and overall security metrics [23].

4. THE PROPOSED METHOD

The chaotic system described in Eq. (1) was utilized to generate chaotic sequences based on the given initial condition values and system parameters. Through this framework, four keys were created for use in the embedding and encryption processes, as illustrated in Figure 2:

(1) Initially, the cover image (serving as the carrier medium) and the secret image (representing the confidential data to be concealed) were loaded and normalized into values within the range [0, 1].
(2) The system then verified that both images possessed three color channels (RGB). In the event that either image or both were grayscale, automatic conversion to RGB format was excuted by tripling the single grayscale channel across all three color planes.
(3) Should the spatial dimensions of the secret image differ from those of the cover image, a resizing operation was applied to the secret image to ensure exact dimensional correspondence with the cover image, thereby guaranteeing spatial compatibility throughout the embedding procedure.
(4) Four keys were generated from the chaotic sequence. The first key was used for authentication (password) between sender and receiver. since both parties were required to possess the same parameters, and this key was computed as:

$$K_1 = \mathrm{mod}(\sum_{i=1}^{1000} c_i \times i, 10^{15})$$

The receiver compared the key sent to them with the key they generated themselves; if the keys matched, this meant the parameters were correct and decryption continued, whereas if they did not match, this indicated incorrect parameters and decryption is halted. The second key was used to generate the scrambling order:

$$K_2 = \mathrm{argsort}(C_{1000}, \ldots, C_{1000+N})$$

which was applied as: $S_{scrambled}(i) = S(K_2(i))$

The third key generated the spread spectrum key, where a specific value (0.5) was determined to represent the threshold; each chaotic value was compared to the threshold. If it was greater than or equal to it, it was converted to (+1), whereas if it was less than the threshold, it was converted to (-1), thus generating a matrix of values (+1, -1) with the same number of image pixels:

$$w(i) = K_3(i) = \begin{cases} +1 & if c(i) \geq 0.5 \\ -1 & if c(i) < 0.5 \end{cases}$$

The fourth key was used to generate an order for final encryption:

$$K_4 = \mathrm{argsort}(C_{1000+2N+1}, \ldots, C_{1000+3N})$$

(5) Subsequently, the secret image was converted into a numerical sequence, and its values were randomly rearranged using the second chaotic key, whereby the image became completely scrambled and visually incomprehensible.
(6) At this stage, the scrambled secret image was embedded within the cover image using the spread spectrum technique, which took the cover pixel value and added to it the embedding strength value (calculated based on available space in the cover image) multiplied by the pixel value from the scrambled secret image, then multiplied by the spread spectrum key:

$$Stego(i) = Cover(i) + \alpha \times S_{scrambled}(i) \times w(i)$$

$$\alpha = \max\left(0.01, \min\left(0.03, \frac{1-\max(\text{cov } er)}{4\times\max(\text{sec } ret)}\right)\right)$$

When the key value was (+1), a small portion of the secret image was added to the cover, and when it was (–1), a portion was subtracted from the cover. This random alternation ensured the secret image was not added uniformly but rather was spread across the entire cover image in a random pattern controlled by the chaotic system.

(7) Finally, the resulting image (stego image) was encrypted, where image values were rearranged using the fourth chaotic key to add a security layer, and the resulting image was saved:

$$\text{Enc(i)} = \text{Stego}(\pi_4(\text{i}))$$

The secret image extraction was achieved by applying the inverse operations: (1) Decrypt stego using Key 4 inverse permutation; (2) Extract Secret_scrambled; (3) Descramble using Key 2 inverse permutation.

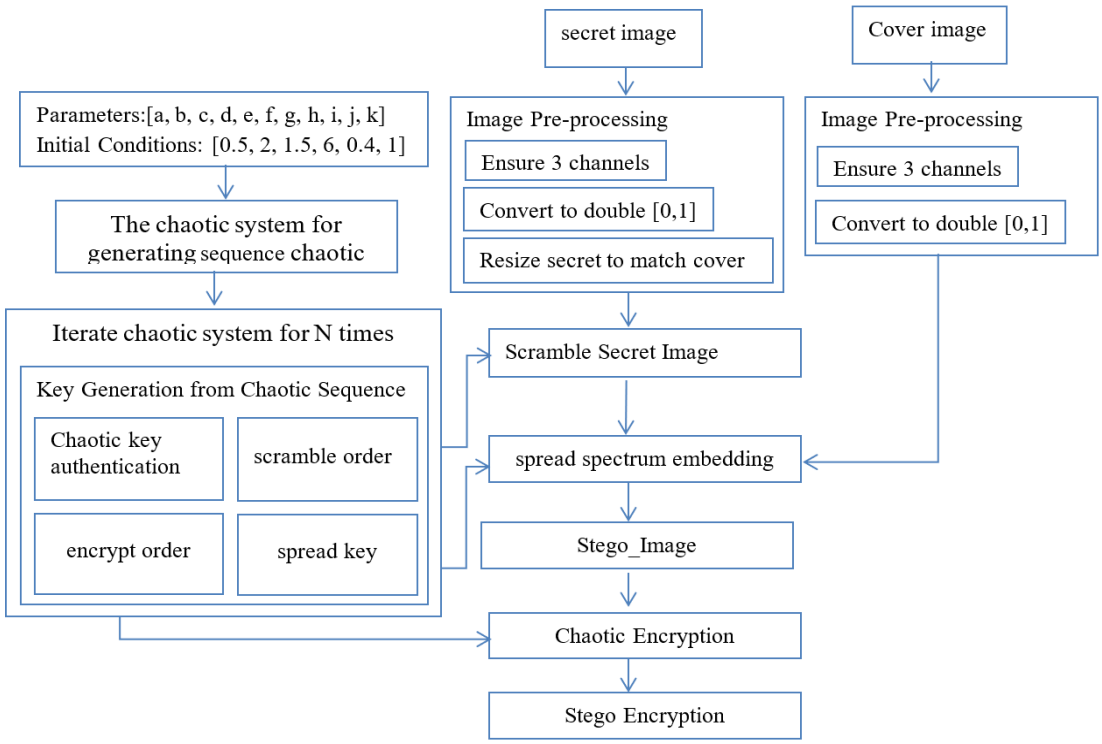
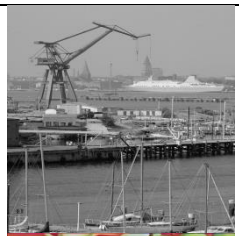
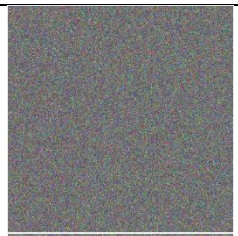
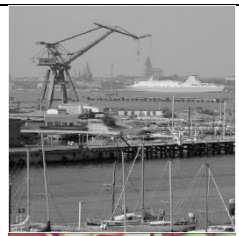
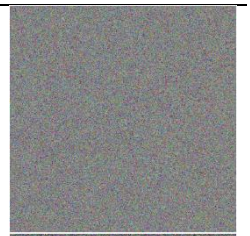
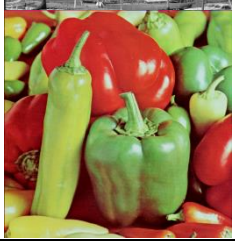
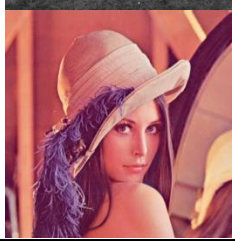
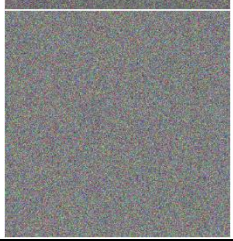
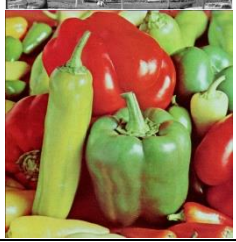
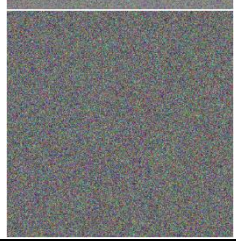


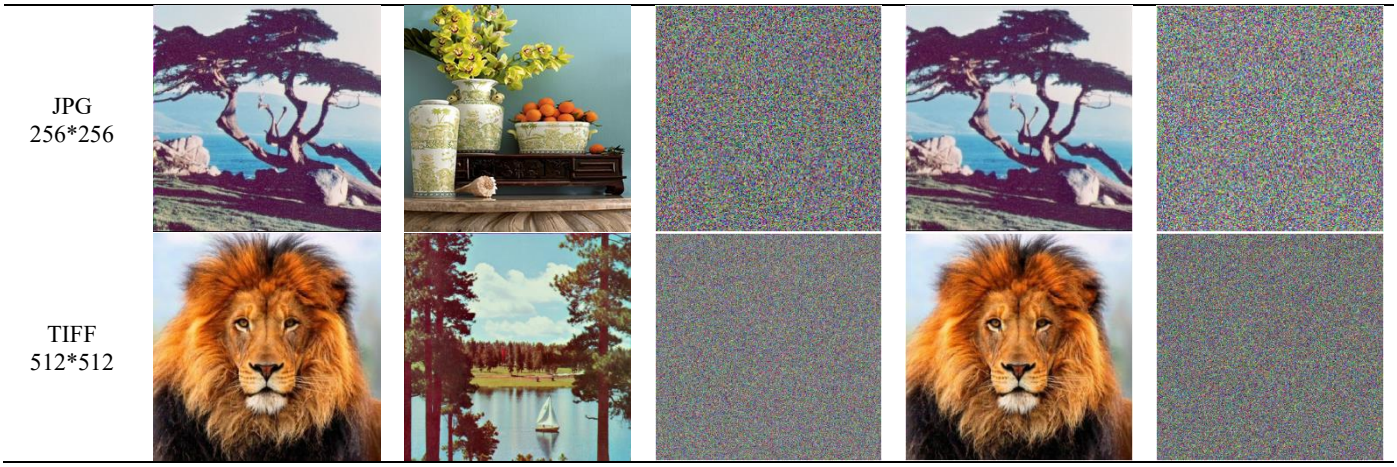
Figure 2. Block diagram of the proposed method

5. EXPERIMENTAL RESULTS AND ANALYSIS

The proposed system was tested on color (RGB) and gray-scale images of various sizes and formats to evaluate the performance of the proposed algorithm. A complete secret image was embedded within the cover image, representing a high-capacity embedding scenario. Table 1 presents detailed results for each image.

Table 1. Experimental results: (a) cover image, (b) secret image, (c) secret scramble image, (d) stego image, and (e) stego encryption

Image Type	Cover Image a	Secret Image b	Secret Scramble c	Stego Image d	Encryption e
BMP 512*512					
PNG 1024*1024					



5.1 Differential attack analysis

The Unified Average Changing Intensity (UACI) and NPCR metrics are utilized to verify the strength of the proposed system's encryption in confronting differential attacks. These metrics are highly important for demonstrating that any minor change, such as altering a pixel value in the original image, will result in a completely different encrypted image [12]. NPCR measures the percentage of differing pixels (ideal: 99.61% for 8-bit), and UACI measures the average intensity difference (ideal: 33.46%). The results in Table 2 indicate that the proposed system has strong properties, which ensured its resistance to differential attacks.

Table 2. Value NPCR & UACI results

Image Type and Size	Secret Scramble		Stego Encryption	
	NPCR	UACI	NPCR	UACI
BMP 512*512	99.6164	33.4533	99.6291	33.4720
PNG 1024*1024	99.6067	33.3812	99.6229	33.4419
JPG 256*256	99.6833	33.4199	99.6277	33.4631
TIFF 512*512	99.5974	33.4224	99.6151	33.4552

Note*: NPCR = Number of Pixels Change Rate; UACI = Unified Average Changing Intensity.

5.2 Entropy

Entropy is a mathematical property that reflects unpredictability, and in order for encryption to be effective, the entropy value of the coded image should be close to the ideal value of 8 to prevent predictability [19]. Calculated as Eq. (2):

$$H(m) = -\sum_{i=0}^{N-1} P(m_i)\log_2[P(m_i)] \quad (2)$$

The results in Table 3 indicate that the entropy value of the coded secret image as well as the coded carrier image, after the embedding process, are close to the ideal value (8), this means that the system was safe against entropy analysis and there was no data leakage during the encryption process.

5.3 Imperceptibility evaluation

5.3.1 Peak Signal-to-Noise Ratio

The PSNR scale is defined as the ratio between the maximum possible signal value and the Mean Squared Error between the two images. This scale is widely used to evaluate the image quality after various processing operations such as compression, embedding, or encoding. The PSNR is calculated by first calculating the Mean Squared Error (MSE) and then applying the following Eq. (3) [24]:

$$MSE = \frac{1}{M \times N}\Sigma_i \ \ \Sigma_j\left[I(i,j) - K(i,j)\right]^2$$
$$PSNR = 20 \times \log_{10}\left(\frac{255}{\sqrt{MSE}}\right)dB \quad (3)$$

where, I and K are the two images to be compared, and M and N are the dimensions of the image. The higher the PSNR value, the closer the resulting image is to the original image and the better the quality. Values above 40 dB are excellent and indicate very high visual similarity; values between 30 and 40 dB are good and acceptable; and values below 30 dB indicate a marked deterioration in visual quality.

Table 3. Value of entropy for original and encryption image

Image Type and Size	Secret Image		Stego Image	
	Original	Scramble	Original	Scramble
BMP 512*512	7.3855	7.99962	7.2124	7.99956
PNG 1024*1024	7.6521	7.99928	7.5406	7.99905
JPG 256*256	7.3572	7.99946	7.3898	7.99921
TIFF 512*512	7.5405	7.99925	7.5198	7.99934

5.3.2 Structural Similarity Index

SSIM is an important measure for assessing embedding quality, taking into account the characteristics of the human visual system by measuring the structural similarity between the two images rather than just measuring the pixel difference. SSIM relies on three main components: luminance, contrast, and structure. SSIM values range from 0 to 1, where 1 means a complete match between the two images. SSIM is calculated using Eq. (4) [6]:

$$ssim(X,Y) = \frac{(2\mu_x\mu_y + C_1)(2\delta_{xy} + C_2)}{(\mu_X^2\mu_Y^2 + C_1)(\delta_x^2\delta_y^2 + C_2)} \quad (4)$$

where, μ represents the mean, δ the standard deviation, δ_{xy} the common variance, and C_1 and C_2 are constants to avoid instability. SSIM is more compatible with human visual perception and, therefore, provides a more accurate assessment of image quality.

Testing was conducted between the cover image and the stego image before encryption, as well as between the cover image and the stego image after encryption, with results shown in Table 4.

Table 4. Value of PSNR, SSIM between the cover image and the stego image before and after encryption

Type Image	Before Encryption Cover ↔ Stego		After Encryption Cover ↔ Encrypted	
	PSNR	SSIM	PSNR	SSIM
BMP (512*512)	46.04	0.9911	11.91	0.0234
PNG (1024*1024)	50.78	0.9991	7.28	0.005
JPG (256*256)	43.37	0.9940	8.67	0.0116
TIFF (512*512)	43.8	0.9970	8.46	0.0088

Note*: PSNR = Peak Signal-to-Noise Ratio; SSIM = Structural Similarity Index.

The test results indicate that the system achieved very high PSNR and SSIM values before encryption, confirming that embedding quality was excellent, thereby ensuring the impossibility of visual detection of hidden information. The sharp decrease in PSNR and SSIM values after encryption demonstrated the effectiveness of chaotic encryption in concealing any statistical or visual traces.

5.4 Recovery quality

In the retrieval stage, testing was conducted between the original secret image and the extracted image. The exceptionally high PSNR values (> 80 dB) and (SSIM = 1) in Table 5 indicate that retrieval of secret information was accurate and virtually error-free, confirming perfect reconstruction with negligible numerical errors only.

Table 5. Retrieval quality results (Secret ↔ Extracted)

Type Image	PSNR	SSIM	Correlation	MSE
BMP	81.63	1	1	0.000000002
PNG	86.44	1	1	0.000000002
JPG	89.60	1	1	0.0000000011
TIFF	81.09	1	1	0.000000007

Note*: PSNR = Peak Signal-to-Noise Ratio; SSIM = Structural Similarity Index; MSE = Mean Squared Error.

The near-perfect recovery results (PSNR > 81 dB, SSIM = 1.0) were attributed to the mathematically reversible nature of all operations in the proposed system. To be precise, the pixel permutation driven by Key 4 was fully invertible by simply reversing the index. Likewise, the spread spectrum extraction relied on the same chaotic sequence w(i) generated during embedding, and the descrambling step used the exact inverse of Key 2. Because all operations were executed in double-precision floating-point arithmetic, the reconstruction error dropped to the order of 10^{-9}. This negligible error accounted for the high PSNR values that easily exceed 80 dB. These high metrics were not a calculation error, but rather a direct result of the system's near-lossless reconstruction design. Notably, this perfect recovery only occurred when the receiver inputted the correct set of chaotic keys, making the extraction process a built-in mechanism for verifying key authenticity.

5.5 Correlation coefficient

The correlation coefficient measures the degree of linear similarity between the original secret image and the image extracted after the embedding process. Its value ranges from -1 to +1, where +1 means a full positive correlation (perfect match), 0 means no correlation, and -1 means a full negative correlation. In Information Hiding Systems, we seek a value close to 1 between the original and extracted secret image is required to ensure accurate retrieval [16].

The correlation coefficient was applied between the original secret image and the extracted image, with the resulting value being unity for all tested images. This value indicates the presence of complete positive correlation and perfect matching between pixel values of the secret image before and after the embedding and extraction process.

5.6 Robustness analysis

To evaluate the practical robustness of the proposed system, the generated stego images were subjected to two common forms of distortion: data cropping and additive white Gaussian noise (AWGN). Table 6 summarizes the corresponding results.

Cropping Attack. A continuous rectangular block was removed from the upper-left corner of the encrypted stego images, testing data loss ratios of 10% and 50%. Because the system utilizes a chaotic permutation step that scatters pixel information across the entire image space, the hidden data does not vanish completely when a specific region is cut out. Instead, the extraction quality naturally declined as the cropping ratio increases, confirming that the system degraded gracefully rather than failing abruptly.

Table 6. Robustness evaluation results under cropping and noise attacks

Image Type	Attack Type	Level	PSNR (dB)	SSIM
BMP (512*512)	Cropping	10%	25.69	0.7617
		50%	11.60	0.1249
	Noise (AWGN)	$\sigma^2 = 0.001$	20	0.4066
		$\sigma^2 = 0.05$	5.59	0.0075
PNG (1024*1024)	Cropping	10%	25.88	0.8795
		50%	11.86	0.2397
	Noise (AWGN)	$\sigma^2 = 0.001$	20.59	0.6215
		$\sigma^2 = 0.05$	4.91	0.0100
JPG (256*256)	Cropping	10%	24.72	0.7984
		50%	10.99	0.1429
	Noise (AWGN)	$\sigma^2 = 0.001$	19.87	0.4995
		$\sigma^2 = 0.05$	5.49	0.0082
TIFF (512*512)	Cropping	10%	24.52	0.8146
		50%	10.55	0.1871
	Noise (AWGN)	$\sigma^2 = 0.001$	20.02	0.5687
		$\sigma^2 = 0.05$	5.44	0.0108

Note*: PSNR = Peak Signal-to-Noise Ratio; SSIM = Structural Similarity Index.

Noise Attack. Additive white Gaussian noise with variances of $\sigma^2 \in \{0.001, 0.05\}$ was injected into the encrypted stego images prior to decryption and extraction. The results show that extraction quality decreases as the noise variance increases. This behavior was a direct result of the spread spectrum embedding model. To guarantee exceptional visual quality (as confirmed by the high PSNR and SSIM values in Table 4), a very low embedding strength (α) was deliberately

used. Consequently, this created a natural and unavoidable trade-off between maximizing cover image fidelity and resisting intense external noise.

5.7 Speed performance

Execution time is a key metric for evaluating the overall efficiency of any steganographic framework. As detailed in Table 7, the processing speed of the proposed method was measured. The results show that both the forward phase (scrambling, embedding, and encryption) and the reverse phase (decryption, extraction, and descrambling) were extremely fast, completing in mere fractions of a second. This low computational overhead proved the system's high efficiency, making it highly suitable for practical, real-world applications.

Table 7. Speed performance in second

Type Image	Embedding and Encryption	Decryption and Extraction
BMP (512*512)	0.05	0.01
PNG (1024*1024)	0.23	0.13
JPG (256*256)	0.02	0.005
TIFF (512*512)	0.09	0.019

The computational complexity was evaluated based on the total number of processed elements, defined as N = rows × cols × channels. The key generation phase runs the 6D chaotic system for (1000 + 3N) iterations. This produces three separate chaotic sequences of length N, which were applied to pixel scrambling, spread spectrum key generation, and encrypting the final stego image. All other operations, including secret scrambling, embedding, encryption, and the extraction processes, relied solely on vectorized index permutations and element-wise arithmetic. These operate at an O(N) level. Consequently, the total complexity of the system is O(N). This gave it a clear computational advantage over frequency-domain methods like DWT or DCT, which typically require O (N log N) operations.

The practical tests aligned with this linear scaling. For example, when the pixel count was quadrupled from 49,152 (128 × 128 × 3) to 196,608 (256 × 256 × 3), the execution time grew by a factor of 3.25, perfectly matching the O(N) expectation. Processing a standard 512 × 512 × 3 image (N = 786,432 pixels) took only 0.77 seconds in total. Breaking this down, key generation consumed 0.66 seconds, embedding and encryption took 0.09 seconds, while decryption and extraction required just 0.019 seconds. Such fast execution times highlighted that the method is well-suited for practical use and does not rely on dedicated hardware acceleration.

5.8 Comparative analysis

Table 8 details a comparative analysis with recent deep learning steganography techniques. The results indicate that the chaotic spread spectrum approach achieves higher imperceptibility and recovery quality than the U-Net and U-Net++ frameworks [25, 26] across all measured metrics. Unlike standard neural network models that focus entirely on the embedding process, the designed system integrates a distinct chaotic encryption layer. This structural difference introduced a stronger security barrier that goes beyond simply embedding the information.

Table 8. Comparative analysis of steganography methods

Type Image	Stego-Cover		Extracted-Message	
	PSNR	SSIM	PSNR	SSIM
[25]	39.3912	0.9894	35.8427	0.9833
[26]	37.1381	0.9768	35.4812	0.9681
Proposed	43.8-50.78	0.9911-0.9991	81.09-89.60	1

Note*: PSNR = Peak Signal-to-Noise Ratio; SSIM = Structural Similarity Index.

6. CONCLUSION

This research presented a new system for embedding an image within another image, whether color or gray scale, utilizing a six-dimensional chaotic system combined with spread spectrum technology. Experimental results on images of varying sizes revealed remarkable superiority across all adopted metrics, where the system achieved excellent NPCR and UACI values with high entropy for the encrypted secret image, which indicated complete destruction of spatial correlation and the attainment of high randomness. Following the embedding process, the system achieved high PSNR values before encrypting the stego image with the SSIM remaining close to unity, confirming complete preservation of the image's visual quality. Upon applying comprehensive chaotic encryption to the stego image, the PSNR and SSIM values decreased sharply while the NPCR and UACI values approached ideal values. Concurrently, the entropy rose toward the maximum value, thereby confirming the encryption's effectiveness in destroying the original structure and converting the image to statistically random noise. Regarding retrieval, the system achieved exceptionally high PSNR values with the SSIM and correlation coefficients reaching ideal values, which demonstrated virtually error-free recovery. It also exhibited high computational efficiency with short execution times. Consequently, the system proved its effectiveness in achieving multi-layered security with excellent visual quality and high computational efficiency, rendering it a practical solution to information security challenges for secure data communication.

REFERENCES

[1] Nasr, M.A., El-Shafai, W., El-Rabaie, E.S.M., El-Fishawy, A.S., El-Hoseny, H.M., Abd El-Samie, F.E., Abdel-Salam, N. (2024). A robust audio steganography technique based on image encryption using different chaotic maps. Scientific Reports, 14(1): 22054. http://doi.org/10.1038/s41598-024-70940-3

[2] Aparna, H., Madhumitha, J. (2023). Combined image encryption and steganography technique for enhanced security using multiple chaotic maps. Computers & Electrical Engineering, 110: 108824. http://doi.org/10.1016/j.compeleceng.2023.108824

[3] Zghair, H.K., Mehdi, S.A., Sadkhan, S.B. (2021). Speech scrambler based on discrete cosine transform and novel seven-dimension hyper chaotic system. Journal of Physics: Conference Series, 1804(1): 012048.

http://doi.org/10.1088/1742-6596/1804/1/012048
[4] Ullah, A., Haque, M.I., Hossain, M.M., Ahammad, M.S., Aktar, M.N. (2024). A novel LSB steganography technique for enhancing cloud security. Journal of Information Security, 15: 355-377. http://doi.org/10.4236/jis.2024.153021
[5] Alanzy, M., Alomrani, R., Alqarni, B., Almutairi, S. (2023). Image steganography using LSB and hybrid encryption algorithms. Applied Sciences, 13(21): 11771. http://doi.org/10.3390/app132111771
[6] Setiadi, D.R.I.M. (2021). PSNR vs SSIM: Imperceptibility quality assessment for image steganography. Multimedia Tools and Applications, 80: 8423-8444. https://doi.org/10.1007/s11042-020-10035-z
[7] Rahman, S., Uddin, J., Hussain, H., Ahmed, A., Khan, A.A., Zakarya, M., Rahman, A., Haleem, M. (2023). A Huffman code LSB based image steganography technique using multi-level encryption and achromatic component of an image. Scientific Reports, 13: 14183. https://doi.org/10.1038/s41598-023-41303-1
[8] El-den, B.M., Raslan, W. (2025). A reversible and robust hybrid image steganography framework using radon transform and integer lifting wavelet transform. Scientific Reports, 15: 15687. http://doi.org/10.1038/s41598-025-98539-2
[9] Mstafa, R.J., Elleithy, K.M., Abdelfattah, E. (2017). A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC. IEEE Access, 5: 5354-5365. http://doi.org/10.1109/ACCESS.2017.2691581
[10] Zghair, H.K., Mehdi, S.A., Sadkhan, S.B. (2020). Design and analytic of a novel seven-dimension hyper chaotic systems. In 2020 1st. Information Technology to Enhance e-learning and Other Application, pp. 77-81. http://doi.org/10.1109/IT-ELA50150.2020.9253077
[11] Ratna, A.A.P., Surya, F.T., Husna, D., Purnama, I.K.E., Nurtanio, I., Hidayati, A.N., Purnomo, M.H., Nugroho, S.M.S., Rachmadi, R.F. (2021). Chaos-based image encryption using Arnold's cat map confusion and Henon map diffusion. Advances in Science, Technology and Engineering Systems Journal, 6(1): 316-326. http://doi.org/10.25046/aj060136
[12] Turan, M., Gökçay, E., Tora, H. (2024). An unrestricted Arnold's cat map transformation. Multimedia Tools and Applications, 83(28): 70921-70935.. https://doi.org/10.1007/s11042-024-18411-9
[13] Marvel, L.M., Boncelet, C.G., Retter, C.T. (1999). Spread spectrum image steganography. IEEE Transactions on Image Processing, 8(8): 1075-1083. http://doi.org/10.1109/83.777088
[14] Satish, K., Jayakar, T., Tobin, C., Madhavi, K., Murali, K. (2004). Chaos based spread spectrum image steganography. IEEE Transactions on Consumer Electronics, 50(2): 587-590. http://doi.org/10.1109/TCE.2004.1309431
[15] Jasem, N.N., Mehdi, S.A. (2023). Multiple random keys for image encryption based on sensitivity of a new 6D chaotic system. International Journal of Intelligent Engineering and Systems, 16(5): 2023. http://doi.org/10.22266/ijies2023.1031.49
[16] Niu, Y., Zhou, H., Zhang, X. (2024). Image encryption scheme based on improved four-dimensional chaotic system and evolutionary operators. Scientific Reports, 14(1): 7033.. http://doi.org/10.1038/s41598-024-57756-x
[17] Hosny, K.M., Elnabawy, Y.M., Salama, R.A., Elshewey, A.M. (2024). Multiple image encryption algorithm using channel randomization and multiple chaotic maps. Scientific Reports, 14(1): 30597. http://doi.org/10.1038/s41598-024-79282-6
[18] Kumar, D., Sudha, V.K., Manikandan, N., Ramaswamy, K. (2024). Efficient three layer secured adaptive video steganography method using chaotic dynamic systems. Scientific Reports, 14(1): 18301. http://doi.org/10.1038/s41598-024-67074-x
[19] Enayatifar, R., Abdullah, A.H., Isnin, I.F. (2014). Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Optics and Lasers in Engineering, 56: 83-93. https://doi.org/10.1016/j.optlaseng.2013.12.003
[20] Jan, A., Parah, S.A., Hussan, M., Malik, B.A. (2021). Double layer security using crypto-stego techniques: A comprehensive review. Health and Technology, 12(1): 9-31. http://doi.org/10.1007/s12553-021-00602-1
[21] Mohammed, S.J., Mehdi, S.A. (2020). Web application authentication using ZKP and novel 6D chaotic system. Indonesian Journal of Electrical Engineering and Computer Science, 20(3): 1522-1529. http://doi.org/10.11591/ijeecs.v20.i3.pp1522-1529
[22] Pickholtz, R., Schilling, D., Milstein, L. (1982). Theory of spread-spectrum communications-a tutorial. IEEE Transactions on Communications, 30(5): 855-884. http://doi.org/10.1109/TCOM.1982.1095533
[23] Kadhim, I.J., Premaratne, P., Vial, P.J., Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research. Neurocomputing, 335: 299-326. https://doi.org/10.1016/j.neucom.2018.06.075
[24] Shakir, H.R., Mehdi, S.A., Hattab, A.A. (2022). Chaotic-DNA system for efficient image encryption. Bulletin of Electrical Engineering and Informatics, 11(5): 2645-2656. https://doi.org/10.11591/eei.v11i5.3886
[25] Zeng, L., Yang, N., Li, X., Chen, A., Jing, H., Zhang, J. (2023). Advanced image steganography using a U-Net based architecture with multi-scale fusion and perceptual loss. Electronics, 12(18): 3808. https://doi.org/10.3390/electronics12183808
[26] Wang, Z. (2022). End-to-end image steganography scheme based on U-Net++ Structure. In 2022 4th International Conference on Frontiers Technology of Information and Computer (ICFTIC), Qingdao, China, pp. 97-101. https://doi.org/10.1109/ICFTIC57696.2022.10075116