

International Journal of Statistics and Applied Mathematics

ISSN: 2456-1452
NAAS Rating (2026): 4.49
Maths 2026; 11(9): 67-76
© 2026 Stats & Maths
<https://www.mathsjournal.com>
Received: 15-07-2026
Accepted: 18-08-2026

Kusum Lata
Research Scholar, Department of
Mathematics, Maharshi
Dayanand University, Rohtak,
Haryana, India

Dr. Meenakshi Hooda
Assistant Professor, Department
of Mathematics, Maharshi
Dayanand University, Rohtak,
Haryana, India

Navita Dhaka
Research Scholar, Department of
Mathematics, Maharshi
Dayanand University, Rohtak,
Haryana, India

Corresponding Author:
Dr. Meenakshi Hooda
Assistant Professor, Department
of Mathematics, Maharshi
Dayanand University, Rohtak,
Haryana, India

DWT-based Chaotic Adaptive Embedding Scheme (DCAES)

Kusum Lata, Meenakshi Hooda and Navita Dhaka

DOI: <https://www.doi.org/10.22271/math.2026.v11.i9a.2688>

Abstract

In the secure image steganography, the trade-off between the embedding capacity, visual imperceptibility and data security is a basic challenge. We propose a "DWT based Chaotic Adaptive Embedding Scheme (DCAES)" which integrates one level Haar Discrete Wavelet Transform, activity based adaptive bit allocation, and Logistic-map based chaotic permutation for secure data hiding. The activity map adaptively allocates the embedding bits according to the local image characteristics. Additionally, chaotic permutation is utilized to scramble the secret message before embedding for security. The secret data are embedded into the high frequency wavelet sub bands to minimize visual distortion and maintain the quality of the image. The proposed framework was tested on five benchmark gray scale images, viz. Airplane, Cameraman, Earth, Flowers and Lena. The experimental results are evaluated in terms of high PSNR and SSIM and low MSE and adaptive embedding capacity, indicating the visual quality and good payload utilization. The results show that DCAES is an efficient and secure solution for image steganography with high imperceptibility and embedding efficiency.

Keywords: Image steganography, Discrete Wavelet Transform (DWT), Haar wavelet, Adaptive embedding, Chaotic scrambling

Introduction

The fast growth in the use of digital communications, cloud computing, social networks and multimedia technologies has led to a great increase in sharing digital images over public networks. However, these advances have improved the efficiency of information sharing but have also raised concerns of data leakage, unauthorised access and privacy violation. Therefore, the protection of confidential information during transmission has become a critical challenge of modern information security, as shown in figure 1. Cryptography and steganography are two complementary techniques that can be used to address this challenge [1]. Cryptography hides the data in an unreadable form whereas Steganography hides the existence of the communication by embedding the secret data in a cover medium which does not look suspicious to the eyes. Digital images are commonly used as cover media for secure information hiding because of their rich visual content and redundancy [2]. An effective image steganography technique should embed a large amount of data while preserving the visual quality, robustness and security. However, increasing payload usually causes noticeable distortion and raises the risk of detection via steganalysis methods. Fixed embedding strategies worsen security because they generate predictable modification patterns. Recent works have therefore proposed adaptive embedding techniques that exploit local image characteristics to choose appropriate embedding locations and payload sizes. According to the embedding strategy, the image steganography methods are often divided into spatial-domain and frequency (transform)-domain approaches. Spatial domain techniques, particularly LSB-based embedding, offer high payload capacity and low computational complexity, but are more vulnerable to statistical analysis. In contrast, the transform domain methods embed information in transformed coefficients giving better attack resistance and maintaining the image quality. Among these, Discrete Wavelet Transform (DWT) has attracted a lot of attention because it provides a simultaneous spatial and frequency representation [3]. Using a

one-level Haar DWT, an image is decomposed into four subbands (LL, LH, HL and HH), where LL represents the low-frequency part of the original image, while the rest of the

bands contains edge and texture information [4]. Change in high-frequency parts is hardly visible, thus it is a good place for data to be hidden.

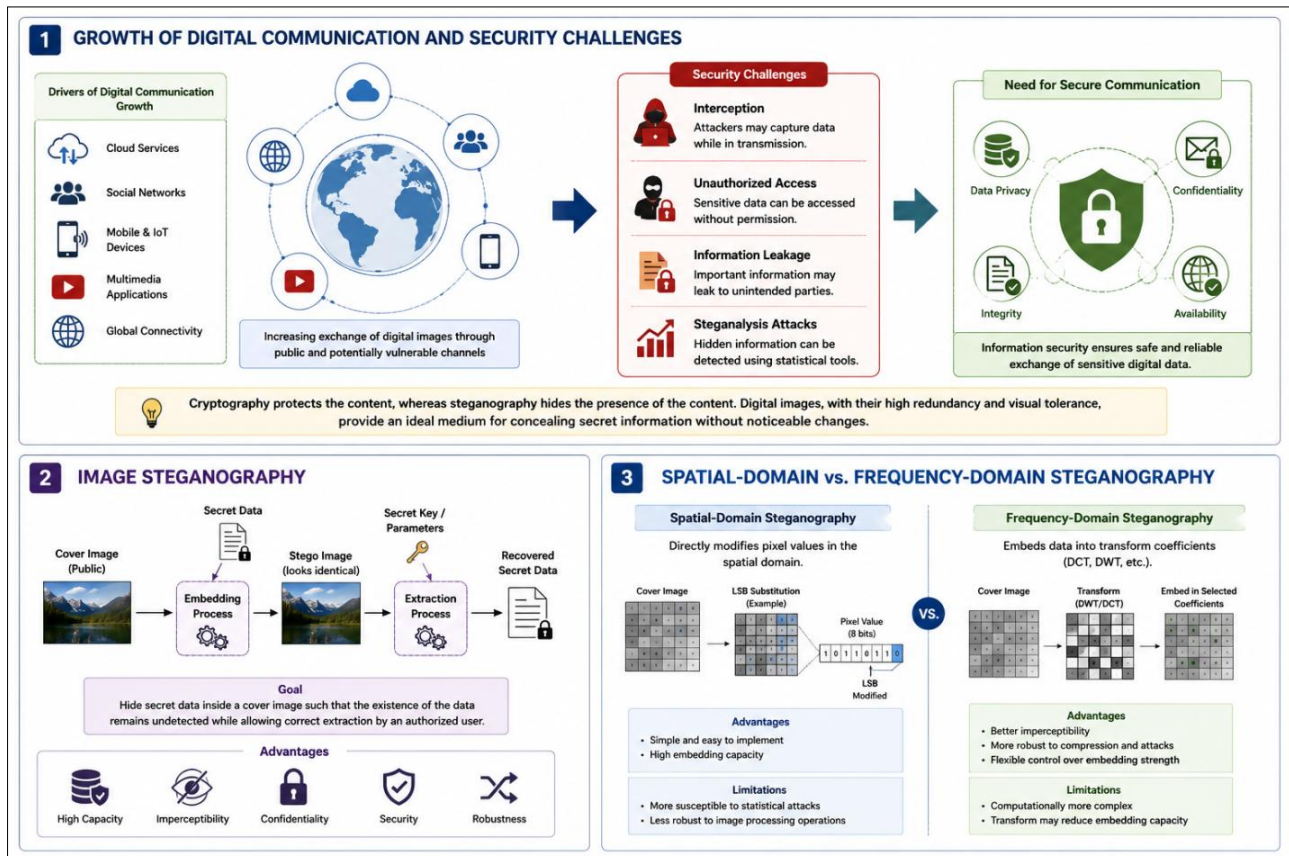


Fig 1: Protection of Sensitive Information

The Haar wavelet is known for its simplicity, low amount of computations needed and the ease of use. The embedding capacity of the image depends on its local content including smooth areas that are very sensitive to changes and edge and textured areas which can conceal a larger amount of information with little alteration in its appearance. Many techniques rely on local activity of the image by measuring energy, variance, gradients and texture, while many advanced techniques still depend on fixed thresholds that is inconsistent with various image types. It is also vital to secure the hidden information after embedding it into a cover image. The chaos theory introduces a suitable solution because it demonstrates that chaotic systems are very sensitive to initial parameters and have some features of unpredictability. Those qualities have been widely used for image encryption, scrambling and secure hiding of information. Among the numerous chaotic systems, the Logistic map is used widely due to its ease in modeling and computation. It is described as $X_{n+1} = \mu X_n(1 - X_n)$ where X_n denotes the the present state of the system, X_0 is the initial state and μ is the control parameter. With the right parameter values, the Logistic map generates very chaotic sequences which can be applied for permuting the binary message before hiding it. This makes the message much more difficult to retrieve as the scrambling depends on the key and does not make the overall complexity of the task as complicated as usual encryption methods [5]. The concept of secure image steganography put forward in this manuscript is called the “DWT-based Chaotic Adaptive Embedding Scheme (DCAES)” based on the earlier observations. The technique encompasses multiple features like one-level Haar wavelet decomposition, local activity analysis of high-

frequency subbands, adaptive multi-bit embedding and the use of Logistic map method for message scrambling, among others. The LL subband is allowed to retain the primary image information, while LH, HL and HH subbands are studied to find the appropriate embedding zones where higher activity areas can accommodate more data while less active zones can be modified less to lower visual distortion. Prior to embedding, the secret information is scrambled using the permutation sequence generated by the Logistic map method for the purpose of enhancing security of the process. The obtained results of the implementation of the DCAES technique were studied with the use of main evaluation parameters.

Literature Review

The comprehensive report on image steganography and steganalysis compiled by Kombrink *et al.* included conventional, transform domain, hybrid and learning-based techniques. It was stated in their report that the spatial domain methods are still widely used as they are simple and computationally convenient, but the transform domain techniques generally provide better invisibility and strength [6]. It was also pointed out that the existing steganalysis methods are targeted to detect certain embedding methods and thus have problems with generalizing their result to the whole variety of steganographic methods. The information obtained allowed to conclude that the necessity for developing adaptive and resilient embedding techniques emerges from the need to work out such methods that would allow for the balance between payload capacity, quality and resistance to steganalysis. Thus, in order to understand the way to make the

balance among invisibility, robustness and resistance, the hybrid adaptive watermarking technique using DWT, HD and SVD techniques was offered, which uses chaotic Logistic encryption to hide the watermark, then applies some entropy-based methods and Alpha blending in order to find the optimal weight of the watermark depending on the characteristics of the host image [7]. The method had some results but it was mainly about digital watermarking. The way it added watermarks to things relied much on figuring out entropy rather than using the activity in the local frequency area to hide data in a secure way. This is important, for watermarking to be secure. The method did not do a job of using local frequency activity for digital watermarking. Recognizing the growing importance of intelligent security mechanisms, Kusum Lata *et al.* reviewed looked at how chaos theory and fuzzy logic can be used in cryptography and steganography [8]. Their survey explained that cryptography is like a lock that keeps the information safe but steganography is like hiding the information so nobody even knows it is there, this makes using both cryptography and steganography a way to keep sensitive information safe. They also talked about how chaotic system are good for keeping things safe because they are random and very sensitive to the starting conditions. This makes them good for encrypting things making keys and hiding information in pictures. The authors further discussed the advantages of chaotic systems, including randomness, ergodicity and high sensitivity to initial conditions, which make them suitable for encryption, key generation, pixel permutation and random embedding. The survey also highlighted the role of fuzzy logic in adaptively selecting embedding parameters and refining chaotic keys, concluding that intelligent chaos-based frameworks offer significant potential for improving both security and robustness in image steganography. Another study by Zhang *et al.* looked at how chaos theory's used to keep images safe [9]. They emphasized about how images are different, from text and need special ways to be protected. The usual ways of encrypting text do not work well for images because images are big and have a lot of uncertainties. The study said that in the future people should use chaos theory and smart algorithms together to keep images safe. This will make it faster and safer to protect images from attacks. Zhang *et al.* also presented different kinds of chaotic systems like discrete and continuous systems and how they can be used to protect images. In the field of multimedia security, Kumar *et al.* developed a three-layer adaptive video steganography scheme that employed chaotic dynamic systems to strengthen secure communication [10]. The proposed framework incorporated an Adaptive Control Block to determine the embedding capacity according to the available cover space and utilized a Chaotic Key Generator based on Logistic and Sine maps to perform permutation, random frame selection and random embedding position generation. Both the secret information and the selected video frames were encrypted before embedding, thereby providing multiple layers of security. Experimental results demonstrated payloads ranging from 0.56 to 2.25 bpp while maintaining PSNR values between 50.25 dB and 62.05 dB. However, because the algorithm was specifically designed for video data and performed embedding in the spatial domain, its applicability to transform-domain image steganography remains limited. Khalil *et al.* presented a secure image steganography algorithm by combining Least Significant Bit (LSB) substitution with hybrid one-dimensional and two-dimensional chaotic maps together with Tabu Search optimization [11]. Chaotic sequences were

initially generated to determine candidate embedding locations, after which the optimization procedure identified positions that minimized visual distortion before the secret information was embedded using the LSB technique. The proposed method supported different forms of secret data, including text, images and audio, while achieving an embedding capacity of approximately 4.2 bpp with PSNR values exceeding 30 dB. The use of a large key space and strong key sensitivity further enhanced protection against unauthorized access. Nevertheless, since the embedding process remained confined to the spatial domain, the method is comparatively more susceptible to statistical steganalysis than frequency-domain approaches. The existing literature shows that we have made progress with adaptive embedding strategies, processing in the transform domain, optimization techniques and security mechanisms that use chaos. However there are still some problems that we have not solved. Many methods that use the transform domain still use fixed strengths, for embedding which do not work well with the characteristics of each image. On the hand many techniques that use chaos mainly focus on encrypting or randomly embedding things but they do not think about how to adapt the payload and extract it reliably at the same time [12]. Furthermore, several recent studies emphasize watermarking or video steganography instead of secure image steganography. These observations reveal the need for a lightweight transform-domain framework capable of integrating adaptive embedding with chaotic security while maintaining high visual quality and reliable message recovery. Motivated by these limitations, the proposed DWT-based Chaotic Adaptive Embedding Scheme (DCAES) combines Haar wavelet decomposition, activity-driven adaptive bit allocation, Logistic-map-based message permutation and header-assisted extraction to achieve an improved balance among embedding capacity, imperceptibility, security and extraction reliability.

Proposed DCAES-Based Adaptive Chaotic Steganographic Framework

This section presents the proposed "DWT-based Chaotic Adaptive Embedding Scheme (DCAES)", developed to achieve a balanced trade-off among embedding capacity, imperceptibility and security in grayscale image steganography.

Proposed Framework

The proposed DCAES framework is designed around the complementary roles of transform-domain embedding, adaptive payload allocation and chaotic scrambling as shown in figure 2. First, the Haar DWT separates the image into frequency components, allowing the embedding process to avoid direct modification of the LL approximation subband. Second, the activity-guided bit allocation mechanism introduces spatial adaptivity into the transform domain. Rather than applying a fixed embedding depth throughout the image, DCAES assigns 1-3 bits according to the normalized high-frequency activity. This allows the available embedding capacity to be distributed according to image content. Third, the chaotic permutation mechanism provides an additional security layer by scrambling the complete header-payload sequence before embedding. Thus the secret bits are hidden in a sequence that does not show their order and to get the bits back we need to make the correct chaotic sequence using the right key and Logistic-map parameter. Finally, the 32-bit message-length header establishes an explicit boundary and

helps us to know what is data and what is just empty space, in the adaptive-capacity steganography. Adaptive-capacity steganography is special because it can hold a lot data than we are actually using. By recovering the message length from the header and extracting only the corresponding number of bits, the proposed method avoids interpreting unused embedding positions as part of the secret message. Overall, DCAES integrates frequency-domain localization, content-adaptive embedding and key-dependent bit scrambling within a unified framework. The resulting architecture is intended to provide a practical balance between imperceptibility, payload flexibility and resistance to direct unauthorized interpretation of the embedded data. The effectiveness of the proposed method is

subsequently evaluated using image-quality, capacity, extraction-reliability and security-oriented metrics. Let the grayscale cover image be denoted by $I \in R^{M \times N}$ where M and N represent the image dimensions. The proposed DCAES framework transforms the cover image into the frequency domain using a one-level Haar DWT, producing four subbands: $LL, LH, HL, HH = DWT(I)$. The LL subband contains the dominant low-frequency structural information, whereas LH, HL and HH contain high-frequency details. The proposed method deliberately preserves the LL subband and utilizes the three detail subbands for secret-data embedding.

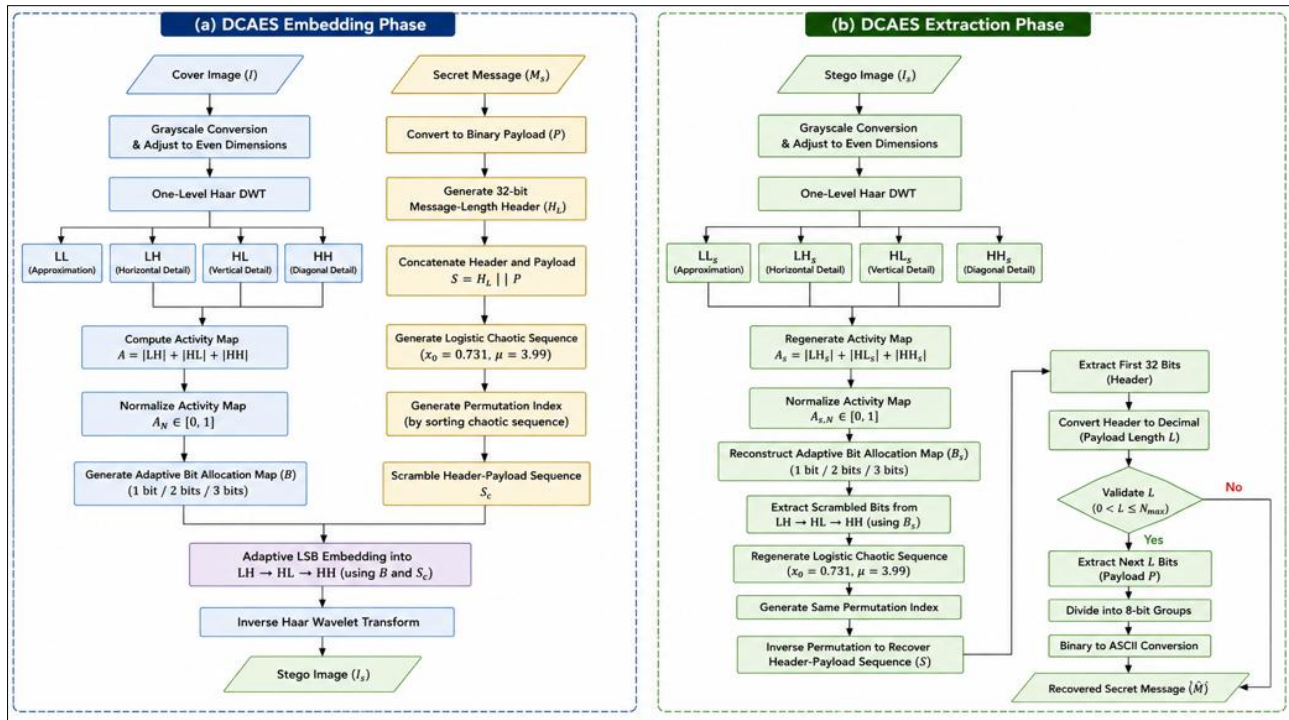


Fig 2: DCAES framework

The embedding process can be summarized as $I \rightarrow LL, LH, HL, HH \rightarrow A \rightarrow B \rightarrow S \rightarrow S_C \rightarrow LH', HL', HH' \rightarrow I_S$

The extraction phase follows the corresponding reverse procedure:

$$I_S \rightarrow LL_S, LH_S, HL_S, HH_S \rightarrow A_S \rightarrow B_S \rightarrow S_C \rightarrow S \rightarrow (H, P) \rightarrow (\hat{H}, \hat{P}) \rightarrow \hat{M}$$

For successful recovery, the embedding and extraction phases must use identical parameterization, including the image preprocessing procedure, Haar transform equations, activity-map computation, adaptive thresholds, subband traversal order, chaotic initial condition, Logistic-map parameter and bit-extraction convention.

Symbol	Definition
I	Original grayscale cover image
M, N	Number of rows and columns of the image
$R^{M \times N}$	Space of real-valued $M \times N$ matrices
$DWT(.)$	One-level Haar discrete wavelet transform
LL	Low-frequency approximation subband
LH	Horizontal-detail high-frequency subband
HL	Vertical-detail high-frequency subband
HH	Diagonal-detail high-frequency subband
A	Activity map generated from the detail subbands
B	Adaptive bit-allocation map
H	Message-length header
P	Original or recovered binary secret payload
S	Original header-payload sequence
S_C	Chaotically permuted/scrambled data sequence
LH', HL', HH'	Modified detail subbands after embedding
I_S	Generated stego image

LL_S, LH_S, HL_S, HH_S	DWT subbands obtained from the stego image
A_S	Activity map regenerated during extraction
B_S	Adaptive bit-allocation map regenerated during extraction
$\hat{P}$	Recovered/estimated secret payload
M	Original secret message
$\hat{M}$	Recovered secret message
$ $	Concatenation operation
$\hat{\cdot}$	Indicates a recovered or estimated quantity
$\cdot_c$ (Subscript C)	Indicates a chaotically scrambled quantity
$\cdot_s$ (Subscript S)	Indicates a quantity associated with the stego image
$\cdot'$	Indicates a modified quantity after embedding

Embedding Phase

The embedding phase of DCAES consists of six major operations: cover-image preprocessing, Haar DWT decomposition, activity-map generation, adaptive bit allocation, chaotic payload scrambling and adaptive embedding. Each stage is described below.

Cover-Image Preprocessing

The input cover image is first converted to grayscale when required. The resulting image is represented as $I_g = [I_g(i, j)]_{M \times N}$. Because the proposed manual Haar transform processes the image using non-overlapping 2×2 blocks, the image dimensions are adjusted to even values. If necessary, the final row or column is excluded so that $M \bmod 2 = 0, N \bmod 2 = 0$. This preprocessing ensures that every image pixel participates in a complete 2×2 Haar decomposition block and that the resulting subbands have dimensions $\frac{M}{2} \times \frac{N}{2}$.

One-Level Haar DWT Decomposition

The preprocessed cover image is decomposed using a manually implemented one-level Haar DWT. For each non-overlapping 2×2 block $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, the corresponding transform coefficients are calculated as $LL = \frac{a+b+c+d}{2}$, $LH = \frac{a+b+c-d}{2}$, $HL = \frac{a+b-c-d}{2}$, and $HH = \frac{a-b-c+d}{2}$. Thus, $I_g \rightarrow \text{Haar DWT}\{LL, LH, HL, HH\}$. The LL subband is retained without modification because it contains the principal low-frequency content of the image. The detail subbands LH, HL and HH are selected as the embedding domain. This selection is motivated by the fact that modifications in high-frequency components are generally less visually noticeable than equivalent modifications in the low-frequency approximation component. The use of three detail subbands also provides a larger embedding space than using a single transform subband.

Activity-Map Construction

To enable content-dependent embedding, DCAES calculates an activity measure for each corresponding coefficient position across the three detail subbands. The activity value at location (i, j) is defined as $A(i, j) = |LH(i, j)| + |HL(i, j)| + |HH(i, j)|$. The activity map therefore combines the magnitude information from all three high-frequency subbands. A high activity value indicates stronger local high-frequency variations, whereas a low activity value corresponds to relatively smooth image content. The raw activity map is normalized to the interval $[0, 1]$ as $A_N(i, j) = \frac{A(i, j) - A_{\min}}{A_{\max} - A_{\min}}$, where $A_{\min} = \min_{i, j} A(i, j)$ and $A_{\max} = \max_{i, j} A(i, j)$. If $A_{\max} = A_{\min}$, the normalized activity map is assigned zero values to avoid numerical instability. The normalized map serves as the basis for adaptive embedding-depth selection.

3.2.4. Adaptive Bit-Allocation Map

Unlike conventional fixed-LSB steganography, DCAES does not assign an identical embedding depth to every transform coefficient. Instead, the number of embedded bits is dynamically determined using the normalized activity value. The adaptive allocation function is defined as $B(i, j) = \begin{cases} 1, 0 \leq A_N(i, j) \leq T_1 \\ 2, T_1 \leq A_N(i, j) \leq T_2 \\ 3, T_2 \leq A_N(i, j) \leq 1 \end{cases}$

where the selected thresholds are $T_1 = 0.33, T_2 = 0.66$. Accordingly,

- Low-activity coefficients receive 1 embedded bit;
- Medium-activity coefficients receive 2 embedded bits;
- High-activity coefficients receive 3 embedded bits.

The resulting matrix B is referred to as the adaptive bit-allocation map. The proposed strategy attempts to reduce unnecessary modifications in relatively smooth regions while utilizing the higher embedding tolerance of active or textured regions. Consequently, the embedding depth becomes dependent on the local characteristics of the host image rather than being globally fixed. Since embedding is performed in three detail subbands, the total theoretical embedding capacity is calculated as $C = 3 \times \sum_{i=1}^{M/2} \sum_{j=1}^{N/2} B(i, j)$.

This capacity represents the total number of available embedding positions across the LH, HL and HH subbands under the generated adaptive bit-allocation map.

3.2.5. Secret Message Formatting and Header Generation

Let the secret message be denoted by M_S . The message is converted into its binary representation to obtain the payload sequence $P = \{p_1, p_2, \dots, p_L\}$, where L represents the payload length in bits. To enable reliable extraction, DCAES prepends a fixed-length 32-bit header containing the payload length. Let the binary representation of the header be denoted by H_L . The complete data sequence before scrambling is therefore $S = H_L || P$, where $||$ denotes concatenation.

3.2.6. Chaotic Permutation of Header and Payload

Before embedding, the complete 232-bit sequence is scrambled using a key-controlled Logistic chaotic map. The Logistic map is defined as $x_{k+1} = \mu x_k$ where x_k is the chaotic state and μ is the control parameter. The proposed implementation uses $x_0 = 0.0731$ as the initial chaotic key and $\mu = 3.99$ as the Logistic-map parameter. A chaotic sequence of length L_{embed} is generated: $X = \{x_1, x_2, \dots, x_{L_{\text{embed}}}\}$. The sequence is sorted and the corresponding sorting indices form the permutation vector P_{chaos} . The original sequence S is then rearranged according to this permutation: $S_C(k) = S(P_{\text{chaos}}(k))$. The resulting

sequence S_C is the scrambled header-payload sequence used for embedding. The chaotic permutation provides a key-dependent rearrangement of the secret bits. Consequently, the embedded data do not retain their original sequential order. Correct recovery therefore requires the same initial chaotic condition, Logistic-map parameter and sequence length.

3.2.7. Adaptive LSB Embedding

The scrambled sequence S_C is embedded into the detail subbands using the adaptive bit-allocation map B . The embedding follows the fixed subband traversal order $LH \rightarrow HL \rightarrow HH$. At each coefficient position (i, j) , the corresponding value $B(i, j)$ determines the number of consecutive bits extracted from S_C and embedded into that coefficient. If $B(i, j) = 1$, one bit is embedded. If $B(i, j) = 2$, two bits are embedded. Similarly, if $B(i, j) = 3$, three bits are embedded. The embedding process continues sequentially until all L_{embed} bits have been embedded. Importantly, the embedding process does not necessarily utilize the entire theoretical capacity of the image. If the capacity is greater than L_{embed} , the embedding process terminates immediately after the complete header-payload sequence has been embedded. The resulting modified detail subbands are denoted by LH', HL', HH' . The LL subband remains unchanged.

3.2.8. Stego-Image Reconstruction

After adaptive embedding, the modified wavelet coefficients LL, LH', HL', HH' are transformed back into the spatial domain using the corresponding inverse Haar transform. The resulting image is the stego image I_S . The generated stego image should preserve the perceptual characteristics of the cover image while carrying the embedded secret information.

3.3. Extraction Phase

The extraction phase is designed as the exact operational counterpart of the embedding phase. Its objective is to recover the secret payload from the stego image without requiring access to the original cover image.

3.3.1. Stego-Image Acquisition and Preprocessing

The stego image I_S is loaded. The same dimension-adjustment procedure used during embedding is applied to ensure that the image dimensions are compatible with the 2×2 Haar decomposition. The resulting image is denoted by $I_S \in R^{M \times N}$. Consistency between the embedding and extraction preprocessing steps is essential because even a difference in image dimensions or grayscale conversion can alter the subsequent DWT coefficients.

3.3.2. Haar DWT of the Stego Image

The stego image is decomposed using the same one-level Haar transform: $I_S \rightarrow DWT \rightarrow LL_S, LH_S, HL_S, HH_S$. The extraction process uses the three detail subbands LH_S, HL_S and HH_S because these contain the modified coefficients carrying the embedded data. The LL_S subband is not used for payload extraction.

3.3.3. Regeneration of the Activity and Bit-Allocation Maps

The activity map is reconstructed from the extracted high-frequency subbands according to $A_S(i, j) = |LH_S(i, j)| + |HL_S(i, j)| + |HH_S(i, j)|$. The activity map is normalized using the same min-max normalization procedure: $A_{S_N}(i, j) =$

$\frac{A(i, j) - A_{S_{\min}}}{A_{S_{\max}} - A_{S_{\min}}}$. The adaptive bit-allocation map is then regenerated using the same thresholds: $B_S(i, j) = \begin{cases} 1, 0 \leq A_{S_N}(i, j) \leq T_1 \\ 2, T_1 \leq A_{S_N}(i, j) \leq T_2 \\ 3, T_2 \leq A_{S_N}(i, j) \leq 1 \end{cases}$

The regenerated map determines how many LSBs must be read from each coefficient during extraction. The extraction sequence must therefore reproduce the same coefficient traversal order as embedding: $LH_S \rightarrow HL_S \rightarrow HH_S$.

3.3.4. Extraction of the Chaotically Scrambled Sequence

The extraction process sequentially reads the embedded bits from the LH_S, HL_S and HH_S subbands according to the regenerated adaptive bit-allocation map. For each coefficient, the value of $B_S(i, j)$ determines the number of LSBs to be recovered. The extraction continues until the complete embedded sequence $\widehat{S}_C$ has been recovered. At this stage, the recovered sequence is still in its chaotic scrambled order and therefore cannot yet be directly interpreted as the original header and payload.

3.3.5. Chaotic Sequence Regeneration

To restore the original bit ordering, the extraction phase regenerates the same Logistic chaotic sequence using the shared parameters $x_0 = 0.0731$ as the initial chaotic key and $\mu = 3.99$ as the Logistic-map parameter. This sequence is made with the number of bits, L_{embed} that was used when the bits were embedded. The new sequence is then sorted to get the order, which is called the permutation vector P_{chaos} . The reason we have to do it this way is that chaotic systems are very sensitive to the starting points and the parameters that control them. So we have to use the values, for x_0 and μ when we extract the bits out that we used when we embed the bits.

3.3.6. Inverse Chaotic Permutation

After extraction, the scrambled bit sequence $\widehat{S}_C$ is reordered using the regenerated permutation vector to restore its original arrangement: $\widehat{S}_C(k) = S_C(P_{\text{chaos}}(k))$. The reordered sequence is represented as $\widehat{S}_C = \widehat{H}_L || \widehat{P}$, where $\widehat{H}_L$ denotes the recovered message-length header and $\widehat{P}$ represents the extracted secret payload. The initial 32 bits correspond to the embedded header, while the remaining bits contain the hidden message. Reconstructing the original bit order before decoding is essential because the scrambled sequence does not preserve the correct bit arrangement. Consequently, directly converting the scrambled bits into ASCII characters would produce invalid or unintelligible output.

3.3.7. Header-Based Payload Length Detection

To determine the size of the embedded message, the first 32 recovered bits are interpreted as a binary representation of the payload length. The detected message length is obtained by converting this binary header into its decimal equivalent: $\widehat{L} = \text{Binary to Decimal}(\widehat{H}_L)$. The recovered payload length is subsequently validated to verify that it is greater than zero and does not exceed the number of available payload bits extracted from the stego image. This verification step prevents errors arising from an incorrectly recovered header, such as invalid memory allocation or attempts to access data beyond the available embedding capacity. Once validated, the detected header serves as a reliable boundary for payload

extraction, ensuring that only the actual embedded message is recovered while excluding any redundant or unrelated bits.

3.3.8. Payload Recovery

Once the payload length has been determined, the valid secret payload $\hat{P}$ is extracted from the recovered sequence. This step ensures that only the actual embedded payload is interpreted as secret information. The remaining unused embedding capacity is ignored.

3.3.9. Binary-to-ASCII Message Reconstruction

The recovered payload $\hat{P}$ is divided into consecutive groups of eight bits where each group contains eight binary bits. Each 8-bit group is converted to its decimal equivalent and then mapped to the corresponding ASCII character. The recovered characters are concatenated to reconstruct the secret message $\hat{M}$. The successful extraction is achieved when $\hat{M} = M_S$.

Experimental Setup

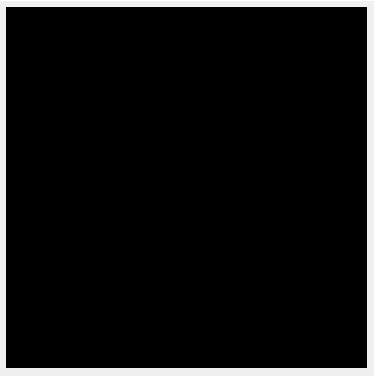
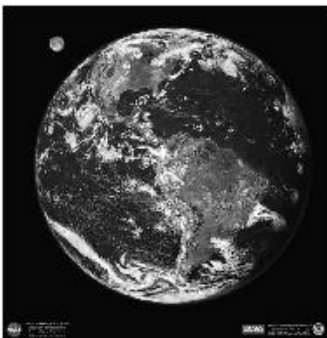
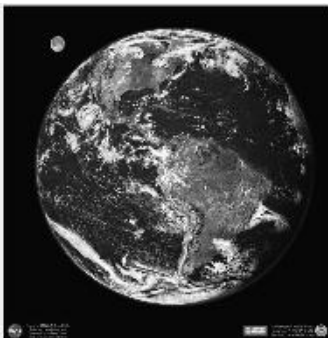
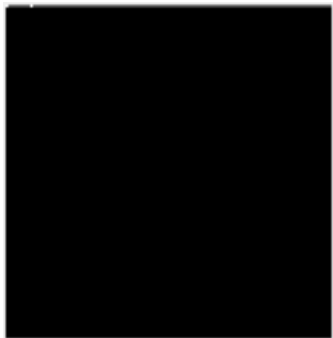
The proposed “DWT-based Chaotic Adaptive Embedding Scheme (DCAES)” was implemented in “MATLAB R2015a”

to evaluate its embedding performance and visual quality. Experiments were carried out on five standard grayscale images, namely “Airplane, Cameraman, Earth, Flowers and Lena”, representing different texture and edge characteristics. A one-level Haar Discrete Wavelet Transform (DWT) was applied to each cover image and the secret message was securely embedded within the high-frequency subbands using adaptive bit allocation guided by the activity map and Logistic-map-based chaotic permutation. The performance of the proposed method was assessed in terms of “Peak Signal-to-Noise Ratio (PSNR)”, “Structural Similarity Index Measure (SSIM)”, “Mean Squared Error (MSE)”, “Bits Per Pixel (BPP)” and embedding capacity to evaluate the trade-off between imperceptibility and payload efficiency.

Results and Discussion

The performance of the proposed “DWT-based Chaotic Adaptive Embedding Scheme (DCAES)” was evaluated using five widely adopted grayscale benchmark images: “Airplane, Cameraman, Earth, Flowers and Lena”.

Table 1: Visual comparison of cover images, stego images and corresponding difference images

Image Name	Cover Image	Stego Image	Difference Image
Airplane			
Cameraman			
Earth			



The proposed framework was assessed through both visual and quantitative evaluations to examine its ability to maintain high image quality while supporting efficient data embedding. Visual results are presented in “Table 1”, quantitative

performance metrics are summarized in “Table 2” and a graphical comparison of the experimental results is provided in “Table 3”, offering a comprehensive assessment of the framework's performance.

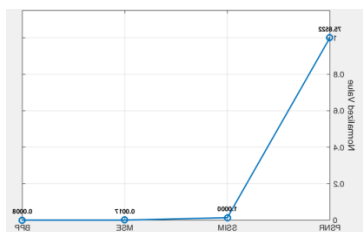
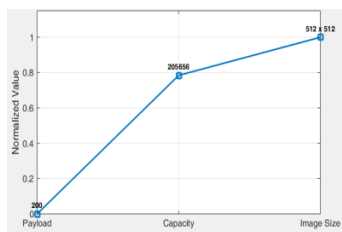
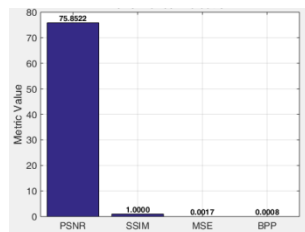
Table 2: Quantitative performance evaluation of the proposed DCAES on benchmark images

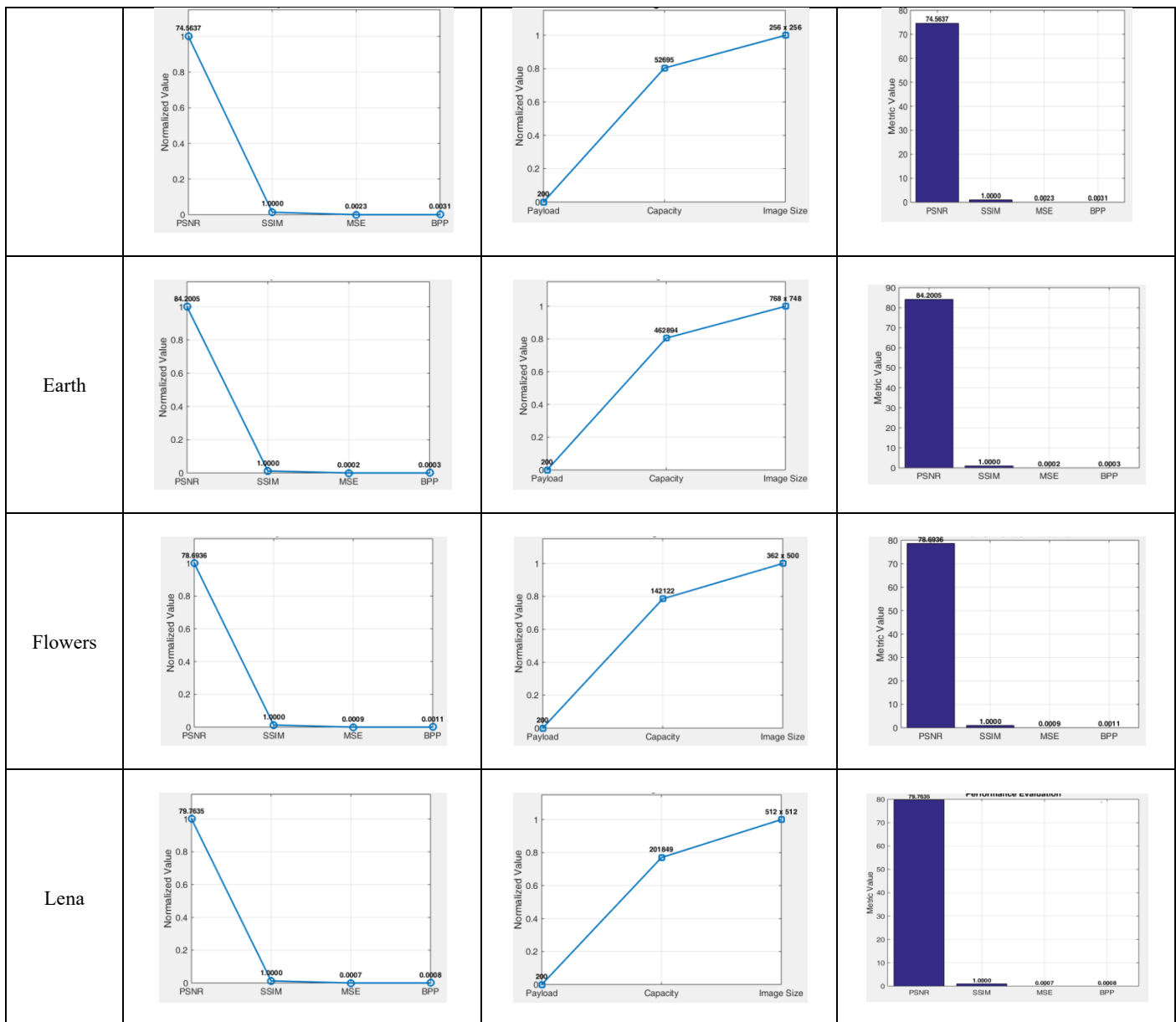
Image Name	Image size	Capacity (bits)	PSNR (dB)	SSIM	MSE	BPP
Airplane	512 x 512	205656	75.8522	0.999996	0.00168991	0.000763
Cameraman	256 x 256	52695	74.5637	0.999985	0.00227356	0.003052
Earth	768 x 748	462894	84.2005	0.999998	0.00024719	0.000348
Flowers	362 x 500	142122	78.6936	0.999994	0.00087845	0.001105
Lena	512 x 512	201849	79.7635	0.999996	0.00068665	0.000763

The visual results presented in “Table 1” indicate that the proposed embedding process introduces only minimal changes to the original images. Across all benchmark images, the stego images remain visually almost identical to their corresponding cover images, making it difficult to distinguish between them through visual inspection alone. The corresponding difference images exhibit only a small number

of localized intensity variations, suggesting that the embedding operation causes very limited pixel modifications. These observations demonstrate that the adaptive embedding strategy effectively places the secret data in regions where alterations are less noticeable, thereby preserving the overall visual appearance and perceptual quality of the host images.

Table 3: Comparative analysis of quality assessment and embedding performance metrics for the proposed DCAES

Image Name	Quality Assessment Metrics	Embedding performances	Performance Evaluation
Airplane			
Cameraman			



“Table 2” presents the quantitative performance of the proposed DCAES framework. The results show that the method maintains high image quality while providing effective data embedding. For all benchmark images, the “PSNR” values range from “74.56 dB” to “84.20 dB”, indicating that the embedding process introduces only a very small amount of distortion. Among all test images, “Earth” achieves the highest PSNR, suggesting that it can hide more information with minimal visual change. In contrast, “Cameraman” records the lowest PSNR because its large smooth regions are more sensitive to pixel modifications. Even so, all PSNR values remain far above the level generally considered acceptable for imperceptible image steganography, showing that the proposed method preserves image quality effectively. A similar trend can be observed from the “SSIM” values. As shown in “Table 2”, the SSIM values vary between “0.999985” to “0.999998”, which are very close to “1”. This indicates that the structural content of the original images is almost completely preserved after embedding. Image features such as edges, textures and fine details remain nearly unchanged, making the stego images visually indistinguishable from their corresponding cover images. The “MSE” values also confirm the high quality of the reconstructed images. Across all benchmark images, the MSE ranges from “0.000247” and “0.002274”, indicating that only

a small number of pixel values are affected during embedding. The “Earth” image produces the lowest MSE, whereas “Cameraman” has the highest. However, the overall error remains extremely small, demonstrating that embedding data into the high-frequency wavelet coefficients helps reduce distortion while maintaining image fidelity. Another key feature of the proposed framework is its “adaptive embedding capacity”. Instead of embedding a fixed amount of data in every image, the framework adjusts the payload according to the local image characteristics. Images with more edges and textured regions naturally provide additional embedding locations, while smoother images offer fewer suitable positions. As a result, “Earth” achieves the highest embedding capacity, whereas “Cameraman” provides the lowest. This adaptive strategy allows the framework to increase payload without causing unnecessary degradation in image quality. The corresponding “BPP” values further indicate that the available embedding space is used efficiently. To provide a clearer comparison, the performance metrics are also illustrated graphically in “Table 3”. The graphs show consistently high PSNR and SSIM values together with very low MSE for all benchmark images. They also highlight the differences in embedding capacity and payload among the test images, reflecting the adaptive nature of the proposed method. The graphical representation makes it easier to compare the

performance across different images and supports the numerical results presented in “Table 2”. Overall, both the visual and quantitative evaluations demonstrate the effectiveness of the proposed DCAES framework. The combination of “Haar wavelet decomposition”, “adaptive activity-based bit allocation” and “Logistic map-based chaotic permutation” enables secure and efficient data embedding while preserving image quality and structural information. The consistently high PSNR and SSIM values, together with the low MSE and adaptive embedding capacity, indicate that the proposed framework achieves a good balance between image quality, payload capacity and embedding security. These results suggest that DCAES is a reliable approach for secure image steganography and can be applied to image communication systems where both data protection and visual quality are important.

Conclusion

This work presented a “DWT-based Chaotic Adaptive Embedding Scheme (DCAES)” for secure image steganography. The framework combines the Haar Discrete Wavelet Transform (DWT) with adaptive bit allocation and Logistic map-based chaotic permutation to improve the security of embedded data while keeping changes to the cover image as small as possible. By selecting embedding locations according to local image characteristics, the method increases payload capacity without noticeably affecting visual quality. The proposed approach was tested on five commonly used grayscale benchmark images: “Airplane, Cameraman, Earth, Flowers and Lena”. The experimental results showed high “PSNR” and “SSIM” values together with very low “MSE”, indicating that the hidden data can be embedded with minimal impact on image quality. The adaptive embedding strategy also makes effective use of edge and textured regions, allowing different images to accommodate different payloads according to their content rather than using a fixed embedding capacity. The results show that combining wavelet-domain embedding with adaptive payload allocation and chaotic permutation provides a reliable approach for secure data hiding. The framework maintains a good balance between embedding capacity, visual quality and data security, making it a practical choice for applications that require confidential image transmission and privacy-preserving multimedia communication.

References

1. Hussain M, Wahab AWA, Idris YIB, Ho ATS, Jung KH. Image steganography in spatial domain: a survey. *Signal Process Image Commun.* 2018;65:46-66. doi:10.1016/j.image.2018.03.012.
2. Gonzalez RC, Woods RE. *Digital image processing*. 4th ed. New York: Pearson; 2018.
3. Sahu AK, Sahu M. Digital image steganography and steganalysis: a journey of the past three decades. *Open Comput Sci.* 2020;10(1):296-342. doi:10.1515/comp-2020-0136.
4. Mallat SG. A theory for multiresolution signal decomposition: the wavelet representation. *IEEE Trans Pattern Anal Mach Intell.* 1989;11(7):674-693. doi:10.1109/34.192463.
5. Alwan HH, Hussain ZM. A multiplicative-additive chaotic-address steganography. *J Kufa Math Comput.* 2023;7(2):16-25. doi:10.31642/JoKMC/2018/070204.
6. Kombrink MH, Geradts ZJMH, Worring M. Image steganography approaches and their detection strategies:

a survey. *ACM Comput Surv.* 2024;57(2):33. doi:10.1145/3694965.

7. Dong Y, Yan R, Yin C. An adaptive robust watermarking scheme based on chaotic mapping. *Sci Rep.* 2024;14:24735. doi:10.1038/s41598-024-76101-w.
8. Lata K, Rathee S, Meenakshi, Yadav V, Dhaka N. A survey of chaos based cryptography and steganography techniques. *J Propul Technol.* 2024;45(3):1452-1465.
9. Zhang H, Feng X, Sun J, Yan P. Chaotic image security techniques and developments: a review. *Mathematics.* 2025;13(12):1976. doi:10.3390/math13121976.
10. Kumar D, Sudha VK, Manikandan N, Ramaswamy K. Efficient three layer secured adaptive video steganography method using chaotic dynamic systems. *Sci Rep.* 2024;14:15234. doi:10.1038/s41598-024-67074-x.
11. Khalil N, Sarhan A, Alshewimy MAM. A secure image steganography based on LSB technique and 2D chaotic maps. *Comput Electr Eng.* 2024;119(Pt B):109566. doi:10.1016/j.compeleceng.2024.109566.
12. VA GA, Devanagavi GD. Hybrid 2D logistic chaotic map and Vernam cipher for secure image encryption and steganography. *Int J Comput Netw Inf Secur.* 2026;18(3):85-104. doi:10.5815/ijcnis.2026.03.05.