



Integrating Genetic and Chaotic Algorithms for Secure Data Hiding: An Enhanced Steganographic Framework

Dineshkumar Thangaraju^{*ID}, Asokan Ramasamy^{ID}

Department of Electronics and Communication Engineering, Kongunadu College of Engineering and Technology, Trich 621215, India

Corresponding Author Email: dineshkumart@kongunadu.ac.in

Copyright: ©2026 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ts.430421>

ABSTRACT

Received: 9 April 2026
Revised: 15 June 2026
Accepted: 22 June 2026
Available online: 31 August 2026

Keywords:

image steganography, integer wavelet transform, chaotic embedding, genetic algorithm, logistic map

Image steganography enables confidential communication by concealing secret information within digital images while minimizing perceptual distortion. This paper proposes a secure image steganography framework that integrates integer wavelet transform (IWT), a logistic-map-based chaotic embedding strategy, and genetic algorithm (GA) optimization. The IWT decomposes the cover image into wavelet sub-bands suitable for data embedding. The logistic map generates pseudo-random embedding locations to improve embedding unpredictability, while the GA optimizes embedding positions using a multi-objective fitness function that considers peak signal-to-noise ratio (PSNR), structural similarity index measure (SSIM), visual information fidelity (VIF), and embedding capacity (EC). Experimental evaluation was conducted on approximately 1000 benchmark images of multiple resolutions. The proposed framework achieved an average PSNR of 55.34 dB, mean squared error (MSE) of 0.36, SSIM of 0.975, VIF of 0.925, and an average EC of 3.67 bits per pixel (BPP). Histogram and statistical analyses indicate that the stego-images maintain characteristics parallel to the original images under the evaluated conditions. The results validate that the proposed combination of IWT, chaotic embedding, and GA optimization provides a favorable balance between EC and visual quality while maintaining resistance against the tested statistical and noise-based analyses.

1. INTRODUCTION

In traditional digital communication, researchers have been analysing data security [1]. Methods for hiding data are implemented to secure information from threats and to sustain data privacy, protection, accuracy, and confidentiality [2, 3]. Data concealment techniques are mainly categorized into three types comprising steganography, digital watermarking, and cryptography. The most widely used data-concealment method for converting raw information into encoded information is cryptography [4, 5]. Raw information is retrieved by decoding the encoded cipher data. Steganography is a process to protect additional information within digital files [6]. The original data and the carrier medium that hides it can be separate digital entities. The embedded data made invisible to an attacker is the core idea of the steganographic method. The presence of secreted information within the communicated protection object is known only to the originator and the receiver; it can be securely sent through a public medium [7].

The digital cover objects are secured through digital watermarking methods. Both a digital signature and a digital watermark provide comparable protection. A digital watermark acts as an embedded marker, for instance, that determines the ownership of a digital object or validates its reliability and originality. Digital watermarking methods are

commonly used to regulate data consistency, validate the data sources, and protect the ownership of multimedia files. Protection of multimedia files is connected to the conventional digital watermarking methods. Currently, employing these methods for protecting data with specific features [8] is beginning to increase recognition.

Image steganography is an effective technique to conceal sensitive information within digital images, offering confidential communication [9-13] and data security. Cryptography ensures that the existence of concealed information leftovers unnoticeable to unauthorized parties, thus improving the protection and confidentiality of hidden information. While encryption encodes the message content into an unreadable format to unauthorized individuals, steganography can be integrated with encryption to offer a further level of protection [14]. Even in the case of an interception occurring in an encrypted message, steganography can secure the information from unauthorized access, revealing the existence of concealed data. Unlike encryption, which generates signals that alert attackers to the occurrence of concealed data, steganography remains difficult to identify without specialized knowledge or advanced evaluation methods. Image steganography consists of multiple approaches, each using a different technique to conceal data effectively.

2. MOTIVATION

The main objective for using image steganography with the integer wavelet transform (IWT), a logistic map-based chaotic algorithm, and genetic algorithm (GA) resides in improving protection, durability, encoding capability, flexibility, and development in embedding communication systems. The proposed method couples IWT, logistic map-based chaotic algorithm, and GA to produce an advanced and robust steganographic technique. The combination of various techniques maximizes the detection complexity, increases encoding capability, and offers flexibility to multiple encoding applications.

Despite significant advances in image steganography, several limitations remain unresolved. First, many IWT-based approaches suffer from restricted embedding capacity (EC) because data insertion is constrained to a limited set of transform coefficients. Second, chaotic embedding methods often rely solely on pseudo-random position selection without evaluating the visual suitability of candidate embedding locations, reducing robustness against statistical detection. Third, optimization-based approaches using GA frequently focus on maximizing payload or image quality independently, leading to instability in the trade-rancid between EC, imperceptibility, and robustness. Therefore, a unified framework capable of simultaneously addressing capacity limitations, secure embedding position selection, and multi-objective optimization remains an open research challenge.

2.1 Contribution

The combination of the three advanced algorithms leads to the expansion of a high-performance scheme that can solve the difficulties of image steganography. Using the improved algorithms helps to enhance the safety and reliability of the material embedded into the cover images. Thus, the proposed system can be used in secure communication, digital forensics, confidential information exchange, and other applications that require the maintenance of the secrecy and integrity of the information transferred. In addition, the planned method improves the current methods of image coding by creating a reliable method for transmitting information secretly in various application contexts, such as military communication systems, forensic investigations, and information exchange over the Internet.

The main objectives of the effort are listed below:

- A technique for embedding into the image is suggested, which is based on the logistic map and which allows choosing pseudo-random positions for hiding the information into the sub-bands created using the IWT.
- A multi-objective inherited optimization procedure is developed, which aims to maximize four metrics of the quality and noiselessness of the resulting copy (EC, peak signal-to-noise ratio (PSNR), structural similarity index measure (SSIM), visual information fidelity (VIF)).
- The method of constraining the fitness function is planned to control the size of the embedded payload and prevent its overloading.
- A comprehensive set of experiments using nearly 1000 images of different sizes and payload sizes is carried out.
- A relative scrutiny of the outcomes found with the best-known IWT-based image steganography algorithms is made.

2.2 Paper organization

The remainder of this paper is organized as follows: Section 3 discloses the study and the conversation of state of art techniques. In Section 4, the future work and its functionality are explained. In Section 5, the research procedures and grades are discussed. Section 6 completes the article.

3. LITERATURE SURVEY

In this part, a literature survey is provided for representative papers on IWT, chaotic-map-based methods, GA and other optimization methods used in image steganography and watermarking.

Muhuri et al. [15] designed an image steganography scheme based on IWT and Particle Swarm Optimization (PSO) to find the proper locations for embedding secret messages. According to the described scheme, PSO explores the existing search space and identifies the proper embedding regions, thereby increasing the robustness and scalability of the data-hiding process. Another optimized steganographic approach that employs IWT was suggested by Sabeti et al. [16]. In particular, the authors used GA for identifying the embedding regions in a flexible manner. In particular, GA represents the candidate solutions in the form of a genetic structure and performs the selection procedure iteratively. As a result, the steganography scheme becomes more adaptive and scalable and thus ensures better robustness of information concealment.

Ambika and Biradar [17] developed an IWT-based steganographic scheme in combination with fractal encryption. In this case, image blocks are transformed one by one using their respective fractal limitations in command to increase the refuge of the hidden information and robustness to any unauthorized access and analysis of the steganography system. An approach that uses an unsupervised neural network for finding suitable cover images and guiding the process of choosing the embedding region was introduced by Kumar and Hussaini [18]. The suggested approach also uses chaotic structures and transformation techniques, including IWT.

Pramanik [19] offered an IWT-based steganographic scheme optimized via GA to make the embedding information more resilient. This scheme uses the edge intensity criterion calculated from the neighbourhood information in order to recognize the appropriate constants for the data implanting. Also, Pramanik et al. [20] presented a steganographic scheme that uses bi-orthogonal wavelet transformation and GA. In particular, the cover duplicate is decayed into various resolution levels and spectral sub-bands using bi-orthogonal ripple transform, and thus creates suitable places for inserting the secret data. The decomposition technique allows to keep the hidden information visually imperceptible and limits the quantity of alteration extra to the original image.

Govindasamy [21] studied a coverless image steganography scheme, where the secret information is directly related to the image without requiring any additional cover image. In this way, the proposed concept offers another direction for data hiding and can allow the image to represent the message without making any changes to its visual representation. Particular attention in this paper is paid to the possibility of increasing the information transmission capability of coverless steganography using Haar IWT.

Li et al. [22] introduced a GAN-based spatial

steganographic framework. In this framework, the generator learns complex probability distributions of images and creates a detailed probability map from the deep-level representations of the images. This probability map then guides the embedding process to the more suitable regions, and therefore increases the capability to hide information using the steganographic system. On the contrary [23], the robustness of the steganographic systems to channel distortions was improved. The authors analysed the sources of the channel errors and divided them into steganography-dependent and steganography-independent ones. The proposed approach improves the fighting to JPEG recompression and improvement sifting, thereby addressing practical channel distortions that were insufficiently considered in traditional steganographic techniques.

Pan et al. [24] use double-matrix decomposition in connection with multi-region coverage for image steganography. In this way, the proposed framework aims to increase the recovery ability of stego-images under external disturbances and to increase the security of the implanting course at the similar time. In particular, the chosen data-hiding positions in the wavelet domain are processed via Hessenberg matrix decomposition, thereby increasing the robustness of the steganographic system. Al-Shaarani and Gutub [25] studied two secret sharing schemes, namely, counting-based and derivative-matrix-based schemes, in conjunction with image steganography. In particular, the authors took into consideration both the Least Significant Bit (LSB) and Discrete Wavelet Transform (DWT)-based methods and aimed to combine cryptographic and steganographic schemes.

Peter et al. [26] suggested a data-hiding framework supporting the encryption and decryption processes in connection with the quick response mechanism and shifting-based mechanism. The combination of these two mechanisms is an alternative to the traditional way of protecting and processing concealed information. Setiadi [27] proposed the hybrid edge-detection technique was suggested in order to expand the regions with edges in the cover images. This technique works on the three Maximum Significant Bits (MSBs) of the iWizart pels and aims to increase the number of regions with edges that can be used for data embedding. As a rule, the regions with edges can endure more changes than the smooth ones, and therefore their use can potentially increase EC while keeping good visual quality.

The Ballot transform was used by Hossain et al. [28] in order to generate integer polynomial sequences serving as the coefficients for the non-overlapping groups of m pixels in the shelter copy. GA was incorporated to increase the quality of the generated stage-double without the need for exhaustive evaluation of all the k -bit combinations. Xu et al. [29] introduced the reversible image steganography method called RIIS was developed. In particular, it uses a provisional regulating flow architecture to perfect the supply of residual high-occurrence machineries and contextual information from the host image. Moreover, distortion-guided modulation is performed for the flow-based blocks in order to create a generalized model capable of meeting different embedding requirements. Mandal et al. [30] and Kaur et al. [31] presented the comprehensive investigations and extensive experimental evaluations of digital image steganography.

Wang et al. [32] aimed at the use content similarity to increase the security of JPEG steganography. In particular, the proposed approach exploits the similarity properties of Discrete Cosine Transform (DCT) blocks and uses 64 parallel

channels for constructing the effective distortion metric. Then, the distortion calculation is optimized created on the content properties of the twin in instruction to improve the concealment of the fixed information.

In the field of digital watermarking, Soualmi and Laouamer [33] suggested a copyright protection framework combining Speeded-Up Robust Features (SURF), DCT, and the Imperialist Competitive Algorithm (ICA). The main goal of this framework is to protect digital images against any unauthorized modification and reproduction. ICA is used to find the suitable embedding region for the watermarks and to reduce the likelihood of selecting improper regions that would decrease watermarking accuracy and decrease image quality. Soualmi et al. [34] developed the blind color-image watermarking scheme using the A* algorithm, DCT, and a chaotic sequence in order to solve the problems of invisibility, robustness, computational complexity, blind extraction and security. First, the swarm copy is changed to the DCT field in order to obtain frequency coefficients. Then, the A* algorithm and the Arnold chaotic map are used to optimally and randomly permute the sequence of image blocks according to the obtained DCT coefficients. Finally, the embedded information is extracted using the data-hiding scheme.

Table 1. Summary of the state of the performance of techniques

Ref.	Year	Modified Technique Name	Performance Metrics
[7]	2020	IWT-Based PSO Optimization	PSNR = 51.15, SSIM = 1.00, QI = 1.00
[8]	2022	IWT-Guided Genetic Optimization	PSNR = 62.04, SSIM = 1.00
[9]	2021	IWT with Fractal-Based Encryption	PSNR = 53.87, SSIM = 0.98
[10]	2021	IWT with Cyclic Chaos and Neural Learning	PSNR = 58.43, SSIM = 1.00
[11]	2023	IWT-Driven GA Optimization	PSNR = 62.57, SSIM = 0.99, CC = 0.99
[12]	2020	IWT-Based genetic algorithm Scheme	PSNR = 54.32, MSE = 0.24, CC = 0.93, VIF = 0.92
[13]	2020	Haar Wavelet-Based IWT Method	PSNR = 53.89
[14]	2022	IWT with Dual-Matrix Decomposition	PSNR = 49.51, SSIM = 0.99
[17]	2022	Matrix-Based Counting Scheme	PSNR = 107.70, MSE = 0.29
[18]	2022	Histogram-Based Shifting Method	PSNR = 52.53, MSE = 4.63, SSIM = 0.96
[19]	2022	Dilated Hybrid Edge-Based Detection	PSNR = 46.44, MSE = 0.01
[20]	2022	Ballot Transform with Genetic Optimization	PSNR = 49.33

Note: IWT = integer wavelet transform; PSO = particle swarm optimization; GA = genetic algorithm; PSNR = peak signal-to-noise ratio; SSIM = structural similarity index measure; CC = correlation coefficient; MSE = mean squared error.

Thus, the surveyed literature demonstrates that the combination of transform-domain techniques, chaotic maps, evolutionary optimization techniques, and intelligent learning models has improved the recital of duplicate coding and watermarking systems significantly. However, the present approaches emphasize the optimization of individual aspects, such as EC, imperceptibility, robustness, etc., without paying enough attention to simultaneous consideration of these

competing aspects. Also, some methods use fixed or manually selected embedding regions, while other methods have certain limitations when keeping image quality at high payload levels. These factors show the need for an adaptive and multi-objective optimization scheme that will allow selecting the secure embedding location, distributing the payload properly, and preserving the perceptual quality of stego-images. The current research aims to provide such an approach by combining chaotic pseudo-random embedding with IWT-based decomposition and GA-based multi-objective optimization.

Table 1 shows a relative appraisal of state-of-the-art image steganography methods with their respective trial results. The efficacy of the future steganography methodologies is measured with the help of some popularly used parameters for evaluating the perceptual quality, structural similarity, degree of distortion, visual fidelity, and security from attack on image-based systems. Some of the most commonly used evaluation metrics are SSIM, PSNR, VIF, Correlation Coefficient (CC), mean squared error (MSE), Quality Index (QI), Image Fidelity (IF), Average Difference (AD), Unified Average Changing Intensity (UACI), and Number of Pixels Change Rate (NPCR).

Overall, these studies effectively facilitate the advancement of image encryption algorithms by offering a variety of approaches to enhance protection, efficiency, and durability for securing confidential image data in a variety of fields of applications.

4. PROPOSED CONCEALED COMMUNICATION SCHEME

The covert communication method starts with selecting an appropriate cover image that will carry the secret information within itself. The planned methodology is built on two chief steps: the primary being an embedding step using IWT-based genetic cryptography combined with logistic-map-based technique and the second step is for decrypting the embedded information.

4.1 Genetic steganography with Wavelet-based & logistic embedding Maps

Figure 1 shows a schematic illustration of the complete embedding process.

Steps 1-3: The initial step in embedding the secret message involves breaking down the shelter copy into several minor sub-pictures or lumps to ease the process of systematic distribution of the hidden information in the host image. The sub-images are kept to contain the localized contents of the original cover image. Later, the Numeral Ripple Convert (IWT) is practical individually to each of the submarine-images to transform their spatial information into distinct frequencies. An integer-to-integer and reversible transformation, IWT provides for the embedding of data without adding distortion to the shelter double.

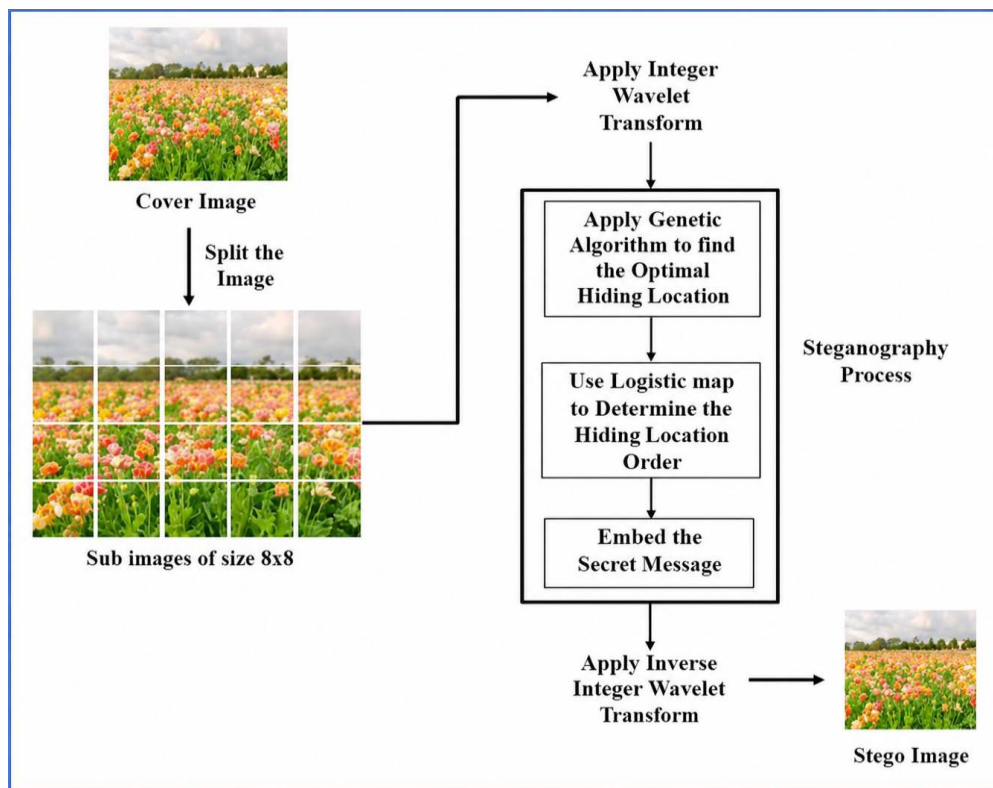


Figure 1. Wavelet-based genetic steganography with logistic map embedding process

Subsequently the transformation procedure, the GA assesses the potential embedding solutions by taking several criteria into consideration such as embedding capacity (EC), perceptual quality of the image and its visual fidelity. The fitness function takes the multi-objective approach in integrating PSNR, SSIM, VIF and EC to formulate a fitness value. Moreover, a penalty criterion is added to the function to

limit the embedding of too much payload that may negatively affect the perceptual quality of the Stege-duplicate.

The suitability purpose is expressed as $F = w_1PSNR_{norm} + w_2SSIM + w_3VIF + w_4EC - P$, where w_1 , w_2 , w_3 , and w_4 denote the allowance constants assigned to each performance metric. In this work, weights of 0.30, 0.25, 0.20, and 0.25 are assigned to PSNR, SSIM, VIF, and EC,

respectively, to achieve a balanced craft-off among inaudibility and payload capacity. To prevent noticeable image degradation, a penalty term P is introduced and calculated as $P = \lambda_{\max}(0, EC - EC_{\max})$, where, λ is the penalty coefficient and $EC_{\max}$ is the maximum allowable EC threshold. The values $\lambda = 0.5$ and $EC_{\max} = 4.0$. Based on preliminary experiments, BPP was chosen as the payload size above which distortions could be noticed in the stego image. As a result, candidate solutions with an EC higher than the prescribed one get penalized in terms of fitness value, which allows GA to find the optimal places for embedding with maximum security and payload but with minimum distortion.

The sub-images are analyzed and represented as matrices

$$\begin{aligned} a[i, j] &= \frac{X[2i, 2j] + X[2i + 1, 2j] + X[2i, 2j + 1] + X[2i + 1, 2j + 1]}{4}, \\ d_h[i, j] &= \frac{X[2i, 2j] + X[2i + 1, 2j] - X[2i, 2j + 1] - X[2i + 1, 2j + 1]}{4}, \\ d_v[i, j] &= \frac{X[2i, 2j] - X[2i + 1, 2j] + X[2i, 2j + 1] - X[2i + 1, 2j + 1]}{4}, \\ d_d[i, j] &= \frac{X[2i, 2j] - X[2i + 1, 2j] - X[2i, 2j + 1] + X[2i + 1, 2j + 1]}{4}. \end{aligned} \quad (1)$$

Here, X denotes the input data matrix, while i and j represent the row and column indices, respectively. The coefficient $a[i, j]$ signifies the estimate coefficient (low-pass module), while $d_h[i, j]$, $d_v[i, j]$, and $d_d[i, j]$ signify the horizontal, vertical, then diagonal detail factors (high-pass mechanisms), correspondingly, at spot (i, j) .

4.1.2 Down-sampling

The calculation and detail factors are down-sampled by a factor of 2 in together extents.

Step 4: After executing IWT, GA is implemented into the sub-images to identify the most suitable embedding region. GA is implemented to improve a specific problem by using a natural evolution-inspired process. In this step, GA is implemented to regulate the most apposite implanting regions within individual transformed sub-twin. This suitable region reduces the visual distortions produced by hiding the confidential message. The algorithm determines embedding positions that reduce the visual distortion of the image, thereby facilitating efficient data concealment. GA has been implemented in this study in the subsequent method.

Initially, the suitability purpose named EC is implemented to check the aptitude of the embedding approach to preserve the excellence of the cover image, thus offering efficient data concealment. In EC, the ratio of hidden data for the available hiding region within the image is calculated. If the data hiding exceeds the pre-determined limit, penalties are executed to maintain the invisibility of the hidden data. The solutions use a significant portion of the accessible hiding region without degrading image quality are encouraged. The EC is determined using Eq. (2). The parameters are depicted in Table 2.

$$EC = \frac{\text{Embedded Data Size}}{\text{Available Embedding Space}} \quad (2)$$

Fitness Evaluation Mechanism. The evaluation technique takes into account a number of factors such as image distortion due to embedding, pixel-level distortions, and the perceptual superiority of the stage-double. The amount of image distortion is estimated through the comparison of cover image

form and applied to the respective processed rows and columns. In particular, the 2D IWT is implemented for employing the 1D IWT principles to together the noises and columns of a 2D gesture (an double in this situation). In this section, a simplified representation of the 2D IWT employing the Haar wavelet as an example is provided.

Given a 2D effort indicator $X[i, j]$, the Haar IWT can be computed as follows:

4.1.1 Decomposition

The normal and change values are computed for respectively 2×2 block of head-to-head basics along the rows and columns, as expressed in Calculation (1):

and its stego-counterpart based on the values of MSE and PSNR. The low level of MSE denotes that there were few pixel-level distortions, while a high PSNR implies that the image was not distorted. Nevertheless, statistical measurements are not always capable of estimating the visual impact of pixel-level distortions since some of them could be statistically insignificant but noticeable to humans. Thus, perceptual distortion measures like SSIM and VIF are introduced in order to assess the level at which the process of steganography preserves visual features of the original cover image.

Table 2. Genetic algorithm (GA) and logistic map configuration parameters

Parameter	Value
Population Size	50
Number of Generations	100
Crossover Rate	0.8
Mutation Rate	0.1
Selection Method	Tournament Selection
Elitism	Top 5%
Fitness Threshold	0.95
Logistic Map Parameter r	3.99
Initial State x_0	0.5678
Secret Key Length	128 bits
Block Size	8×8

Optimization Phase. At this phase, a GA produces the population of candidate solutions for image embedding. Each chromosome represents a possible solution that includes selection of the pixels, coefficients, or spatial positions for hiding information in the protection double. The generation of the initial population is performed randomly ensuring the adequate size and diversity of the population in order to conduct efficient search in the solution space. After the initialization, two evolutionary operations are applied to generate the new candidate solutions. These operations include crossover and mutation. Crossover is aimed at producing the offspring by combination of genetic material of two parent solutions. This way, it is possible to get offspring with enhanced embedding configurations. Mutation consists

in introducing random variations in the already existing candidates in order to allow GA to perform exploration of the embedding solution space.

4.1.3 Crossover

The crossover operator is responsible for combining the genetic elements of two parent solutions to produce new offspring solutions which may possess improved properties. Within the proposed framework, this operator combines the embedding properties of two parent solutions and produces new data-hiding strategies. The crossover is implemented in the following steps:

1. Parent Selection: Two parent solutions with good performance according to the defined optimization objectives are chosen from the existing population.

2. Crossover Point Choice: The crossover point within the representation of the chosen parent solutions is identified. This point determines the positions where the embedding strategies of the parents will be separated and further recomposed. This crossover point is chosen randomly in directive to surge the variety of produced offspring.

3. Crossover Implementation: The inherited substructure of the two maternal explanations is exchanged at the chosen crossover point to produce two new offspring. One offspring consists of the initial part of the first parent combined with the end part of the second one. The second offspring is produced similarly but with the roles of the parents swapped.

4. Offspring Assessment: The newly produced offspring are evaluated by the fitness function. The effectiveness of each offspring is determined according to its ability to minimize the impact on the visual appearance of images while hiding the secret information.

5. Population Updating: The newly produced offspring are evaluated according to their fitness and included in the population instead of those candidate solutions whose fitness values are inferior.

Mutation: This operator makes controlled changes to the selected candidate solutions in order to surge the variety of the population and expand the search of the optimization process to other parts of the hunt planetary. The mutation operator involves the following steps:

- Individual Selection: An individual candidate solution from the current population is chosen as a target for the mutation operator.

- Mutation Point Choice: One or more positions within the representation of the chosen individual are selected as points of change to be made. This means that certain components of the embedding strategy will be modified. Within the proposed image steganography framework, these positions are preferably chosen from those places of the cover image where modifications will have a minimal impact on its perceptual properties, such as areas with complex texture or high variability of pixels and coefficients from transform domains.

- Mutation Implementation: The selected embedding strategy is changed according to the chosen mutation points. In the case of image steganography, it means that either certain embedding positions are modified or transform domain constants are adapted in order to hide the top-secret information.

- Mutant Descendants Assessment: The modified embedding strategy is evaluated with the use of the multi-objective fitness function.

- Replacement Decision: The suitability value of the mutant offspring is likened to that of the chosen candidate

explanation. If the mutated offspring proves to have a superior fitness value, it is used to replace the chosen candidate. Otherwise, the chosen individual is preserved in the population.

The candidate embedding strategies created during the processes of crossover and mutation are evaluated via a multi-objective fitness function. Presentation system of measurement like PSNR, MSE, SSIM, and VIF are occupied into account to measure the level of distortion and perceptual changes introduced through each candidate. Candidates that have better fitness values meaning lesser distortion and less perceptibility, are kept for further evolution. Crossover, mutation, fitness measurement, and selection are repeated through a predetermined number of repetitions, predetermined as the number of generations. Over the course of evolution, inferior embedding strategies are discarded while the better ones are kept and evolved further. The whole process of optimization ensures that embedding strategies that offer the right balance between capacity for data hiding and preserving visual properties of the cover image emerge. The process of evolution ends once a certain fitness condition is achieved. The candidate with the best fitness score is designated as the ideal inserting policy. The ideal embedding strategy specifies the embedding pattern that is going to be used to hide the confidential information.

Step 5: Once GA finds the most appropriate embedding region and embedding strategy, the secure embedding sequence will be generated using the logistic chaotic map. The chaotic sequence thus obtained will be used to define the order and locations where secret information will be embedded as well as where it will be removed from the steno-duplicate. Sequence generation includes the following steps:

Key Generation: Secret original disorder x_0 and regulator limit r are set up by both the sender and the authorized receiver. They will be used as the security keys and will be required to regenerate the chaotic sequence during the data extraction phase.

Embedding Locations Determination: Numerical values generated by the logistic chart are cast-off to form the sequence of embedding sites in the selected areas of the transformed image. The logistic map is a nonlinear mathematical model that generates deterministic yet highly sensitive chaotic sequences. Iterative equation to generate the sequence is given as:

$$x_{n+1} = rx_n(1 - x_n) \quad (3)$$

where, x_n represents the present public of the chaotic arrangement, x_{n+1} denotes the subsequent state, and r represents the control parameter governing the dynamic behavior of the map. For suitable values of r , the generated sequence exhibits chaotic characteristics and strong sensitivity to the initial condition. The resulting sequence is therefore utilized to establish a pseudo-random ordering of the embedding positions, making the locations of the concealed information difficult for unauthorized parties to predict. The generated positions serve as the designated pull-out opinions for embedding the secret facts.

Steps 6 and 7: The underground information is then fixed in the selected blocks by means of the optimized placement scheme found from the GA and the pseudo-random embedding position created by the logistic map. After the embedding of the secret information, the inverse IWT is performed on the new set of wavelet coefficients to create the

final stego image. The whole process performed in the steganography framework for hiding the secret information is shown in Algorithm 1.

Algorithm 1. Embedding process

```

1.    Steganography_Using_IWT_and_GA: Input:
    cover_image - Original cover image
    secret_data - Data to be hidden
    population_size - Size of GA population
    crossover_rate - Probability of crossover
    mutation_rate - Chance of alteration
    fitness_threshold - Threshold for stopping GA iterations
2.    Split_Image_into_Subimages(cover_image, size):
    subimages = empty list
    for each 8×8 block in cover_image:
        subimages.append(block)
    return subimages
3.    Apply_IWT(subimage):
    # Apply Inverse Wavelet Transform
    transformed_subimage = IWT(subimage)
    return transformed_subimage
4.    Initialize_Population(population_size):
    population = random population of size population_size
    return population
5.    Choose_Fitness_Evaluation_Method(population):
    # Choose a fitness evaluation method (e.g., based on image quality)
    fitness_values = calculate fitness for each individual in population
    return fitness_values
6.    Perform_Crossover(population, crossover_rate):
    # Perform crossover between individuals in the population
    new_population = empty list
    while length(new_population) < population_size:
        parent1 = select parent from population
        parent2 = select parent from population
        if random() < crossover_rate:
            offspring1, offspring2 = crossover(parent1, parent2)
            new_population.append(offspring1)
            new_population.append(offspring2)
        else:
            new_population.append(parent1)
            new_population.append(parent2)
    return new_population
7.    Perform_Mutation(population, mutation_rate):
    # Perform mutation on individuals in the population
    for individual in population:
        if random() < mutation_rate:
            mutated_individual = mutate(individual)
            population[population.index(mutated_individual)] = mutated_individual
8.    Use_Logistic_Map_To_Generate_Positions(population_size):
    # Use Logistic Map to generate pseudorandom values for positions
    logistic_map_sequence = generate_logistic_map_sequence(population_size)
    return logistic_map_sequence
9.    Apply_Steganographic_Modifications(subimages, positions, secret_data):
    # Apply steganographic modifications using logistic map positions
    for idx, position in enumerate(positions):
        subimage =

```

```

subimages[idx] modified_subimage =
modify_subimage(subimage, position, secret_data[idx])

10.   Apply_Inverse_IWT(transformed_subimages):
    # Reconstruct stego image
    stego_image = Inverse_IWT(transformed_subimages)
    return stego_image
11.   Main Algorithm
    subimages = Split_Image_into_Subimages(cover_image, 8x8)
    transformed_subimages = Apply_IWT(subimages)
    population = Initialize_Population(population_size)
    while True:
        fitness_values = Choose_Fitness_Evaluation_Method(population)
        if max(fitness_values) >= fitness_threshold:
            break
        new_population = Perform_Crossover(population, crossover_rate)
        new_population = Perform_Mutation(new_population, mutation_rate)
        population = new_population
    Use_Logistic_Map_To_Generate_Positions(population_size)
    Apply_Steganographic_Modifications(transformed_subimages, logistic_map_positions, secret_data)
    stego_image = Apply_Inverse_IWT(transformed_subimages)
    Output: stego_image

```

4.2 Wavelet-based logistic map genetic steganography with extraction

The extraction procedure is executed using an inverse process of the operations applied during embedding. To start with, the received stego-double is separated into 8×8 chunks, and the IWT is conducted for each corresponding sub-image to generate the transformed-domain representation of the stego-image. Then the concealment information is obtained via the following procedures:

Logistic-Map-Based Key Reconstruction: In this step, the legitimate receiver generates the chaotic sequence by providing the same initial condition x_0 and control parameter r , which were provided during embedding phase. Such secret parameters ensure generation of the same pseudo-random sequence for identifying the locations of the embedded information.

Identification of Data-Hiding Locations: Using the generated logistic-map sequence, the receiver obtains the order of the embedding locations. By using this order, the receiver identifies the particular pixels or transform coefficients of the stego-image where secret data have been embedded.

Modification Analysis: Further on, the found embedding locations are analyzed to find out what modifications have been made during the data-hiding process. Such modification is analyzed by checking the values of the pixels or coefficients to find out the changes made to these values as a result of the data embedding process. If needed during decoding, the values of these pixels or coefficients are compared with the values of the corresponding pixels or constants of the unique shelter twin to determine the modifications.

Embedded Bits Extraction: Having determined a modified location, the receiver extracts the concealed bit. In accordance with the chosen embedding method, the information about this bit, such as LSB is analyzed to extract this bit of the secret binary sequence. In about suitcases, the shelter image can be used as a reference for comparison while extracting the bits in the above-described way.

Algorithm 2. Non-blind extraction process

Input:
Original Cover Image (required)
Stego Image
Logistic Map Parameters (x0, r)
Embedding Positions
1. Logistic_Map_Key_Regeneration_For_Steganography: Input:
x0 - Initial value used in logistic map r - Parameter used in logistic map
n - Length of logistic map sequence
embedding_positions - List of positions where data was embedded
cover_image - Original cover image
stego_image - Stego image with embedded data
2. Generate_Logistic_Map_Sequence(x0, r, n):
values = array of length n
values[0] = x0 for i from 1 to n:
values[i] = r * values[i-1] * (1 - values[i-1]) return values
3. Determine_Embedding_Positions(logistic_seq, embedding_positions):
positions = empty list
for each idx, value in enumerate(logistic_seq): if idx in embedding_positions:
positions.append(int(value * len(logistic_seq))) return positions
4. Pixel_Value_Analysis(original_image, stego_image, positions):
modified_positions = empty list for each pos in positions:
if original_image[pos] != stego_image[pos]:
modified_positions.append(pos)
return modified_positions

Compare stego image pixels with the corresponding pixels of the original cover image.

Note:

The extraction process is non-blind because recovery of hidden bits requires access to the original cover image.

5. Bit_Extraction(original_image, stego_image, modified_positions):
hidden_data = empty string
for each pos in modified_positions: hidden_bit = stego_image[pos] & 1 hidden_data += str(hidden_bit)
return hidden_data

6. Main Algorithm
logistic_seq = Generate_Logistic_Map_Sequence(x0, r, n)
positions = Determine_Embedding_Positions(logistic_seq, embedding_positions)
modified_positions = Pixel_Value_Analysis(cover_image, stego_image, positions)
hidden_data = Bit_Extraction(cover_image, stego_image, modified_positions)

Output: hidden_data

Secret Information Reconstruction: Having obtained the bits from the designated embedding locations, the receiver combines these bits in accordance with the order of generation of the logistic map. The obtained binary sequence is further reordered according to the original data organization and encoding method applied at the embedding phase.

The removal process is non-unsighted because the unique cover image is required for pixel comparison during hidden-bit recovery. This requirement represents a limitation of the current framework and motivates future development of a blind extraction mechanism.

5. EXPERIMENTAL VALIDATION AND ANALYSIS

The research uses a standard desktop PC with an enhanced added feature and equipped with a processor operating at 2.3 GHz and able to handle tasks efficiently. The PC is also equipped with memory of 16 GB RAM, providing temporary storage for prompt access. The publicly accessible databases contain standard images comprising Baboon, Barbara, Cameraman, Lena, and Peppers, are incorporated in the data collection.

5.1 Dataset description

Experimental evaluation was done by means of a dataset that included 1000 benchmark grayscale images obtained from open-source image processing repositories such as the USC-SIPI Copy Record and others standard copy-dispensation benchmarks. This dataset included various categories of images including natural images, human faces, urban constructions, plants, texture images, animals, and artificial objects.

The resolution statistics of the dataset were as follows:

- 200 images of resolution 64 × 64 pixels
- 250 imageries of resolve 128 × 128 pixels
- 300 imageries of resolve 256 × 256 pixels
- 250 imageries of resolve 512 × 512 pixels

For the sake of visualization, eight sample images (Lena, Ape, Peppercorns, Love apple, Fortress, Greeneries, Cameraman, and Chute) of resolution 256 × 256 pixels were chosen for further results presentation.

In order to assess payload capacity, a random set of 500 images was chosen from the full dataset since the payload capacity measurement required repeating payload embedding at various payload levels. Image quality measures (PSNR, MSE, SSIM, VIF, histogram evaluation, and robustness evaluation) were performed on the whole set of 1000 images.

The payload levels were 1.0-4.0 bits per pixel (BPP) and the average cargo level reached 3.67 BPP. The performance parameters used in this study represent the average performance on the tested dataset.

5.2 Performance metrics

5.2.1 Peak signal-to-noise ratio

The usually used measured in copy and video dispensation is the PSNR, which is used to appraise the excellence of a recreated or trodden image comparative to the innovative image. The PSNR is calculated using Eq. (4):

$$\text{PSNR} = 10\log_{10} \left(\frac{L^2}{\text{MSE}} \right) \quad (4)$$

where, L denotes the supreme imaginable pixel intensity cost of the image (typically 255 for an 8-bit twin), and MSE denotes the ‘mean squared error’, intended as the regular formed alteration among the conforming pels of the unique and reconstructed pictures.

The MSE is defined as:

$$MSE = \frac{1}{M*N} \sum_{i=0}^M \sum_{j=0}^N [I(i,j) - \hat{I}(i,j)]^2 \quad (5)$$

where, M and N represent the quantity of rackets and pillars in the image, individually, $I(i,j)$ means the original image pel at location (i,j) , and $\hat{I}(i,j)$ denotes the corresponding reconstructed or stego image pixel.

5.2.2 Mean squared error

MSE is a basic measure used extensively in image processing to determine how different an original image and a processed or reconstructed one are from each other. It is the MSE between corresponding pixels in the two images. The inferior the MSE worth, the lesser will be the deviation of the processed image from the original one, hence the lower level of distortion in it. The formula for MSE is:

$$MSE = \frac{1}{n} \sum_{im}^n (x_t - y_t^2) \quad (6)$$

where, n is the entire quantity of rudiments in the datasets (e.g., pixels in a double), x_i and y_i are the respective basics in the source and the reproduced signal, individually.

5.2.3 Structural similarity index measure

SSIM is a double quality valuation metric that aims at measuring the physical comparison among a position double and an image that is subjected to some transformation. Unlike error measures like MSE, the SSIM metric takes into account the nature of human vision and hence is based on three different elements which include: luminance, contrast, and structure.

The variety of morals for SSIM is -1 to 1 ; the developed the value of SSIM, the higher the structural comparison among the images. SSIM for identical images is very close to 1 . SSIM is computed as:

$$SSIM(x,y) = \left[\frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \right] \left[\frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \right] \left[\frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \right] \quad (7)$$

where, x and y denote the reference and processed images, respectively. The parameters μ_x and μ_y represent the mean intensities of the two images, while σ_x and σ_y denote their corresponding typical deviations. The term σ_{xy} represents the covariance between the pixel intensities of x and y . The constants C_1 , C_2 , and C_3 are stabilization parameters introduced to prevent numerical instability and avoid division by zero during computation. By jointly considering luminance, contrast, and structural consistency, SSIM provides an effective measure for evaluating the extent to which the proposed steganographic technique preserves the visual characteristics of the original protection twin.

5.2.4 Visual information fidelity

VIF metric is utilized to evaluate the quality of images or videos based on human visual observations. In which, how

effectively the perceptual data in a degraded image matches with an original (source) image is computed by the way of VIF. The human visual perceptual factors of the VIF metric include perceptual contrast sensitivity, light intensity, and spatial frequencies, thus enhancing a more visually significant quality metric. The evaluation of the resolution of rebuilt or degraded images is performed by VIF, which considers the perceptual data as more essential to human viewers. The purpose of VIF is to eliminate the constraints of established pixel-based metrics comprise MSE and PSNR, that non match with human interpretation is given in Table 3. Eq. (8) represents the formula for calculating VIF, which differentiates the structural resemblances between the source and degraded images at multiple scales and orientations:

$$VIF = \frac{1}{N} \sum_{n=1}^N \frac{1}{\sigma_n^2} \rho_n \left(\frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \right) \quad (8)$$

where, N is the number of scales, σ_n is the typical eccentricity of the Gaussian filter at ruler n , ρ_n is the CC amongst the source and degraded imageries at gauge n , μ_x and μ_y are the mean morals of the source and degraded descriptions, individually. C_1 is an endless added to avert partition by zero.

Table 3. Statistical summary across 1000 test images

Metric	Mean	Standard Deviation
PSNR	55.34	3.82
MSE	0.362	0.141
SSIM	0.974	0.006
VIF	0.927	0.009
BPP	3.67	0.28

Note: PSNR = peak signal-to-noise ratio; MSE = mean squared error; SSIM = structural similarity index measure; VIF= visual information fidelity; BPP = bits per pixel.

5.3 Results and discussion

The proposed method has been validated by utilizing approximately 1000 test images of multiple dimensions, comprising 64×64 , 128×128 , 256×256 , and 512×512 . Among these, the results of 8 important test images of dimensions 256×256 are highlighted. The 8 important test images shown in this method include Lena, Baboon, Peppers, Tomato, Castle, Leaves, Cameraman, and Parachute. Furthermore, the descriptions with various cargoes were confirmed and the recital was assessed through the system of measurement provided in Section 4.1. Initially, Table 4 shows the fair comparison setting which is applied to evaluate benchmark. The proposed approach is compared with those proposed in these studies [15, 16, 20] according to the criteria of data set, payload, image resolution, and evaluation measures. As the payloads used in these previous studies are different, this comparison can only give us an indicative estimation of performance. The fact that the data sets, payloads, embedding schemes, and experimental settings do not standardize between the different research studies means that this comparison can only serve as an indicator.

In order to analyze the presentation of the system, it was likened with some of the latest and broadly secondhand steganographic methods described in the poetry. Nevertheless, it is important to understand here that the results used for benchmarking purposes are from previously published studies where different sets of data, payloads, resolution, and other evaluation parameters can be considered. Despite the best

efforts to compare the techniques based on the most similar parameters available in the literature, it was not possible to completely standardize all the parameters used for evaluation purposes. The above comparison thus serves the purpose of a performance comparison and not a controlled and balanced one.

The PSNR and MSE morals for the planned exertion are represented in Table 5.

Table 4. Fair comparison setup used for benchmark evaluation

Method	Dataset	Payload	Resolution	Metrics
Proposed	Same	3.67 BPP	256 × 256	PSNR, SSIM, VIF
Ref [15]	Published Result	Reported Payload	256 × 256	PSNR, SSIM
Ref [16]	Published Result	Reported Payload	256 × 256	PSNR, SSIM
Ref [20]	Published Result	Reported Payload	256 × 256	PSNR, VIF

Table 5. Peak signal-to-noise ratio (PSNR) and mean squared error (MSE) values for the proposed scheme

Image	PSNR	MSE
Lena	57.7029	0.0352
Baboon	54.2342	0.5275
Peppers	53.5414	0.7699
Tomato	48.1660	0.1914
Castle	57.2204	0.3320
Leaves	55.2426	0.4455
Cameraman	56.7832	0.3681
Parachute	59.8231	0.2271



Figure 2. Histogram analysis of unique images and stego images of size 256 × 256

Furthermore, the mean PSNR and MSE morals of the

developed method were associated with the conventional state of art approaches. The comparison histogram analysis is represented in Figure 2. In simple, the PSNR measures the difference in pixel intensity values and dimensions between the degraded and source images. Higher PSNR values indicate minimal information loss or distortion across the encryption and decryption phases, thereby offering an improved quality reconstructed image.

The PSNR measurements in Figure 3 indicate robustness of the decrypted images against cropping threats. This study evaluates the performance with respect to Pramanik [19], Peter et al. [26], and Setiadi [27]. The experimental findings indicate that an encrypted image is reproduced successfully even with pixel occlusion as high as 60%. In simple, our proposed encryption method offers robustness against cropping threats, ensuring that the image is successfully recovered even with significant data loss.

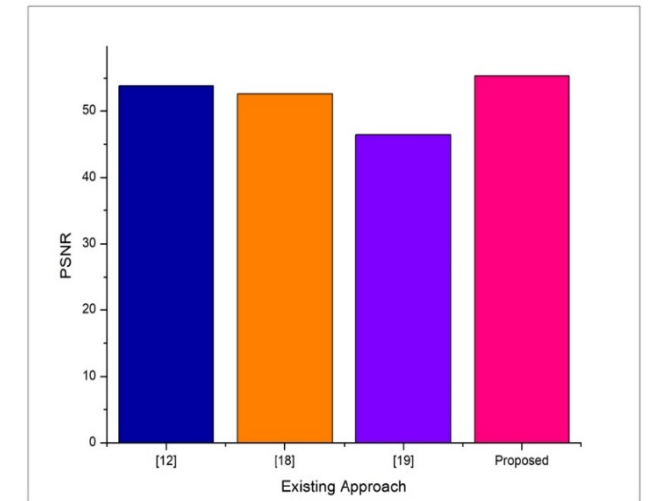


Figure 3. Comparison in terms of peak signal-to-noise ratio (PSNR)

Table 6. Structural similarity index measure (SSIM) and visual information fidelity (VIF) values for the planned scheme

Image	SSIM	VIF
Lena	0.99	0.912
Baboon	0.981	0.932
Peppers	0.975	0.928
Tomato	0.968	0.925
Castle	0.975	0.935
Leaves	0.976	0.924
Cameraman	0.976	0.935
Parachute	0.968	0.926

The SSIM and VIF values for the planned work are represented in Table 6.

Moreover, the SSIM price in the suggested method is substantially closer to 1 compared to the single LSB-based steganography approach, showing that the embedded message in the stego images remains closely resembles the original image (Figures 4–6). In the case of file size, the proposed approach offers a stego image with minimized file sizes compared to the LSB-based method, achieving approximately 15%. Moreover, the suggested method and the single LSB possess different error rates of approximately 41-44%, as calculated using an MSE-reliant statistical framework. Table 4 represents a summary of the findings obtained from the

dataset.

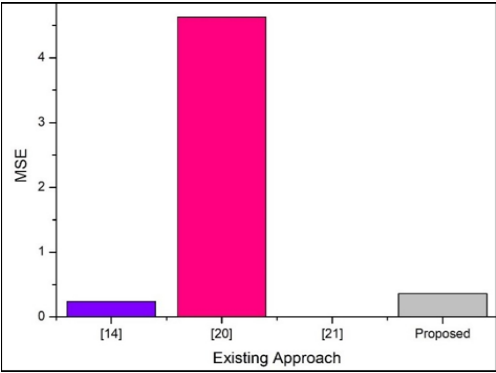


Figure 4. Contrast in terms of mean squared error (MSE)

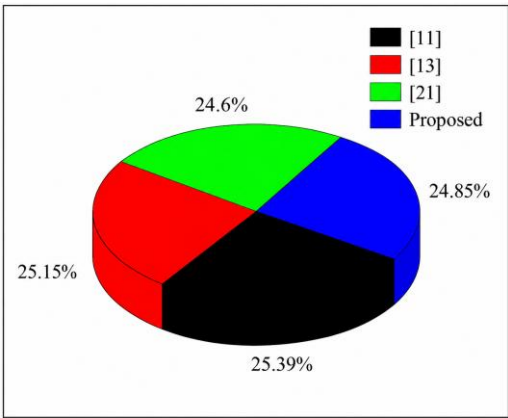


Figure 5. Comparison in terms of structural similarity index measure (SSIM)

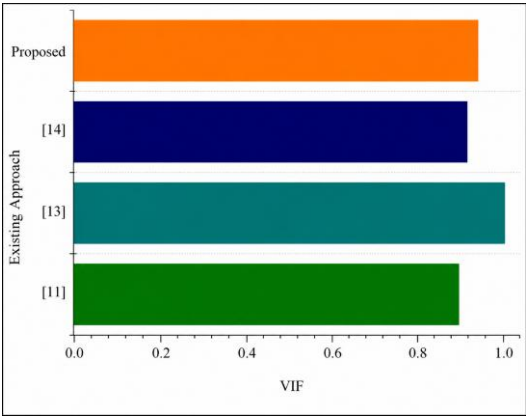


Figure 6. Comparison in terms of visual information fidelity (VIF)

Table 7. Unseen image volume of the planned scheme

Image	Bits Per Pixel (BPP)
Lena	3.25
Baboon	3.75
Peppers	3.63
Tomato	3.24
Castle	3.38
Leaves	2.95
Cameraman	3.87
Parachute	3.49

The embedded data capability is calculated by testing over

500 images, thereby establishing the average embedding capability of 3.67 BPP. Table 7 represents the freight volume of the depicted taster imageries.

For evaluating the robustness of our encryption approach against clamor-based threats, we intentionally implemented three distinct noise masses 0.005, 0.05, and 0.1, into the encrypted images: Salt and Pepper. Next, we calculated the PSNR by comparing the original images with the conforming deciphered images. Table 8 represents the PSNR values, which indicate the robustness of the decoded descriptions against the noise threats. Additionally, the present encryption approach incorporates the insights of Pramanik [19], Peter et al. [26], and Setiadi et al. [27]. The outcome of the experiment shows that the decrypted images preserve strong recognition despite the noise interference from the existence of Salt and Pepper distortions.

Table 8. Robustness against noise attack

Image Type	Density of Noise	Proposed	Pramanik [19]	Peter et al. [26]	Setiadi et al. [27]
Baboon	0.005	33.1352	33.2058	33.1462	33.2135
	0.05	23.6537	23.4251	23.1735	23.2634
	0.1	20.3219	20.4320	20.3840	20.4280
Lena	0.005	32.3312	32.3324	32.8256	32.7452
	0.05	22.6382	22.6387	22.2395	22.3759
	0.1	19.6396	19.2667	19.3485	19.4875
Cameraman	0.005	32.7248	32.7263	32.1176	32.2341
	0.05	22.2218	22.0912	22.1265	22.2846
	0.1	19.5275	19.1176	19.7365	19.6935
Peppers	0.005	32.3620	32.7258	32.5521	32.6341
	0.05	22.7253	22.2314	22.7356	22.6634
	0.1	19.2624	19.5234	19.8257	19.7437

Table 9. Comparison of the embedding rate between current solutions using the MBS plane

Method	Baboon	Barbara	Lena	Man	Peppers
Proposed	0.7179	0.5103	0.7011	0.7488	0.7295
Yu et al. [35]	0.2476	0.2471	0.2481	0.2480	0.2481
Zhang and Chen [36]	0.7171	0.5010	0.6231	0.7429	0.7219

Table 10. Comparison of peak signal-to-noise ratio (PSNR) between current solutions using the MBS plane

Method	Baboon	Barbara	Lena	Man	Peppers
Proposed	54.2342	48.12416	57.7029	56.61382	48.84850
Yu et al. [35]	39.8784	36.2451	+∞	45.7004	60.1720
Zhang and Chen [36]	26.0855	27.0917	49.7581	33.7971	34.6697

Table 9 represents the evaluation between [35, 36] and the planned technique on the MSB even. The projected process achieves a developed volume than other means, as the table shown. The location map of the proposed approach reduces the capacity cost for correcting prediction errors, and the interpolation procedures accomplish higher prediction accuracy than [35]. The suggested method allows the use of additional pixels as carrier pixels compared to the study [36].

Table 10 represents the evaluation between the conventional approaches and the proposed approach on the MSB smooth, as determined by PSNR. In all three devices, the approximated images are generated by predicting and recreating every MSB as all three approaches implement the MSB smooth for data inserting operations. This confirms that

PSNR values of the approached imageries are stable by the various inserting rates. The PSNR value of the future approach PSNR is lower than [36] but higher than in the study [35]. Even though the proposed approach implements the identical pixels as the study [35], the reproduced image achieves a higher quality because of its enhanced prediction efficiency. In contrast, the study [36] implements a considerably lower number of pixels than the planned method, thereby reducing the number of MSBs to be recreated and resulting in reduced alteration; however, this results in decreased capacity.

5.4 Security evaluation under tested conditions

Resistance to Statistical Analysis: The randomness is introduced into the embedding phases through GA and logistic maps, thereby complicating challenges to determine the occurrence of unseen data using numerical evaluation unaided. The pel morals distribution in the stage twin is carefully similar to the shelter twin, thereby providing the challenge to distinguish between them. A mean pixel intensity analysis and computed standard deviation are implemented on all the images and the outcomes of the images are illustrated in this study. The mean pixel intensity and standard deviation are widely used statistical measures to depict the delivery of pixel morals in a double. The results are represented in Table 11 below. The present security assessment is limited to histogram analysis, statistical similarity measurements, key-space analysis, and noise-based robustness testing. Advanced steganalysis techniques such as RS analysis, Chi-square attacks, Spatial Rich Models (SRM), and deep-learning-based detectors, including XuNet, were not evaluated in the current study. Consequently, the reported security observations should be interpreted as resistance under the tested experimental conditions rather than proof of comprehensive steganographic security.

Table 11. Statistical analysis on the proposed scheme – mean pixel intensity and standard deviation

Image	Cover Mean Intensity	Stego Mean Intensity	Cover Std Deviation	Stego Std Deviation
Lena	127	128	35	37
Baboon	110	112	30	32
Peppers	120	122	33	35
Tomato	100	102	28	30
Castle	140	142	40	42
Leaves	115	117	31	33
Camera man	105	107	29	31
Parachute	125	127	34	36

(1) Effective Main Planetary Complexity

One of the crucial influences contributing to the refuge of a steganographic framework is the complexity of its key space that includes all possible combinations of embedding parameters. The key space of the proposed framework involves multiple parameters of both GA (crossover probability, mutation rate, selection mechanisms) and logistic map (initial condition and control parameter). The use of multiple parameters greatly increases the key space that makes exhaustive search attacks unfeasible in case when an adversary does not know the correct secret configuration.

(2) Sensitivity of the Logistic Chaotic Map

Chaotic maps usually demonstrate a great sensitivity to their initial values; a minor alteration in the initial state chiefs to a

drastically different chaotic sequence. Such a characteristic provides extra security to the proposed steganographic framework since the adversary should possess the exact initial value and control parameter to reconstruct the embedding sequence. Thus, a slight error in the key configuration results in totally different sequence of embedding positions, which makes reconstruction of the concealed information very complicated.

(3) Steganalysis and Attacks Resistance

The proposed steganographic framework can withstand various attacks and steganographic analysis methods (LSB-based, histogram-based, noise attacks). Firstly, a combination of evolutionary optimization and pseudo-random embedding sequence based on a chaotic map decreases the predictability of the implanting course. Secondly, the optimization of inserting places makes the statistical and visual modifications caused by the embedding process almost imperceptible.

(4) Optimizing Payload Capacity

A major advantage of the GA-based embedding strategy is the ability to optimize the process of determining the optimal locations and configurations for hiding the secret information. The adaptive optimization approach takes into account the properties of the image and selects regions that can hold the largest amount of information with minimal visual degradation. Therefore, it allows achieving a reasonable cooperation among the payload volume and the inaudibility of the embedding process.

(5) Resisting Recognized-Shelter and Identified-Stage Attacks

In case of recognized-shelter and recognized-stego doses the adversary possesses both the innovative copy and the stego-twin. It makes possible to find the difference amid the two descriptions and detect the entrenched statistics. The sanctuary of the planned framework in such a case relies on minimization of statistical and perceptual difference between the images and unpredictability of the embedding process. GA optimization of embedding configurations minimizes the distortion while logistic embedding distribution is pseudo-random.

(6) Key Space Sensitivity and Security

The important space of the planned steganographic agenda includes the parameters that control the optimization (GA crossover probability, mutation rate, selection strategy) and embedding process (initial condition and regulator stricture of the logistic map). The refuge of the system relies on the sensitivity of the inserting course to the key space parameters; even a trivial alteration in one of the parameters chiefs to an incorrect reembedding configuration/sequence and fails the process of reconstruction.

6. CONCLUSION

The suggested algorithm provides a unified image steganography technique that merges the IWT, GA, and chaotic logistic map embedding. Such unification allows taking advantage of the properties of each algorithm individually: the reversible transform provided by IWT, adaptive optimizing opportunities of GA, as well as sensitivity and randomness of the chaotic map. Thus, the inserting course can be optimized regarding security, imperceptibility, and efficient data hiding. Moreover, the chaotic map mechanism increases the level of security of the embedding process due to the usage of the unpredictable sequence of the data placement,

whereas GA ensures the appropriate configuration choice for the embedding process. In consequence, the planned approach allows reaching a good balance among the EC, imperceptibility, and safety of the stego-twin. Given the experimental conditions, the proposed method provides a PSNR of 55.34 dB, MSE of 0.36, SSIM of 0.97, and VIF of 0.93 while allowing an embedding volume of 3.67 bits per pixel (BPP). These metrics prove that the developed framework is capable of embedding relatively high amount of the payload while preserving high excellence of the obtained stego-twin. Nevertheless, there are certain aspects that necessitate additional attention. The suggested technique is non-blind and requires the initial cover image for successful removal of the payload; besides, only offline image-based experiments were carried out in the course of the investigation. Furthermore, the security assessment of the algorithm does not take into account such steganalysis techniques as RS analysis, Spatial Rich Model (SRM)-based analysis, and deep learning steganalysis methods. Therefore, in the upcoming, the work will be absorbed on development of the blind data extraction techniques, security assessment of the approach using modern steganalysis algorithms, and testing on the large scale of public benchmarks.

REFERENCES

- [1] Kunhoth, J., Subramanian, N., Al-Maadeed, S., Bouridane, A. (2023). Video steganography: Recent advances and challenges. *Multimedia Tools and Applications*, 82(27): 41943-41985. <https://doi.org/10.1007/s11042-023-14844-w>
- [2] Al-Khater, W.A., Al-Maadeed, S., Ahmed, A.A., Sadiq, A.S., Khan, M.K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access*, 8: 137293-137311. <https://doi.org/10.1109/ACCESS.2020.3011259>
- [3] Selvi, K., Muthumanickam, K., Vijayalakshmi, P., Mahesh, P.S. (2023). ECC-reliant secure authentication protocol for cloud server and smart devices in IoT: K. Selvi et al. *The Journal of Supercomputing*, 79(11): 12191-12218. <https://doi.org/10.1007/s11227-023-05135-0>
- [4] Koppanati, R.K., Kumar, K. (2020). P-MEC: Polynomial congruence-based multimedia encryption technique over cloud. *IEEE Consumer Electronics Magazine*, 10(5): 41-46. <https://doi.org/10.1109/MCE.2020.3003127>
- [5] Sharma, S., Kumar, K. (2018). Guess: Genetic uses in video encryption with secret sharing. In *Proceedings of 2nd International Conference on Computer Vision & Image Processing: CVIP 2017*, pp. 51-62. https://doi.org/10.1007/978-981-10-7895-8_5
- [6] Evsutin, O., Melman, A., Meshcheryakov, R. (2020). Digital steganography and watermarking for digital images: A review of current research directions. *IEEE Access*, 8: 166589-166611. <https://doi.org/10.1109/ACCESS.2020.3022779>
- [7] Fridrich, J. (2009). *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press. <https://doi.org/10.1017/CBO9781139192903>
- [8] Panah, A.S., Van Schyndel, R., Sellis, T., Bertino, E. (2016). On the properties of non-media digital watermarking: A review of state of the art techniques. *IEEE Access*, 4: 2670-2704. <https://doi.org/10.1109/ACCESS.2016.2570812>
- [9] Chan, C.K., Cheng, L.M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition*, 37(3): 469-474. <https://doi.org/10.1016/j.patcog.2003.08.007>
- [10] Flikkema, P.G. (1997). Spread-spectrum techniques for wireless communication. *IEEE Signal Processing Magazine*, 14(3): 26-36. <https://doi.org/10.1109/79.587050>
- [11] Dutta, S., Saini, K. (2021). Securing data: A study on different transform domain techniques. *WSEAS Transactions on Systems and Control*, 16: 110-120. <https://doi.org/10.37394/23203.2021.16.8>
- [12] Chen, O.T.C., Wu, W.C. (2008). Highly robust, secure, and perceptual-quality echo hiding scheme. *IEEE Transactions on Audio, Speech, and Language Processing*, 16(3): 629-638. <https://doi.org/10.1109/TASL.2007.913022>
- [13] Lucchese, L., Doretto, G., Cortelazzo, G.M. (2002). A frequency domain technique for range data registration. *IEEE Transactions on Pattern Analysis & Machine Intelligence*, 24(11): 1468-1484. <https://doi.org/10.1109/TPAMI.2002.1046160>
- [14] Dagar, S. (2014). Highly randomized image steganography using secret keys. In *International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014)*, Jaipur, India, pp. 1-5. <https://doi.org/10.1109/ICRAIE.2014.6909116>
- [15] Muhuri, P.K., Ashraf, Z., Goel, S. (2020). A novel image steganographic method based on integer wavelet transformation and particle swarm optimization. *Applied Soft Computing*, 92: 106257. <https://doi.org/10.1016/j.asoc.2020.106257>
- [16] Sabeti, V., Sobhani, M., Hasheminejad, S.M.H. (2022). An adaptive image steganography method based on integer wavelet transform using genetic algorithm. *Computers and Electrical Engineering*, 99: 107809. <https://doi.org/10.1016/j.compeleceng.2022.107809>
- [17] Ambika, Biradar, R.L. (2021). A robust low frequency integer wavelet transform based fractal encryption algorithm for image steganography. *International Journal of Advanced Intelligence Paradigms*, 19(3-4): 342-356. <https://doi.org/10.1504/IJAIP.2021.116355>
- [18] Kumar, M., Hussaini, T. (2021). A neural network based image steganography method using cyclic chaos and integer wavelet transform. In *2021 Asian Conference on Innovation in Technology (ASIANCON)*, Pune, India, pp. 1-6. <https://doi.org/10.1109/ASIANCON51346.2021.9544831>
- [19] Pramanik, S. (2023). An adaptive image steganography approach depending on integer wavelet transform and genetic algorithm. *Multimedia Tools and Applications*, 82(22): 34287-34319. <https://doi.org/10.1007/s11042-023-14505-y>
- [20] Pramanik, S., Singh, R.P., Ghosh, R. (2020). Application of bi-orthogonal wavelet transform and genetic algorithm in image steganography. *Multimedia Tools and Applications*, 79(25): 17463-17482. <https://doi.org/10.1007/s11042-020-08676-1>
- [21] Govindasamy, V., Sharma, A., Thanikaiselvan, V. (2020). Coverless image steganography using Haar integer wavelet transform. In *2020 Fourth International Conference on Computing Methodologies and*

- Communication (ICCMC), Erode, India, pp. 885-890. <https://doi.org/10.1109/ICCMC48092.2020.ICCMC-000164>
- [22] Li, F., Yu, Z., Qin, C. (2022). GAN-based spatial image steganography with cross feedback mechanism. *Signal Processing*, 190: 108341. <https://doi.org/10.1016/j.sigpro.2021.108341>
- [23] Zeng, K., Chen, K., Zhang, W., Wang, Y., Yu, N. (2022). Improving robust adaptive steganography via minimizing channel errors. *Signal Processing*, 195: 108498. <https://doi.org/10.1016/j.sigpro.2022.108498>
- [24] Pan, P., Wu, Z., Yang, C., Zhao, B. (2022). Double-matrix decomposition image steganography scheme based on wavelet transform with multi-region coverage. *Entropy*, 24(2): 246. <https://doi.org/10.3390/e24020246>
- [25] Al-Shaarani, F., Gutub, A. (2022). Securing matrix counting-based secret-sharing involving crypto steganography. *Journal of King Saud University-Computer and Information Sciences*, 34(9): 6909-6924. <https://doi.org/10.1016/j.jksuci.2021.09.009>
- [26] Peter, G., Sherine, A., Teekaraman, Y., Kuppasamy, R., Radhakrishnan, A. (2022). Histogram shifting-based quick response steganography method for secure communication. *Wireless Communications and Mobile Computing*, 2022(1): 1505133. <https://doi.org/10.1155/2022/1505133>
- [27] Setiadi, D.R.I.M. (2022). Improved payload capacity in LSB image steganography uses dilated hybrid edge detection. *Journal of King Saud University Computer and Information Sciences*, 34(2): 104-114. <https://doi.org/10.1016/j.jksuci.2019.12.007>
- [28] Hossain, S., Mukhopadhyay, S., Ray, B., Ghosal, S.K., Sarkar, R. (2022). A secured image steganography method based on ballot transform and genetic algorithm. *Multimedia Tools and Applications*, 81(27): 38429-38458. <https://doi.org/10.1007/s11042-022-13158-7>
- [29] Xu, Y., Mou, C., Hu, Y., Xie, J., Zhang, J. (2022). Robust invertible image steganography. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, New Orleans, LA, USA, pp. 7875-7884. <https://doi.org/10.1109/CVPR52688.2022.00772>
- [30] Mandal, P.C., Mukherjee, I., Paul, G., Chatterji, B.N. (2022). Digital image steganography: A literature survey. *Information Sciences*, 609: 1451-1488. <https://doi.org/10.1016/j.ins.2022.07.120>
- [31] Kaur, S., Singh, S., Kaur, M., Lee, H.N. (2022). A systematic review of computational image steganography approaches: S. Kaur et al. *Archives of Computational Methods in Engineering*, 29(7): 4775-4797. <https://doi.org/10.1007/s11831-022-09749-0>
- [32] Wang, Z., Feng, G., Qian, Z., Zhang, X. (2022). JPEG steganography with content similarity evaluation. *IEEE Transactions on Cybernetics*, 53(8): 5082-5093. <https://doi.org/10.1109/TCYB.2022.3155732>
- [33] Soualmi, A., Laouamer, L. (2023). A blind watermarking approach based on hybrid imperialistic competitive algorithm and SURF points for color Images' authentication. *Biomedical Signal Processing and Control*, 84: 105007. <https://doi.org/10.1016/j.bspc.2023.105007>
- [34] Soualmi, A., Laouamer, L., Altı, A. (2024). A novel intelligent approach for color image privacy preservation. *Multimedia Tools and Applications*, 83(33): 79481-79502. <https://doi.org/10.1007/s11042-024-19402-6>
- [35] Yu, M., Yao, H., Qin, C. (2022). Reversible data hiding in encrypted images without additional information transmission. *Signal Processing: Image Communication*, 105: 116696. <https://doi.org/10.1016/j.image.2022.116696>
- [36] Zhang, Q., Chen, K. (2023). Reversible data hiding in encrypted images based on two-round image interpolation. *Mathematics*, 12(1): 32. <https://doi.org/10.3390/math12010032>