Iraqi Journal of Intelligent Computing and Informatics (IJICI)
Vol. 5, 1, June 2026, pp. 1~12
ISSN: 2791-2868, DOI: 10.52940/ijici.v5i1.100

Optimised Hybrid Approach for Secure and Imperceptible Image Data Hiding Systems

Bushra Abdullah Shtayt[1], Hiba A.Alahmed[2], Zainab Mohammed Jiwar[3], Karrar Ali Abdullah[4], Mohanad S. AL-Musaylh[5]

[1, 2,5]Department of Information Technology, Management Technical College, Southern Technical University, Basra, Iraq
[3]Department of Computer Networking and Software Techniques, Basra Technical Institute, Southern Technical University, Basra, Iraq
[4]Computer Science Department, Shatt Al-Arab University College, Basra, Iraq

Article Info

Article history:

Received February 5, 2026
Revised March 10, 2026
Accepted March 24, 2026

Keywords:

Genetic algorithm
Image steganography
Imperceptibility
Security
Tabu search

ABSTRACT

Digital communication has witnessed remarkable growth since the advent of the internet. However, security concerns can be attributed to the inherent openness of the existing internet environment. Steganography is an effective technique for hiding sensitive information within a digital medium. The proposed research presents an enhanced spatial domain image steganography approach developed using the least significant bit (LSB) technique. This approach is further enhanced using two meta-heuristics: the genetic algorithm (GA) and Tabu search (TS). However, no existing approach has simultaneously employed GA and TS optimisers. Therefore, the proposed approach is a unique contribution to the field of image steganography. In this approach, GA is utilised as an optimiser to facilitate the selection of the most suitable image pixels for data embedding. The optimisation process helps minimise image distortion. The method is further improved using the TS optimiser, thus achieving the least image distortion. Results indicate the effectiveness of the proposed approach in image steganography. Compared with the conventional LSB steganography technique, the proposed approach achieves a 55.120% improvement in peak signal-to-noise ratio and a 0.26% improvement in mean squared error. Thus, the proposed approach represents a remarkable contribution to digital communication, demonstrating its effectiveness in protecting confidential information. Overall, the proposed approach can be further enhanced and explored for applications in other fields.

Corresponding Author:

Bushra Abdullah Shtayt
Department of Information Technology, Management Technical College, Southern Technical University, Basra, Iraq
Email: bushra.abdullah@stu.edu.iq

1. INTRODUCTION

In the current world, where data volume continues to grow rapidly, transferring critical data over exposed channels poses considerable security risks. With the increasing flow of data across digital channels, digital security risks such as hacking, tampering and eavesdropping have become prevalent concerns in the online environment (Rasras[1], [2]). In response to these challenges, information and data are secured via three essential security concepts: confidentiality (in which unauthorised entities are prevented from accessing or intruding into the data), data integrity (in which data consistency and accuracy are maintained without any level of tampering or data modification) or disturbance and data availability (in which data or information is available in a timely manner when needed). Encryption generally represents a basic form of protection focused on secrecy, rendering the information unreadable through the aid of a specific key. However, these messages might raise suspicion, thus providing an opportunity for unauthorised access [3], [4]. Conversely, steganography represents a contrasting form, focused on hiding the communication using plain digital media such as images, music, videos or texts, presenting an opportunity for the message itself to be kept hidden. It represents a combination of science and art geared towards protecting the message whilst keeping it hidden inside the medium and preserving its quality [5], [6]. Least significant bit (LSB) replacement in digital images is one of the most widely used steganographic techniques due to its ease of use and large embedding capacity. However, a crucial tradeoff exists between three crucial aspects of traditional LSB techniques: robustness against detection, imperceptibility and embedding capacity. In image steganography, striking a balance

between these requirements is still highly demanding. Recent research has focused on combining intelligent optimisation techniques with traditional steganographic methods to address these restrictions [7].

The present work proposes a hybrid optimisation methodology that merges the wide searching capability of genetic algorithms (GAs) with the precise local optimisation strength of Tabu search (TS). The objective of the hybrid framework is to determine optimal embedding positions, reduce image distortion and enhance security by complicating the detection of hidden messages. A literature review revealed that no one has so far combined GA with TS to optimise LSB steganography. Although each of these methods has been independently applied, their combination opens a novel research direction. This paper fills this gap and presents a novel hybrid framework aimed at improving the efficacy and security of LSB-based image steganography.

2. RELATED WORK

Over the past two decades, various data-hiding applications that use steganographic techniques such as LSB, GA and TS have been developed. The following section provides an analysis comparing these data-hiding techniques, their strengths and weaknesses and the advantages of the proposed model over them.

Xia et al. (2009) focused on one of the advanced metaheuristic techniques associated with GA, which is used for image analysis, particularly concealed details in images. The developed hybrid GA aids in identifying appropriate features that enhance the capability of classifiers to detect stealth techniques. The findings reveal the superiority of the introduced hybrid GA method over conventional feature selection algorithms in terms of accuracy and computational time. However, the study concludes that the success rate of this particular approach depends on the stealth type used and recommends algorithm modifications in subsequent studies [8]. Soleimanpour et al. (2013) proposed a new approach to hide information using a GA in the spatial domain of digital images, thereby identifying the best embedding region to minimise the image quality distortion due to the embedding process. The findings showed that the proposed approach reached a remarkable balance between image quality and embedding capacity through the PSNR value, outperforming conventional methods. However, the proposed method suffers from computational time with increased cover image size; therefore, additional research is needed to optimise the method and reduce the required time to execute the algorithm [9]. Douiri & Elbernoutti (2017) have offered an information-hiding technique for enhancing the robustness and security of the embedded information using a TS method, thus minimising the distortion to the target image. A study indicates that the new methods outperform the traditional ones not only in disappearance but also in integration. However, the study raises concerns regarding the complexity of the computing process but challenges future work on the matter [5]. In the study by Wazirali et al. (2019), a spatial-domain image steganography method based on the LSB method is introduced. GAs optimise the sequencing of stages in the embedding process, including pixel analysis, pixel alteration, the replacement of hidden bits and other related tasks. The peak signal-to-noise ratio (PSNR) is commonly used to evaluate the quality of hidden bits in the host image [10]. In 2021, a research team led by Shyla adopted a novel line of investigation by applying GAs to enhance the performance potential of data steganography in images. For the first time, a GA was used to select an appropriate host image and identify the precise locations for data embedding. As a result, an enhanced hidden image was obtained, with the stego-image showing higher PSNR and lower MSE. However, the study revealed extended computation times for large images. They also suggested further investigation into enhancing efficiency for handling such cases. Nonetheless, the results demonstrate the effectiveness of GAs in steganography [11].

Nokhwal et al. (2024) presented an alternative for information concealment by utilising the hybrid firefly algorithm to encode the information into cover images. They mainly focused on minimising distortion and enhancing the embedding capacity in cover images. The results indicated a reduction in distortion and rapid convergence in the search process, increasing the security and robustness of embedded data against analytical attacks. However, the study shows that challenges are likely to emerge in the areas of implementation and computing resources due to the complexity of the hybrid algorithm. Thus, further research in this field is required to enhance processing speed without compromising embedding efficiency and the quality of the resulting images [12].

The above studies demonstrate the potential of the GA and TS algorithms to improve security and resistance to steganalytic techniques when hiding information at optimal locations in cover images. However, the current research only focused on the use of GAs over other algorithms due to the time complexity of the TS algorithm. Table 1 compares the aforementioned approaches and details the potential improvements with the hybrid model.

Table 1: Comparison of Steganography Optimisation Techniques

Method	Strengths	Weaknesses	Proposed Hybrid Model Improvement
LSB	Simple to implement, low computational cost	High distortion, low security, easily detectable by steganalysis tools	Reduces distortion and enhances security by optimising embedding locations using GA and TS.

GA	Global optimisation is effective in determining optimal solutions in large spaces.	Computationally expensive, sensitive to parameter settings	Combines the global search of GA with the local optimisation of TS to reduce computational cost and improve efficiency.
Tabu Search	Avoids local optima, effective in local search	High complexity with large datasets requires careful tuning of parameters	Uses TS to refine GA solutions, ensuring superior local optimisation and reducing the risk of local optima.
Hybrid GA–TS	Balances global and local search, reduces distortion and enhances security	Slightly higher computational cost compared to individual methods	Achieves superior PSNR and lower MSE, making it more robust and secure than individual methods.

Despite the advantages of LSB, GA and TS as individual approaches, the above table indicates that they still have serious drawbacks. The proposed hybrid model addresses the limitations of GA and TS. The proposed system is robust and secure because it utilises the optimisation power of GA and the efficiency of TS.

3. METHODOLOGY

This hybrid model combines GA and TS to optimally embed secret messages into a cover image. The process starts with image and message preparation, followed by optimisation using GA and TS, respectively. This process ends with the embedding the secret message and its extraction. Figure 1 depicts the flowchart of the proposed integrated scheme.

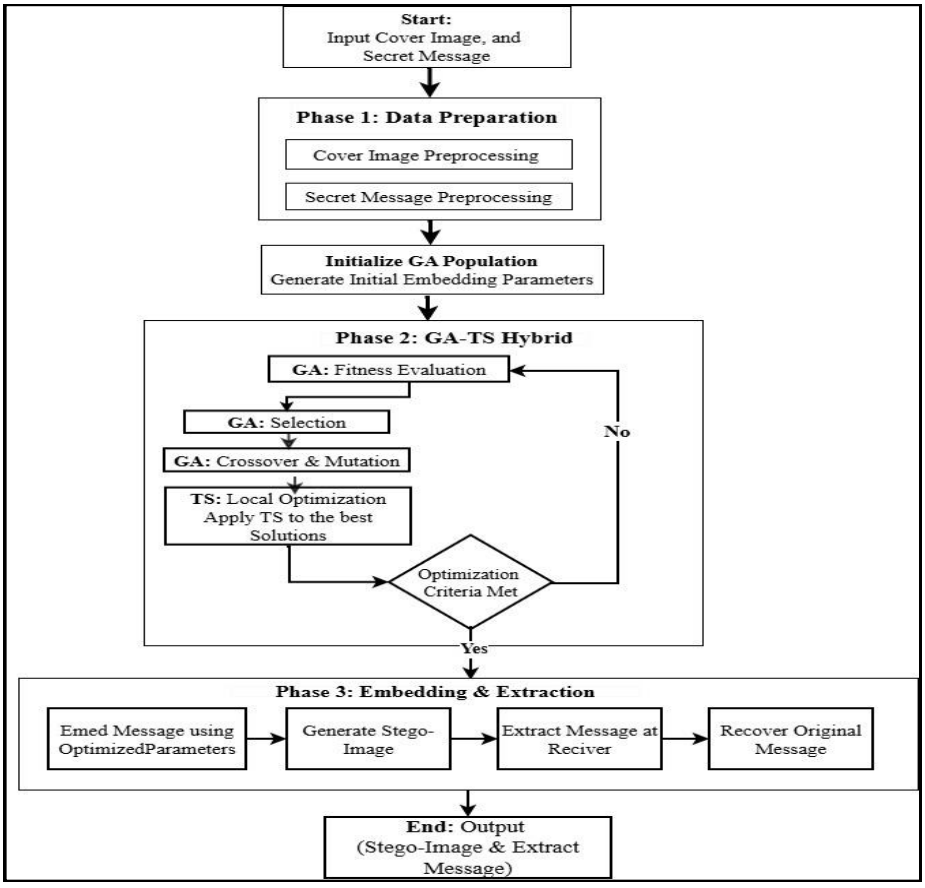

Figure 1. Flowchart of the Hybrid Model

Figure 1: Describes the workflow of the proposed hybrid steganography model, which comprises three successive phases as follows:

1. **Preparation Phase:** In this phase, the original cover image and the message are preprocessed, such as formatting changes, prior to embedding.
2. **Hybrid Optimisation Phase:** The focus of the proposed strategy lies in the optimisation phase. Initially, a GA employs a population of candidate parameter sets and iteratively refines them through fitness evaluation, crossover and mutation. The resulting candidates are then passed to a TS module, which helps avoid convergence to local optima and promotes the exploration of globally optimal solutions. This process ensures the identifcataion of the best parameter sets for data embedding.
3. **Steganography Phase:** In this phase, the optimised parameters obtained during the second phase of the algorithm are utilised to embed the secret information within the cover image, thereby creating the stego image. The extraction of the embedded information, which requires the same or associated parameters, is assured to be successful. In the diagram above, the components of the algorithm's phase are clearly described. The GA–TS optimising phase of the algorithm's design is considered the primary innovation.

3.1. Image Setting and Secret Messages

The first step in the steganography process involves preparing the main cover (image) for embedding secret messages. This step aims to convert the medium in such a way that its quality is maintained after conversion.

3.1.1. Image Setting

The process commences with uploading a cover image that will be used to convey the hidden message. The cover images used are selected based on their resolution, where each should be at least 512 × 512 pixels. The images should be in either PNG or JPEG format. The uploaded image is then converted to a uint8 image, where each pixel is represented by a numerical value ranging from 0 to 255. After this step, the uploaded image is verified to ascertain that it is original image, thus avoiding any compromise in quality.

3.1.2. Preparation of Confidential Messages

The secret message may be hidden by inserting it within the picture itself through data embedding. This embedded information may be plain or complex data. In this method, the hidden message is essentially converted to its binary form to match the digital content of the image in which it will be embedded. The following outlines the process by which the text is converted into its binary form:

1. Each character is mapped to its ASCII numeric value.
2. The number is converted to an 8-bit binary representation, where each bit represents a small portion of the data.
3. These numbers are then combined into one long continuous binary string that encodes the secret message.

This step enables the insertion or embedding of the hidden message within the image in a simple and useful manner, using the LSB or other methods [13]. By converting the hidden message into binary, embedding flexibility is realised despite the nature of the original message, especially for text or data. Moreover, this step facilitates an easy length estimation of the hidden message, potentially affecting the selection of positions within the image through smart algorithms such as GA and TS.

3.2. Optimise Sites with GA

Optimising sites using the GA is crucial for hiding confidential messages within images, as this algorithm allows for the systematic and intelligent selection of optimal embedding locations. Other ideas such as natural selection, derived from the theory of evolution of Charles Darwin, can be found in GAs. Considering GAs, elements such as mutations, selection and crossover are utilised to traverse vast and complicated landscapes in search of decent answers to complex questions, as described in [12]. The difficulty lies in striking a balance between picture edits that are visually attractive and those that facilitate precise interpretation of the hidden message, without alerting image analysis software to the tactics. Therefore, fitness functions can be utilised to evaluate how well a chromosome performs based on PSNR, message precision and modifications to images. For instance, even if a chromosome is not considered, achieving a PSNR value of more than 70 dB enables the easy recovery of the hidden message with minimal distortion. The evaluation aims to ascertain that the fitness value is sufficiently achieved during embedding, allowing message recovery with the required precision. However, determining appropriate embedding locations within an image is challenging, considering the vast number of possible locations. Using a random number to determine a location may lead to some distortions or reveal the hidden secret. An efficient scheme for selecting embedding locations within an image, based on GA, addresses this challenge by identifying optimal locations that mitigate image distortion while maximising concealment efficiency. The GA performs best by balancing the quality of the embedded data with the quality of the host image, which is a critical factor for data concealing methods [14]. This structured process addresses

the shortcomings associated with using random number selection for embedding locations, thus improving overall image quality.

3.2.1. GA Work Steps

1. **Generation (Initial Population):** A first set of stochastic solutions is produced, each representing a set of candidate sites for message embedding within the image. Each solution, called a chromosome, has a list of bits to be changed.
2. **Fitness Function Calculation:** A fitness function is used to evaluate the efficiency of each chromosome. If messages are hidden, then the evaluation function is designed to consider the following factors:
   - Effect of adjustment on image quality: The difference between the original and the modified images is measured using PSNR or MSE.
   - Message Extractability: The sites guarantee that a message can be extracted.
   - Visual continuity: The changes are ensured to not be discernible during image observation.
3. **Selection:** The value of the evaluation function is used to identify the most suitable chromosomes from the current generation. Notably, the chosen solutions should be the most effective in terms of the tradeoff between quality and concealment.
4. **Crossover:** Some of the selected chromosomes are combined to create new solutions through information exchange. This crossover is realised to explore new areas of solutions. Genetic diversity is also increased.
5. **Mutations:** Some chromosomes are randomly modified to improve diversity and prevent falling into local solutions (Local Optima). For example, one or more locations within a chromosome can be switched.
6. **Process Repetition:** The algorithm continues replicating selections, crossover and mutations across several generations until deactivation criteria are met, such as a specific level of quality or a certain number of generations.

3.2.2. Pseudo Code-GA [15]

Start Algorithm
Input: Cover image, Binary Message, Population Size and Maximum number of generations.
Output: Optimal positions for embedding are pointed in Best_Solution.
1. Initialise the population:
Establish a first set of solutions (input: chromosomes) that shows potential locations for the message.
2. Chromosome Fitness Evaluation:
- For each chromosome in the population: Embed the message inside the image related to the positions in the chromosome.
- Compute the FitnessValue using the following criteria:
  a. Resultant Image Quality (such as PSNR or MSE).
  b. The capability to extract the message with a high level of fidelity.
  c. Small changes in the image (attempts to avoid sharp changes in the image).

3. Repeat for MaxGenerations or until stopping criteria are met:
a. Selection:
- Choose parent chromosomes from amongst all the chromosomes using the selection method depending on the fitness values (roulette wheel or tournament selections).

b. Crossover:
- Perform crossovers concerning certain selected parents to create new offspring (such as single point/multipoint crossover).
- Ensuring that the output has characteristics from both parents.

c. Mutation:
- It produces diversity by randomly mutating one or several locations in the offspring's chromosomes.
- The same checks must be performed to confirm that all the mutations are valid (e.g. position values are within the image matrix range).

d. Create a new population:
- Exchange the old population with the offspring (use the elitism method to hold the best solutions from the prior generation).

e. New Population Fitness Evaluate:
- Repeat step 2 for the newly obtained chromosomes through the crossover process from mating the two current chromosomes.

4. Return the best solution:

- Recognise the chromosome with the most significant fitness value as the best solution.

End Algorithm

3.3. Optimise Sites with TS

The TS algorithm is a powerful optimisation technique that complements the initial site selection performed by the GA. TS improves the quality of embedding locations through refined solutions provided by GA, minimising noise introduced during updates and maintaining image quality [16]. As an iterative optimisation technique based on Local Search, TS aims to explore solutions adjacent to the initial solution to find alternatives and hopefully improve solutions. What differentiates TS is the use of a Tabu list to prevent revisiting previously explored solutions and avoiding moves that could lead to poor solutions. For example, in the optimisation procedure, if an optimisation solution decreases the PSNR, then it may be added to the Tabu list: when the position of the pixel (x, y) decreases, the PSNR value may be marked as 'tabu' for the following five iterations. The chances of local optima trapping and the probability of finding highly efficient solutions increase [11]. Consequently, the hybrid approach ensures secure embedding by leveraging the global and local optimisation capability of GA and TS, respectively.

In many ways, the TS algorithm is special due to the following reasons:

- The algorithm aids the GA search by generating superior initial solutions through the identification of highly efficient locations to hide messages.
- TS optimises the masking step through minimisation and reducing changes to the image.
- Messages are guaranteed to be easily retrievable without negatively affecting the quality of the altered image.

In other words, TS is highly efficient and safe.

3.3.1. TS Work Steps

1. Initial Solution Configuration: The optimal location determined by the GA algorithm serve as the initial solutions for the optimisation process. These solutions comprise a list of locations that are considered to provide a balance between image quality and message confidentiality.
2. Neighbourhood definition: A set of solutions near the existing solution is determined. Regarding the hiding process of the message, the neighbourhood may be determined by adjusting some of the selected locations or by replacing them with other locations in the image.
3. Evaluate Solutions: The Fitness Function is employed to ascertain the quality of each solution in the vicinity, which calculates the following:
   - Modified image quality (PSNR or MSE).
   - How accurately is the message embedded and retrievable?
   - The number of visual changes that occur in the image.
4. Choosing the best solution (Best Neighbour): Amongst the available neighbourhood options, the 'best' option is selected by evaluating them using the Objective Function whilst ensuring the selected option is not in the Tabu List.
5. Update Tabu List: The step that produced the new solution is then added to the Tabu List. This list helps prevent exploring previous solutions or duplication in research.
6. Update Current Solution: The solution is updated to become the best solution selected in the previous step.
7. Check stop conditions: The algorithm continues to iterate until a certain number of iterations are reached or when no better solutions are identified within a specified number of steps.
8. Final Solution Returns: When duplicates end, the resulting current solution is the final solution, representing the optimal locations for message embedding.

3.3.2. Pseudo Code-TS [17]

Start Algorithm
Input: StartingSolution (sites from GA), Neighbourhood_Size, maximum number of iterations (Max_Iterations), size of the taboo list (Tabu_List_Size)
Output: Optimised positions of where to embed (Best_Solution).
1. Initialise:
- Current_Solution = Initial_Solution
- Best_Solution = Current_Solution
- TabuList = Empty (to hold tabu move)

2. While Iteration < MaxIterations:
a. Generate Neighbourhood:

- A Neighbour_Solution can be defined and obtained by modifying the Current_Solution.
- Make sure the Neighbour_Solutions are not out of image range.

b. Evaluate Neighbourhood:

- Every solution in Neighbour_Solutions:
- Compute FitnessValue by criteria such as:
  1. PSNR & MSE: Depict the quality of the modified Image.
  2. Decoding the hidden message in the most precise way possible.
  3. Distortion Minimisation.

c. Select Best_Neighbour:

- Select the Neighbour_Solution, which corresponds to the maximum FitnessValue; however, it should not be a part of Tabu_List.
- If Tabu_List contains all neighbours, relax the Tabu_List limitations to permit the least penalised move.

d. Update Tabu_List:

- Append the move (change in the solution) that puts the Current_Solution to the TabuList.
- If the Tabu_List override Tabu_List_Size, remove the oldest entry from Tabu_List.

e. Update Current_Solution:

Set Current_Solution = Best_Neighbour.

- If the FitnessValue of the Current_Solution > FitnessValue of Best_Solution
  Best_Solution = Current_Solution

f. Increment Iteration: Iteration = Iteration + 1.

3. Return Best_Solution.

End Algorithm

3.4. Embedding and Extraction

Embedding and extraction are central components of categorised data steganography systems, focusing on maintaining image quality by limiting visual distortions without compromising the confidentiality of the embedded data or increasing the chance of detection via image-based steganalysis techniques. These processes are achieved by identifying key embedding spots to enhance data confidentiality without increasing steganalytic detection. Using a hybrid system of GA and TS, the hybrid model distributes the stegotext to optimum embedding pixels, thus increasing the detection difficulty using steganalytic software by avoiding clear visual alterations in the covered image. Such an application holds numerous implications in terms of its potential uses. One such application includes the utilisation of the said media as channels for secure communication, ensuring confidentiality in the communication process over insecure media. Intellectual property protection through digital watermarking is another notable application. Digital media documents can also be used to conceal sensitive information, such as digital signatures and medical information [18].

3.4.1. Embedding

This embedding step conceals the secret message in the cover image intelligently by maintaining the quality of the original image itself, allowing message recovery later on [4]. This step relies on the preselected optimal locations determined with GA and TS algorithms. The embedding process involves the following steps:

1. **Binary Representation:**
   - The binary encoding process uses ASCII, which is the American Standard Code for Information Interchange, to convert the secret message into a sequence of bits.
   - This process allows digital data storage within the image. For example, the message ‘Hi’ is represented as H ➔ 01001000 and I ➔ 01101001.
2. **Choosing websites:**
   - Locations identified by GA and TS algorithms represent the most convenient places to embed bits.
   - These locations are selected to minimise the visual impact on the image and ensure the confidentiality of the message.
3. **Edit image bits:**
   - LSBs are modified to hide the message in selected locations.
   - This adjustment is sufficiently small that humans do not notice any image variations.

   Example: If the original pixel value is 10110010, and the LSB represents 0 and is replaced by 1 of the message, then the modified pixel becomes 10110011.
4. **Stego Image Production:**
   - The secret message is embedded within the image, creating a new stego image.

- The stego image looks similar to the original image through the naked eye but contains an embedded message.

5. **Save editing information:**
   - Information such as the locations of modified bits is retained to facilitate the subsequent message extraction process.

Embedding Pseudo Code

Start Algorithm Embedding
Input: Original_Image, Secret_Message, Embedding_Positions
Output: Stego_Image
1. Convert Secret_Message to Binary_Code:
- Message_Binary ← Convert each character of Secret_Message into an 8-bit binary representation.
- Message_Length ← Length_of_ Message_Binary.

2. Load Original_Image:
- Image_Pixels ← Pixel_values_of_Original_Image.

3. Embed Binary_Message:
For j← 1 to Message_Length, do:
- Position ← Embedding_Positions[j] (fetch the next embedding_Position).
- Current_Pixel_Image_Pixels ← [Position].
- Change the LSB of the Current Pixel:
  - If Message_Binary[j] = 1, set LSB_of_ Current_Pixel to 1.
  - If Message_Binary[j] = 0, set the LSB_of_ Current_Pixel to 0.
- Update Image_Pixels[Position] with the modified value.

4. Created Stego_Image:
- Substitute the pixels in Original_Image with pixels of ImagePixels.
– Save the altered image as Stego_Image.

5. Return Stego_Image.
End Algorithm

3.4.2. Extraction

The extraction process is the reverse step of embedding, where the hidden secret message in the modified image is extracted. The success of this process lies in the identification of the exact locations of the modified bits and the encryption method used. The extraction process involves the following steps:

1. **Upload edited image (Stego Image):**
   - The image containing the hidden message is entered.
2. **Use predefined locations:**
   - Within the embedding procedure, the embedded bits are linked to the recorded data points.
3. **Bit Extraction:**
   - LSBs are read from the selected locations.
   - These bits are then grouped to form the binary string representing the message.

   Example:
   - If the bits turn out to be 01001000 and 01101001, then the words H and i correspond to the bits.
4. **Reconstructing the original message:**
   - Most often, the encoding used for embedding, such as ASCII, is used to convert a binary string back into text.
   - The result is the retrieval of the original secret text.
5. **Verify the extraction accuracy:**
   - The extracted message is compared with the original message to validate the process.

Extraction Pseudo Code

Start Algorithm Extraction
Input: Stego_Image, Embedding_Positions, Message_Length
Output: Extracted_Message
1. Load Stego_Image:
- Image_Pixels ← Pixel_values_of_Stego_Image.

2. Extract Binary_Message:

Initialise_Message_Binary ← Empty_List.
Forj ← 1 to Message_Length, do:
- Position← Embedding_Positions[j] (Fetch the embedding_Position).
- Current_Pixel_Image_Pixels ← [Position].
- Extract_LSB from Current_Pixel:
  - Message_Binary[j] ← LSB (Current_Pixel).

3. Convert_Binary_Message_to_Text:
- Collection Message_Binary into an 8-bit parts.
- Convert each 8-bit part to its corresponding ASCII character.
- Extracted_Message ← Join characters to compose the text.

4. Return Extracted_Message.
End Algorithm

4. RESULTS AND DISCUSSION

This section reports the results obtained by applying the LSB steganography technique and the corresponding improvements achieved through the GA, TS and the synergistic application of GA–TS. The performance of each method was evaluated based on two key image quality metrics: a comparison of the different metric values, including PSNR and MSE, obtained using multiple images as the test cover images. The analysis results and a comparison of the two metrics are presented below.

$$MSE = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} (A_{mn} - B_{mn})^2, \quad (1)$$

$$PSNR = 10\, log_{10} \left[\frac{W * H}{MSE}\right], \quad (2)$$

where A_{mn} and B_{mn} are the host image and the stego-image, respectively, and W, H are the dimensions of the images. μ_A and μ_B denote A and B mean values, respectively.

The dataset in the proposed steganography system is derived from the USC-SIPI dataset that supports studies in image processing, analysis and vision analysis, including lena.png, man.tiff, Baboon Pepper, Splash House and Camera.

In the present work, four types of embedding were used to evaluate the performance of the developed steganography system with different LSBs: simple LSB embedding, embedding using LSB and GA, LSB and TS algorithm and the hybrid embedding of LSB with the previous algorithms. The results obtained are shown in Table 2, which includes the PSNR values for the greyscale images used.

Table 2: PSNR and MSE values for greyscale images

Images	LSB	LSB and GA	LSB and TS	LSB, GA and TS	MSE
lena.png	53.820	54.120	55.200	55.410	~0.5–1.02
man.tiff	49.690	52.003	54.370	54.720	~0.5–1.5
Baboon	54.030	52.476	55.230	55.226	~0.1–0.3
Pepper	53.910	52.012	55.340	55.860	~0.05–0.2
Splash	50.102	51.800	53.680	54.180	~0.01–0.1
House	49.789	52.030	54.830	54.852	~0.3–1.05
Camera	48.970	50.980	54.940	55.590	~0.45–1.33
Average	51.473	52.203	54.799	55.120	

4.1. LSB Method

The standard LSB approach yielded an average PSNR of 51.473 dB, and the MSE values for all methods were relatively low, ranging from 0.01 to 1.5, indicating moderate image quality with some visible distortions. The first basic embedding method is LSB, where the LSBs of the cover image are substituted with the secret message bits. This strategy provides easily computable solutions, and the modification process is simple but only partially optimised in terms of pixel selection, thus causing noticeable distortion in some regions of the stego-image. The slightly higher MSE values imply the need for further refinement to minimise the degree of distortion and improve imperceptibility, thereby achieving near-lossless data hiding. Table 3 presents the PSNR values for the greyscale images that used the LSB technique.

Table 3: Comparison of the PSNR value from the literature

Cover Image	Refe.	PSNR

lena.png	[19]	50.99
	[20]	49.2668
	[21]	53.7618
	proposed	53.820
Baboon	[19]	50.98
	[20]	48.8766
	[21]	53.7558
	proposed	54.030
Pepper	[19]	50.06
	[20]	47.9887
	[21]	53.7869
	proposed	53.910

4.2. LSB with GA

The SNR reached 52.203 dB when using the GA as an optimisation algorithm, relying on evolutionary techniques to find an optimal set of pixels with less noticeable changes. These improvements also eliminate noise introduced by the embedding process, resulting in embedding images with superior image quality. However, the GA technique is sensitive to the choice of its parameters, such as initialisation and population diversity, potentially preventing further improvements in performance in some cases. However, the method is more successful in reducing distortion compared with the LSB standard approach. Table 4 presents the PSNR values for the greyscale images that were used with the LSB and GA techniques.

Table 4: Comparison of the PSNR value from the literature

Cover Image	Refe.	PSNR
lena.png	[22]	51.32
	[23]	52.2
	[24]	52.4
	Proposed	54.120
Baboon	[22]	48.76
	[23]	52.18
	[10]	51.37
	Proposed	52.476
Pepper	[22]	52.012
	[10]	51.36
	Proposed	52.012

Applying the TS optimisation algorithm resulted in remarkable improvements in the performance of the LSB method. The method presented high outcomes when comparing the PSNR of 54.799 dB with all examined methods, proving high image quality and slight distortions. The TS algorithm combines accurate local optimisation with structured search through the solution space and prohibits revisiting non-improving solutions by utilising the Tabu list. This algorithm increases the probability of correctly selecting pixels when hiding, thereby easily attaining a realistic and undetectable outcome. Consequently, the above findings prove that TS excels over GA when considering clean outcomes. However, one area where the use of TS increases over GA relates to computing needs—that is, the more iterations conducted and the greater the size of the Tabu list, the greater the computing needs will be.

Despite the success of TS as a meta-heuristic optimisation approach for different kinds of applications such as scheduling, routing, combinatorial optimisation and machine learning, its application in image hiding in digital image steganography is still surprisingly limited. From a scan of the broad existing image steganographic literature, no specific attempt to apply TS to image hiding in greyscale image steganography has been identified thus far. Moreover, most image steganographic literature discussed various general methods in either spatial or frequency domains but failed to utilise advanced meta-heuristic optimisation techniques such as TS to improve their performance in monochrome image steganography. However, one attempt to apply TS to image steganography has been observed in a specific case of colour image steganography with promising results in capacity, imperceptibility and security of image steganography. Table 5 represents the outcomes of applying LSB substitution and TS methods to various kinds of colour images assessed in terms of specific parameters of PSNR and MSE by Sandhu et al. 2024 [25].

Table 5: Comparison of the PSNR and MSE values from the literature (Sandhu et al., 2024)

Name of images	PSNR	MSE
Boat	78.565	0.00175
Aeroplane	79.12	0.00191
Lena	78.871	0.00019
Baboon	80.5472	0.000187
Miramar	80.855	0.004285

1. This gap provides a fertile area that warrants future investigation. Future research steps could entail the application and assessment of TS-based steganography schemes in greyscale and colour images. As presented in a side-by-side manner, a comparative analysis would enable an improved understanding of how.
2. Is TS providing continuous optimisation benefits across distinct types of images?
3. How does the dimensionality affects the algorithm's convergence and the way the algorithm embeds the data efficiently?
4. What are the necessary modifications for maximum performance in single-channel images as opposed to multi-channel images?

The study of filling the current gap will extend the applicability of the TS method in steganography as well as enhance the comprehension of the relationship between the data structure of images and the nature of metaheuristic optimisation methods.

4.4. LSB with Combined GA and TS

Furthermore, to avoid over-reliance on thorough investigations in GA and localised enhancements in TS, the combination of GA and TS was utilised in the current study to obtain PSNRs as high as 55.120 dB, representing the least image distortion. The GA–TS hybrid exhibited superior MSE results and generated high-quality images with minimal degradation. Although the improvement beyond TS alone was marginal, the combination consistently achieved higher PSNR values, thus highlighting its effectiveness in improving the performance of the LSB algorithm.

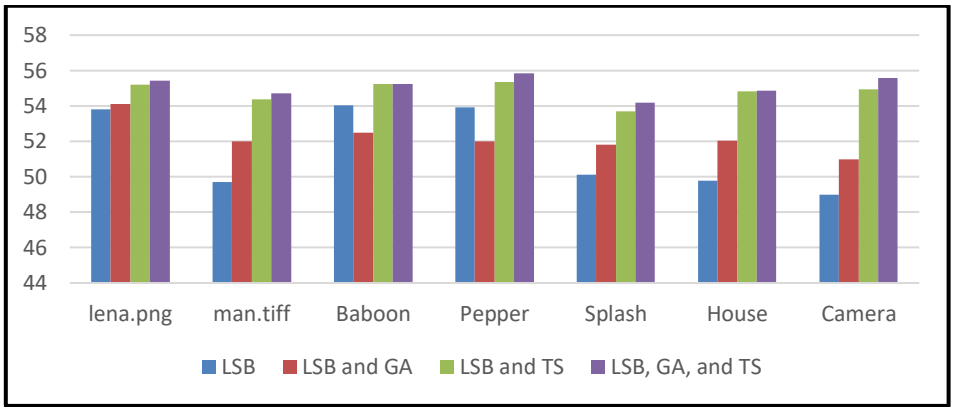

Figure 2: Comparison of PSNR values for the LSB, LSB with GA, LSB with TS and the hybrid LSB–GA–TS

Figure 2 demonstrates a comparison of four steganographic methods in terms of PSNR: simply LSB, a simple steganographic approach; LSB GA, steganography with fine-tuning using a GA approach; LSB TS, another steganography method with fine-tuning using TS; and a hybrid approach combining LSB, GA and TS. Simply LSB presents the least PSNR amongst all four approaches, yielding maximum distortion during embedding. These experiments show that fine-tuning with GA followed by further fine-tuning using TS yields higher PSNR values. The combined GA–TS approach consistently achieves the maximum PSNR values across all experiments.

5. CONCLUSION

LSB-based image steganography is a practical method for improving security in communication, allowing sensitive messages to be securely transmitted through insecure channels. This method also serves to facilitate the protection of intellectual property by using digital watermarking and supports verification of authenticity through the concealment of critical data, such as digital signatures and medical records. Owing to its numerous advantages, LSB steganography can be applied across a wide range of fields, particularly in communication security. Despite its simplicity, the traditional LSB embedding strategy often results in noticeably distorted images. These inherent weaknesses create a desperate need to alter this critical issue. Aiming to achieve this challenge, the present work incorporates optimisation techniques into the LSB

embedding process, with a specific focus on GAs and TS. In contrast to the classical LSB embedding method, the GA- and TS-based embedding methods substantially enhance the stego-image quality. Whilst TS has higher computational overheads, it achieves lower distortion and higher PSNR values compared to its alternative. Furthermore, no previous work has ever focused on this exact combination towards improving LSB-based image embedding; therefore, the hybridisation of GA with TS is a novel contribution to steganographic research. The resistance of the system to steganalysis and hacking is enhanced by combining the two methods, thereby producing stego-images with improved visual quality, reduced distortion and improved security characteristics. The achieved results confirm the benefits of integrating advanced optimisation techniques for substantially improving the steganographic performance. The hybrid model could also expand future research horizons by being extended to other forms of media types, such as video and audio steganography. Moreover, the framework should be adjusted to handle large datasets and high-resolution images to ensure improved scalability and usability. Multi-objective optimisations that balance embedding capacity, imperceptibility and security should be pursued further in the future to obtain a robust and versatile steganographic system.

REFERENCES

[1] R. Rasras, M. Sara, and Z. Al Qadi, 'Enhanced Efficiency and Security in LSB2 Steganography: Burst Embedding and Private Key Integration', *Traitement du Signal*, vol. 40, pp. 1795–1805, Oct. 2023, doi: 10.18280/ts.400502.

[2] L. Sultan, S. Abdulateef, and B. Shtyat, 'Prediction of student satisfaction on mobile-learning by using fast learning network', *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 27, Jul. 2022, doi: 10.11591/ijeecs.v27.i1.pp488-495.

[3] Y. A. Alsalhi, L. Songfeng, A. A. G. Al-Hamodi, A. H. Al-Mter, and Z. Zhangv, 'New Qubits steganography algorithm to conceal a secret file in compressed edge detection operators based on optimized adaptive neural networks', *2017 19th International Conference on Advanced Communication Technology (ICACT)*, pp. 167–176, 2017, [Online]. Available: https://api.semanticscholar.org/CorpusID:43577567

[4] K. Rao and S. Mandapati, 'A Tabu Search Algorithm for General Threshold Visual Cryptography Schemes', *Ingénierie des systèmes d information*, vol. 26, pp. 329–335, Jun. 2021, doi: 10.18280/isi.260310.

[5] S. M. Douiri and S. Elbernoussi, 'A steganographic method using tabu search approach', in *2017 16th mexican international conference on artificial intelligence (MICAI)*, IEEE, 2017, pp. 30–33.

[6] A. Gutub and M. Al-Ghamdi, 'Hiding shares by multimedia image steganography for optimized counting-based secret sharing', *Multimed. Tools Appl.*, vol. 79, no. 11–12, pp. 7951–7985, Mar. 2020, doi: 10.1007/s11042-019-08427-x.

[7] J. Yang, K. Liu, X. Kang, E. K. Wong, and Y.-Q. Shi, 'Spatial image steganography based on generative adversarial network', *arXiv preprint arXiv:1804.07939*, 2018.

[8] Z. Xia, X. Sun, J. Qin, and C. Niu, 'Feature selection for image steganalysis using hybrid genetic algorithm', *Information Technology Journal*, vol. 8, no. 6, pp. 811–820, 2009.

[9] M. Soleimanpour, S. Talebi, and H. Azadi-Motlagh, 'A Novel Technique for Steganography Method Based on Improved Genetic Algorithm Optimization in Spatial Domain', *Iranian Journal of Electrical and Electronic Engineering*, vol. 9, pp. 67–75, Jun. 2013.

[10] R. Wazirali, W. S. Alasmary, M. Mahmoud, and A. Alhindi, 'An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Algorithms', *IEEE Access*, vol. 7, pp. 133496–133508, 2019, [Online]. Available: https://api.semanticscholar.org/CorpusID:203169273

[11] S. M.K, K. B. Kumar, and R. Das, 'Image Steganography Using Genetic Algorithm For Cover Image Selection And Embedding', *Soft Computing Letters*, vol. 3, p. 100021, Sep. 2021, doi: 10.1016/j.socl.2021.100021.

[12] S. Nokhwal, M. Chandrasekharan, and A. Chaudhary, 'Secure information embedding in images with hybrid firefly algorithm', *Neural Comput. Appl.*, vol. 37, pp. 27675–27688, Nov. 2024, doi: 10.1007/s00521-024-10712-2.

[13] B. A. Shtayt, N. H. Zakaria, and N. H. Harun, 'A comprehensive review on medical image steganography based on LSB technique and potential challenges', *Baghdad Science Journal*, vol. 18, pp. 957–974, Jun. 2021, doi: 10.21123/bsj.2021.18.2(Suppl.).0957.

[14] A. Aljumaili, M. Noby, and S. Guirguis, 'A secure image steganography technique based on Data Mapping and Genetic Algorithm', Oct. 2022.

[15] S. Katoch, S. Chauhan, and V. Chahar, 'A review on genetic algorithm: past, present, and future', *Multimed. Tools Appl.*, vol. 80, pp. 8091–8126, Oct. 2020, doi: 10.1007/s11042-020-10139-6.

[16] Z. Kang, Y. Guan, J. Wang, and P. Chen, 'Research on Genetic Algorithm Optimization with Fusion Tabu Search Strategy and Its Application in Solving Three-Dimensional Packing Problems', *Symmetry (Basel).*, vol. 16, p. 449, Apr. 2024, doi: 10.3390/sym16040449.

[17] T.-K. Dao, T.-T. Nguyen, T.-D. Nguyen, T.-X.-H. Nguyen, and T.-T. Nguyen, 'A Review of the Tabu Search Algorithm for Industrial Applications. Journal of Information Hiding and Multimedia Signal Processing', vol. 15, no. 3, 2024.

[18] M. Hashim, M. Taha, A. Aman, A. Hashim, M. Rahim, and S. Islam, *Securing Medical Data Transmission Systems Based on Integrating Algorithm of Encryption and Steganography*. 2019. doi: 10.1109/ICOM47790.2019.8952061.

[19] S. M. M. Karim, Md. S. Rahman, and M. Hossain, *A new approach for LSB based image steganography using secret key*. 2011. doi: 10.1109/ICCITechn.2011.6164800.

[20] S. Dagar, *Highly randomized image steganography using secret keys*. 2014. doi: 10.1109/ICRAIE.2014.6909116.

[21] S. Maurya and V. Shrivastava, 'International Journal of Computer Science and Mobile Computing An Improved Novel Steganographic Technique for RGB and YCbCr Colorspace', 2014. [Online]. Available: www.ijcsmc.com

[22] Hayat Al-Dmour and Ahmed Al-Ani, 'Optimizing LSB image steganography using genetic algorithm for enhanced security and capacity', *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1525–1537, 2019.

[23] P. Shah and R. Bichkar, 'A Secure Spatial Domain Image Steganography Using Genetic Algorithm and Linear Congruential Generator', 2018, pp. 119–129. doi: 10.1007/978-981-10-5520-1_12.

[24] R. P. Singh and S. Singh, 'Genetic algorithm based optimized LSB steganography using multi-objective function', *Multimed. Tools Appl.*, vol. 80, no. 15, pp. 22879–22901, 2021.

[25] M. Sandhu, D. Ahmed, M. Hussain, S. Head, and I. Khan, 'Protecting Sensitive Images with Improved 6-D Logistic Chaotic Image Steganography', *The International Arab Journal of Information Technology*, vol. 21, p. 1064, Nov. 2024, doi: 10.34028/iajit/21/6/10.