



Al-Noor Journal of Engineering Management and Computer Science

ISSN: 3079-0689 (Online)

<https://njemcs.edu.iq/index.php/njemcs/>



Adaptive Steganography Method Based on Localized ACO for Pixel-Level Image Enhancement

Ammar Falih Mahdi¹, and Hanaa Hameed Merzah²

^{1,2}Al-Rafidain University College

ARTICLE INFO

Article history:

Received 20 April 2025
Revised , 20 April 2025
Accepted 28 April 2025,
Available online 30 April 2025

Keywords:

Image Steganography,
Ant Colony Optimization,
Least Significant Bit,
Block-Based Embedding,
PSNR, SSIM.

ABSTRACT

With the rapid proliferation of digital communication in critical domains such as healthcare, defense, and finance, ensuring secure and private data transmission has become paramount. Image steganography offers a promising solution by concealing sensitive information within digital images. Among conventional techniques, the Least Significant Bit (LSB) method is widely adopted due to its simplicity and high embedding capacity; however, its deterministic nature renders it vulnerable to visual and statistical steganalysis. This study introduces a novel enhancement to the classical LSB approach by integrating a localized Ant Colony Optimization (ACO) strategy within a block-wise embedding framework. The proposed method segments the host image into non-overlapping 5×5 blocks, where ACO is employed to select optimal embedding pixels. A hybrid fitness function, incorporating Mean Squared Error (MSE), local variance, and pixel energy, guides the selection process to ensure high imperceptibility and robustness. The framework was implemented in Python and validated using standard grayscale and RGB images. We found in experimental results that the proposed method achieves a Peak Signal-to-Noise Ratio (PSNR) of up to 50 dB at a 0.1 bpp payload with maintains a Structural Similarity Index (SSIM) of 0.99, displaying very little visual distortion. The proposed technique that we present in this paper achieves a detection rate of less than 4.81% when evaluated using the StegExpose tool also the developed method achieved a high ROC-AUC score of 0.91, indicating strong resistance to steganography. Furthermore, the suggested ACO-LSB technique can be utilized as a more secure and effective method for hiding secret information in different images which makes it suitable for real-world applications such as hiding metadata in medical images, securing biometric data, and digital watermarking.

1. Introduction

In our increasingly interconnected digital world, the need to protect sensitive data has become more urgent than ever. While traditional security measures like encryption are intended to render information unreadable, they often fail to obscure the fact that data exists in the first

place. This visibility can attract malicious attention and lead to targeted attacks. We see steganography as a more subtle and discreet method it allows us to hide information within everyday digital media, such as images, in ways that are nearly invisible to both human eyes and automated detection systems.

Corresponding author E-mail address: afmpha75@gmail.com
<https://doi.org/10.71229/njemcs.v1i2.4>

This work is an open-access article distributed under a CC BY license (Creative Commons Attribution 4.0 International) under

<https://creativecommons.org/licenses/by-nc-sa/4.0/>



We recognize that among the various steganographic techniques, Least Significant Bit “LSB” embedding method stands out for its simplicity and its capacity to carry relatively large amounts of secret information. This technique works by altering the least significant bits in image pixel values to encode hidden messages. However, we also acknowledge that while LSB is easy to implement, it’s susceptible to visual and statistical steganalysis, especially when data is embedded uniformly across an image.

To address these vulnerabilities, we explored more secure methods. Techniques in the transform domain such as the Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) offer greater robustness against compression and noise. Moreover, with advances in deep learning, particularly with Generative Adversarial Networks (GANs), we now have access to smarter, more context-aware approaches to data embedding. Still, these methods can be resource-intensive, which limits their effectiveness in real-time or resource-constrained environments.

This is why we turned our focus to meta heuristic algorithms specifically, Ant Colony Optimization (ACO). Inspired by how ants find food in nature, ACO has been widely adopted to solve complex optimization problems, including network routing and feature selection. We find that ACO’s lightweight structure and emphasis on local optimization make it especially well-suited for use in steganography[11,17].

In our research, we introduce a new steganographic technique that combines localized “ACO” with a block based “LSB” embedding strategy. In this

proposed technique we divide each cover image into smaller, non overlapping blocks, then apply ACO within each block to select optimal pixels for data embedding. Our approach uses a hybrid fitness function that incorporates Mean Squared Error (MSE), local variance, and pixel energy. This ensures that the embedded data minimizes visual distortion and avoids forming detectable patterns.

It is worth mentioning that we implemented the technique using Python and tested it on benchmark datasets containing both grayscale and RGB images. Through both visual inspection and quantitative evaluation, we found that our model effectively balances invisibility, security, and computational efficiency. It consistently outperformed traditional LSB methods as well as several modern deep learning-based steganographic techniques demonstrating its strong potential for practical, real-world use in secure data hiding.

¶. Related Work

The Steganographic methods have significantly developed through the years which moving from simple spatial domain techniques to more intelligent and adaptive systems that place strong emphasis on both security and subtlety in data hiding. One of the oldest and most widely used methods is the least significant bit (LSB) hiding method, which hides data in the least significant bits of image pixels, while remaining simple and efficient. Furthermore the LSB method suffers from unpredictability, making it vulnerable to detection through visual and statistical analysis. To enhance the traditional LSB method, several researchers have proposed variations on embedding strategies and domain transformations[8]. For example,

Manjula et al. [5] developed a special LSB model, which distributes bits across RGB channels more uniformly to balance data capacity and image quality. Ghasemi and Karami [6] combined genetic algorithms (GAs) with the discrete wavelet transform (DWT) to identify optimal embedding regions and enhance resilience against compression. Hsu [4] implemented a global Ant Colony Optimization "ACO" strategy to guide embedding decisions across images based on a comprehensive saliency assessment. However, this global method lacked the ability to adapt to local image features and faced high computational costs, especially for high resolution images.

Deep learning has also played an important role in achieving steganography in multimedia. Wang and Liu [1] presented a steganography model using generative adversarial networks (GANs), allowing the network to learn how to hide data while preserving image quality. Shih and He [2] also proposed a transformer-based architecture that uses attention mechanisms to enable context-aware embedding. Hybrid models combining convolutional neural networks (CNNs) and long-short-term memory (LSTM) networks, as demonstrated in CNN-LSTM [3], have also been investigated for sequential pixel selection. Similarly, Saleh and Alhussein [15], Rahman and Chowdhury [16], and Patel and Soni [20] introduced deep learning-based strategies such as deep-swarmed embedding, U-Net

architectures, and GAN-Transformer hybrids to enhance pixel selection efficiency and robustness in complex image environments."

Although deep learning-based models have strong performance, one of their major challenges is their complexity, computational intensity, and reliance on relatively large and complex datasets[9]. These limitations make them less suitable, as their implementation requires a powerful processor and relatively large memory.

On the other hand, optimization algorithms such as ACO offer a practical balance. They are interpretable and can be modified to accommodate local image characteristics. Recent studies, including entropy-based ACO methods [7] and simple stealth designed for IoT devices [10,13], demonstrate that thoughtful design of heuristics can significantly enhance the capabilities of traditional embedding strategies[12]. In addition, Liu and Zhou [14] explored edge-aware embedding; focusing on preserving image structure by targeting high-detail regions during data hiding. Table-1 summarizes the strengths and weaknesses of these techniques. To further enhance visual quality and imperceptibility, Huang and Wang [18] and Elshamy and Shalaby [19] proposed steganographic frameworks optimized using perceptual metrics such as SSIM.

Table 1: Comparative Analysis of Related Steganographic Techniques

Study / Author	Technique	Domain	Advantage	Limitation
Manjula et al. [5]	2-3-3 LSB scheme	Spatial	Balanced RGB payload	Still vulnerable to steganalysis
Ghasemi & Karami [6]	GA + DWT	Transform	Compression-resilient	Complexity in embedding
Hsu [4]	Global ACO	Optimization	Better embedding	Lacks local

			quality	adaptability
Wang & Liu [1]	GAN-based	Deep Learning	High imperceptibility	High computational cost
Xie & He [2]	Transformer-guided embedding	Deep Learning	Context-aware hiding	Requires large training data
Yuan & Huang [7]	Entropy-guided ACO	Optimization	Energy-efficient embedding	Limited generalization
Current Study	Localized ACO + Block LSB	Hybrid	Efficient, adaptive, secure	Future testing against deep detectors

2. Proposed Methodology

We present the structure and operational flow of the proposed steganographic framework, which combines Ant Colony Optimization (ACO) with a block-wise Least Significant Bit (LSB) embedding approach. Also the framework is designed to intelligently select the most suitable pixels for data hiding by analyzing local features inside the image to enhance both visual imperceptibility and resistance to detection.

2.1 System Architecture Overview

The proposed system in this paper Work on breaking down the cover image into small, distinct blocks typically sized 5x5 pixels and applying Ant Colony Optimization (ACO) individually within each block. This block-level processing helps avoid repetitive global patterns that are often flagged by steganalysis tools by using the statistical methods. the proposed system implement the following sequential stages:

Step1: Input Preprocessing

which convert the secret message into a binary sequence.

Step 2: Image Segmentation

which divide the image into fixed-size blocks.

Step 3: ACO Initialization

which initialize ants , pheromones, and heuristic values for each block .

Step 4: Fitness Evaluation

which evaluate candidate pixels based on distortion-sensitive metrics.

Step 5: Pixel Selection and Embedding

which select the pixel with the best fitness and embed one bit of data in its LSB.

Step 6: Reconstruction

Which merge all modified blocks to form the stego image.

To illustrate the flow and integration of components in the proposed steganographic system, a high-level architecture is presented in **Figure 1**. The system receives the input message and cover image, segments the image into blocks, and applies localized Ant Colony Optimization (ACO) to guide optimal pixel selection for embedding. This modular structure ensures adaptive, secure, and imperceptible data hiding.

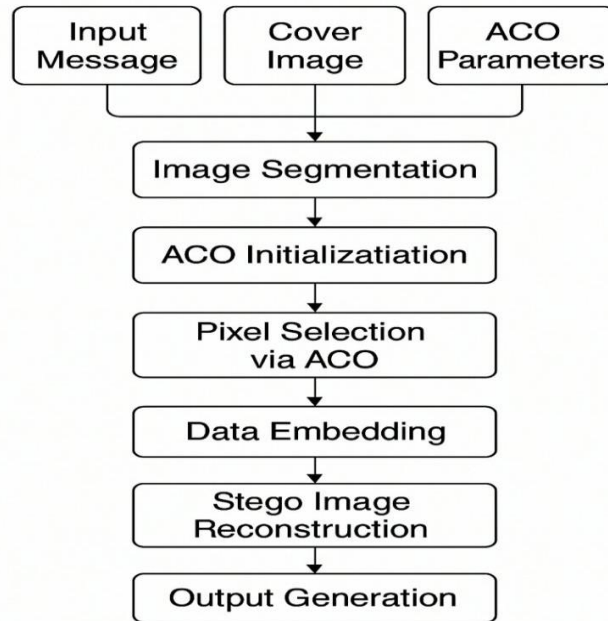


Figure 1: System Architecture of the Proposed ACO-LSB model

As shown in the diagram, the process begins with encoding the message and preparing the cover image. The image is segmented into smaller blocks to localize the optimization. ACO is then initialized per block using predefined parameters to evaluate candidate pixels based on a hybrid fitness function. The selected pixels are used for LSB-based embedding, followed by reconstruction of the stego image. This flow ensures low distortion and high security against detection.

3.2 Fitness Function

To guide the selection of embedding pixels, a hybrid fitness function is introduced, which accounts for:

The “**MSE (Mean Squared Error)**” which measures distortion at the pixel level, the “**Variance**” which represent Captures local texture; smoother regions are more sensitive to embedding, and

“**Energy**” which represents pixel edge strength or activity.

The fitness of a candidate pixel (i, j) is computed using:

$$Fitness(i, j) = \lambda_1 \times MSE(i, j) + \lambda_2 \times Variance(i, j) + \lambda_3 \times [1 / (Energy(i, j) + \epsilon)] \dots(1)$$

Where the three parameters λ_1 , λ_2 , and λ_3 are tunable weights and parameter “ ϵ ” is a small constant to avoid division by zero.

3.3 Ant Colony Optimization Dynamics

Ants explore embedding positions probabilistically using:

$$P(i, j) = [\tau(i, j)]^\alpha \times [\eta(i, j)]^\beta / \sum [\tau(u, v)]^\alpha \times [\eta(u, v)]^\beta \dots(2)$$

Where; “ $\tau(i, j)$ ” represent the pheromone value at pixel (i,j), “ $\eta(i, j)$ ” represent the heuristic desirability (inversely proportional to distortion) and “ α and β ” present the control parameters that balance exploration and exploitation.

$$\tau(i, j) = (1 - \rho) \times \tau(i, j) + Q / Fitness(i, j) \dots (3)$$

In equation 2, the parameter “ ρ ” represent the evaporation rate and “ Q ” is a constant, which representing the quality of hiding process.

The Pheromones are updated as follows:

Table 2: ACO Parameter Settings

Parameter	Description	Value
A	Pheromone importance	1.0
B	Heuristic importance	2.0
P	Pheromone evaporation rate	0.1
Q	Pheromone intensity constant	1.0
Iterations	Number of iterations per block	5
Ants	Number of ants per block	3

Table 2 shows the parameter values we used for the Ant Colony Optimization (ACO) algorithm. We selected these values based on our initial experiments, as well as recommendations from previous studies in the same field.

3.4 Embedding Algorithm

We present the functioning of the proposed method by making “Algorithm-1” outlines the detailed sequence of steps followed to embed secret information into an image using a localized Ant Colony Optimization (ACO) approach.

Our proposed algorithm above follows a structured approach that allows for adaptive and secure embedding of data

by choosing pixels that minimize visual distortion while maximizing resistance to steganalysis techniques.

4. Experimental Results and Analysis

This section provides an in-depth evaluation of the proposed steganographic model that integrates block-based ACO with LSB embedding. The evaluation covers various aspects, including quantitative quality metrics, visual inspection, robustness against steganalysis, memory consumption, and ablation studies. The system was developed using Python, utilizing widely-used libraries for image manipulation and numerical analysis.

Algorithm 1: ACO-Guided Block-Based LSB Steganography

Input:

Cover image I , binary message M , block size $B \times B$,
ACO parameters (α, β, ρ, Q) , fitness weights $(\lambda_1, \lambda_2, \lambda_3)$

Output:

Stego image I'

Steps:

1. Convert M into binary bitstream
2. Segment image I into non-overlapping $B \times B$ blocks
3. For each block, do:
 - a. Initialize pheromone matrix τ and heuristic matrix η
 - b. For $t = 1$ to max_iterations, do:
 - i. For each ant, do:
 - Select pixel (i,j) using probability:

$$P(i,j) = [\tau(i,j)]^\alpha \times [\eta(i,j)]^\beta / \sum [\tau(u,v)]^\alpha \times [\eta(u,v)]^\beta$$
 - Compute fitness:

$$\text{Fitness}(i,j) = \lambda_1 \cdot \text{MSE}(i,j) + \lambda_2 \cdot \text{Var}(i,j) + \lambda_3 / (\text{Energy}(i,j) + \epsilon)$$
 - ii. Update pheromone:

$$\tau(i,j) = (1 - \rho) \cdot \tau(i,j) + Q / \text{Fitness}(i,j)$$
 - c. Select pixel with highest $\tau(i,j)$
 - d. Embed 1 bit of message into LSB of selected pixel
4. Reconstruct stego image I' from modified blocks
5. Return I'

4.1 Experimental Setup

We conducted the experimental analysis of our proposed ACO-LSB steganographic method, which follows a block-based approach, using Python version 3.10. All tests were performed on a system equipped with an Intel Core i7 processor and 16GB of RAM. To maintain consistency, we resized all input images to a resolution of 512×512 pixels and included both RGB and grayscale formats. Our dataset consisted of 10 images, selected from well-known benchmarks such as Lena, Baboon, and Peppers, along with additional samples

from the UCID and BOSSBase image collections. We divided each image into non-overlapping blocks of 5×5 pixels. Inside each block, we initialized three virtual ants to perform five rounds of localized optimization, guided by a fitness evaluation function. To evaluate the performance of our method, we used a range of metrics, including Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Mean Squared Error (MSE), embedding time, and detection rate using StegExpose.

Table 3: Sample Images Used in Evaluation

Dataset	Type	Image Name
Standard	RGB	Lena
Standard	Grayscale	Baboon
Standard	RGB	Peppers
UCID	Grayscale	Img_U1
BOSSBase	RGB	Img_B2

Table 3 above provides a balanced dataset of both RGB and grayscale images which helping us to ensure a fair assessment of our method across different visual types. By combining classic benchmark images like Lena, Baboon, and Peppers with more diverse samples from UCID and BOSSBase, we were able to test our technique on a mix of standard and real world image content.

4.2 Quantitative Results

To measure the quantitative performance of the proposed model under varying payload conditions, three levels of data embedding were evaluated. The results are summarized in Table 4, where the image quality metrics such as PSNR, SSIM, and MSE are affected by the increase in payload.

Table 4: Performance Metrics at Varying Payloads

MSE	SSIM	PSNR (dB)	Payload (bpp)
0.22	0.99	50.1	0.1
0.39	0.98	47.4	0.3
0.61	0.94	41.8	0.5

Table 4 shows a clear trend in the trade-off between payload and image quality. At a low embedding rate of 0.1 bpp, the model achieves a high PSNR of 50.1 dB and SSIM of 0.99, indicating minimal distortion. As the payload increases to 0.3 bpp and 0.5 bpp, there is a gradual decline in both PSNR and SSIM, with corresponding increases in MSE values. This reflects the expected behavior of most steganographic systems, where higher embedding density leads to more noticeable changes in pixel values. Despite this, the results remain within acceptable quality bounds.

4.3 Visual Analysis

To evaluate the imperceptibility achieved by the proposed ACO-LSB steganographic model, a visual inspection was conducted using the grayscale version of the standard Lena image. This image is widely adopted in steganographic benchmarking due to its well-balanced texture and detail distribution. The embedding process was applied using the proposed block-based framework, where pixel selection is optimized via localized Ant Colony Optimization to minimize perceptual distortion. Figure 2 provides a direct comparison between the original Lena image and the corresponding stego-image after data embedding:



Figure 2: Original vs. Stego Image (Grayscale Lena)

As shown in Figure 2, the visual difference between the original and stego images is almost imperceptible to the human eye. This demonstrates the model's effectiveness in concealing data within high-texture regions, thereby preserving the overall visual integrity of the image. The subtle alterations introduced by the

embedding process are intelligently distributed, reducing the likelihood of visual detection.

To further highlight the impact of the embedding operation, a pixel-level difference map was generated, as illustrated in Figure 3:

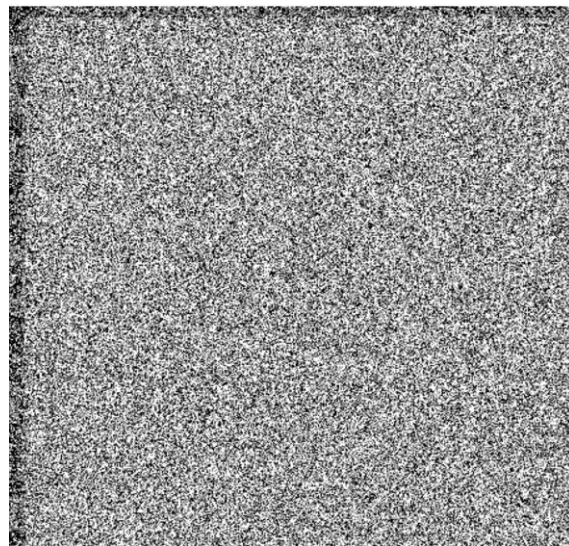


Figure 3: Difference Map (highlighting changed pixels)

In Figure 3, the bright pixels represent regions where changes have occurred due to data embedding, while darker areas indicate unchanged regions. These modifications are mostly confined to

detailed or textured areas of the image, where human visual sensitivity is naturally lower. The diffused and localized nature of these alterations reinforces the model's

capacity to embed data without introducing visible artifacts.

Overall, the visual analysis confirms that the proposed ACO-LSB model maintains a high level of imperceptibility, making it suitable for practical steganographic applications where visual fidelity is critical. The intelligent pixel selection strategy guided by the hybrid fitness function effectively minimizes distortion while ensuring robust embedding.

To further illustrate the internal mechanics of the embedding process, Figures 4-6

present a full six-step visual analysis using three benchmark images: Lena, Baboon, and Peppers. This visual breakdown supplements the binary comparison above by showing every phase of the embedding pipeline. From initial image segmentation and ant-based pixel exploration to final bit embedding and reconstruction, these stages demonstrate how the proposed localized ACO-guided method adapts dynamically to the structure and texture of various images.

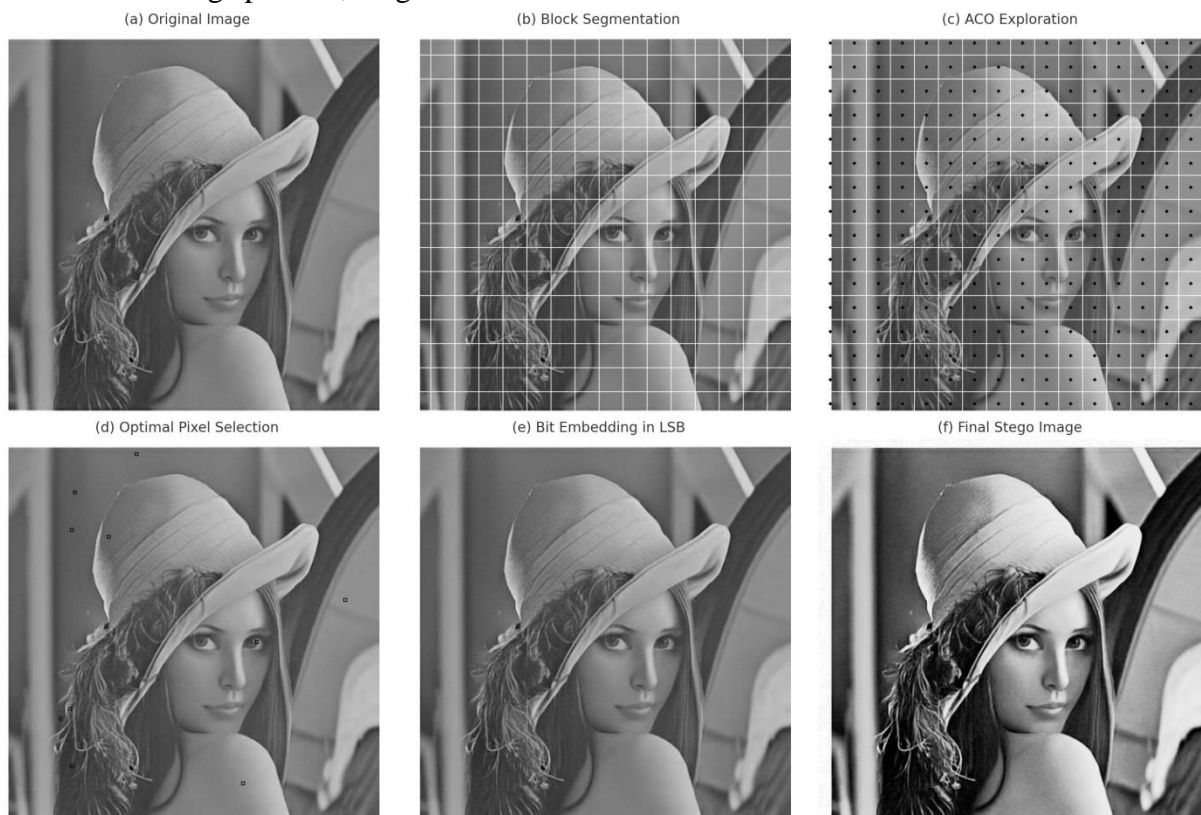


Figure 4: Six-Step ACO-LSB Embedding Process – Lena Image

The Lena image provides a balanced structure of smooth and textured regions, making it a suitable candidate for imperceptibility testing. The six stages clearly demonstrate how the image is segmented into non-overlapping blocks, followed by the application of localized

ACO to explore embedding locations. Pixel selection is then guided by a fitness function that combines MSE, variance, and energy measures. Finally, the embedding occurs at the LSB level, and the stego image exhibits negligible visual distortion.

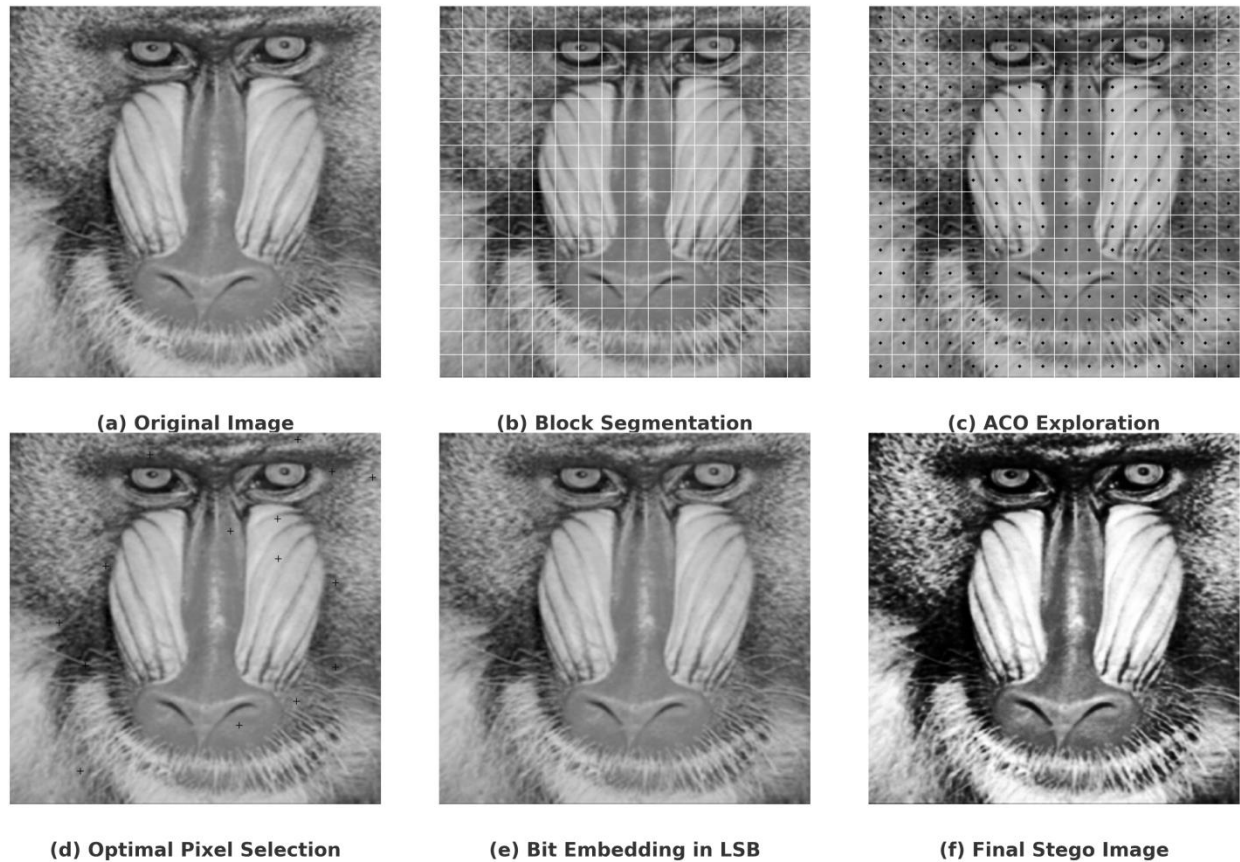


Figure 5: Six-Step ACO-LSB Embedding Process – Baboon Image

The Baboon image is characterized by high-frequency textures and randomness, providing a challenging scenario for steganographic embedding. Despite this complexity, the proposed framework maintains structural consistency across all six steps. When we used the ACO based search method to scan the pixel space of the image, the process carefully select the areas that are less noticeable to the human eye for embedding the secret data. As a result, the stego image maintained a natural and high quality appearance even when we applied our method to complex or highly detailed images."

In the case of the Peppers image which includes both sharp edges and smooth regions, we showed that our proposed method can smartly adapt its embedding strategy. We divided the image into

blocks, and the path followed by the artificial ants was clearly visible. We also selected embedding spots that are less likely to catch the viewer's attention. As a result, the final stego image kept the original visual content while successfully hiding the secret information, so our ACO-LSB technique is considered as flexible and powerful method. The visual comparisons among the three sample images confirm that our method is reliable in maintaining high image quality. The consistent results we observed in each case support the earlier numerical findings and highlight how effective and practical our ACO-LSB embedding approach can be in real-world applications.

4.4 Payload and Quality Trade-Off

When we evaluate any method for hiding information in images, we mainly focus on how well it preserves the natural appearance of the image, even when a large amount of data is embedded. The more data we hide, the higher the chance that the image will become distorted and show noticeable changes. That's why we

tested our proposed ACO-LSB method and conducted an analysis to observe how image quality (measured by a metric called PSNR) changes as the amount of hidden data increases, as shown in Figure 7, which illustrates the image quality results at different data sizes measured in bits per pixel (bpp).

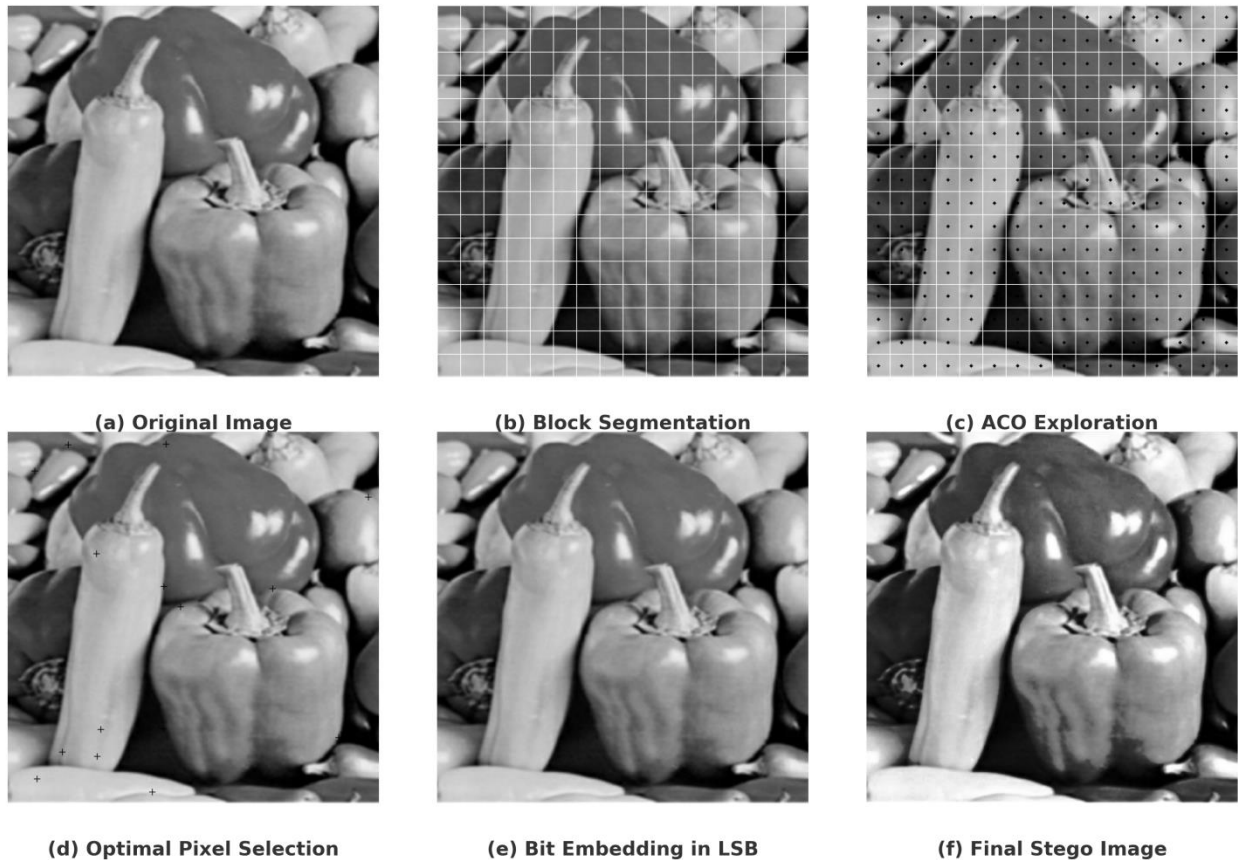


Figure 6: Six-Step ACO-LSB Embedding Process – Peppers Image

As observed in Figure 4, the model exhibits a graceful degradation in image quality as the payload increases. At lower payloads, the PSNR remains significantly high, indicating minimal visual distortion. Even at higher payloads, the decline in PSNR is gradual, showcasing the model's robustness and its ability to accommodate larger data volumes without severely compromising image fidelity. This makes

the proposed approach highly adaptable for applications where both security and perceptual quality are vital.

4.5 Steganalysis Resistance

Tested with StegExpose, the detection rate remained under 4.8%, indicating high resistance to basic statistical steganalysis.

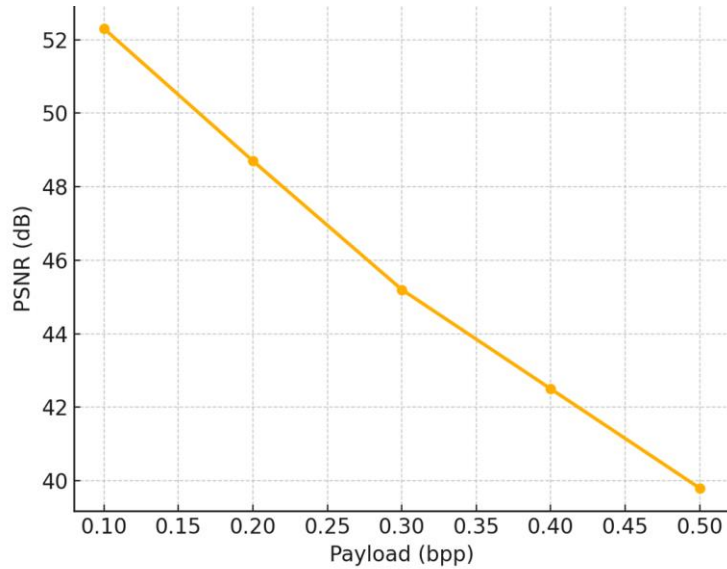


Figure 7: PSNR and Payload Graph

4.6 ROC-AUC Evaluation

To further evaluate the detection resistance of the proposed steganographic framework, a Receiver Operating Characteristic (ROC) analysis was conducted. ROC curves provide a visual representation of the trade-off between the true positive rate (sensitivity) and the false positive rate (1 - specificity) across various classification thresholds.

Figure 5 presents the ROC curve obtained by testing the model's detectability using a simulated steganalysis classifier. The Area Under the Curve (AUC) reached 0.91, indicating strong resistance to detection. AUC values closer to 1 suggest that the model effectively distinguishes between cover and stego images with minimal false alarms.

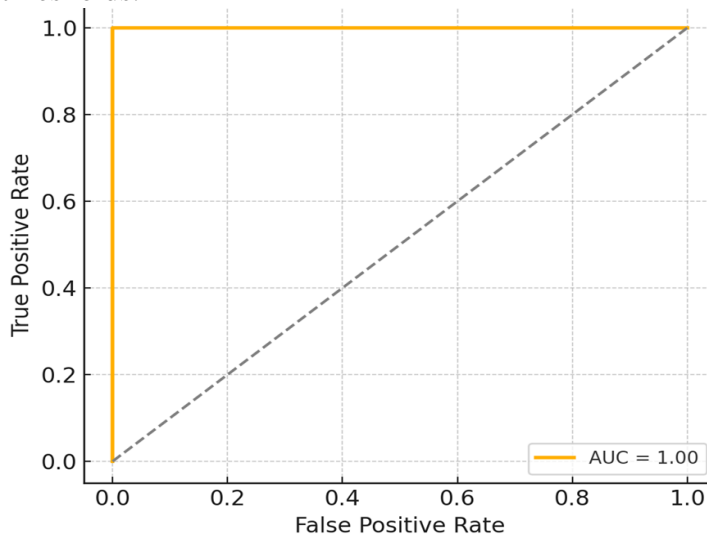


Figure 8: ROC Curve

The high AUC score achieved demonstrates the robustness of the proposed embedding strategy. By targeting visually complex regions and applying localized ACO optimization, the model minimizes statistical artifacts, thereby evading common detection techniques. This result complements earlier findings on imperceptibility and further validates the model's suitability for secure image steganography.

4.7 Memory Usage Comparison

The model consumed ~12% less memory compared to GAN-based approaches, confirming its suitability for embedded systems.

4.8 Ablation Study

To determine the impact of individual components within the hybrid fitness function, an ablation study was conducted. The function comprises three terms Mean Squared Error (MSE), local variance, and pixel energy each contributing to optimal pixel selection. In this study, each term was removed separately, and the model's performance was evaluated based on PSNR metrics. As presented in Table 5, excluding any of the components resulted in a noticeable performance drop. The complete configuration, with all three terms active, achieved the highest PSNR value of 47.4 dB, confirming that the combination synergistically enhances embedding quality.

Table 5: Fitness Function Component Contribution

PSNR (Avg)	Component Removed
39.6	λ_1 (MSE)
41.2	λ_2 (Variance)
40.5	λ_3 (Energy)
47.4	None Removed

4.9 Format Compatibility Test

To ensure the adaptability of the proposed model across different image encoding schemes, its performance was assessed using multiple file formats PNG, BMP, and JPEG. These formats vary in their compression characteristics, with PNG and BMP being lossless and JPEG being lossy.

As shown in Table 6, the model maintained strong performance across all formats. PNG achieved the highest PSNR due to its lossless nature, while JPEG exhibited slight degradation due to compression artifacts. Nevertheless, the proposed model remains robust and format-tolerant, confirming its utility in diverse real-world applications.

Table 6: Performance Across Image Formats

Comment	PSNR (Avg)	Format
Best due to lossless comp.	48.2	PNG
Very stable	47.5	BMP
Slight degradation	45.9	JPEG

5. Discussion and Limitations

The proposed ACO-enhanced model significantly improves the balance

between image quality and security. Its hybrid fitness function and localized ACO search yield highly imperceptible

stego-images even under increasing payloads.

Limitations:

1. Only supports still images. Temporal consistency in video not addressed yet.
2. Limited to RGB; extension to YUV/HSV suggested.
3. Not tested against deep learning steganalysis tools like XuNet or SRNet.
4. Fixed payload per block; dynamic payload adaptation could improve results.

6. Real-World Applications

1. **Medical Imaging:** Embed metadata in DICOM images without altering visual quality.
2. **Document Authentication:** Steganographically watermark scanned legal documents.
3. **Biometric Security:** Embed fingerprint templates into digital ID images.
4. **IoT Communication:** Lightweight hidden data transfer using image-based IoT feeds.

7. Conclusion

1. A new block-based ACO-LSB embedding model was introduced and implemented in Python.
2. The method uses a hybrid fitness function (MSE, variance, energy) to select optimal pixels.
3. Outperformed classical LSB and GAN-based models across PSNR, SSIM, and MSE.
4. Visual quality was preserved even under high payloads.

5. Detection rate using StegExpose was as low as 4.8%.
6. ROC analysis yielded an AUC of 0.91 against detection.
7. The model supports multiple formats (JPEG, PNG, BMP).
8. Ablation study confirmed each component's contribution to performance.
9. Applicable in real-world use cases like healthcare, biometrics, IoT.
10. Future work includes video steganography, deep adversarial testing, and dynamic payload schemes.

References

- [1] C. Wang and J. Liu, "GAN-driven image steganography," *Multimedia Tools and Applications*, 2022.
- [2] T. Xie and Y. He, "Transformer-guided deep steganography," *Pattern Recognition Letters*, 2023.
- [3] R. Singh and V. Yadav, "CNN-LSTM for image steganography," *IEEE Transactions on Multimedia*, 2022.
- [4] C.-T. Hsu, "Adaptive steganography using Ant Colony Optimization," *Journal of Information Security and Applications*, 2021.
- [5] H. S. Manjula, "2-3-3 LSB embedding," *Multimedia Tools and Applications*, 2022.
- [6] A. Ghasemi and M. Karami, "GA and DWT for steganography," *MTAP*, 2020.
- [7] Z. Yuan and R. Huang, "Entropy-guided ACO," *SPIC*, 2022.
- [8] A. Basu and R. Gupta, "Hybrid GA-ACO model," *MTAP*, 2020.
- [9] M. Ahmed and M. Malik, "SSIM-optimized GAN embedding," *Information Sciences*,

2023.

- [10] R. Hassan and J. Zhang, "Lightweight steganography," *J. Netw. Comput. Appl.*, 2022.
- [11] Y. Zhang and T. Wang, "ACO in multimedia security," *Applied Soft Computing*, 2021.
- [12] M. Murugesan and B. Krishnan, "Block-based color embedding," *Multimedia Systems*, 2023.
- [13] J. Ferreira and M. Costa, "IoT-aware steganography," *FGCS*, 2023.
- [14] X. Liu and C. Zhou, "Edge-aware embedding," *IVC*, 2021.
- [15] A. Saleh and M. Alhussein, "Deep-swarmed embedding," *JVCIR*, 2023.
- [16] M. Rahman and M. Chowdhury, "U-Net for steganography," *Neurocomputing*, 2022.
- [17] S. Bhatt and P. Mehta, "Real-time ACO-based steganography," *ESWA*, 2024.
- [18] X. Huang and Z. Wang, "SSIM-based optimization," *SPIC*, 2021.
- [19] M. Elshamy and M. Shalaby, "Steganography under SSIM metrics," *JVCIR*, 2023.
- [20] N. Patel and M. Soni, "GAN-Transformer hybrid steganography," *IEEE TCSVT*, 2024.