An Intelligent Multi-Objective Optimization Approach for High-Capacity Secure Image Steganography

A. V. Gahan
School of Electronics and Communication Engineering, REVA University, Bengaluru, India
gahanbit@gmail.com (corresponding author)

Geetha D. Devanagavi
School of Computer Science and Engineering, REVA University, Bengaluru, India
dgeetha@reva.edu.in

Received: 19 February 2026 | Revised: 12 March 2026 | Accepted: 23 March 2026

 DOI: https://doi.org/10.48084/etasr.18267

ABSTRACT

In this paper, an optimization-based and secure image steganography model, termed Multi-Objective Adaptive Firefly Optimized Secure Steganography (MOAFOSS), is proposed. The model formulates pixel selection as a multi-objective optimization problem to minimize Mean Square Error (MSE), maximize Peak Signal-to-Noise Ratio (PSNR), maximize entropy, and minimize the Standard Deviation (SD) to increase its resistance to steganalysis attacks. The Firefly Algorithm (FA) is used to find the best embedding points using a fitness criterion defined as a brightness function based on joint fitness. In addition, an adaptive Least Significant Bit (LSB) embedding mechanism is employed to conditionally adjust pixel values in order to minimize visual artifacts while maintaining accurate embedding. The additional encryption of secret data before embedding further enhances confidentiality. The experimental outcomes demonstrate that the suggested framework possesses better embedding capacity and Compression Ratio (CR) with a lower level of perceptible distortion. A comparative study with conventional optimization and compression methods demonstrates that MOAFOSS offers a balanced trade-off between image quality, security strength, and the amount of data carried, making it suitable for secure digital communication applications.

Keywords-multi-objective optimization; image steganography; Firefly Algorithm (FA); adaptive LSB embedding; secure data hiding; entropy-based security; steganalysis resistance; Compression Ratio (CR)

I. INTRODUCTION

With the exponentially rapid growth in digital communication over open and heterogeneous networks, there is an increasing need for secure data communication mechanisms to ensure that the privacy of information is not violated by unauthorized individuals, unauthorized interception, and unauthorized alteration of data [1]. Even though traditional cryptography methods are effective in the encryption of confidential data, they are prone to attack, as they tend to disclose the presence of confidential communication [2]. Steganography is a security method of hidden communication which involves incorporating confidential content into digital media in a manner that is not detected during communication [3], thus guarding confidential information against unauthorized access, interception, as well as manipulation [4]. Digital images are the most popular types of digital media that can be used in steganography because they have extensive use, high storage capacity, and redundancy [5]. Nevertheless, traditional image steganographic methods, such as Least Significant Bit (LSB) substitution and frequency domain embedding, are typically subject to statistical attacks, image degradation, and are vulnerable to insecure communication environments [6]. Thus, smart and optimization-based image steganography is required to achieve the goals of improving security, imperceptibility, and reliability in communication [7]. Recent developments based on nature-driven metaheuristic optimization algorithms have provided state-of-the-art tools to solve complex optimization problems in secure data steganography [8]. Due to its simplicity, strong search capability, and efficient convergence, the Firefly Algorithm (FA), which is inspired by the bioluminescent communication of fireflies, is highly effective for optimization tasks [9]. In FA, objective function values determine that fireflies are attracted toward brighter individuals, thereby enabling the algorithm to explore optimal solutions while avoiding local optima [10]. These properties ensure that FA is ideal in the optimization of steganographic locations and embedding parameters [11].

Here, a secure image steganography framework based on the FA is proposed, and the embedding process is formulated

as a multi-objective optimization problem [12]. FA intelligently chooses the best pixel positions based on a variety of goals such as minimal perceptual distortion, greater embedding randomness, and better resistance to steganalysis attacks [13]. The strategy guarantees good stego-image quality and effective security by incorporating data in less predictable areas with visual complexity [14]. Its advantages are optimized randomized embedding, high imperceptibility, attack resistance, and convergence efficiency [15], whereas its drawbacks include higher computational complexity and sensitivity to parameter tuning [16]. The method has applications in secure communication, defense [17], medical image exchange [18], digital rights management, cloud and Internet of Things (IoT) security, and confidential information sharing. The stochastic nature of FA further enhances robustness against transmission impairments and attacks [19], and performance evaluation using Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), and embedding capacity confirms superiority over conventional methods [20]. Numerous image steganography techniques have been proposed for enhancing security, imperceptibility, and embedding capacity of data hiding techniques. Table I provides a comparative review of various existing steganography, cryptography, and steganalysis techniques in terms of their methods, advantages, and limitations.

It has been identified that, despite the advancements in the field of image steganography, existing methods are not efficient enough to provide the desired results in terms of capacity, imperceptibility, and resistance to the latest steganalysis attacks. Therefore, there is a need for an optimized method.

II. PROPOSED METHODOLOGY

The proposed Multi-Objective Adaptive Firefly Optimized Secure Steganography (MOAFOSS) framework considers image steganography as a multi-objective optimization problem. It begins with the preprocessing of the data and the embedding of the data into the image at complex locations, which are identified using spatial features such as edges and texture. To select these optimal positions, it utilizes the FA, which enables fireflies to move in directions of increasing brightness by optimizing the fitness function to reduce MSE and increase PSNR and robustness. By choosing high-texture and edge-rich locations, it reduces image distortion and enhances security against attacks. The quality of the stego-images is measured using PSNR, MSE, embedding capacity, and robustness, showing improved results in comparison to existing techniques.

Figure 1 shows the methodology of the proposed MOAFOSS framework. In this proposed framework, the process begins with the acquisition and preprocessing of the cover images. Next, statistical features such as edge intensity, texture complexity, and intensity distribution are extracted to identify the embedding region of interest. These features are fed into the Firefly optimization module to determine the optimal embedding positions using the fitness function. The determined positions are then utilized in the adaptive LSB module to embed the secret data in their encrypted form. Finally, the stego-image is evaluated to ensure it has minimal distortion and is resistant to steganalysis attacks.

TABLE I. COMPARATIVE ANALYSIS OF EXISTING STEGANOGRAPHY-CRYPTO APPROACHES

Ref.	Methodology	Merits	Key limitations
[21]	Chaotic Lorenz–Rössler encryption with ECC and Firefly-based steganography	Multi-layer security and good imperceptibility	Higher complexity and parameter sensitivity
[22]	AES–ECC encryption with inverted LSB and WebP compression	High visual quality and secure transmission	Limited embedding optimization
[23]	PVDMF steganography optimized using IAOA variants	High PSNR and strong imperceptibility	Increased optimization complexity
[24]	CNN-CBAM attention-based steganography	Improved image quality and feature-guided embedding	High training and computation cost
[25]	Firefly optimization with blockchain for IoT routing	Energy efficiency and secure data exchange	Blockchain overhead and latency
[26]	Lightweight ECC with AEAD secure communication	Low energy secure authentication	Implementation and tuning complexity
[27]	Bio-inspired pixel correlation disruption steganography	Better imperceptibility and embedding capacity	Multiple algorithm integration increases cost
[28]	Firefly-optimized reversible DWT data hiding	High PSNR with reversible recovery	Higher processing time
[29]	RSA encryption with compression and DWT-LSB embedding	Strong security and efficient compression	Multi-stage computational overhead
[30]	YCbCr color-space steganography	Improved visual imperceptibility	Limited optimization for payload
[31]	Compression + AES + 2-LSB steganography	Multi-layer data protection	Increased computational load
[32]	ECC encryption with LSB steganography	Secure medical data transmission	Focus mainly on encryption
[33]	Multi-image hiding using LSB and DWT	Higher embedding capacity	Transform reconstruction complexity
[34]	IWT steganography with Hamming code and secret sharing	Better error resilience	Higher algorithm complexity
[35]	ML-based steganalysis using feature classification	Improved detection accuracy	Focus on detection, not embedding
[36]	AI-based QR code steganography framework	Intelligent secure QR embedding	Limited experimental validation
[37]	SPAM feature steganalysis with ensemble classifier	High detection performance	Requires large datasets and resources

A. Data Input and Preprocessing

The proposed method uses BOSSBase v1.01 [38] as input data, a widely recognized benchmark dataset in image steganography and cryptography. It was developed to facilitate standardized evaluation of steganographic and cryptographic methods. The dataset consists of 20,000 images. A two-dimensional intensity matrix is used to represent the chosen cover image:

$$I = \{ I(i,j) \mid 1 \le i \le M,\ 1 \le j \le N \} \quad (1)$$

where M and N refer to the height and width of the image, respectively, and $I(i,j) \in [0,255]$ represents the grayscale intensity value of the pixel located at position (i,j).

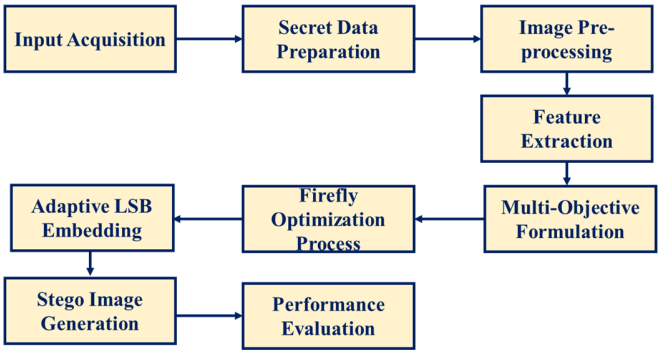

Fig. 1. Proposed methodology of the MOAFOSS framework.

For a color image, the model is extended as:

$$I = \{ I_c(i,j) \mid c \in \{ R, G, B \} \} \quad (2)$$

The image can be preprocessed before embedding, including normalization, noise filtering, or conversion to grayscale to ensure a uniform intensity distribution and better embedding stability. S is a secret message which is initially encoded into a binary sequence:

$$S = \{ s_k \mid k = 1,\ 2, \dots, L \},\ s_k \in \{0,1\} \quad (3)$$

where L is the number of bits of the secret to be embedded. The binary sequence can be optionally encrypted with a secret key K to increase the level of confidentiality by using either a symmetric or asymmetric cryptographic scheme. The encrypted stream of bits is provided by:

$$S_e = \mathrm{Enc}(S, K) \quad (4)$$

where $\mathrm{Enc}(\cdot)$ represents the encryption algorithm and S_e represents the encrypted secret information. Such an extra encryption level ensures that even if the hidden bits are decoded by an attacker, the original information cannot be retrieved without the proper key K. Therefore, this mechanism ensures the structured representation of the cover image as well as the secure preparation of the secret information before embedding through the optimization process.

B. Cover Image Feature Extraction

The statistical and structural properties of the cover image $I(i,j)$ are examined to intelligently identify the most appropriate embedding locations. The goal is to determine visually dense and statistically unpredictable areas in which secret data may be embedded with minimal perceptual distortion and detectability.

1) Edge Intensity Using Sobel Operator

Edges are the areas of high spatial variation in which the modifications are less visibly perceived by the Human Visual System (HVS). The horizontal and vertical gradients are calculated by the Sobel convolution masks:

$$G_x = I * S_x,\ G_y = I * S_y \quad (5)$$

where $*$ denotes convolution and S_x,S_y are Sobel kernels. The gradient magnitude (edge strength) at pixel (i,j) is then computed as:

$$E(i,j) = \sqrt{\{G_x(i,j)^2\}} + \sqrt{\{G_y(i,j)^2\}} \quad (6)$$

Higher values of $E(i,j)$ indicate strong edge regions, which are preferred for embedding because small pixel modifications are less perceptible in these areas.

2) Texture Complexity

Texture complexity measures the local intensity variation within a neighborhood window Ω centered at pixel (i,j). First, the local mean is computed:

$$\mu_{i,j} = \frac{1}{|\Omega|} \sum_{(m,n)\in\Omega} I(m,n) \quad (7)$$

where $|\Omega|$ is the total number of pixels in the neighborhood. Then, the local variance is computed:

$$T(i,j) = \frac{1}{|\Omega|} \sum_{(m,n)\in\Omega} \big(I(m,n) - \mu_{i,j}\big)^2 \quad (8)$$

Higher values of variance signify strong textures or complex areas. Embedding in these areas reduces the statistical impact of pixel modifications and enhances immunity to steganalysis.

3) Pixel Intensity Probability Distribution

In order to express the global statistical behavior, the probability distribution of the global gray levels is calculated using the histogram as shown below:

$$P_x = \frac{n_x}{(MN)} \quad (9)$$

where n_x is number of pixels having intensity value x, and MN is the total number of pixels. This probability distribution is subsequently used to compute entropy and Standard Deviation (SD) between cover and stego images. A homogeneous or high-entropy distribution usually indicates increased randomness and enhanced security.

C. Multi-Objective Optimization Formulation

In the suggested MOAFOSS, the steganography embedding algorithm is described as a multi-objective optimization problem. Every member of the population of fireflies is a candidate embedding pattern that is described as:

$$X = \{(i_k, j_k)\} \mid k = 1, 2, \dots, L \quad (10)$$

where (i_k, j_k) represents the position of the pixel pointing at which the k^{th} hidden secret bit is to be embedded, and L is the overall number of bits that are to be concealed. A firefly thereby encodes an entire embedding map of the secret message. The optimization problem is based on the fact that optimal pixel placement is required to minimize image distortion and achieve maximum security and randomness. The stego image $I_s(i,j)$ is produced according to the embedding specified by X, and the quality of such a candidate solution is judged using several objective functions.

1) Objective Functions

The proposed model formulates image steganography as a multi-objective optimization problem with the following objective criteria.

The first objective is to minimize the distortion between the cover image $I(i,j)$ and the stego image $I_s(i,j)$ measured by MSE:

$$\text{MSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I(i,j) - I_s(i,j)\right)^2 \quad (11)$$

A lower MSE indicates little embedding distortion. In line with this, PSNR is maximized to enhance visual quality:

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{\text{MSE}}\right) \quad (12)$$

An increase in PSNR indicates increased imperceptibility. Randomness is incorporated to improve security by using Shannon entropy:

$$H = -\sum_{x=0}^{255} P(x)\log_2 P(x) \quad (13)$$

where $P(x)$ is the probability of gray level x. An increase in entropy indicates increased statistical unpredictability. Additionally, histogram deviation between cover and stego images is minimized to enhance resistance to steganalysis:

$$D = \sum_{x=0}^{255}\left|P_I(x) - P_{I_S}(x)\right| \quad (14)$$

where $P_I(x)$ and $P_{I_S}(x)$ are the probability distributions of the cover and stego image intensities, respectively.

2) Combined Multi-Objective Fitness Function

A weighted fitness function is constructed to achieve all objectives simultaneously:

$$F(X) = w_1 \cdot \frac{1}{\text{MSE}} + w_2 \cdot \text{PSNR} + w_3 \cdot H - w_4 \cdot D \quad (15)$$

subject to:

$$w_1 + w_2 + w_3 + w_4 = 1 \quad (16)$$

where w_1, w_2, w_3, w_4 are weighting coefficients that interact to trade off imperceptibility, quality, randomness, and statistical similarity:

$$X^* = \arg\max F(X) \quad (17)$$

FA therefore represents an iterative algorithm that optimizes the candidate embedding solutions to maximize $F(X)$ to achieve a balanced trade-off between minimal distortion and maximum security.

D. Firefly Algorithm Optimization

The FA, which was proposed by Xin-She Yang, is based on the attractiveness and brightness of fireflies, whereby attractiveness is associated with brightness. In the proposed MOAFOSS model, a firefly is considered as a candidate embedding solution X_i, and its brightness represents the fitness value of the solution. The intensity of the light of the i^{th} firefly is therefore determined as:

$$I_i = F(X_i) \quad (18)$$

In the context of the multi-objective fitness $F(X_i)$ (imperceptibility, randomness, and steganalysis resistance), the higher the value of I_i, the better the embedding configuration. The attractiveness of two fireflies with respect to distance is given by the following:

$$\beta(r) = \beta_o e^{-\gamma r^2} \quad (19)$$

The Euclidean distance between the fireflies is denoted as r, the initial attractiveness at $r = 0$ is denoted as β_o, and the coefficient that regulates the speed of convergence is denoted as γ. The distance between fireflies i and j is calculated as:

$$r_{i,j} = \sqrt{\sum_{k=1}^{L}\left(x_{i,k} - x_{j,k}\right)^2} \quad (20)$$

where $x_{i,k}$ and $x_{j,k}$ are the k^{th} embedding coordinates of solution X_i and X_j, respectively. In case the brightness of a firefly j is higher than that of firefly i, i.e., $I_j > I_i$, firefly i moves toward j according to:

$$X_i^{t+1} = X_i^t + \beta_0 e^{-\gamma r_{i,j}^2}\left(X_j^t - X_i^t\right) + \alpha(\text{rand} - 0.5) \quad (21)$$

where α is the randomization parameter controlling exploration, and $\text{rand} \in [0,1]$. The second term allows exploitation toward better solutions, whereas the third term ensures stochastic global exploration to avoid premature convergence to local optima.

E. Adaptive Least Significant Bit Embedding

Once the optimum embedding positions $X^* = (i_k, j_k)$ are found during the Firefly optimization phase, a secret bit is embedded with the help of an adaptive LSB substitution strategy. The LSB of a pixel is defined as:

$$\text{LSB}(I) = I \bmod 2 \quad (22)$$

For every chosen pixel $I(i_k, j_k)$, the embedding rule alters the pixel value when the current LSB is not equal to the secret bit S_k. The value of the stego pixel is determined as:

$$I_S(i_k, j_k) = \begin{cases} I(i_k, j_k) - 1, & \text{if LSB}\left(I(i_k, j_k)\right) \neq s_k \text{ and } I(i_k, j_k) \text{ is odd} \\ I(i_k, j_k) + 1, & \text{if LSB}\left(I(i_k, j_k)\right) \neq s_k \text{ and } I(i_k, j_k) \text{ is even} \\ I(i_k, j_k), & \text{otherwise} \end{cases} \quad (23)$$

This adaptive adjustment ensures that pixel modification is limited to a maximum change of ±1, thereby minimizing distortion. Since embedding occurs primarily in edge and high-texture regions, perceptual degradation remains negligible while maintaining strong statistical security.

1) Stego Image Formation

Once all L secret bits are embedded at optimized positions X^*, the final stego image is formed as:

$$I_s = \text{Embed}(I, S_e, X^*) \quad (24)$$

where $\text{Embed}(\cdot)$ represents the adaptive LSB substitution process applied only at selected coordinates. All other pixels remain unchanged:

$$I_s(i,j) = \begin{cases} \text{Modified pixel}, & (i,j) \in X^* \\ I(i,j), & \text{otherwise} \end{cases} \quad (25)$$

2) Data Extraction

At the receiver side, extraction is performed using the same optimized pixel positions X^*. The hidden bits are retrieved as:

$$\widehat{s_k} = \mathrm{LSB}\left(I_s(i_k, j_k)\right) \quad (26)$$

The recovered encrypted bit stream is: $\widehat{S_e} = \{\widehat{s_k}\}_{k=1}^{L}$.

If encryption was applied, the original message is reconstructed using the decryption function:

$$\hat{S} = \mathrm{Dec}\left(\widehat{S_e}, K\right) \quad (27)$$

where K is the secret key. Accurate recovery is ensured as long as the stego image is not severely distorted. Figure 2 depicts the operational framework of the proposed MOAFOSS technique. It illustrates the system workflow, which includes secret data preparation, optimization-based pixel selection, adaptive embedding, and stego-image generation. This workflow highlights the combination of optimization and steganographic embedding within the proposed framework.

III. RESULTS AND DISCUSSION

The performance of the proposed MOAFOSS framework is assessed for secure and imperceptible image data hiding using standard grayscale images. This approach combines the power of Firefly-based multi-objective optimization with adaptive LSB image hiding to optimize the selection of image pixels while minimizing distortion and maintaining image quality. Performance is measured using quantitative measures like MSE, PSNR, Compression Ratio (CR), and SD. Comparative studies are conducted using optimization-based image hiding techniques such as Cuckoo Search Optimization (CSO), Bee Colony Optimization (BCO), Cat Swarm Optimization (CS), Genetic Algorithm (GA), and Particle Swarm Optimization (PSO) [27]. Additional comparisons are performed with conventional image coding and transformation techniques, including Embedded Zerotree Wavelet (EZW), Set Partitioning in Hierarchical Trees (SPIHT) [28], Huffman coding, Discrete Wavelet Transform (DWT), and Rivest–Shamir–Adleman (RSA) [29]. The results demonstrate the enhanced security performance, resilience, and imperceptibility of the suggested method.

A. Comparative Analysis of Peak Signal-to-Noise Ratio

The average PSNR values are employed to evaluate the imperceptibility level of various optimization-based steganographic techniques, as defined in (12). Based on the obtained results, it is clear that the proposed MOAFOSS method attains the highest PSNR value of 42.58 dB compared to the other techniques. Among the various existing techniques, the method based on the CSO algorithm attains the second-highest PSNR value of 40.82 dB. The GA attains a PSNR value of 40.2 dB. The PSO method offers a moderate PSNR value of 37.02 dB. However, lower PSNR values are obtained by the CS and BCO methods, with values of 34.58 dB and 34.28 dB, respectively. The comparative results with respect to PSNR are shown in Figure 3. The higher PSNR value of the proposed framework indicates that very little distortion is introduced during data embedding, thereby maintaining the similarity between the original image and the stego image. Since a PSNR value above 40 dB is generally considered excellent for imperceptibility, the results demonstrate that the proposed MOAFOSS method is effective for secure data embedding while preserving image quality.

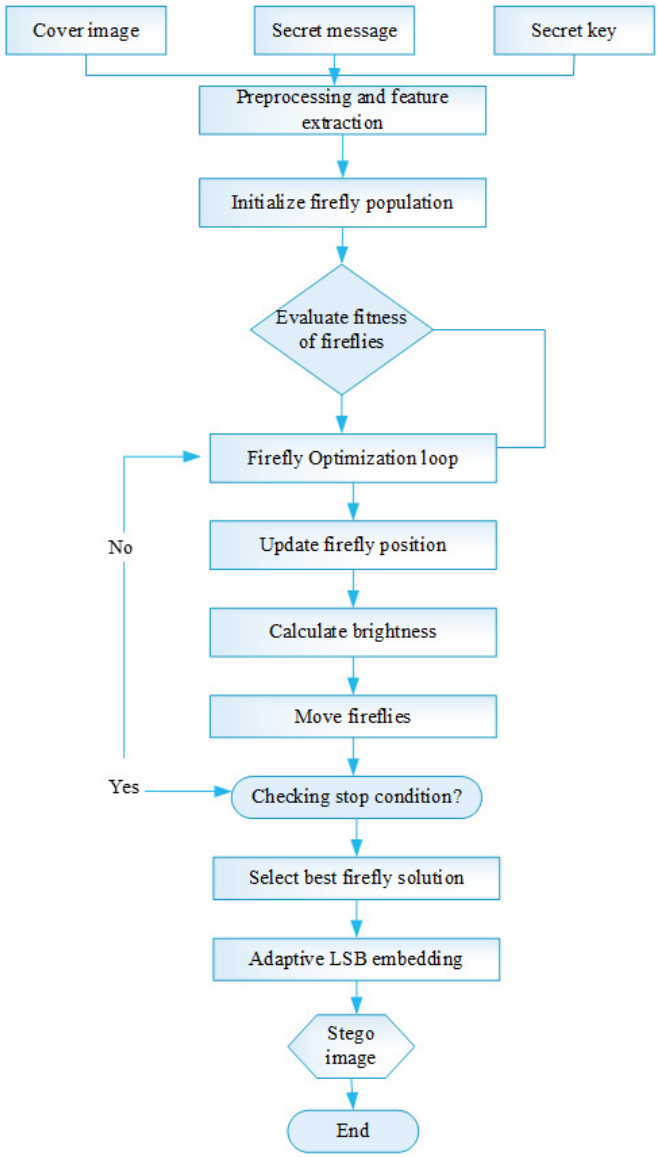

Fig. 2. Operational framework of the proposed MOAFOSS technique.

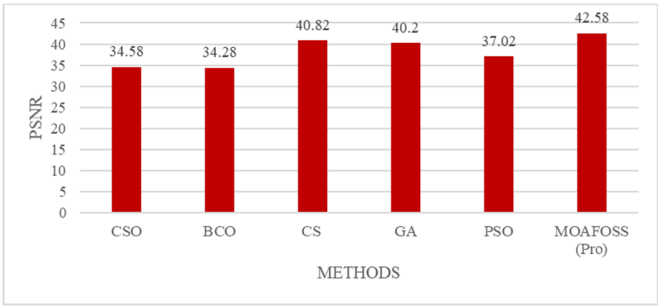

Fig. 3. Comparison of PSNR for the proposed and existing methods.

B. Comparative Analysis of Standard Deviation

SD measures the statistical variation between the cover and stego images. Lower SD values indicate greater similarity, making the stego image more difficult to detect. Among all the methods evaluated, the CS method achieves the lowest SD value of 0.384, indicating the highest level of statistical consistency. The SD value of the proposed MOAFOSS method is 0.45, which is lower than that of the GA (0.635), PSO (0.58), CSO (1.013), and BCO (0.9). This demonstrates the effectiveness of the proposed MOAFOSS technique in preserving statistical similarity between the cover and stego images. Although it does not achieve the lowest SD, it provides a balanced trade-off between security and statistical similarity, enhancing the resistance against histogram-based steganalysis attacks. Figure 4 presents the comparison of SD values for the proposed and existing methods. The mathematical expression of SD is given as:

$$SD = \sqrt{\left(\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(I(i,j)-\mu)^2\right)} \quad (28)$$

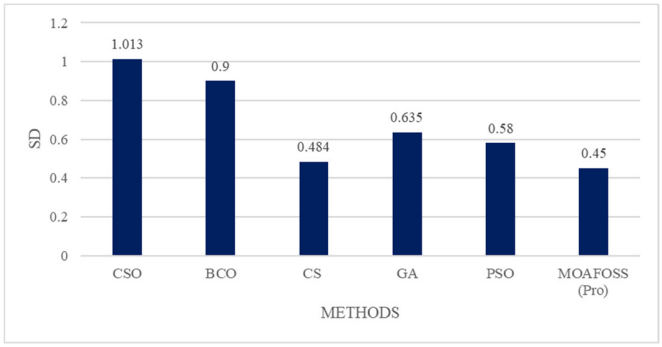

Fig. 4. Comparison of SD for the proposed and existing methods.

C. Comparative Analysis of Mean Square Error

MSE measures the distortion introduced by each embedding or compression scheme, as defined in (11). Among the evaluated methods, SPIHT exhibits the highest distortion with an MSE of 135.65, whereas EZW shows a comparatively lower value of 15.95. RSA and Huffman coding achieve much lower MSE values of 2.72 and 1.36, respectively, whereas DWT achieves a very low MSE of 0.16. The proposed MOAFOSS method achieves the lowest MSE of 0.14, outperforming all compared methods. Figure 5 presents the comparison of MSE values for MOAFOSS and the other methods.

D. Comparative Analysis of Compression Ratio

CR measures the efficiency of different embedding and compression algorithms in reducing data size while preserving information. Among the evaluated methods, SPIHT achieves a CR of 65.12%, whereas RSA, EZW, Huffman coding, and DWT achieve CR values of 37.53%, 36.56%, 35.02%, and 29.7%, respectively. The proposed MOAFOSS method outperforms all compared techniques, achieving a CR of 75.34%. This demonstrates that the proposed approach can embed a larger amount of secret information within a given image size without compromising steganographic effectiveness. Figure 6 presents the comparison of CR values for MOAFOSS and the existing methods. The CR is defined as:

$$CR = \left(\frac{S_{original} - S_{compressed}}{S_{original}}\right) \times 100 \quad (29)$$

To visually evaluate the imperceptibility of the proposed MOAFOSS method, a comparison between the cover image and the stego image is presented in Figure 7.

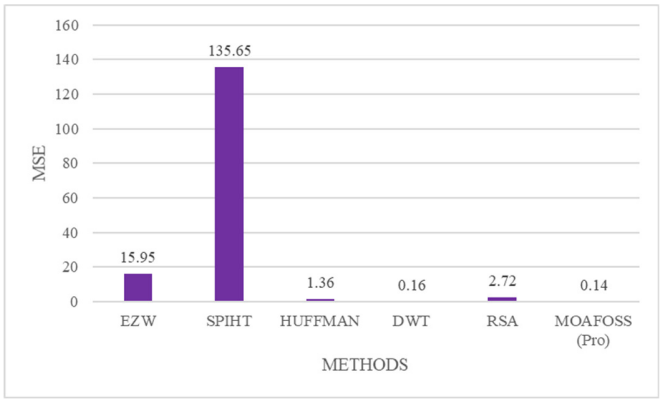

Fig. 5. Comparison of MSE for the proposed and existing methods.

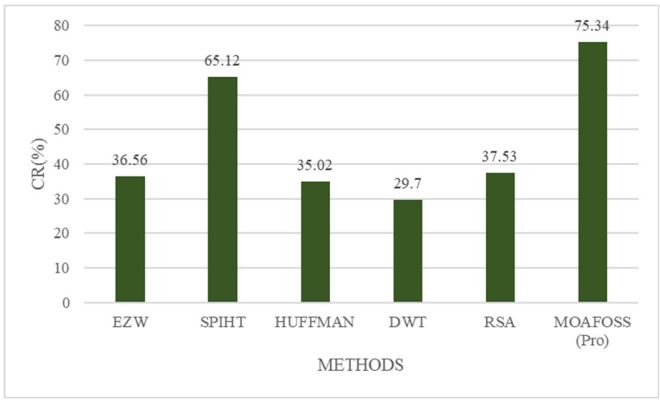

Fig. 6. Comparison of CR for the proposed and existing methods.

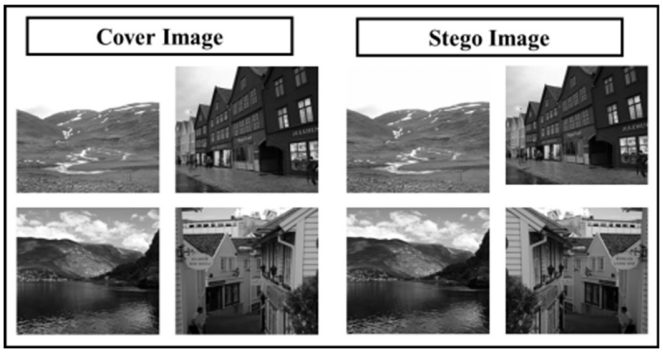

Fig. 7. Visual comparison between the original cover image and the stego image generated using the proposed MOAFOSS method.

E. Comparison with Deep Learning–Based Steganography Methods

To further demonstrate the effectiveness of the proposed framework, a comparative analysis is conducted with existing steganographic schemes based on deep learning, including Convolutional Neural Networks (CNN), Generative Adversarial Networks (GAN), and Transformer-based models. The performance evaluation is carried out using the metrics PSNR, SD, MSE, and CR (Table II). The results show that the proposed MOAFOSS method achieves superior performance with PSNR of 32.58 dB, SD of 0.45, MSE of 0.14, and CR of 75.34%. The lower values of MSE and SD indicate reduced distortion and improved statistical stability compared to CNN, GAN, and Transformer-based methods.

TABLE II. PERFORMANCE COMPARISON OF MOAFOSS WITH CNN, GAN, AND TRANSFORMER-BASED METHODS

Parameter	MOAFOSS	CNN	GAN	Transformer -based
PSNR (dB)	32.58	31.4	30.95	31.72
SD	0.45	0.52	0.58	0.49
MSE	0.14	0.21	0.27	0.19
CR (%)	75.34	68.5	66.8	70.25

F. Steganalysis Resistance Analysis

The proposed framework is also evaluated using steganalysis methods to assess the robustness of the suggested approach. In general, Regular-Singular (RS) analysis and machine learning-based techniques can detect hidden information by identifying anomalies introduced during the embedding process. In the proposed method, the Firefly optimization algorithm selects pixels in edge and texture regions, whereas the adaptive LSB embedding modifies the minimum number of pixels to preserve statistical similarity. The low standard deviation value of 0.45 indicates that only slight modifications are introduced, making the image more resistant to RS and histogram-based steganalysis attacks. The simulation results presented in Table III show that the proposed method achieves a lower detection rate compared to CNN, GAN, and Transformer-based methods, demonstrating its reliability and robustness in terms of image quality.

TABLE III. STEGANALYSIS DETECTION RATE COMPARISON OF MOAFOSS AND DEEP LEARNING–BASED STEGANOGRAPHY METHODS

Method	RS analysis detection rate (%)	ML-based detection rate (%)
CNN	14.2	12.5
GAN	11.8	10.7
Transformer-based	9.6	8.9
MOAFOSS	5.4	4.8

IV. CONCLUSION

In this paper, a novel multi-objective optimization-based steganographic framework, called Multi-Objective Adaptive Firefly Optimized Secure Steganography (MOAFOSS), is proposed for secure and imperceptible data hiding in digital images. In this approach, the distortion is minimized, the entropy is maximized, and the statistical stability is achieved using a single fitness function. The Firefly Algorithm (FA) is employed to find the optimal embedding positions, and the adaptive Least Significant Bit (LSB) technique is utilized to minimize pixel modification. The experimental results demonstrate promising performance in terms of visual quality, embedding capacity, compression efficiency, and resistance to statistical steganalysis. Although the Peak Signal-to-Noise Ratio (PSNR) is slightly compromised compared to traditional methods, the proposed approach offers enhanced security and robustness through the multi-objective optimization framework. Future work will focus on extending the framework to color images and developing hybrid optimization strategies for enhanced performance and robustness.

DECLARATION OF COMPETING INTERESTS

The authors declare no conflicts of interest.

ACKNOWLEDGMENT

The authors declare that no external funding was received for this work.

DATA AVAILABILITY

This study uses BOSSBase v1.01 [38] as the input dataset. The data supporting the findings of this study are available upon reasonable request from the corresponding author.

AI USE AND DECLARATION OF GENERATIVE AI USE

The authors confirm that this work was carried out independently and that all content is original.

REFERENCES

[1] M. Kumar, J. Aggarwal, A. Rani, T. Stephan, A. Shankar, and S. Mirjalili, "Secure video communication using firefly optimization and visual cryptography," *Artificial Intelligence Review*, vol. 55, no. 4, pp. 2997–3017, Apr. 2022, https://doi.org/10.1007/s10462-021-10070-8.

[2] P. Chinnasamy, R. Kumar Ayyasamy, K. Anuradha, I. Alam, D. M. Narayanan Nair, and A. Kiran, "Enhancing IoT Data Security: Integrating Elliptic Galois Cryptography with Matrix XOR Steganography and Adaptive Firefly Optimization," in *2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, Kirtipur, Nepal, 2024, pp. 29–33, https://doi.org/10.1109/I-SMAC61858.2024.10714687.

[3] M. Swathi, A. Punitha, K. P. Kumar, S. N. Bhukya, D. N. Reddy, and U. Hemalatha, "A Unique Method for Using Steganography and Cryptography Techniques to Secure Data in the Internet of Things (IoT)," in *Proceedings of the 12th International Conference on Frontiers in Intelligent Computing: Theory and Applications*, London, UK, 2024, pp. 493–504, https://doi.org/10.1007/978-981-96-0143-1_39.

[4] R. Vishalchandar and P. Madhavan, "Securing IoT Medical Data using Cryptography and Steganography," in *2022 International Conference on Data Science, Agents & Artificial Intelligence*, Chennai, India, 2022, pp. 1–6, https://doi.org/10.1109/ICDSAAI55433.2022.10028894.

[5] V. Elakia, M. Enush, and R. Shoba, "Improvised Secure data transfer through the use of steganography for IoT network node data security," in *2024 International Conference on Advances in Computing, Communication and Applied Informatics*, Chennai, India, 2024, pp. 1–7, https://doi.org/10.1109/ACCAI61061.2024.10602320.

[6] M. M. Hashim, J. J. Aleiwi, R. K. Ibrahim, W. R. Mohammed, and A. A. Nahi, "Concealing Secret Data in Medical Images Based on Even/Odd Pixels and PSO Algorithm for Improve Steganography System," in *2024 IEEE International Conference on Artificial Intelligence and*

Mechatronics Systems, Bandung, Indonesia, 2024, pp. 1–5, https://doi.org/10.1109/AIMS61812.2024.10513027.

[7] P. Batta, S. Ahuja, and A. Kumar, "A hybrid framework for secure data transfer for enhancing the Blockchain Security," in *2023 Seventh International Conference on Image Information Processing*, Solan, India, 2023, pp. 645–650, https://doi.org/10.1109/ICIIP61524.2023.10537655.

[8] K. Sashi Rekha, M. Joe Amali, M. Swathy, M. Raghini, and B. Priya Darshini, "A steganography embedding method based on CDF-DWT technique for data hiding application using Elgamal algorithm," *Biomedical Signal Processing and Control*, vol. 80, Feb. 2023, Art. no. 104212, https://doi.org/10.1016/j.bspc.2022.104212.

[9] K. Upendra Raju and N. Amutha Prabha, "Data hiding steganography model based on hyper chaos 2D compressive sensing inhabited with manchester encoder/decoder using circular queue exploiting modification direction," *Journal of Intelligent & Fuzzy Systems*, vol. 44, no. 6, pp. 10357–10367, June 2023, https://doi.org/10.3233/JIFS-223131.

[10] M. K. Bhatia, C. Komalavalli, and C. Laroiya, "Secure communication in Internet of Things devices using steganography," in *Next Generation Communication Networks for Industrial Internet of Things Systems*, S. Perumal, M. Tabassum, M. Sharma, and S. Mohanan, Eds. Boca Raton, FL, USA: CRC Press, 2022, ch. 9, https://doi.org/10.1201/9781003355946-9.

[11] B. B. Reddy, A. Hasan Jumaa, B. Rakesh, V. Ganna, D. Deepika, and Z. Alassedi, "Encrypting Image and Transferring Secure Data Over the Internet Using Cryptography," in *2024 International Conference on Augmented Reality, Intelligent Systems, and Industrial Automation*, Manipal, India, 2024, pp. 1–4, https://doi.org/10.1109/ARIIA63345.2024.11051599.

[12] P. Garg and R. Rama Kishore, "A robust and secured adaptive image watermarking using social group optimization," *The Visual Computer*, vol. 39, no. 10, pp. 4839–4854, Oct. 2023, https://doi.org/10.1007/s00371-022-02631-x.

[13] J. Rani, A. Anand, and S. Shivani, "SecECG: secure data hiding approach for ECG signals in smart healthcare applications," *Multimedia Tools and Applications*, vol. 83, no. 14, pp. 42885–42905, Apr. 2024, https://doi.org/10.1007/s11042-023-17049-3.

[14] B. M. Issac and S. N. Kumar, "Lifting Wavelet Transform Based Data Steganography for Health Care and Military Applications," in *First International Conference on Intelligent Computing, Smart Communication and Network Technologies*, Chennai, India, 2023, pp. 69–81, https://doi.org/10.1007/978-3-031-75957-4_7.

[15] P. Batta, S. Ahuja, and A. Kumar, "Performance Validation of Secret Data in IoT using Blockchain," in *2023 World Conference on Communication & Computing*, Raipur, India, 2023, pp. 1–6, https://doi.org/10.1109/WCONF58270.2023.10234981.

[16] S. Jaya Prakash and K. Mahalakshmi, "Improved reversible data hiding scheme employing dual image-based least significant bit matching for secure image communication using style transfer," *The Visual Computer*, vol. 38, no. 12, pp. 4129–4150, Dec. 2022, https://doi.org/10.1007/s00371-021-02285-1.

[17] S. Dhawan, R. Gupta, A. K. Rana, and S. Sharma, "Internet of Medical Things (IoMT) & Secured Using Steganography for Development of Smart Society 5.0," in *Decision Analytics for Sustainable Development in Smart Society 5.0: Issues, Challenges and Opportunities*, V. Bali, V. Bhatnagar, J. Lu, and K. Banerjee, Eds. Singapore: Springer Nature, 2022, pp. 173–189, https://doi.org/10.1007/978-981-19-1689-2_11.

[18] N. Hafsi, H. Hachimi, D. Benterki, and Y. Slimani, "Genetic-Firefly Algorithm Based Approach in Image Steganography," in *2025 11th International Conference on Optimization and Applications*, Kenitra, Morocco, 2025, pp. 1–6, https://doi.org/10.1109/ICOA66896.2025.11236921.

[19] K. Muthulakshmi and K. Valarmathi, "A secure video data streaming model using modified firefly and SVD technique," *Multimedia Systems*, vol. 30, no. 2, Mar. 2024, Art. no. 86, https://doi.org/10.1007/s00530-024-01268-1.

[20] H. Y. Naser, A. K. Mattar, M. A. Saare, M. A. Almaiah, and R. Shehab, "A Comparison of Lightweight Cryptographic Protocols for Energy-Efficient and Sustainable IoMT Authentication," *Engineering, Technology & Applied Science Research*, vol. 15, no. 4, pp. 25746–25756, Aug. 2025, https://doi.org/10.48084/etasr.12204.

[21] S. Ali and F. Anwer, "A Novel Lightweight Framework for Secure and Efficient IoT Communication Using Chaotic Cryptography and Adaptive Steganography," *IEEE Transactions on Dependable and Secure Computing*, 2025, https://doi.org/10.1109/TDSC.2025.3648316.

[22] A. Badhan and S. S. Malhi, "Enhancing Data Security and Efficiency: A Hybrid Cryptography Approach (AES + ECC) Integrated with Steganography and Compression Algortihm," in *2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things*, Bengaluru, India, 2025, pp. 450–456, https://doi.org/10.1109/IDCIOT64235.2025.10914830.

[23] L. Akhila and V. J. Manoj, "PVDMFWO: a novel steganographic method using PVDMF and optimization," *International Journal of Computers and Applications*, vol. 47, no. 5, pp. 438–458, May 2025, https://doi.org/10.1080/1206212X.2025.2484763.

[24] G. S. Kumar, K. Sethi, P. Subudhi, and P. Joshi, "Securing patient data in IoT-enabled medical imaging: A steganographic approach," in *IoT Security*, S. H. Islam, D. Samanta, A. K. Pal, and U. Iqbal, Eds. Cambridge, MA, USA: Academic Press, 2026, pp. 53–71, https://doi.org/10.1016/B978-0-443-34125-0.00025-8.

[25] K. Nagarathna, K. K S, N. Krishnan, Dhananjeyan. S, S. Srikanth, and T. Geetha, "IoT Driven Wireless Sensor Network Routing Optimization using Improved Firefly Algorithm and Block Chain Technology," in *2025 International Conference on Intelligent Computing and Knowledge Extraction*, Bengaluru, India, 2025, pp. 1–6, https://doi.org/10.1109/ICICKE65317.2025.11136475.

[26] H. Yi, Q. Jiang, H. Huang, L. Tang, S. Yao, and X. Jin, "MDL-Net: Multi-task Learning Network for Face Forgery Detection and Localization Using Dual-Stream Feature Extraction and Reconstruction," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2026, https://doi.org/10.1109/TBIOM.2026.3656922.

[27] S. Rezaei and A. Javadpour, "Bio-Inspired algorithms for secure image steganography: enhancing data security and quality in data transmission," *Multimedia Tools and Applications*, vol. 83, no. 35, pp. 82247–82280, Oct. 2024, https://doi.org/10.1007/s11042-024-18776-x.

[28] S. Sharma and H. Patil, "Secure data hiding scheme using firefly algorithm with hidden compression," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 23, no. 2, pp. 525–534, Feb. 2020, https://doi.org/10.1080/09720529.2020.1729502.

[29] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques," *IEEE Access*, vol. 9, pp. 31805–31815, 2021, https://doi.org/10.1109/ACCESS.2021.3060317.

[30] S. Alharthi and A. Gutub, "Adjusting image stego practicality via YCbCr color space formation," *Journal of Engineering Research*, vol. 14, no. 1, pp. 756–764, Mar. 2026, https://doi.org/10.1016/j.jer.2025.07.008.

[31] N. Alanizy, A. Alanizy, N. Baghoza, M. AlGhamdi, and A. Gutub, "3-Layer PC Text Security via Combining Compression, AES Cryptography 2LSB Image Steganography," *Journal of Research in Engineering and Applied Sciences*, vol. 3, no. 4, pp. 118–124, Oct. 2018, https://doi.org/10.46565/jreas.2018.v03i04.001.

[32] E. S. B. Hureib and A. A. Gutub, "Enhancing Medical Data Security via Combining Elliptic Curve Cryptography and Image Steganography," *International Journal of Computer Science and Network Security*, vol. 20, no. 8, pp. 1–8, Aug. 2020, https://doi.org/10.22937/IJCSNS.2020.20.08.1.

[33] A. Gutub and F. Al-Shaarani, "Efficient Implementation of Multi-image Secret Hiding Based on LSB and DWT Steganography Comparisons," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 2631–2644, Apr. 2020, https://doi.org/10.1007/s13369-020-04413-w.

[34] Z. Saeidi, A. Yazdi, S. Mashhadi, M. Hadian, and A. Gutub, "High performance image steganography integrating IWT and Hamming code within secret sharing," *IET Image Processing*, vol. 18, no. 1, pp. 129–139, Jan. 2024, https://doi.org/10.1049/ipr2.12938.

[35] A. Aljarf, H. Zamzami, and A. Gutub, "Integrating machine learning and features extraction for practical reliable color images steganalysis

classification," *Soft Computing*, vol. 27, no. 19, pp. 13877–13888, Oct. 2023, https://doi.org/10.1007/s00500-023-09042-7.

[36] N. A. Roslan, M. S. Lydia, and A. Gutub, "Enhancing Secure QR Code Steganography through Artificial Intelligence: A Conceptual Framework," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 62, no. 4, pp. 224–231, Sept. 2026, https://doi.org/10.37934/araset.62.4.224231.

[37] J. Hemalatha, M. Sekar, C. Kumar, A. Gutub, and A. K. Sahu, "Towards improving the performance of blind image steganalyzer using third-order SPAM features and ensemble classifier," *Journal of Information Security and Applications*, vol. 76, Aug. 2023, Art. no. 103541, https://doi.org/10.1016/j.jisa.2023.103541.

[38] "BOSSbase 1.01." Digital Data Embedding Laboratory, Binghamton University, [Online]. Available: https://dde.binghamton.edu/download/.