

A Minimax-Based Deep Learning Framework for Secure IoT Communication via Steganography

Sharath Babu CG^{1*}, Dr. Komala K²

¹Research Scholar, Assistant Professor, Department of Computer Science and Engineering, SSIT, Sri Siddhartha Academy of Higher Education, Tumkur, Karnataka - 572105.

E-mail: sharathbabucg@ssit.edu.in

²Associate Professor, Department of Electronics and Communication Engineering, SSIT, Sri Siddhartha Academy of Higher Education, Tumkur, Karnataka - 572105.

E-mail: komalak@ssit.edu.in

Abstract

The rapid expansion of Internet of Things (IoT) deployments has intensified the demand for secure and imperceptible communication methods capable of protecting sensitive information on lightweight devices. Conventional cryptographic techniques, while important, cannot independently provide the level of concealment and reliability required in constrained IoT environments. Many existing steganography and deep learning-based techniques offer partial solutions but still struggle with visual distortion, low embedding efficiency, and limited resilience to attacks. To address these limitations, this work introduces DLSIS, a deep learning-enabled steganography model enhanced with an Optimized Dragonfly Algorithm (ODA) for adaptive pixel selection. The framework employs a convolutional encoder-decoder and 2-bit LSB substitution to embed information effectively while preserving image quality. Experimental evaluation using standard image datasets shows that DLSIS achieves a PSNR of 55.3 dB and consistently surpasses prior methods. These results establish DLSIS as a reliable and efficient approach for secure data transmission and authentication in IoT systems.

Keywords: DLSIS, IoT security, image steganography, deep learning, Dragonfly Algorithm, PSNR

1. Introduction

The rapid expansion of the Internet of Things (IoT) has transformed how modern systems sense, communicate, and make autonomous decisions across sectors such as healthcare, industrial automation, transportation, and smart cities [1], [2]. As billions of IoT devices continuously capture and transmit sensitive information—including authentication credentials, physiological readings, and user identifiers—the security of these communications has become a critical concern [3], [4]. Although cryptographic methods provide strong protection, they often introduce computational overhead and reveal the presence of encrypted data, which is unsuitable for resource-constrained IoT devices [5]. These limitations have increased interest in image steganography, where confidential information is concealed within visual media to ensure security through imperceptibility [6].

Artificial Intelligence (AI), especially Machine Learning (ML) and Deep Learning (DL), has further influenced steganographic research by enabling adaptive embedding and resistance to steganalysis attacks [7], [8]. ML-based methods optimize embedding rules and improve detection resistance, while DL-based models—particularly convolutional architectures—enable feature-aware embedding and high-quality reconstruction [9]. Despite these advantages, many existing approaches struggle to strike a balance between embedding capacity, imperceptibility, robustness, and computational efficiency, all of which are critical for IoT deployment [10]. Methods that increase payload size tend to create visible distortions, whereas techniques that prioritize visual quality often reduce payload capacity [11], [12]. In addition, embedding processes based on sequential or predictable pixel patterns generate detectable artifacts that weaken system security against modern steganalysis tools [13].

Recent studies highlight both the progress and limitations of current AI-driven steganography [5]-[14]. Coverless approaches, including generative methods that synthesize camouflage images from secret data, demonstrate high imperceptibility but require large datasets and heavy computation, limiting their practicality in IoT settings [14]. Autoencoder-based steganography improves reconstruction fidelity but

often suffers from restricted payload size and vulnerability under channel noise [12], [13], [14]. Lightweight adversarial embedding techniques support identity-based authentication and tamper detection but may lack sufficient randomness to resist advanced attacks [7], [10]. Reversible or invertible models improve recoverability and noise suppression, though their multi-stage architectures increase complexity and reduce scalability for low-power IoT nodes [12], [13]. Medical imaging steganography frameworks have shown strong robustness within IoMT applications; however, their specialized designs limit applicability in broader IoT environments [1], [14].

Other hybrid models focus on maximizing security by integrating compression, encryption, QR coding, or multi-layer embedding [13], [14]. While these techniques enhance robustness, they often introduce significant computational cost. Spatial–frequency fusion approaches and edge-driven embedding strategies achieve better PSNR and SSIM values but still lack intelligent pixel selection mechanisms required to counter adaptive steganalysis [12], [14]. Evolutionary algorithms such as Adaptive Particle Swarm Optimization (APSO) have been used for pixel optimization, yet they frequently converge prematurely and yield suboptimal embedding distributions [13], [14].

The limitations in existing literature indicate that current AI-based steganographic systems cannot simultaneously achieve high capacity, strong imperceptibility, and resilience under noisy IoT channels while maintaining low computational complexity [14]. Moreover, many deep-learning methods do not incorporate global optimization strategies, resulting in redundant embedding and weaker resistance to detection [12]–[14].

To address these challenges, this study proposes the Dragonfly-based Deep Learning Steganography for IoT Security (DLSIS) framework, which integrates CNN-based encoder–decoder learning with an Optimized Dragonfly Algorithm (ODA) for adaptive pixel selection [26]. The ODA module performs multi-objective optimization to maximize payload capacity, enhance visual fidelity, and maintain randomness in embedding patterns, while the CNN encoder–decoder ensures reliable feature extraction and robust data recovery even under compression, noise, or adversarial distortions [14]. A 2-bit Least Significant Bit (2-LSB) substitution mechanism is adopted to retain high payload size without compromising image quality [13], [14]. Through the coordinated use of DL-driven learning and swarm-based optimization, the proposed approach achieves near-lossless imperceptibility, high extraction accuracy, scalability across IoT environments, and improved resistance to statistical and deep-learning-based steganalysis attacks [14].

The remainder of the paper presents the technical depth and experimental validation of DLSIS. Section II provides a detailed explanation of the proposed methodology. Section III presents performance evaluation and comparative analysis, followed by conclusions and future enhancements in Section IV.

2. Methodology

The rapid expansion of the Internet of Things (IoT) has intensified the need for lightweight security mechanisms that ensure authentication, integrity, and privacy during device-to-device communication. As billions of IoT nodes continuously transmit sensitive information, these exchanges become susceptible to interception, manipulation, and other forms of malicious interference. Traditional cryptographic techniques, although essential, are often insufficient by themselves because they do not guarantee imperceptibility and may impose computational burdens that exceed the capabilities of constrained IoT hardware. This has led to growing interest in steganography as a complementary method for concealing confidential data within innocuous media.

In this work, we introduce DLSIS, an enhanced steganographic framework that integrates an Optimized Dragonfly Algorithm (ODA) to determine suitable pixel positions within a cover image for data embedding. Unlike conventional strategies that rely on sequential or random pixel selection, the ODA module performs adaptive and intelligent positioning based on a multi-objective fitness evaluation, ensuring both security and robustness. To maintain visual quality and minimize noticeable distortions, the model employs a 2-LSB substitution strategy for embedding the secret information. The proposed DLSIS framework is further reinforced with a deep-learning-based authentication component, enabling secure and reliable operation within IoT environments.

The working of Deep learning-based secured image steganography (DLSIS) Scheme is presented in Algorithm 1. The DLSIS framework integrates an optimized dragonfly-based search mechanism with convolution-driven feature learning to achieve secure and imperceptible image steganography for IoT environments. The unified algorithm combines both embedding and extraction processes, enabling a

complete end-to-end model for hiding and retrieving confidential information. The workflow begins by transforming the secret message into an 8-bit binary format so that each character can be efficiently mapped into the image's least significant bits. The cover image is reshaped into a single-dimensional form, which simplifies pixel-level manipulation during optimization.

The core of DLSIS is the Optimized Dragonfly Algorithm (ODA), which intelligently selects pixel positions for embedding. Instead of relying on random or sequential placement, ODA simulates swarm intelligence behaviors—separation, alignment, cohesion, attraction to optimal regions, and avoidance of poor search areas. These forces collectively balance exploration and exploitation, preventing premature convergence while steadily guiding the search toward pixel locations that minimize perceptual distortion. Each candidate solution (dragonfly) is evaluated using a multi-objective fitness function that considers embedding capacity, structural similarity (SSIM), and entropy-based randomness. This ensures that the chosen embedding pattern simultaneously supports high payload, strong visual quality, and resistance against statistical attacks.

Algorithm 1. Deep learning-based secured image steganography (DLSIS) Scheme

Input: Cover image Q_c of size $W \times H \times 3$, secret message M_{text}

Output: Stego image Q'_s and recovered message M_{rec}

Step 1: Start

Step 2: Convert M_{text} into binary stream M_{bin} using 8-bit ASCII

Step 3: Compute message length $ML = 8n$

Step 4: Flatten Q_c into 1-D array img_{flat}

Step 5: Initialize ODA swarm (positions, velocities, parameters)

Step 6: For each iteration $t = 1 \dots T$:

 Compute separation S_i , alignment A_i , cohesion $C_{h,i}$

 Compute food attraction F_i and enemy distraction $E_{d,i}$

 Update velocity using

$$V_i^{t+1} = wV_i^t + sS_i + aA_i + cC_{h,i} + fF_i + eE_{d,i}$$

 Update position using

$$P_i^{t+1} = clip(P_i^t + V_i^{t+1}, 0, 1)$$

 Evaluate fitness $f(C, SSIM_{avg}, E)$

 Update personal and global best

End For

Step 7: Obtain global best embedding positions P_{global}

Step 8 (Embedding):

For each pixel p where $P_{global}[p] = 1$:

 Extract 2 bits from M_{bin}

 Replace pixel using $Q'_p = (Q_p \& \sim 3) \mid s$

Reshape modified array to form stego image Q'_s

Step 9 (Extraction):

Flatten Q'_s

For each pixel p where $P_{global}[p] = 1$:

 Extract 2 bits using $e = Q'_p \& 3$

Append to extraction stream EM_{bin}

Step 10: Convert every 8 bits of EM_{bin} to characters to obtain M_{rec}

Step 11: End

Once ODA identifies the optimal embedding indices, the algorithm performs 2-LSB substitution on selected pixels. This lightweight modification method provides a high-capacity channel for inserting secret bits with minimal effect on image appearance. The modified pixel array is then reconstructed into a stego image, which preserves the original structure and visual characteristics of the cover image. The extraction phase mirrors the embedding process. Using the same global best positions obtained during optimization, the algorithm isolates the two least significant bits from each chosen pixel. These retrieved bits are reassembled and converted back into text, enabling accurate message recovery even in noisy IoT communication scenarios. Because the embedding positions are optimally chosen and structurally robust, the hidden

message can be reconstructed with high reliability. Overall, DLSIS provides an efficient, secure, and IoT-compatible solution for concealing authentication tokens or sensitive sensor data within images, offering a practical method for enhancing confidentiality and integrity in distributed networks.

3. Results and Discussion

The experimental assessment of the proposed DLSIS was carried out on a system powered by an Intel Core i7 processor with Intel Iris Xe graphics and 16 GB RAM, using Python 3.11 and standard libraries for deep learning and image processing. To evaluate embedding quality and robustness, the USC-SIPI image dataset [15] was selected due to its broad variety of grayscale and color images. Following earlier studies such as ParticleStego [14], color images of 512×512 pixels were chosen and uniformly resized to 256×256×3 to align with the encoder–decoder structure while reducing computational load. Figure 1 shows representative samples—including Airplane, Mandrill, and Peppers—which offer diverse textures and color characteristics suitable for thorough performance validation.

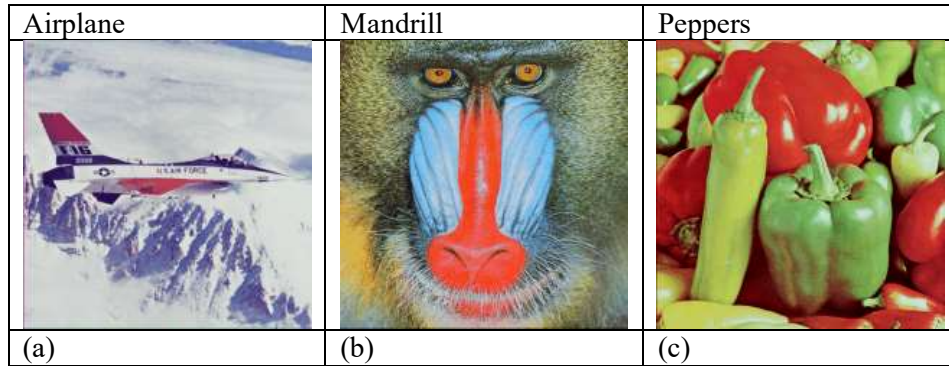


Figure 1. Sample images from dataset used for evaluation of DLSIS.

A. Performance Metrics

To assess the visual quality of stego images generated by DLSIS, Peak Signal-to-Noise Ratio (PSNR) was employed as the primary evaluation metric. PSNR measures the level of distortion introduced during embedding and is mathematically expressed as:

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

where 255 represents the maximum pixel intensity for an 8-bit image and MSE reflects the difference between the original and the stego image.

B. DLSIS Evaluation

DLSIS was evaluated on the USC-SIPI dataset [15], which provides a broad range of images with varied textural complexity. Representative outputs for Airplane, Mandrill, and Peppers are illustrated in Figure 2. A visual review of these results shows that the stego images retain their natural appearance, indicating that the embedding operation does not introduce noticeable artifacts.

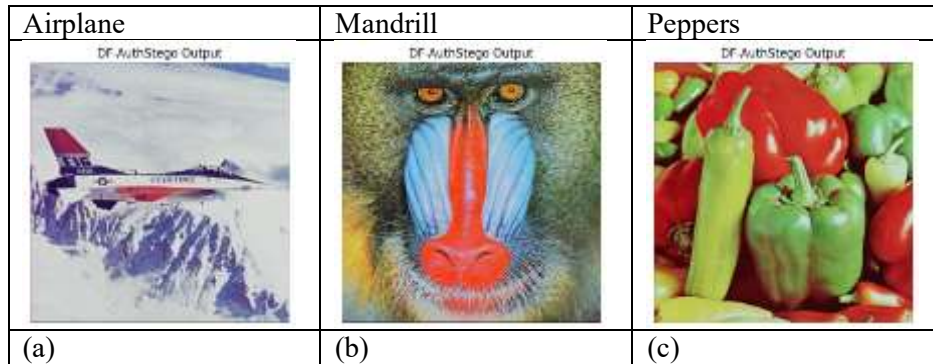


Figure 2. DLSIS Visual Output.

Further analysis using PSNR presented in Figures 1 shows consistently high values exceeding 55 dB for all test samples. Such values indicate that the embedding process introduces extremely small perturbations, reinforcing the imperceptibility of the hidden content. These results confirm that DLSIS maintains strong visual quality while supporting secure information concealment—an essential requirement for IoT-based communication.

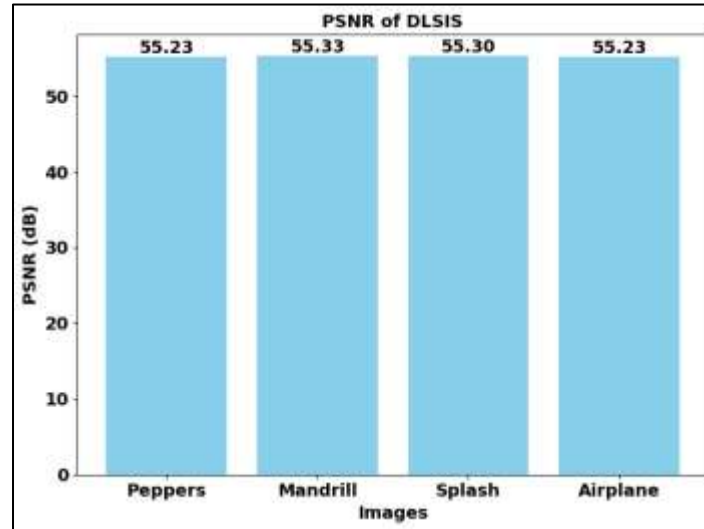


Figure 3. PSNR of DLSIS on different images from USC-SIPI image dataset.

C. Comparative Study

A comparative assessment was conducted to evaluate how DLSIS performs relative to earlier steganography approaches. Table 1 compares DLSIS with the APSO-based method in [14] under different payload conditions. Across images such as Peppers, Mandrill, and Airplane, DLSIS consistently records higher PSNR values. For example, for the Peppers image with a payload of 81584 bits, DLSIS achieves 57.2 dB, significantly higher than the 51.14 dB reported in [14]. Similar improvements—typically in the range of 5–12 dB—were observed for the other images. These gains indicate that the proposed method produces stego images with substantially lower visible distortion.

Table 1. Comparative Study with different payloads.

Image	Payload	Ref [24] PSNR	DLSIS PSNR
Peppers	81584	51.1464	57.2
Mandrill	—	51.2486	57.3
Airplane	—	51.1046	57.2

Table 2 extends this comparison by evaluating DLSIS against other AI-based and traditional steganography approaches. Methods such as [10], and [13] report PSNR values between 31 dB and 40 dB, whereas DLSIS achieves an average of 55.3 dB. Even advanced frameworks like [14], which produce PSNR values above 48 dB, fall short of the performance achieved by DLSIS. These findings highlight the advantage of incorporating an optimized Dragonfly-based pixel selection mechanism along with a CNN-driven encoder–decoder. The joint optimization strategy effectively minimizes detectable distortions, enabling high-quality stego image generation suitable for secure IoT environments.

Table 2. Comparative Study with existing steganography approaches.

Ref	PSNR
[10]	39.85
[13]	39.02
[14]	48.37
DLSIS [Proposed]	55.3

Overall, the comparative study demonstrates that DLSIS provides substantially higher PSNR than existing steganography approaches, ensuring minimal embedding distortion while supporting large payloads. These characteristics make DLSIS a strong candidate for IoT-based secure communication, where the concealment of sensitive information must occur without compromising visual quality or drawing attention to the transmission process.

4. Conclusion

This study introduced DLSIS, a deep learning-driven steganography and authentication model developed to enhance secure communication in IoT environments. The work emphasized the growing need for reliable embedding methods due to rising threats such as forgery and steganalysis. Many existing schemes struggle to balance capacity, imperceptibility, and security, leaving a clear gap in achieving all three simultaneously. DLSIS was designed to overcome these limitations by enabling high-quality embedding and accurate recovery using a DL-based encoder–decoder framework. Experiments conducted on the USC-SIPI dataset show that the model attains a PSNR of 55.3 dB, surpassing earlier methods and offering stronger robustness. Future enhancements may incorporate integrity-verification components to ensure tamper resistance in dynamic IoT communication settings.

REFERENCES

- [1] W. Wen, H. Huang, S. Qi, Y. Zhang and Y. Fang, "Joint Coverless Steganography and Image Transformation for Covert Communication of Secret Messages," in *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 3, pp. 2951-2962, May-June 2024, doi: 10.1109/TNSE.2024.3354941.
- [2] H. K. Channi, "Real-Time Applications of Deep Learning-Based Steganography in IoT Networks," *Advances in information security, privacy, and ethics book series*, pp. 331–360, Jul. 2024, doi: 10.4018/979-8-3693-2223-9.ch015.
- [3] X. Li, L. Chen, J. Jia, Z. Qin and Z. Fu, "A Lightweight Image Forgery Prevention Scheme for IoT Using GAN-Based Steganography," in *IEEE Transactions on Industrial Informatics*, vol. 21, no. 1, pp. 167-177, Jan. 2025, doi: 10.1109/TII.2024.3449995.
- [4] L. Zhang, Y. Lu and G. Lu, "Contrastive Noise-Guided Invertible Network for Image Steganography," in *IEEE Transactions on Consumer Electronics*, vol. 71, no. 1, pp. 673-685, Feb. 2025, doi: 10.1109/TCE.2024.3509479.
- [5] K. Chen, Y. Chen, G. Coatrieux, J. Wu and J. -L. Coatrieux, "Restoration-Enhanced Reversible Information Steganography Network for CT Images in the Internet of Medical Things," in *IEEE Transactions on Instrumentation and Measurement*, vol. 74, pp. 1-15, Feb. 2025, Art no. 4011615, doi: 10.1109/TIM.2025.3542878.
- [6] Y. Sanjalawe, S. Al-E'mari, S. Fraihat, M. Abualhaj, and E. Alzubi, "A deep learning-driven multi-layered steganographic approach for enhanced data security," *Scientific Reports*, vol. 15, no. 1, Feb. 2025, doi: 10.1038/s41598-025-89189-5.
- [7] A. Liguori, M. Zuppelli, D. Gallo, M. Guarascio, and Luca Caviglione, "A deep learning-based approach for stegomalware sanitization in digital images," *Journal of Intelligent Information Systems*, Apr. 2025, doi: 10.1007/s10844-025-00936-6.
- [8] P. Ji, Y. Zhang, and Z. Lv, "Edge-Guided Dual-Stream U-Net for Secure Image Steganography," *Applied Sciences*, vol. 15, no. 8, p. 4413, Apr. 2025, doi: 10.3390/app15084413.
- [9] B. Kallapu *et al.*, "Multi-Layered Security Framework Combining Steganography and DNA Coding," *Systems*, vol. 13, no. 5, p. 341, May 2025, doi: 10.3390/systems13050341.
- [10] R. Al-Rawashdeh, M. M. Rahman and M. Niazi, "Robust Image Steganography Approach Based on Edge Detection Combined With CNN Algorithm," in *IEEE Access*, vol. 13, pp. 109099-109115, June. 2025, doi: 10.1109/ACCESS.2025.3582159.
- [11] K. R. Malik *et al.*, "A hybrid steganography framework using DCT and GAN for secure data communication in the big data era," *Scientific Reports*, vol. 15, no. 1, Jun. 2025, doi: 10.1038/s41598-025-01054-7.

- [12] Y. M. Younis, R. J. Mstafa, and Shamal AL-Dohuki, "AttenHideNet: A novel deep learning-based image steganography method using a lightweight U-net with soft attention," *Applied Soft Computing*, vol. 182, pp. 113583–113583, Jul. 2025, doi: 10.1016/j.asoc.2025.113583.
- [13] B. M. Issac, S. N. Kumar, S. Zafar, K. A. Shakil, and M. A. Wani, "Deep learning steganography for big data security using squeeze and excitation with inception architectures," *Scientific Reports*, vol. 15, no. 1, Aug. 2025, doi: 10.1038/s41598-025-16394-7.
- [14] S. Mukherjee, S. Mukhopadhyay and S. Sarkar, "ParticleStego: A Steganographic Algorithm for Securing Consumer Electronics Enabled Social Internet of Things (SIoT)," in *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 2592-2602, May 2025, doi: 10.1109/TCE.2025.3574628.
- [15] "SIPI Image Database," *Usc.edu*, 2025.
<https://sipi.usc.edu/database/database.php?volume=misc> (accessed Sep. 05, 2025).
- [16] M. Driss, L. Berriche, S. B. Atitallah and S. Rekik, "Steganography in IoT: A Comprehensive Survey on Approaches, Challenges, and Future Directions," in *IEEE Access*, vol. 13, pp. 74844-74875, 2025, doi: 10.1109/ACCESS.2025.3564120.
- [17] Yu Ren, Di Xiao, Lvjun Chen, Min Li, ACPP-MIH: A robust multiple image hiding framework with adaptive cover image privacy protection, *Expert Systems with Applications*, Volume 288, 2025, 128152, <https://doi.org/10.1016/j.eswa.2025.128152>.