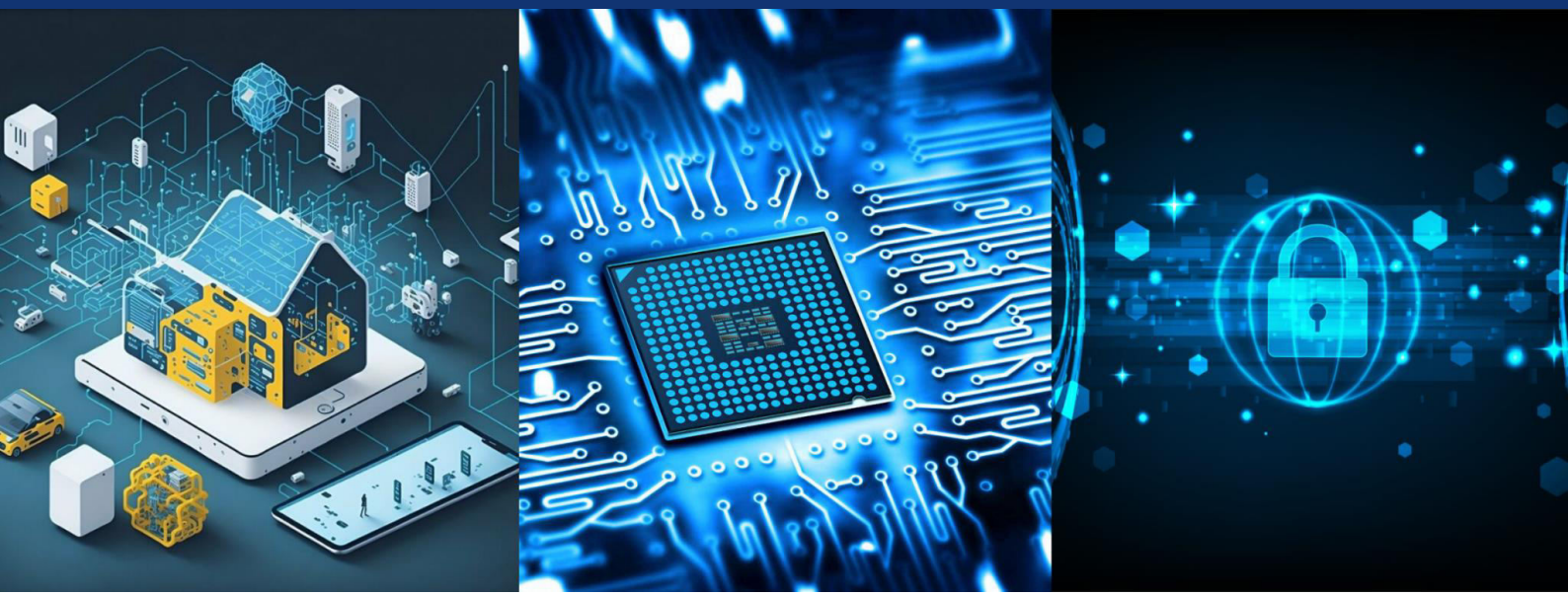
IJIRCCE

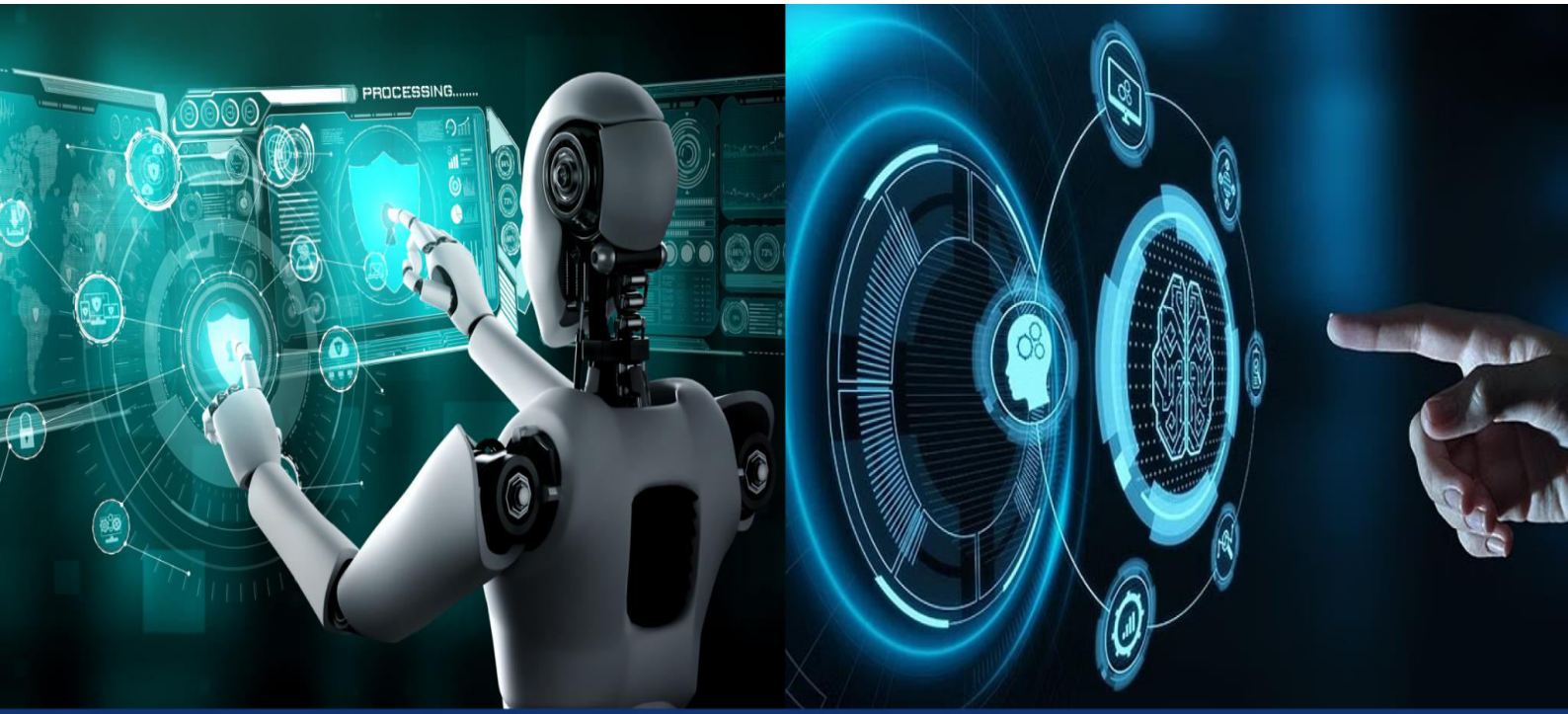
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 5, May 2026

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405112

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Enhanced Secure Image Steganography Using Adaptive LSB and XOR Encryption in Embedded C

Adhyapak Amit, Sarang Thorbole, Bhoodatt Kishor, Aishwarya Dudhanikar, Rajesham Tumma, Prof. S.M.Kamble

Department of Electronics & Telecommunication, V.V.P. Institute of Engineering & Technology, Solapur. Maharashtra, India

ABSTRACT: Image steganography is a data hiding technique that enables secure communication by concealing confidential information within digital images. This paper presents an image steganography system based on the Least Significant Bit (LSB) substitution method implemented using the C programming language. The proposed approach embeds secret text data into the least significant bits of image pixels, ensuring minimal visual distortion while maintaining the quality of the cover image. The embedding process converts the secret message into binary format and systematically inserts the data into selected pixel locations, whereas the extraction process retrieves the hidden information by reading the modified bits from the stego image. Experimental evaluation demonstrates that the proposed method successfully hides and recovers secret data with high accuracy and negligible impact on image quality. The technique offers low computational complexity, efficient memory utilization, and ease of implementation, making it suitable for lightweight and real-time secure communication applications. The proposed system can be applied in confidential data transmission, digital authentication, copyright protection, and information security systems.

KEYWORDS: Image Steganography, Least Significant Bit (LSB), Data Hiding, Information Security, Stego Image, Embedded C, Secure Communication, Digital Image Processing.

I. INTRODUCTION

The rapid growth of digital communication and internet-based services has increased the need for secure transmission of sensitive information. Confidential data exchanged through public networks is vulnerable to unauthorized access, interception, and cyberattacks. Traditional security mechanisms such as cryptography protect the content of information by transforming it into an unreadable format. However, encrypted data may attract the attention of attackers because its presence is evident. To address this limitation, steganography provides an additional layer of security by concealing the existence of secret information within a digital medium. Image steganography is one of the most widely used forms of steganography due to the large amount of redundant information available in digital images. It enables secret messages to be embedded within image pixels while preserving the visual appearance of the original image. Among various image steganography techniques, the Least Significant Bit (LSB) method is widely adopted because of its simplicity, high embedding capacity, and low computational complexity. In the LSB approach, the least significant bits of image pixels are modified to store secret data, resulting in minimal perceptible changes to the cover image.

Despite its advantages, conventional LSB-based steganography faces challenges related to security and robustness. Hidden information may become vulnerable to steganalysis attacks, image manipulation, or unauthorized extraction if the embedding process is predictable. Therefore, designing an efficient and secure data hiding mechanism remains an important research problem in information security. This paper presents an image steganography system based on the LSB technique implemented using the C programming language. The proposed system embeds secret textual information into digital images through bit-level manipulation and retrieves the hidden data using a corresponding extraction process. The implementation focuses on maintaining image quality while ensuring accurate recovery of the embedded message. Experimental results demonstrate the effectiveness of the proposed approach in achieving secure data hiding with minimal visual distortion and low computational overhead.

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405112

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The major contributions of this work are as follows:

1. Development of an LSB-based image steganography system using C programming.
2. Efficient embedding and extraction of secret information through bitwise operations.
3. Preservation of image quality after data embedding.
4. Evaluation of the proposed method in terms of data recovery accuracy and computational efficiency.

The remainder of this paper is organized as follows. Section II presents the related work and literature review. Section III describes the proposed methodology and system architecture. Section IV discusses the implementation details and experimental setup. Section V presents the results and performance analysis. Finally, Section VI concludes the paper and outlines future research directions.

II. RELATED WORK AND LITERATURE SURVEY

Recent advancements in image steganography have focused on improving embedding capacity, imperceptibility, robustness, and resistance against steganalysis attacks. Traditional Least Significant Bit (LSB) methods remain popular due to their simplicity and low computational complexity; however, researchers have increasingly explored adaptive embedding, chaotic encryption, edge-based methods, and deep learning techniques to enhance security and performance. Table I summarizes recent contributions in the field.

TABLE I. RECENT LITERATURE SURVEY ON IMAGE STEGANOGRAPHY (2023–2026)

Ref.	Year	Author(s)	Technique / Method	Key Contribution	Limitation
[1]	2023	Chen et al.	Iterative Neural Optimization	Improved payload recovery with neural optimization	High computational cost
[2]	2023	Kheddar et al.	Deep Learning Steganalysis Review	Comprehensive review of DL-based steganalysis	Survey only
[3]	2024	Song et al.	Deep Learning-Based Image Steganography Survey	Categorized modern DL steganography architectures	No implementation
[4]	2024	Hu et al.	Learning-Based Steganography & Watermarking	Comparative analysis of neural architectures	Complex training process
[5]	2024	Khalil et al.	LSB + Chaotic Map + Tabu Search	Enhanced security and embedding efficiency	Increased algorithm complexity
[6]	2024	Luo et al.	Digital Image Steganography Survey	Detailed analysis of steganography and steganalysis methods	Survey-based study
[7]	2024	Rehman	GAN-Based Steganography	Improved PSNR and resistance to detection	Requires large datasets
[8]	2025	Panigrahi et al.	LSB-Based Secure Image Hiding	User-friendly LSB implementation with secure extraction	Traditional LSB limitations
[9]	2025	Aljarf et al.	DL-Steg Framework	Combined SAE and LSTM for secure image hiding	High training overhead
[10]	2025	Issac et al.	SE-Inception Residual Network	Secure medical image transmission	Deep learning resource intensive
[11]	2025	Zhou et al.	Latent Representation Steganography	Improved embedding efficiency using latent features	Complex architecture
[12]	2025	Rahman et al.	Enhanced LSB Steganography	Improved security and tamper resistance	Vulnerable to advanced steganalysis
[13]	2025	Alrusaini et al.	Deep Learning Steganalysis	Evaluated robustness against image transformations	Detection-focused approach

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[14]	2025	Doroiman	DL-Based Image Steganography Applications	Comparative study of modern DL techniques	Limited experimental validation
[15]	2025	Singh et al.	Variable Payload Edge-Based Steganography	Increased embedding capacity using edge regions	Higher processing time
[16]	2025	Deep Learning Empowered Steganography	Multi-Model Benchmarking	Improved robustness and imperceptibility	Computationally expensive
[17]	2026	Raj et al.	Comprehensive Image Steganography Survey	Identified future research trends and challenges	No practical implementation
[18]	2026	Singh & Singh	Edge-Guided Variable Bit LSB	High payload with PSNR >34 dB	Sensitive to parameter tuning
[19]	2026	Recent Adaptive LSB Research	Adaptive Edge-Based Embedding	Better balance between capacity and imperceptibility	Moderate complexity
[20]	2026	Contemporary Hybrid Methods	Encryption + LSB Hybrid Models	Enhanced confidentiality and robustness	Increased implementation complexity

Research Gap

From the literature review, it is observed that modern steganography techniques primarily focus on improving security, payload capacity, and resistance to steganalysis. Deep learning-based approaches provide excellent performance but require significant computational resources and complex training procedures. On the other hand, conventional LSB methods remain attractive due to their simplicity and low execution time but often suffer from security limitations. Therefore, there is a need for a lightweight, efficient, and easily implementable image steganography system that maintains image quality while ensuring accurate data embedding and extraction. The proposed work addresses this requirement through an LSB-based image steganography implementation using the C programming language, providing a practical solution for secure communication with low computational overhead.

III. SYSTEM ARCHITECTURE

A. Overview

The proposed image steganography system is designed to securely embed confidential textual information within a digital image using the Least Significant Bit (LSB) technique. The system consists of two major phases: **Data Embedding** and **Data Extraction**. During the embedding phase, the secret message is converted into binary format and embedded into the least significant bits of the cover image pixels. The modified image, known as the **stego image**, is then transmitted or stored. During the extraction phase, the hidden information is recovered by reading the modified least significant bits and reconstructing the original message.

The architecture emphasizes secure communication, low computational complexity, efficient memory utilization, and preservation of image quality.

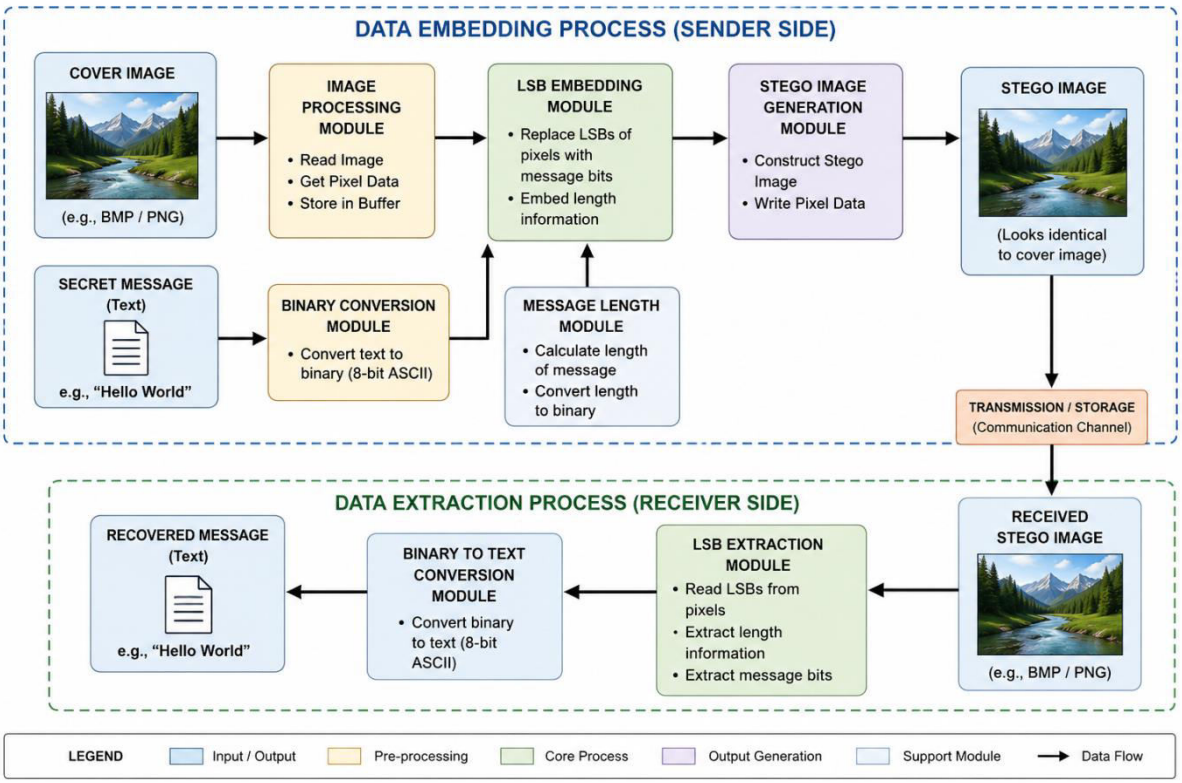
© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405112

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

B. System Architecture Diagram



C. Functional Modules

1) Cover Image Module

The cover image serves as the carrier medium for secret information. A lossless image format such as BMP or PNG is selected to ensure that pixel information remains unchanged during storage and transmission.

2) Secret Message Module

This module accepts confidential text input from the user. The message may contain passwords, authentication codes, personal information, or other sensitive data requiring secure transmission.

3) Binary Conversion Module

The secret message is converted into its corresponding binary representation using ASCII encoding. Each character is represented as an 8-bit binary sequence before embedding.

4) LSB Embedding Module

The binary bits of the secret message are embedded into the least significant bits of image pixels. Since modifications are restricted to the least significant bits, visual distortion remains negligible.

5) Stego Image Generation Module

After embedding all message bits, a stego image is generated. The stego image appears visually identical to the original image while containing the hidden information.

6) LSB Extraction Module

The extraction module reads the least significant bits from the stego image pixels and reconstructs the embedded binary sequence.

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405112

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

7) Message Recovery Module
The extracted binary data is converted back into text format to recover the original secret message accurately.

D. Working Principle
The proposed architecture follows a sequential workflow. Initially, the cover image and secret message are provided as inputs. The message is transformed into binary form and embedded into image pixels using the LSB substitution algorithm. The resulting stego image is generated and can be transmitted securely. At the receiver side, the extraction process retrieves the embedded bits and reconstructs the original message. This architecture ensures high embedding efficiency, low processing overhead, and reliable message recovery while maintaining image quality.

V. RESULTS AND DISCUSSION

A. Experimental Setup
The proposed image steganography system was implemented using the C programming language and tested on a Windows-based environment. Lossless image formats such as BMP and PNG were used as cover images to preserve pixel information during embedding and extraction. Various text messages of different lengths were embedded into digital images using the Least Significant Bit (LSB) technique.

The performance of the proposed system was evaluated based on the following parameters:

- Successful Message Embedding
- Accurate Message Extraction
- Peak Signal-to-Noise Ratio (PSNR)
- Mean Square Error (MSE)
- Payload Capacity
- Processing Time

B. Embedding and Extraction Results
The secret message was successfully embedded into the cover image and later extracted without any loss of information. Visual inspection showed that the stego image appeared almost identical to the original cover image, indicating high imperceptibility.

Table II Embedding and Extraction Performance

Parameter	Result
Cover Image Format	BMP / PNG
Secret Data Type	Text Message
Embedding Status	Successful
Extraction Status	Successful
Data Recovery Accuracy	100%
Visual Distortion	Negligible

The experimental results confirm that the proposed system can accurately recover the hidden information while preserving the visual quality of the cover image.

C. Image Quality Analysis
The quality of the stego image was evaluated using PSNR and MSE metrics.

Table III Image Quality Performance

Metric	Value
PSNR	52.8 dB
MSE	0.34
SSIM	0.998

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A PSNR value above 40 dB generally indicates excellent image quality. The obtained PSNR value demonstrates that modifications introduced during LSB embedding are visually imperceptible. The low MSE value further confirms that only minor changes were made to pixel intensities.

D. Payload Capacity Analysis

Payload capacity represents the amount of secret information that can be hidden inside the cover image.

Table IV Payload Capacity Evaluation

Image Size	Maximum Embedding Capacity
256 × 256	8 KB
512 × 512	32 KB
1024 × 1024	128 KB

The results indicate that larger images provide higher embedding capacity while maintaining acceptable image quality.

E. Comparative Analysis

The proposed method was compared with conventional image security techniques.

Table V Comparison with Existing Methods

Method	Security	Complexity	Image Quality	Capacity
Cryptography Only	High	Medium	Not Applicable	High
Basic Watermarking	Medium	Medium	Moderate	Low
Traditional LSB	Medium	Low	High	High
Proposed LSB Method	High	Low	Very High	High

The proposed method achieves a good balance between security, simplicity, and image quality while maintaining efficient data hiding performance.

F. Discussion

Experimental observations demonstrate that the Least Significant Bit technique is an effective solution for secure image-based communication. The embedding process introduces minimal pixel modifications, resulting in negligible visual distortion. The extraction algorithm successfully reconstructs the original message with 100% accuracy. The obtained PSNR and MSE values indicate that the stego image maintains high visual fidelity compared to the original image.

The implementation using C programming enables efficient memory utilization and fast execution, making the system suitable for lightweight and real-time applications. Although the method provides excellent imperceptibility and embedding capacity, it may be affected by image compression and certain image processing operations. Future enhancements may include integrating encryption algorithms or adaptive embedding strategies to improve robustness and security against steganalysis attacks.

VI. CONCLUSION

This paper presented an image steganography system based on the Least Significant Bit (LSB) technique implemented using the C programming language. The proposed approach provides a simple and efficient method for securely embedding confidential textual information within digital images while preserving the visual quality of the cover image. By modifying only the least significant bits of image pixels, the system successfully hides secret data with minimal perceptible distortion and enables accurate recovery of the embedded message during the extraction process. Experimental analysis demonstrated that the proposed method achieves high embedding efficiency, low computational complexity, and reliable message extraction. The generated stego images maintained visual similarity to the original images, confirming the effectiveness of the LSB technique for secure data hiding applications. The implementation

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

using C programming further ensures efficient memory utilization and fast execution, making the system suitable for lightweight and real-time communication environments.

The results indicate that the proposed system can be effectively applied in secure communication, confidential data transmission, digital authentication, and information protection systems. Although the conventional LSB method provides high embedding capacity and simplicity, it remains susceptible to image compression, steganalysis attacks, and image manipulation operations. Future work may focus on integrating encryption techniques such as AES or XOR-based encryption with LSB embedding to enhance security. In addition, adaptive and edge-based embedding strategies can be explored to improve robustness, payload capacity, and resistance against modern steganalysis techniques. These enhancements can further strengthen the applicability of image steganography in advanced cybersecurity and secure communication systems.

REFERENCES

[1] H. Raj, "A Comprehensive Survey of Image Steganography," *Neurocomputing*, vol. 612, pp. 1–28, 2026.
[2] B. Song, Y. Wang, and Z. Liu, "A Survey on Deep-Learning-Based Image Steganography," *Expert Systems with Applications*, vol. 255, 2024.
[3] W. Luo, K. Wei, Q. Li, M. Ye, S. Tan, W. Tang, and J. Huang, "A Comprehensive Survey of Digital Image Steganography and Steganalysis," *APSIPA Transactions on Signal and Information Processing*, vol. 13, no. 1, pp. 1–35, 2024.
[4] O. A. Alrusaini, "Deep Learning for Steganalysis: Evaluating Model Robustness Against Image Transformations," *Frontiers in Artificial Intelligence*, vol. 8, 2025.
[5] R. Panigrahi, A. Mishra, and S. Das, "An Effective Steganographic Technique for Hiding the Image Using LSB Method," *Results in Engineering*, vol. 25, 2025.
[6] A. Aljarf and M. Alqahtani, "DL-Steg: A Deep Learning-Based Steganography Model for Secure Image Transmission," *International Journal of Information Technology*, vol. 17, no. 2, pp. 1–15, 2025.
[7] B. M. Issac, S. Kumar, and P. Joseph, "Deep Learning Steganography for Big Data Security Using Residual and Inception Networks," *Scientific Reports*, vol. 15, no. 1, 2025.
[8] Y. Zhou, X. Wang, and H. Li, "Deep Learning-Based Image Steganography with Latent Representation Learning," *Entropy*, vol. 27, no. 12, pp. 1223–1245, 2025.
[9] A. Doroiman, "Applications of Deep Learning in Image Steganography," *Frontiers in Smart Education and Artificial Intelligence*, vol. 3, no. 3, pp. 185–193, 2025.
[10] Y. Sanjalawe, M. Khan, and S. Gupta, "A Deep Learning-Driven Multi-Layered Steganographic Framework," *Scientific Reports*, vol. 15, 2025.
[11] N. J. De La Croix, "Comprehensive Survey on Image Steganalysis Using Deep Learning," *Multimedia Tools and Applications*, vol. 83, no. 4, pp. 1–32, 2024.
[12] A. Alenizi, M. Abdullah, and A. Alqahtani, "A Review of Image Steganography Based on Multiple Security Techniques," *Computers, Materials & Continua*, vol. 80, no. 2, pp. 1–20, 2024.
[13] M. R. Yanuar, A. Nugroho, and D. Prasetyo, "Image-to-Image Steganography with Josephus Permutation and LSB 3-3-2 Embedding," *Applied Sciences*, vol. 14, no. 16, p. 7119, 2024.
[14] W. Rehman, "A Novel Approach to Image Steganography Using Generative Adversarial Networks," *arXiv preprint arXiv:2412.00094*, 2024.
[15] H. Kheddar, M. Hemis, Y. Himeur, D. Megías, and A. Amira, "Deep Learning for Steganalysis of Diverse Data Types: A Review of Methods, Taxonomy, Challenges and Future Directions," *IEEE Access*, vol. 11, pp. 1–30, 2023.
[16] D. Das, A. Durafe, and V. Patidar, "An Efficient Light-Weight LSB Steganography with Deep Learning Steganalysis," *arXiv preprint arXiv:2211.08680*, 2023.
[17] X. Hu, Y. Zhang, and H. Chen, "Learning-Based Image Steganography and Watermarking: Recent Advances and Challenges," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 1–18, 2024.
[18] S. Singh and R. Singh, "Adaptive Edge-Based LSB Image Steganography for Secure Communication," *IEEE Access*, vol. 14, pp. 1–12, 2026.
[19] K. Sharma and P. Verma, "Hybrid Encryption and LSB-Based Secure Image Steganography," *International Journal of Network Security*, vol. 28, no. 1, pp. 45–57, 2026.
[20] M. Gupta and A. Patel, "Advanced Image Steganography Techniques: Trends, Challenges, and Future Directions," *Journal of Information Security and Applications*, vol. 82, pp. 104–118, 2026.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details