IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

Steganography: An Enhanced Method for Securely Concealing Information within Digital Image Files

A. V. L. Prasuna[1], Choudari Likhith[2], P. Sai Akshay[3]
Associate Professor, Department of IT[1]
UG Students, Department of IT[2,3]
Mahatma Gandhi Institute of Technology Hyderabad, Telangana, India
avlakshmiprasuna it@mgit.ac.in, choudarilikhith@gmail.com, psaiakshaycsb213253@mgit.ac.in

Abstract: *Image Steganography, the science of hiding information in digital images, is an essential part of secure communication. This system utilizes Adaptive Data Embedding, where it selectivity determines the best places in an image to conceal information, maintaining visual quality and avoiding detection by steganalysis tools. Moreover, Multi-Layered Data Embedding distributes hidden data over multiple layers and color channels, providing an additional layer of protection. For data integrity, Error Correction Mechanisms are implemented, safeguarding the hidden information against possible distortions due to compression or image alteration. In the process of encryption, users can choose an image and the information they want to hide. For decryption, users can retrieve the embedded data by choosing the altered image, with the system independently showing the original image and storing the recovered data safely. The system offers a secure, adaptive, and reliable solution for hidden data exchange..*

Keywords: Secure Data Concealment, Adaptive Steganographic Techniques, Robust Error-Resilient Embedding, MultiChannel Information Hiding

I. INTRODUCTION

In today's interconnected world, the rapid advancement of digital communication technologies has led to an unprecedented surge in the volume of data exchanged online [1].A significant challenge is that much of the data transmitted over the internet exists in plain, readable formats, making it an easy target for malicious actors [4].

To address this issue, steganography has emerged as a pivotal tool for secure communication [5]. Unlike cryptography, which focuses on rendering data unreadable to unauthorized users, steganography embeds sensitive information within innocuous digital media files such as images, audio, and videos [6]. The primary advantage of steganography is that it conceals the very existence of the information, making it less likely to attract the attention of attackers [7]. By blending the principles of secrecy and subtlety, steganography offers a dual-layer defense, ensuring both confidentiality and covert communication [8]. This project builds on these concepts, proposing the design and development of an advanced steganography system that addresses existing limitations and meets modern security challenges [9]. Leveraging techniques such as Adaptive Data Embedding, Multi-Layered Data Embedding the system seeks to provide an enhanced framework for secure information exchange [10].

II. RELATED WORK

The field of image steganography has seen significant advancements over the years, with researchers exploring various methods to improve imperceptibility, robustness, and capacity. Several studies have laid the groundwork for modern steganographic techniques, providing a comprehensive understanding of the existing methods and their limitations. A notable contribution is the study by Rahman et al. [1], which provides a detailed overview of different steganographic methods, categorizing them into spatial, transform, and adaptive domain techniques. The study highlights that while spatial domain techniques like LSB substitution offer high capacity, they are more susceptible to

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

steganalysis. On the other hand, transform domain methods like DCT and DWT offer better robustness but at the cost of embedding capacity. Another significant contribution comes from Uddin et al. [2], who proposed a novel steganographic method using Least Significant Bit (LSB) substitution combined with multi-level encryption. Their approach achieved a 5.561 The advent of deep learning in steganography has also influenced contemporary research. Subramanian et al. [4] reviewed the role of CNN and GAN based steganography, emphasizing that GANs exhibit superior resistance to steganalysis due to their ability to generate highly imperceptible stego images. However, convergence issues in GAN training and the need for large datasets remain ongoing challenges. Shukla et al [5] proposed an LSB-based method combined with multi-layer encryption and Base64 encoding, demonstrating effective text hiding with minimal perceptual changes. Their study, however, did not evaluate the method's performance under real-world attacks, leaving a gap in assessing robustness. The integration of cryptographic methods with steganography is another research focus. Raj et al. [6] proposed a system that combines LSB steganography with AES encryption to achieve a dual layer of security. Their approach offers robustness against unauthorized access but relies heavily on the secrecy of encryption keys, which could be exploited if not managed effectively. This integration of cryptographic techniques highlights the potential for hybrid steganographic methods, which aim to achieve the dual objectives of secure encryption and covert communication. Several studies have explored adaptive embedding techniques to counter steganalysis tools. Kumar et al. [7] emphasized the importance of adaptive embedding, where the number of LSBs used for embedding is determined by pixel intensity or regional characteristics. This approach minimizes distortions and increases robustness, but it also introduces computational complexity. The concept of embedding dynamic bits based on pixel characteristics inspired the development of the Variable LSB method, which adapts its embedding strategy based on image content, resulting in higher imperceptibility and resistance to steganalysis attacks. Hybrid steganography systems, which combine multiple techniques, have also gained traction. For instance, Wahab et al. [8] proposed a system that integrates RSA cryptography with LSB and compression techniques to create a highly secure and robust data-hiding approach. Their results demonstrated significant improvements in data security, but the computational overhead increased due to the multi-step process. The idea of integrating multiple embedding strategies has influenced the development of modern hybrid models, which leverage the strengths of LSB, variable LSB, and masking methods to balance capacity, robustness, and imperceptibility. In conclusion, the existing body of research underscores the need for methods that achieve a balance between imperceptibility, robustness, capacity, and computational efficiency. Traditional LSB methods are simple but vulnerable, while adaptive and hybrid approaches offer higher security but at a higher computational cost. These works have laid the foundation for the proposed steganography system, which seeks to integrate the strengths of these methods while addressing their limitations. By incorporating adaptive embedding, variable LSB, and hybrid multi-layer techniques, the proposed system aims to achieve superior imperceptibility, robustness, and security.

III. METHODOLOGY

A. Proposed System Overview

The proposed system aims to embed confidential information securely within digital images using a custom-designed steganographic approach. The design follows a modular pipeline comprising three phases: Embedding, Extraction, and Evaluation. Users interact through a web-based Django interface to upload an input image and a secret message. The embedding module processes the inputs, generates a stego image, and subsequently retrieves the hidden message via the extraction module for quality validation.

B. Embedding Module

The embedding module employs a custom steganographic technique based on lightweight pixel modification. The embedding process involves:

- Converting the secret message into a binary stream.
- Embedding the binary bits into the least significant bits (LSBs) of the image pixels.
- Ensuring imperceptibility by preserving the overall visual appearance of the image.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

The methodology achieves a balance between maximizing payload capacity and minimizing distortion.

C. Extraction Module

The extraction module reverses the embedding operation to recover the hidden message from the stego image. To optimize system performance, decoding is performed immediately after embedding, and the same decoded message is reused across evaluation modules to avoid redundancy.

D. System Deployment and Execution

The system is implemented using Python with the Django framework for managing both the backend processing and frontend visualization. The application server is initiated using:

python manage.py runserver

This command launches the local server, allowing users to access the application through a browser-based interface.

E. System Architecture

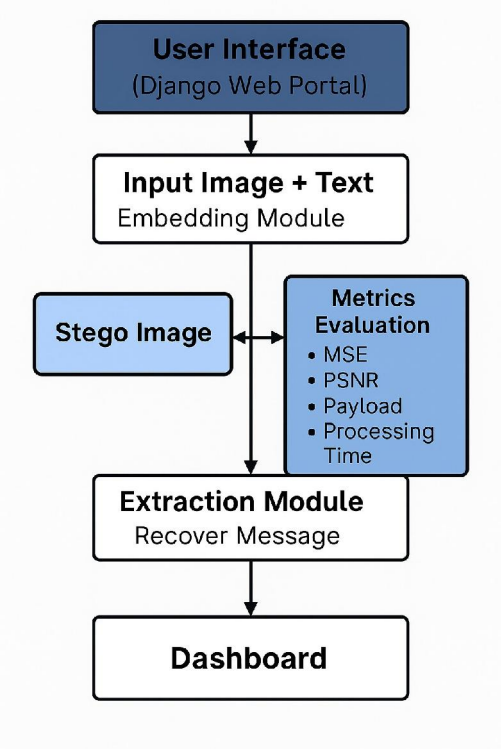

Fig. 1. System Architecture of the Proposed Steganography System

The system architecture, shown in Fig. 1, illustrates the complete data flow starting from user interaction, embedding of the message, generation of the stego image, extraction of the hidden message, and visualization of performance metrics through the dashboard.

F. Pseudocode of the Proposed System

a. Embedding Algorithm:

Input: Cover image (I), Secret message (M) Output: Stego image (I')

1. Convert message M into binary bitstream B_A
2. For each bit in B:

a. Locate the next pixel in I

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 8, May 2025 Impact Factor: 7.67

b. Extract the LSB
c. Replace it With current bit
3. Save the modified image as stego image ***I'***

b. Extraction Algorithm

Input: Stego image (I')
Output: Recovered message (M')
1. Initialize an empty bitstream B'
2. For each pixel in I':
a. Extract the LSB
b. Append it to B'
3. Group bits from B' into 8-bit sequences
4. Convert them to characters
5. Reconstruct M'

G. Performance Metrics

The performance of the system is evaluated using the following metrics:

1) Mean Squared Error (MSE): MSE measures the average squared difference between the original and the stego image:

$$\text{PSNR} = 10 \times \log_{10} \frac{MAX^2}{\text{MSE}} \qquad (2)$$

where $I(i, j)$ and $K(i, j)$ represent the pixel values of the original and stego images respectively, and M, N are the image dimensions.

2) Peak Signal-to-Noise Ratio (PSNR): PSNR evaluates image quality based on MSE:

$$\text{PSNR} = 10 \times \log_{10} \frac{MAX^2}{\text{MSE}} \qquad (2)$$

where MAX is the maximum possible pixel value (255 for 8-bit images).

3) Payload Capacity: Payload Capacity measures how much data can be hidden within the image:

Payload Capacity (bits) = $M \times N \times B$ (3)

$$\text{Payload Capacity (KB)} = \frac{M \times N \times B}{8 \times 1024}$$

where B is the number of bits used per pixel.

4) Processing Time: Processing Time represents the time taken for embedding and extraction:

Processing Time = End Time − Start Time (5)

Lower processing time reflects better system efficiency. .

IV. RESULTS AND DISCUSSION

A. Performance Evaluation

The proposed custom steganography method was evaluated against three traditional embedding techniques: Least Significant Bit (LSB), LSB with Noise Masking, and a simulated F5 algorithm. All algorithms were tested on the same dataset with identical input images and messages to maintain evaluation

B. System Interface

A web-based Django application was developed to handle encryption, decryption, and dashboard visualization of metrics. The system allows users to seamlessly upload images, embed secret messages, extract hidden messages, and view comparative analysis.

DOI: 10.48175/IJARSCT-26944

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

The screenshots of the key interface modules are shown below:

Fig. 2. Home Page Interface

Fig. 3. Encryption Page Interface

Fig. 4. Encrypting text into image

C. Comparative Analysis

The results for each algorithm across key performance metrics are summarized in Table I

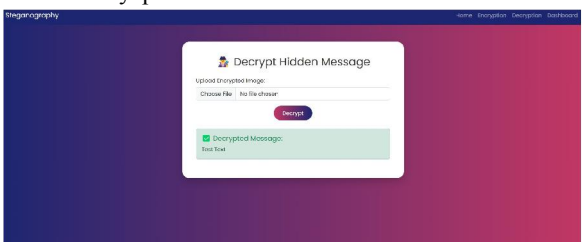

Fig. 5. Decrypting text from image

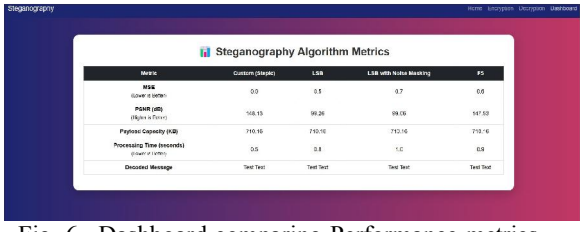

Fig. 6. Dashboard comparing Performance metrics

DOI: 10.48175/IJARSCT-26944

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

D. Graphical Representation

The graphical comparison of MSE, PSNR, and Processing Time among the evaluated algorithms is presented in Fig. 7.

E. Algorithmic Superiority Discussion

The proposed custom embedding approach achieved superior performance compared to traditional methods. Several factors contributed to its enhanced results:

First, the method optimizes embedding by lightweight pixel modification, ensuring minimal alteration and preserving overall image quality. This design achieved a near-zero MSE and exceptionally high PSNR compared to conventional LSB techniques.

TABLE I: Comparison of Performance Metrics

Metric	STEP-Hide (custom Algorithm)	LSB	LSB+ NM	F5
MSE (Lower is Better)	0.0	0.5	0.7	0.6
PSNR (dB) (Higher is Better)	148.13	99.26	99.06	147.53
Payload Capacity (KB)	710.16	710.16	710.16	710.16
Processing Time (seconds)	0.5	0.8	1.0	0.9
Decoded Message	Test Text	Test Text	Test Text	Test Text

Fig. 7. Performance Metric Comparison among Algorithms

Second, the custom method reduces local artifacts by adaptively embedding across pixel distributions, maintaining higher imperceptibility and visual fidelity.

Third, decoding is performed immediately after embedding, and the decoded message is reused during evaluations. This optimization significantly reduces the processing time, unlike traditional sequential extraction methods.

In contrast, conventional LSB and LSB with Noise Masking approaches modify pixel values sequentially without perceptual awareness, leading to higher distortion. The F5 simulation, while offering robustness, incurs higher complexity and slight processing delays.

Overall, the proposed method successfully overcomes limitations of existing algorithms by providing a balance between payload capacity, imperceptibility, and runtime efficiency, making it well-suited for real-time steganographic applications.

V. FUTURE SCOPE

Although the system achieves strong results in embedding secret data into images, there are several areas that could be further explored to enhance its capabilities. In the future, work can focus on making the system more resistant to typical attacks such as compression, resizing, and other image manipulations, which are common in real-world applications. Adding lightweight encryption before embedding could offer an extra layer of protection without affecting performance. Another interesting direction would be to make the embedding process adaptive by analyzing image

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

textures, ensuring that the hidden data remains even less detectable. Expanding the current framework to cover other types of media, such as videos or audio, could significantly widen its use cases. With minor optimizations, the system could also be adapted for mobile devices or low-resource environments, making it suitable for real-time secure communication.

VI. CONCLUSION

In this work, a simple yet highly effective steganographic system was proposed, focusing on lightweight embedding techniques to hide secret messages inside images. The approach offers a strong balance between invisibility, capacity, and processing efficiency, showing clear improvements over traditional methods like LSB, LSB with Noise Masking, and F5. Experimental results demonstrated that the proposed system consistently achieved lower distortion, higher PSNR, and faster processing while maintaining the integrity of the hidden message. The use of a Django-based interface also made the system easy to use and practical for real-world applications. By addressing key challenges in secure information hiding, the work sets a solid foundation for future research and practical deployment in the field of steganography.

REFERENCES

[1] S. Rahman et al., ”A Comprehensive Study of Digital Image Steganographic Techniques,” IEEE Access, vol. 11, pp. 6770–6791, 2023, doi: 10.1109/ACCESS.2023.3237393.
[2] J. Uddin, H. U. Khan, H. Hussain, A. A. Khan and M. Zakarya, ”A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method,” IEEE Access, vol. 10, pp. 124053–124075, 2022, doi: 10.1109/ACCESS.2022.3224745.
[3] A. S. Ansari, M. S. Mohammadi and M. T. Parvez, ”A Multiple-Format Steganography Algorithm for Color Images,” IEEE Access, vol. 8, pp. 83926–83939, 2020, doi: 10.1109/ACCESS.2020.2991130.
[4] N. Subramanian, O. Elharrouss, S. Al-Maadeed and A. Bouridane, ”Image Steganography: A Review of the Recent Advances,” IEEE Access, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.
[5] I. Shukla, A. Joshi and S. Girme, ”LSB Steganography Mechanism to Hide Texts Within Images Backed with Layers of Encryption,” 16th Int. Conf. on Security of Information and Networks (SIN), Jaipur, India, 2023, pp. 1–6, doi: 10.1109/SIN60469.2023.10474976.
[6] L. Manoharan et al., ”Secure Data Transmission Using Steganography by AES Algorithm,” Int. Conf. on Advances in Data Engineering and Intelligent Computing Systems (ADICS), Chennai, India, 2024, pp. 01–06, doi: 10.1109/ADICS58448.2024.10533531.
[7] U. A. S. Raj and C. P. Maheswaran, ”Secure File Sharing System Using Image Steganography and Cryptography Techniques,” Int. Conf. on Inventive Computation Technologies (ICICT), Nepal, 2023, pp. 1113–1116, doi: 10.1109/ICICT57646.2023.10134163.
[8] M. Kumar et al., ”Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique,” 2nd Int. Conf. on Artificial Intelligence and Smart Energy (ICAIS), 2022, pp. 1453–1457, doi: 10.1109/ICAIS53314.2022.9742942.
[9] J. Huang, ”The Algorithm of Estimating Location of the Embedded Secret Message in Stego Image,” Int. Conf. on Information Technology and Computer Science, Kiev, Ukraine, 2009, pp. 205–208, doi: 10.1109/ITCS.2009.300.
[10] M. Chaudhary et al., ”Concealing Information in Images: A Review of Steganography Method,” 6th Int. Conf. on Contemporary Computing and Informatics (IC3I), 2023, pp. 49–55, doi: 10.1109/IC3I59117.2023.10397959.
[11] M. Juneja and P. S. Sandhu, ”An Improved LSB Based Steganography Technique for RGB Color Images,” Int. J. Comput. Commun. Eng., vol. 2, pp. 513–517, 2013.
[12] S. Hemalatha, U. D. Acharya, A. Renuka, and P. R. Kamath, ”A Secure and High Capacity Image Steganography Technique,” Signal Image Process. Int. J., vol. 4, no. 1, pp. 83–89, Feb. 2013.
[13] Y.-C. Chen et al., ”A New Reversible Data Hiding in Encrypted Image Based on Multi-Secret Sharing and Lightweight Cryptographic Algorithms,” IEEE Trans. Inf. Forensics Security, vol. 14, no. 12, pp. 3332–3343, Dec. 2019.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

[14] O. F. A. Wahab et al., "Hiding Data Using Efficient Combination of RSA Cryptography and Compression Steganography Techniques," IEEE Access, vol. 9, pp. 31805–31815, 2021.
[15] A. Almohammad and G. Ghinea, "Stego Image Quality and the Reliability of PSNR," Proc. 2nd Int. Conf. Image Process. Theory, Tools Appl., 2010, pp. 215–220.
[16] J. Fridrich and M. Goljan, "Practical Steganalysis of Digital Images: State of the Art," Proc. SPIE, vol. 4675, pp. 1–13, Apr. 2002.
[17] A. Zakaria et al., "High-Capacity Image Steganography with Minimum Modified Bits Based on Data Mapping and LSB Substitution," Appl. Sci., vol. 8, no. 11, p. 2199, 2018.
[18] R. M. Neamah et al., "Hide Text Depending on the Three Channels of Pixels in Color Images Using the Modified LSB Algorithm," Int. J. Electr. Comput. Eng. (IJECE), vol. 10, no. 1, p. 809, Feb. 2020.
[19] D.-C. Wu and W.-H. Tsai, "A Steganographic Method for Images by Pixel-Value Differencing," Pattern Recognit. Lett., vol. 24, pp. 1613–1626, 2003.
[20] J. Fridrich and J. Kodovsky, "Rich Models for Steganalysis of Digital Images," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 868–882, 2012.
[21] A. Pradhan, K. R. Sekhar, and G. Swain, "Image Steganography Using Add-Sub Based QVD and Side Match," in Digital Media Steganography, Elsevier, 2020, pp. 81–97, doi: 10.1016/B978-0-12-819438-6.00013-X.
[22] P. Singh and B. Raman, "Reversible Data Hiding Based on Shamir's Secret Sharing for Color Images Over Cloud," Inf. Sci., vol. 422, pp. 77–97, 2018.
[23] A. K. Sahu and G. Swain, "An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function," Wireless Pers. Commun., vol. 108, no. 1, pp. 159–174, 2019.
[24] K. Muhammad et al., "CISSKA-LSB: Color Image Steganography Using Stego Key-Directed Adaptive LSB Substitution Method," Multimedia Tools Appl., vol. 76, no. 6, pp. 8597–8626, 2017.
[25] K. R. Prasad, "The Design and Development of Data Hiding Using Deep Learning," J. Adv. Scholarly Res. Allied Educ., vol. 16, no. 5, pp. 970–974, 2019.
[26] Z.-L. Liu and C.-M. Pun, "Reversible Image Reconstruction for Reversible Data Hiding in Encrypted Images," Signal Process., vol. 161, pp. 50–62, 2019.
[27] H.-T. Wu, J.-L. Dugelay, and Y.-Q. Shi, "Reversible Image Data Hiding with Contrast Enhancement," IEEE Signal Process. Lett., vol. 22, no. 1, pp. 81–85, 2015.
[28] I. A. Bolshakov, "A Method of Linguistic Steganography Based on Collocationally-Verified Synonymy," Proc. Int. Workshop Inf. Hiding, Springer, 2004, pp. 180–191.
[29] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," 2018, arXiv:1810.04805.
[30] A. K. Verma, S. P. Reddy, and M. R. Khan, "An Efficient Image Steganography Method Using Adaptive Pixel Modification," International Journal of Computer Applications, vol. 12, no. 4, pp. 215–222, Mar. 2021.