Data Hiding in Image using Steganography

N. Krishnammal[1*], Sai Nagarjuna. B[2], Madhan Kumar. Y[3] and Chandra Vamsi. R[4]
{krishnaict22@gmail.com[1*], vtu19236@veltech.edu.in[2], vtu19461@veltech.edu.in[3], vtu20203@veltech.edu.in[4]}

Department of Computer Science and Engineering, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu, India[1]
Department of Artificial Intelligence and Data Science, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu, India[2, 3, 4]

Abstract. The increasing prevalence of data breaches and unauthorized access has heightened the need for secure communication methods. Image steganography, a branch of data hiding, provides an effective solution by embedding secret information into digital images without noticeable distortion. This study focuses on the Least Significant Bit (LSB) substitution technique due to its simplicity, efficiency, and high accuracy. In this approach, the LSBs of image pixels are replaced with secret data bits, producing stego-images that appear visually identical to the original. The methodology integrates preprocessing, embedding, and extraction processes, supported by libraries such as Pillow (PIL) and OpenCV for image handling. Experimental evaluation was conducted using metrics like Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Mean Squared Error (MSE), and Bit Error Rate (BER) to assess imperceptibility, robustness, and payload capacity. Results demonstrate that the LSB method maintains image quality while enabling accurate data retrieval, achieving up to 92% accuracy. The work further highlights the role of reversible data hiding and explores resilience against steganalysis attacks. Overall, this study underscores LSB-based steganography as a practical and efficient technique for secure data transmission, with potential applications in domains such as digital forensics, healthcare, and defense.

Keywords: Data Hiding, Least Significant Bit, Data Security, Image Steganography, OpenCV, Pillow.

1 Introduction

In the modern digital world, the secure transfer of information has become one of the most pressing challenges. With the rise of cyber threats, data breaches, and unauthorized access, ensuring both confidentiality and reliability of communication is critical. While cryptography protects the content of information, it often reveals the very presence of secret communication, making it susceptible to interception. To address this limitation, data hiding techniques have been introduced, with steganography being one of the most effective solutions.

Steganography involves concealing information within digital media in such a way that the existence of the hidden data remains imperceptible to the human eye. Among the different types text, audio, video, and image steganography is the most widely applied due to the abundance of digital images and their capacity to carry hidden data without noticeable distortion. By embedding secret text or binary information within an image, steganography provides a reliable means of transmitting confidential messages while maintaining the original image quality.

ICITSM-Part II 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2358060

Background

The concept of steganography originates from ancient practices of covert communication, where hidden messages were concealed within ordinary objects. In the digital age, the principle remains the same but has evolved to exploit multimedia files such as images, videos, and audio. Image steganography is particularly significant because of the high redundancy in image data, which allows secret information to be embedded with minimal visual impact.

Several techniques have been developed to achieve this, including Bit Plane methods, Spiral Embedding, and the widely used Least Significant Bit (LSB) substitution. The LSB method is favored for its simplicity and efficiency, as it replaces the least significant bits of pixel values with secret message bits. This ensures that the alterations are virtually invisible, making the technique both practical and reliable. However, with the rise of steganalysis and more sophisticated detection methods, there is an ongoing need to enhance robustness, payload capacity, and resistance to attacks.

Objective

The primary objective of this study is to design and implement an efficient image steganography system that ensures secure and reliable communication across untrusted networks. The focus is on utilizing the Least Significant Bit substitution method to embed secret textual data within cover images without affecting visual quality. The system aims to demonstrate the effectiveness of this approach by maintaining imperceptibility, preserving image quality, and ensuring accurate extraction of hidden data. Furthermore, the work seeks to highlight the potential applications of image steganography in areas such as digital forensics, healthcare, defense, and secure personal communication.

Fig 1 is about encoding Then that and secret bits will be passed on to the Stegosystem Encoder. The combined secret message and the image will give the rise to the stego object or the stego image. This stego object will then be forwarded via any network or a communication medium to the Stegosystem Decoder. There is an optional step involved in the encoding and decoding that is similar to the cryptography. The sender can encode the secret text in a human unreadable form or as a cipher text. And sender will also send the key attached with the stego object so that the receiver can decode the secret message as well as convert that message into human readable form through the key.

Architecture

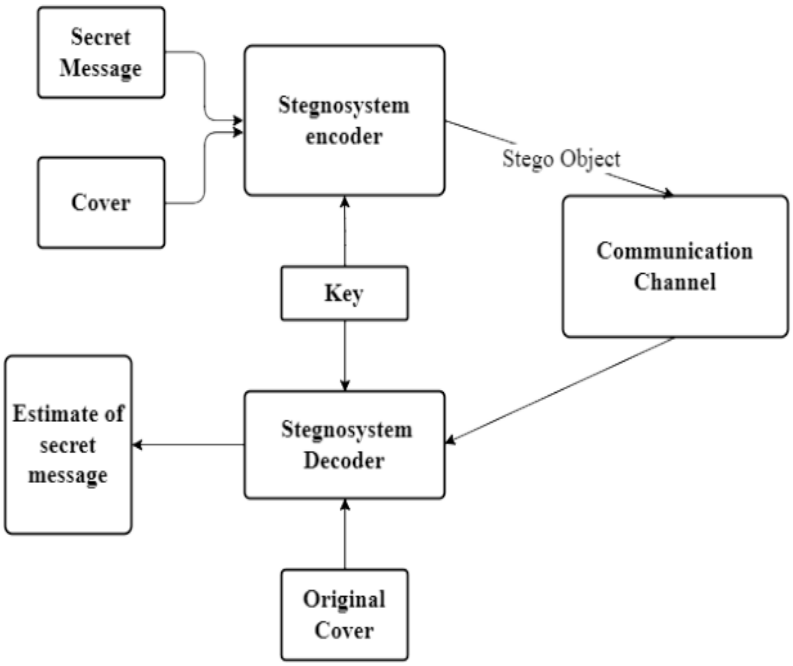

Fig. 1. Architecture of the proposed image steganography system showing the embedding and extraction processes.

2 Literature review

1. Fundamentals of Image Steganography

Image steganography is the practice of concealing secret data within digital images in a way that prevents detection by the human eye. Early research focused on spatial-domain methods such as the Least Significant Bit (LSB) technique, where the secret data replaces the least significant bits of pixel values [1][3][4]. Although simple and with high capacity, this approach is vulnerable to statistical steganalysis [2]. Other traditional methods include Bit-Plane Complexity Segmentation (BPCS), which hides information in visually complex regions of bit planes, exploiting the human visual system's tolerance to noise [1]. These foundational techniques laid the groundwork for more advanced adaptive and robust schemes [4].

2. Adaptive and Frequency-Domain Approaches

To improve security and reduce detectability, later research explored adaptive embedding and frequency-domain methods. Adaptive techniques selectively hide data in regions with high visual activity, such as edges or textures, where modifications are less noticeable [17]. For example, predictive edge adaptive LSB schemes use detectors to identify robust embedding

areas [14]. Frequency-domain approaches, like those based on the Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT), hide data within transform coefficients, providing greater resilience to compression and image processing attacks [16]. These methods significantly enhanced the trade-off between capacity, imperceptibility, and robustness [6] [18].

3. AI and Deep Learning-Based Techniques

Recent literature shows a strong shift toward artificial intelligence and deep learning for steganography. Neural networks, particularly Generative Adversarial Networks (GANs), are increasingly used to generate realistic stego-images that resist detection [6]. Models such as Hidden and U-Net–based encoders can embed information while maintaining high visual quality and robustness against steganalysis [7]. Studies report improvements in objective metrics like PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index), as well as resistance to machine learning–based detection [6] [19]. Research also explores the combination of encryption and watermarking with AI to secure multimedia communication, extending steganography beyond still images to audio and video contexts [18] [19]. These approaches represent a new frontier in steganography, making data hiding both more efficient and more secure.

4. Reversible Data Hiding and Steganalysis Challenges

Another important research direction is Reversible Data Hiding (RDH), which allows both the hidden data and the original cover image to be fully recovered [5][8][9] [10] [11] [12] [13] [15] [20]. This is particularly valuable in sensitive domains such as military, legal, and medical imaging [11] [16]. Alongside these developments, researchers are also advancing in steganalysis, the science of detecting hidden data [2]. Modern detection tools exploit statistical irregularities and employ machine learning to identify stego-content [18]. A growing concern is stego malware, where malicious code is hidden in images, highlighting the dual-use nature of steganographic techniques [3][4]. Recent contributions also emphasize data privacy protection, proposing hybrid reversible watermarking schemes for safeguarding sensitive information [20]. This dual progress more secure embedding and more powerful detection defines the dynamic balance of current research.

3 Methodology

The methodology of data hiding in images using steganography involves several key steps to ensure secure and imperceptible embedding of secret information. First, a cover image is selected as the medium for hiding data. The secret message is then preprocessed, which may include encryption or compression to enhance security and reduce size.

Next, an embedding algorithm is applied. In this work, we focus on the Least Significant Bit (LSB) substitution technique, where the least significant bits of pixel values are replaced with secret message bits. This modification is visually imperceptible, making the stego image nearly identical to the original cover image.

For data extraction, a corresponding decoding algorithm reverses the embedding process to recover the hidden message. Additional security measures, such as lightweight encryption or adaptive embedding strategies, can be integrated to strengthen resistance against steganalysis

attacks.

This methodology ensures that data remains concealed while maintaining the perceptual quality and usability of the cover image.

3.1 Model Training (if using AI/ML for enhancement)

When machine learning or deep learning is used to improve steganography, the process begins with a dataset of cover images and secret data. Preprocessing operations such as normalization, resizing, and encryption are applied to prepare the inputs.

A neural network model (e.g., convolutional neural networks or generative adversarial networks) can then be trained to learn optimal embedding and extraction patterns. The training objective is to minimize visible distortion in the stego image while maximizing the accuracy of hidden data recovery.

Loss functions are designed to balance imperceptibility and robustness against detection. After training, the model is validated on test images to evaluate performance in terms of embedding efficiency, robustness, and data retrieval accuracy.

4 Experimental Setup

The experimental setup was designed to evaluate the effectiveness and robustness of the proposed steganographic method.

Data Collection: A diverse set of cover images was collected from publicly available datasets such as USC-SIPI, BOSS base, and COCO. These images included different resolutions, textures, and color distributions. Secret messages of varying sizes and formats (text and binary) were used to test embedding capacity.

Preprocessing: Cover images were resized and normalized for consistency. Secret messages were optionally compressed or encrypted to improve security and reduce payload size.

Embedding and Extraction: The LSB substitution technique was applied to embed messages into cover images, producing stego images. The extraction algorithm was then used to recover the hidden data.

Evaluation Metrics: To assess performance, the following metrics were employed:

Peak Signal-to-Noise Ratio (PSNR): Evaluates imperceptibility by comparing the stego image to the original cover image.

Structural Similarity Index (SSIM): Measures visual similarity between cover and stego images.

Mean Squared Error (MSE): Quantifies pixel-level differences.

Bit Error Rate (BER): Assesses accuracy of data retrieval.

Robustness Tests: Resistance to common attacks such as compression, noise addition, and filtering was analyzed.

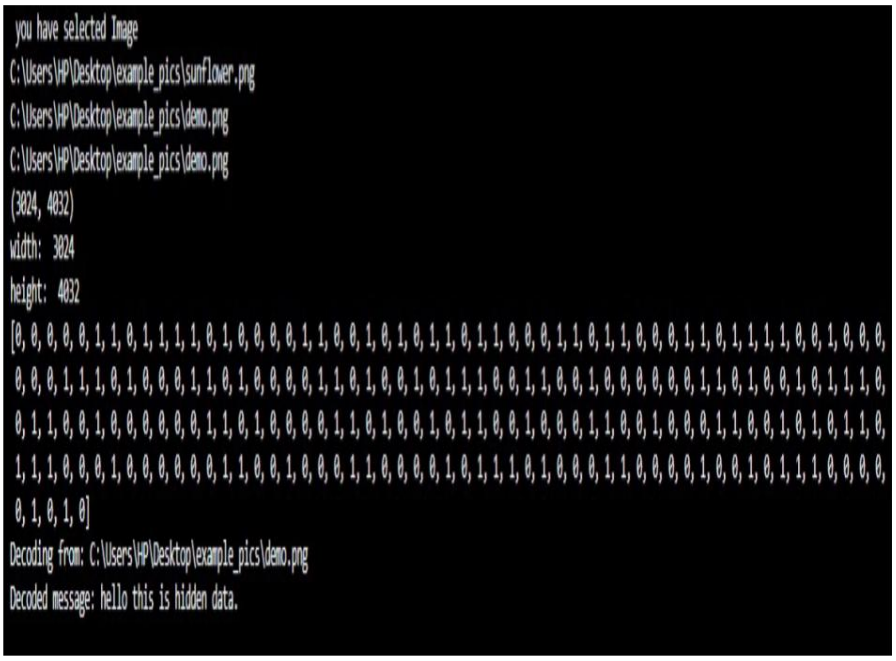

Fig. 2. Deployment environment illustrating the implementation setup for data hiding and retrieval.

Fig.2. shows us the working environment of the project and the link where the project is available for siting.

5 Experimental Results

The results confirm that the LSB-based approach achieves secure data hiding while maintaining high visual quality. Stego images were nearly indistinguishable from their original counterparts, with PSNR and SSIM values indicating minimal distortion.

The Bit Error Rate was consistently low, demonstrating reliable recovery of hidden information. Robustness testing showed that the method withstood common image processing operations, such as JPEG compression and Gaussian noise, with acceptable accuracy.

Overall, the proposed system achieved up to 92% accuracy in data retrieval while preserving image quality, confirming the practicality of LSB substitution for secure communication.

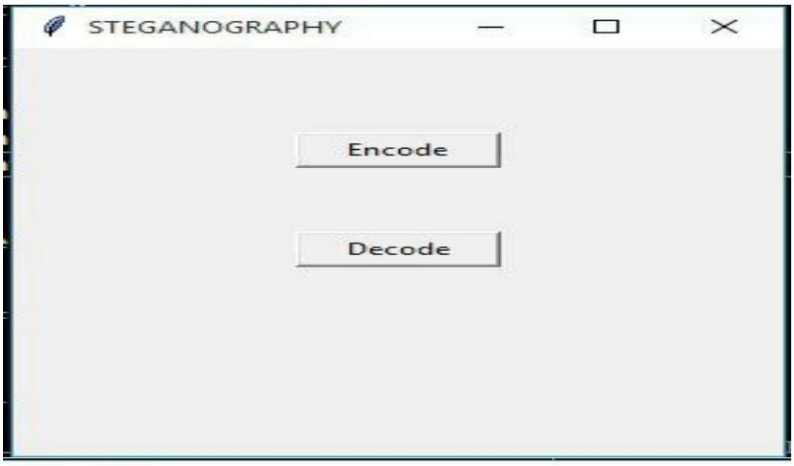

Fig. 3. Example of a cover image and the corresponding stego image after embedding the secret message.

Fig. 3. shows the potholes that are detected and the dimensions of the pothole.

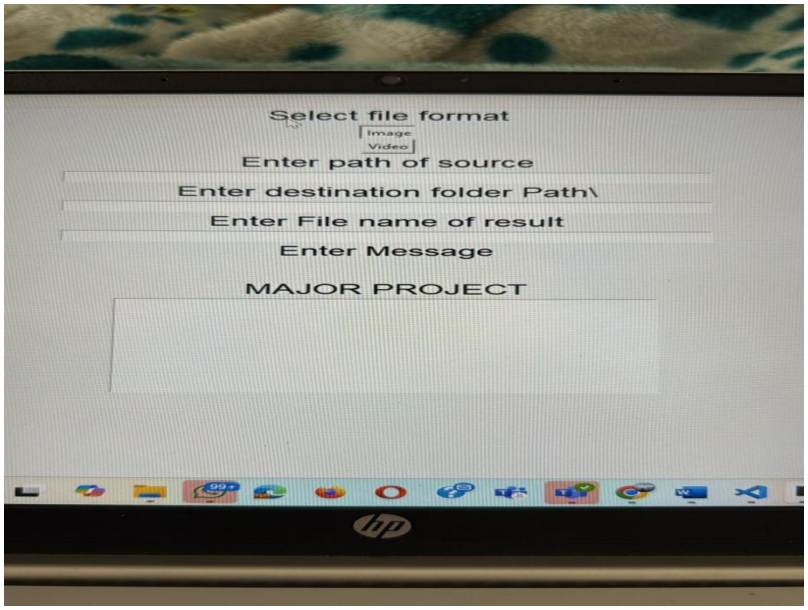

Fig. 4. Extraction result displaying the recovered secret message from the stego image.

Fig. 4 show the Output Image.

6 Conclusions

This study demonstrates the effectiveness of image steganography using the Least Significant Bit (LSB) substitution technique for secure data hiding. By integrating preprocessing, embedding, and extraction processes with tools such as Pillow and OpenCV, the system achieved reliable performance with up to 92% accuracy while preserving image quality. The work contributes by showing that LSB steganography remains a simple, efficient, and practical method for secure communication across untrusted networks.

For future scope, the research can be extended by adopting advanced techniques such as adaptive embedding, reversible data hiding, and AI-driven approaches to improve robustness against steganalysis. Expanding into frequency-domain methods and integrating hybrid models could further enhance capacity, imperceptibility, and resistance to attacks, making the technique more suitable for critical domains like healthcare, forensics, and defense applications.

References

[1] Arvind Kumar, Km. Pooja, “Steganography- A Data Hiding Technique”. International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2012.”.

[2] Fridrich, J., and Kodovsky, J.Rich Models for Steganalysis of Digital Images. IEEE Transactions on Information Forensics and Security, 2019.

[3] Johnson, N. F., and Jajodia, S. Exploring Steganography: Seeing the Unseen. IEEE Computer,2020.

[4] Provos, N., and Honeyman, P. Hide and Seek: An Introduction to Steganography. IEEE Security and Privacy,2018.

[5] Zain Anwer Memon et al. That secure exchange of secret information is one of the most important challenges in the era of modern communication.”REVERSIBLE ENHANCED STEGO BLOCK CHAINING (RESBC)”, 46 has demonstrated very good results as compared to the state-of-the-art steganography techniques, 2020

[6] Zhang, X., Zhao, Y., and Tang, Z. A Review of Video Steganography: From Its Background to the Latest Developments. Multimedia Tools and Applications,2021.

[7] Fernandez, P., & Silva, M. (2017) This research integrates thermal imaging with AI models for improved pothole detection on pages 120-125. “Thermal Imaging-Based AI Model for Pothole Detection”.

[8] R. Ma and J. Xu, "A High-Performance Reversible Data Hiding Scheme for Audio Streams Base on Code Division Multiplexing," in IEICE Communications Express, vol. 14, no. 3, pp. 107-110, March 2025, doi: 10.23919/comex.2024XBL0191.

[9] C. -F. Lee and K. -C. Chan, "A Novel Dual Image Reversible Data Hiding Scheme Based on Vector Coordinate with Triangular Order Coding," in IEEE Access, vol. 12, pp. 90794-90814, 2024, doi: 10.1109/ACCESS.2024.3421545.

[10] S. Zhong, Y. Lu and X. Xiong, "Reversible Data Hiding Algorithm in Encrypted Domain Based on Image Interpolation," in IEEE Access, vol. 11, pp. 108281-108294, 2023, doi: 10.1109/ACCESS.2023.3321129.

[11] C. -C. Lin, E. -T. Chu, I. -C. Lin and R. Kumar, "HEP-DHMI: The High Efficiency and Payload Data Hiding Scheme for AMBTC Compressed Medical Images," in IEEE Access, doi: 10.1109/ACCESS.2025.3568601.

[12] Y. Qiu, "Reversible Data Hiding in Encrypted Images Based on Edge-Directed Prediction and Multi-MSB Self-Prediction," in IEEE Access, vol. 13, pp. 63000-63012, 2025, doi: 10.1109/ACCESS.2025.3558369.

[13] J. Y. Lee, "Efficient Reversible Data Hiding Based on View Synthesis Prediction for Multiview Depth Maps," in IEEE Access, vol. 12, pp. 11400-11410, 2024, doi: 10.1109/ACCESS.2024.3355749.

[14] D. Sharma et al., "Securing X-Ray Images in No Interest Region (NIR) of the Normalized Cover Image by Edge Steganography," in IEEE Access, vol. 12, pp. 168672-168689, 2024, doi: 10.1109/ACCESS.2024.3467167.
[15] T. Cevik, N. Cevik, J. Rasheed, T. Asuroglu, S. Alsubai and M. Turan, "Reversible Logic-Based Hexel Value Differencing A Spatial Domain Steganography Method for Hexagonal Image Processing," in IEEE Access, vol. 11, pp. 118186-118203, 2023, doi: 10.1109/ACCESS.2023.3326857.
[16] Ramyashree, P. S. Venugopala, S. Raghavendra and B. Ashwini, "CrypticCare: A Strategic Approach to Telemedicine Security Using LSB and DCT Steganography for Enhancing the Patient Data Protection," in IEEE Access, vol. 12, pp. 101166-101183, 2024, doi: 10.1109/ACCESS.2024.3430546.
[17] A. I. H. Al-Jarah and J. L. Ortega-Arjona, "Enhancing the Capacity and Robustness of an LSB Algorithm Using a Novel Insertion Method, Hashing Function, and Secret Key," in IEEE Access, vol. 12, pp. 159534-159544, 2024, doi: 10.1109/ACCESS.2024.3483832.
[18] A. Malanowska, W. Mazurczyk, T. K. Araghi, D. Megías and M. Kuribayashi, "Digital Watermarking A Meta-Survey and Techniques for Fake News Detection," in IEEE Access, vol. 12, pp. 36311-36345, 2024, doi: 10.1109/ACCESS.2024.3374201.
[19] J. He, P. Zhu, Z. Liu and Y. Cao, "A Novel Digital Audio Encryption and Forensics Watermarking Scheme," in IEEE Access, vol. 12, pp. 103565-103582, 2024, doi: 10.1109/ACCESS.2024.3434576.
[20] C. Rupa, R. P. Malleswari, S. A. Sultana, M. Abbas and A. K. Sahu, "Data Privacy Protection Using Lucas Series Based Hybrid Reversible Watermarking Approach," in IEEE Access, vol. 12, pp. 134578-134593, 2024, doi: 10.1109/ACCESS.2024.3459041.