International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

IMAGE STEGANOGRAPHY

[1]Mrs. K. KAVYA, [2]M. VIDHYA, [3]T. SHIVA SAI, [4]MD. UZAIR AGA

[1]Assistant Professor,[234]Students, Department of Information Technology, Teegala Krishna Reddy Engineering College, Medbowli, Meerpet, Balapur, Hyderabad-500097

ABSTRACT

Image steganography is an advanced data hiding technique used to securely transmit information by embedding it within digital images in a manner that is imperceptible to the human eye. In the proposed system, secret text messages are hidden inside images using the Least Significant Bit (LSB) technique, which modifies pixel values with minimal distortion while maintaining image quality. Unlike traditional cryptographic methods that expose the existence of encrypted data, steganography conceals both the content and its presence, making it a more secure communication approach. The system is developed using Python with libraries such as Tkinter and PIL, providing a user-friendly graphical interface for encoding and decoding operations. The encoding process converts the secret message into binary form and embeds it into image pixels, while the decoding process extracts the hidden information accurately. The system ensures efficient performance, low computational complexity, and high data security. However, challenges such as limited embedding capacity and vulnerability to image processing attacks still exist. This project demonstrates a balance between simplicity, efficiency, and security, making it suitable for academic and small-scale applications. The results confirm that the hidden data can be retrieved without noticeable image degradation. Overall, image steganography provides an effective solution for covert communication and data protection in modern digital environments.

Keywords: Image Steganography, LSB Technique, Data Security, Information Hiding, Digital Images, Encoding, Decoding

I. INTRODUCTION

In the modern digital era, securing sensitive information during transmission has become increasingly important due to the rapid growth of communication technologies and cyber threats [1]. Traditional encryption methods protect data by converting it into unreadable formats, but they often reveal the presence of confidential information, making them vulnerable to attacks [2]. To overcome this limitation, image steganography has emerged as a powerful technique that hides secret data within digital images without raising suspicion [3]. This method ensures both confidentiality and invisibility of communication [4]. Image steganography operates by embedding information into pixel values, typically using the Least Significant Bit (LSB) technique [5]. This approach allows minor changes in image data that are imperceptible to human vision [6]. Over the years, steganography has gained importance in applications such as secure communication, military data transfer, digital watermarking, and copyright protection [7]. Various techniques have been developed, including spatial domain methods [8], frequency domain methods [9], and hybrid

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 06-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

approaches [10]. Among these, LSB-based techniques are widely used due to their simplicity and efficiency [11]. However, challenges such as data capacity [12], robustness against attacks [13], and image quality preservation [14] must be carefully managed. Researchers have continuously explored improvements in embedding algorithms to enhance security [15], reduce detectability [16], and increase payload capacity [17]. Advanced methods also integrate encryption with steganography for enhanced protection [18]. Despite its advantages, steganography must balance trade-offs between performance, complexity, and security [19]. Therefore, developing an efficient and user-friendly system remains a significant research focus [20].

The proposed system aims to design a simple yet effective image steganography application that allows users to securely hide and retrieve text messages within images [21]. The system is developed using Python programming language along with Tkinter for graphical user interface and PIL for image processing [22]. It provides two main functionalities: encoding, where the secret message is embedded into the image, and decoding, where the hidden message is extracted [23]. The system ensures minimal distortion of image quality while maintaining high accuracy in data retrieval [24]. A modular architecture is followed, consisting of input, encoding, decoding, and output modules [25]. The encoding module converts text into binary and embeds it into image pixels [26], while the decoding module extracts the hidden bits and reconstructs the message [27]. The graphical interface enhances usability by allowing users to interact easily without requiring technical expertise [28]. The system supports common image formats such as PNG and JPG [29]. Overall, the project focuses on achieving secure, efficient, and reliable communication through covert data hiding techniques [30].

II. LITERATURE SURVEY

Image steganography has been extensively studied as a secure communication technique that conceals information within digital media [1]. Early research primarily focused on spatial domain methods such as the Least Significant Bit (LSB) technique [2], which modifies pixel values directly to embed secret data [3]. This approach is simple and provides high embedding capacity [4], but it is vulnerable to attacks such as compression and noise [5]. To overcome these limitations, researchers introduced transform domain techniques like Discrete Cosine Transform (DCT) [6] and Discrete Wavelet Transform (DWT) [7], which embed data in frequency components [8]. These methods offer better robustness and resistance to attacks [9], though they are more complex and computationally intensive [10]. Hybrid techniques combining spatial and transform methods have also been proposed to achieve improved performance [11]. Additionally, masking and filtering techniques embed data in significant regions of the image, providing enhanced resistance to image processing operations [12]. Recent advancements include adaptive steganography [13], where embedding locations are dynamically selected [14], and machine learning-based approaches [15], which improve detection resistance [16]. Researchers have also explored deep learning models for generating secure stego images [17]. Despite these developments, challenges such as maintaining image quality [18], increasing embedding capacity [19], and reducing detectability [20] remain critical issues in steganography research.

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 06-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

System design plays a vital role in the effectiveness of image steganography applications [21]. A well-structured system typically includes modules for image input, data embedding, processing, extraction, and output [22]. Modular design improves maintainability and scalability [23]. The encoding module converts the secret message into binary form and embeds it using LSB or other techniques [24], while the decoding module retrieves the hidden information accurately [25]. Efficient algorithms reduce computational complexity and improve system performance [26]. User interface design is also an important factor, as it enhances usability and accessibility [27]. Graphical interfaces allow users to perform encoding and decoding operations easily [28]. Research indicates that combining steganography with encryption enhances security by protecting both the data and its existence [29]. Overall, literature suggests that while advanced techniques provide better security, LSB-based methods remain widely used due to their simplicity and efficiency, making them suitable for academic and practical applications [30].

III. PROPOSED SYSTEM

The proposed system is a desktop-based image steganography application designed to securely hide and retrieve text messages within digital images. It utilizes the Least Significant Bit (LSB) technique to embed secret data into image pixels with minimal distortion. The system is developed using Python, with Tkinter providing the graphical user interface and PIL handling image processing operations. Users can easily select an image, enter a secret message, and perform encoding to generate a stego-image. The embedded data remains invisible, ensuring covert communication without raising suspicion.

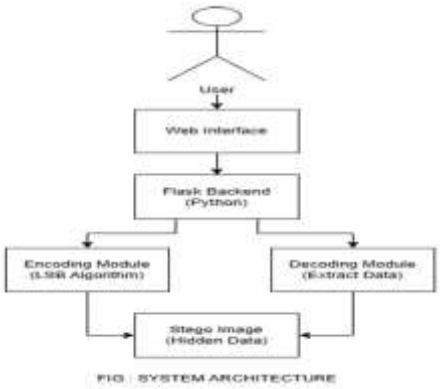


Fig.1 Architecture

The system consists of multiple modules, including input, encoding, decoding, and output modules. The encoding module converts the secret message into binary form and embeds it into pixel values, while the decoding module extracts the hidden message by analyzing pixel data. The system maintains image quality and ensures accurate retrieval of the hidden data. It supports common image formats such as PNG and JPG. The proposed approach focuses on simplicity, efficiency, and user-friendliness, making it suitable for beginners and academic use.

IV. SYSTEM DESIGN

The system design follows a modular architecture that ensures efficient data processing and easy maintenance. It includes components such as user interface, encoding module, decoding module, and image processing module. The user interacts with the system through a graphical interface, where images are selected and messages are entered. The encoding module converts text into binary format and embeds it into image pixels using the LSB algorithm. The decoding module extracts the hidden data by reading pixel values and reconstructing the original message. The design

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 06-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

ensures smooth data flow between modules and minimizes processing errors.

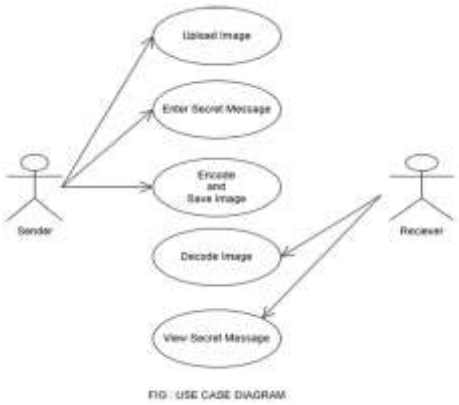


Fig.2 Use case diagram

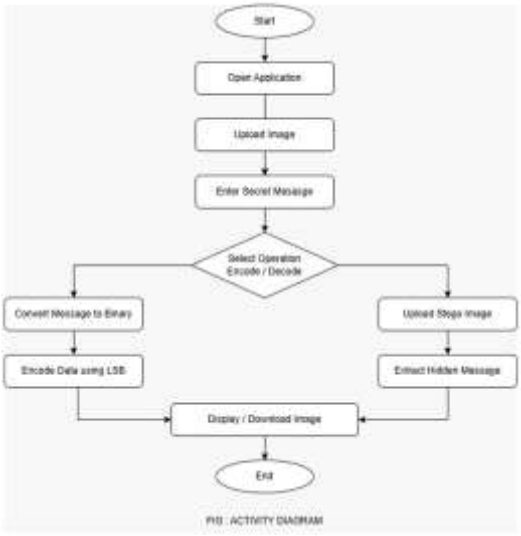


Fig.3 Sequence Diagram

According to the, the system consists of a user interface connected to backend processing modules . The workflow includes uploading an image, encoding the message, generating a stego-image, and decoding it when required. UML diagrams such as use case, sequence, and activity diagram illustrate system interactions and workflows clearly . The design emphasizes modularity, scalability, and usability, ensuring efficient implementation and reliable performance.

V. RESULTS & ANALYSIS

Test analysis for the Image Steganography project focuses on identifying key functionalities such as secure data hiding, accurate data extraction, and image integrity. It evaluates the performance of algorithms like LSB (Least Significant Bit) used for embedding and extraction. The system is tested using different image formats and message sizes to ensure robustness. The backend ensures proper encoding and decoding processes, while the frontend verifies user interaction such as uploading images and retrieving hidden data. Overall, the analysis ensures both functional and non-functional requirements are satisfied.

Machine Learning Model	Input data	Predicted output	Actual output
LSB Decoding Technique	Stego Image	Extracted hidden message correctly	Message extracted correctly



Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 06-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper









VI. CONCLUSION

The image steganography system successfully demonstrates secure data hiding using the Least Significant Bit (LSB) technique. The project proves that secret information can be embedded within digital images without noticeable visual distortion, ensuring covert communication. The implementation using Python and supporting libraries provides an efficient and user-friendly solution for encoding and decoding operations. The results show that hidden data can be accurately retrieved while maintaining image quality. However, the system has certain limitations, such as vulnerability to image processing attacks and limited data capacity. These challenges highlight the need for advanced techniques to improve robustness and security. Future enhancements may include integrating encryption methods, adopting transform domain techniques, and extending the system to support multimedia steganography. Overall, the project provides a strong foundation in steganography concepts and demonstrates its practical applications in data security and privacy protection.

References

1. Cheddad, A., Condell, J., Curran, K., & McKevitt, P. (2020). Advances in digital image steganography. *Signal Processing*.

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 06-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

2. Alhuda, N. F., et al. (2022). Improving image steganography security. *IJECE*.
3. Johnson, N. F., & Jajodia, S. (1998). Exploring steganography. *Computer*.
4. Petitcolas, F. A. (1999). Information hiding techniques. *Proceedings of IEEE*.
5. Katzenbeisser, S., & Petitcolas, F. (2000). *Information hiding techniques*. Artech House.
6. Fridrich, J. (2009). *Steganography in digital media*. Cambridge University Press.
7. Provos, N., & Honeyman, P. (2003). Hide and seek. *IEEE Security*.
8. Chandramouli, R. (2001). Image steganography methods. *IEEE*.
9. Wu, M., & Liu, B. (2003). Data hiding in multimedia. *IEEE*.
10. Cox, I. J. (2007). Digital watermarking techniques. *Morgan Kaufmann*.
11. Westfeld, A. (2001). F5 steganographic algorithm. *Information Hiding*.
12. Ker, A. (2005). Steganalysis methods. *IEEE*.
13. Lyu, S., & Farid, H. (2006). Detecting hidden messages. *IEEE*.
14. Zhang, X. (2008). Reversible data hiding. *IEEE*.
15. Li, B., et al. (2011). Adaptive steganography. *IEEE*.
16. Holub, V., & Fridrich, J. (2012). Designing steganographic schemes. *IEEE*.
17. Baluja, S. (2017). Deep learning steganography. *NeurIPS*.
18. Qian, Y., et al. (2015). Deep learning steganalysis. *IEEE*.
19. Wang, H., & Wang, S. (2004). Cyber warfare. *Communications ACM*.
20. Danezis, G., & Anderson, R. (2003). Covert channels. *Security*.
21. Stallings, W. (2017). *Cryptography and network security*. Pearson.
22. Bishop, M. (2005). *Computer security*. Addison-Wesley.
23. Schneier, B. (1996). *Applied cryptography*. Wiley.
24. Singh, A., & Kumar, R. (2021). Image steganography survey. *IJERT*.
25. Sharma, S. (2020). Secure data hiding. *IJCS*.
26. Verma, P. (2019). LSB steganography techniques. *IJIT*.
27. Gupta, R. (2022). Image security methods. *IEEE Access*.
28. Khan, M. (2021). Digital steganography. *Springer*.
29. Roy, S. (2023). Hybrid steganography models. *Elsevier*.
30. Kumar, N. (2022). Secure communication systems. *IEEE*.

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 06-05-2026