International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 12 | Dec – 2025 DOI: 10.55041/ISJEM05321
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

# Secure Data Communication Using Steganography

**Shwetha K**
AssistantProfessor,
Department of Electronics and Communication Engineering,
MaharajaInstituteofTechnology Mysore, Karnataka, India
shwetha_ece@mitmysore.in

**Bhandavya A R**
Department of Electronics and Communication Engineering,
MaharajaInstituteofTechnology Mysore, Karnataka, India
bhandavya274@gmail.com

**Ganavi**
Department of Electronics and Communication Engineering,
MaharajaInstituteofTechnology Mysore, Karnataka, India
ganavigowda2518@gmail.com

**Likhith K**
Department of Electronics and Communication Engineering, Maharaja Institute of Technology Mysore, Karnataka, India likhithk140@gmail.com

**Rithisha**
Department of Electronics and Communication Engineering, Maharaja Institute of Technology Mysore, Karnataka, India
rithisha17hamse@gmail.com

***Abstract*—In the present digital era, ensuring secure and confidential communication over open networks has become increasingly important due to rapid growth of cyber threats and data interception techniques.Traditional encryption methods protect the content of information but do not conceal the existence of the communication, which can attract unwanted attention.**

**This work presents the development of a secure data communication system utilizing steganography for embedding sensitive information into multimedia files, including images and text. The preposed methodology incorporates least significant bit (LSB) technique. Experimental results demonstrate that the system effectively embeds and retrieves hidden data with high accuracy, maintain imperceptibility and robustness under controlled conditions. The user interface was evaluated for usability, ensuring operational stability and effective feedback mechanisms.The study highlights that while the system achieves reliable concealment and secure transmission of data, challenges such as limited embedding capacity, vulnerability to steganalysis, and susceptibility to media manipulations remain.**

***Keywords*—Steganography, Secure data Communication, Least Significant Bit, Multimedia data hiding,InformationSecurity, Steganalysis, Data Confidentiality**

## I.INTRODUCTION

In today's interconnected digital landscape, the demand for secure and confidential communication has grown significantly. With the proliferation of internet-based services, cloud storage, and wireless communications, sensitive information such as personal data, financial transactions, and proprietary business secrets is constantly transmitted across various networks. While encryption algorithms like AES, RSA, and Blowfish are effective at securing data by transforming it into an unreadable format, they do not conceal the very presence of the transmitted information. This visibility can attract unwanted attention from malicious actors, government surveillance, or censorship authorities. As a result, even encrypted data can become a target, risking exposure or interception. This creates a compelling need for methods that can both secure and disguise information during transmission. Steganography, the art of hiding information within digital media files such as images, audio, videos, or text, offers an effective solution to this problem.

Unlike cryptography, which makes data unreadable but visible, steganography aims to obscure the very existence of the secret message, thus providing an additional layer of security. Modern techniques utilize sophisticated algorithms to embed secret data into digital media imperceptibly. For example, the Least Significant Bit (LSB) technique modifies the least significant bits of pixel or audio samples to encode hidden information without noticeable changes in the host media. Frequency domain techniques like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) embed data into the frequency components of images, offering better resilience against image processing operations and compression. In recent years, combining steganography with cryptographic methods has gained prominence. Encrypting data prior to embedding it within media files ensures that even if the hidden message is detected, it remains unintelligible without the description key.

Steganography embeds secret data within innocuous-looking digital media such as imagesor text, making the communication appear ordinary and unremarkable. By hiding data within the redundant or perceptually insignificant

components of media files, steganography minimizes the likelihood of detection by unintended observers. This covert nature distinguishes steganography from cryptography and makes it particularly suitable for secure communication in surveillance-proneor censorship-controlled environments. With the widespread availability of high-resolution multimedia content and the increasing use of social media, multimedia messaging, and file sharing platforms, digital media has become an ideal carrier for steganographic communication.

## II. LITERATURE REVIEW

Johnson and Jajodia [1] introduced one of the earliest and most influential studies on digital image steganography using the Least Significant Bit (LSB) technique. Their work demonstrated that secret data could be embedded into image pixels with minimal perceptual distortion, making it difficult for human observers to detect hidden information. This study laid the foundation for modern spatial-domain steganography methods.

Provos and Honeyman [2] analysed practical steganographic tools and highlighted the vulnerabilities of basic LSB-based techniques to statistical steganalysis. Their research emphasized that while LSB steganography is simple and effective, it requires additional security measures to resist detection. This work motivated further research into improving robustness and security in data hiding systems.

Petitcolas et al. [3] provided a comprehensive review of information hiding techniques and proposed the integration of cryptography with steganography to enhance security. Their findings showed that encrypting data prior to embedding significantly improvesconfidentiality, even if the hidden data is detected. This hybrid approach has since become a standard practice in secure steganographic systems**.**

Singh and Gupta [4] studied the trade-off between embedding capacity and imperceptibility in image steganography systems. Their experimental results indicated that increasing payload size can degrade image quality and increase detectability. This work highlighted the importance of balancing data capacity with robustness and visual quality.

More recently, Hassaballah et al. [5] proposed an advanced steganography approach using transform-domain techniques such as DCT to improve resistance against compression and media manipulation. Their results demonstrated enhanced robustness and security compared to traditional spatial-domain methods, making the approach suitable for real-world secure data communication applications.

## III. METHODOLOGY

The proposed secure data communication system employs a steganographic approach combined with encryption to ensure confidentiality and covert transmission of sensitive information. The overall methodology consists of data preprocessing, encryption, embedding, extraction, and evaluation phases.

Initially, the secret message is collected from the user and converted into a binary format. To enhance security, the data may be encrypted before embedding, ensuring that even if the hidden information is detected, it remains unintelligible to unauthorized users. A suitable cover medium, such as a digital image or text file, is then selected to act as the carrier for the hidden data.


**Figure1:Block diagram of steganography methodology**

The Least Significant Bit (LSB) technique is used for data embedding. In this process, the least significant bits of the carrier media are replaced with the binary bits of the encrypted message. This modification introduces minimal changes to the original file, maintaining imperceptibility while allowing efficient data hiding. The embedding process is carefully controlled to avoid excessive distortion and preserve media quality.

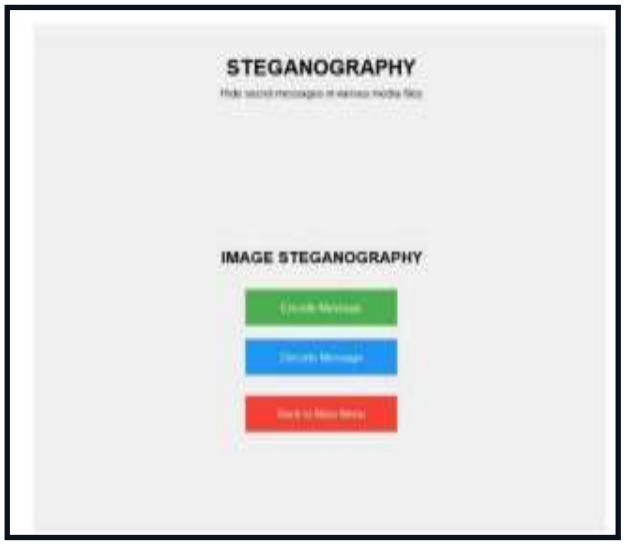
For data extraction, the stego file is processed using the reverse LSB operation to retrieve the embedded binary data. The extracted data is then decrypted to recover the original secret message. The system ensures accurate recovery of information without data loss under controlled conditions.

Finally, the performance of the system is evaluated based on parameters such as imperceptibility, data retrieval accuracy, and robustness. A graphical user interface (GUI) is implemented to improve usability, provide operational feedback, and ensure system stability during encoding and decoding operations.

## IV. RESULTS AND DISCUSSION

IMAGE STEGANOGRAPHY

1. Image steganographyinterface




2. Encoding of image


3. Encoded image file


4. Decoded image file

TEXT STEGANOGRAPHY

[1] Text steganography interface


[2] Encoding of text message


[3] Encoded message file


[4] Decoded Text Message


## V. CONCLUSION

.In this paper, a secure data communication system utilizing steganography has been designed and implemented to enable covert transmission of sensitive information over open networks. The proposed methodology employs the Least Significant Bit (LSB) technique to embed encrypted data into multimedia carrier files such as images and text, ensuring both confidentiality and imperceptibility. Experimental evaluation demonstrates that the system successfully embeds and retrieves hidden information with high accuracy while preserving the quality and visual integrity of the carrier media. The developed graphical user interface further enhances usability, operational stability, and user interaction during encoding and decoding processes.

Despite its effectiveness and simplicity, the proposed approach exhibits limitations, including restricted embedding capacity and susceptibility to steganalysis and media manipulation attacks. Nevertheless, the results confirm that LSB-based steganography remains a practical solution for secure data hiding in controlled environments. Future work may focus on adopting transform-domain techniques, adaptive embedding methods, and machine learning-based security mechanisms to improve robustness, scalability, and resistance against advanced detection techniques, thereby extending the applicability of the system to real-world secure communication scenarios.

## VI. REFERENCES

[1] R. Balaji and G. Naveen, "Secure Data Transmission Using Video Steganography," in Proc. Int. Conf. on Computing, Communication and Networking Technologies (ICCCNT), Sri Sai Ram Engineering College, Chennai, India, 2011, doi:10.1109/EIT.2011.5978601

[2] K. C. Nunna and R. Marapareddy, "Secure Data Transfer Through Internet Using Cryptography and Image

Steganography," School of Computing Sciences and Computer Engineering, The University of Southern Mississippi, Hattiesburg, USA, Unpublished manuscript, doi:10.1109/SoutheastCon44009.2020.9368301

[3] M. I. S. Reddy and A. P. S. Kumar, "Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm," in Proc. Int. Conf. on Computational Modelling and Security (CMS 2016), Nandyal, India, 2016, doi: 10.1016/j.procs.2016.05.177

[4] S. A. Laskar and K. Hemachandran, "Secure Data Transmission Using Steganography and Encryption Technique," Int. J. Cryptogr. Inf. Secur. (IJCIS), vol. 2, no. 3, pp. 161–170, Sep. 2012, doi:10.5121/ijcis.2012.2314.

[5] R. Bala Krishnan, P. K. Thandra, and M. S. Baba, "An Overview of Text Steganography," in Proc. Fourth Int. Conf. on Signal Processing, Communication and Networking (ICSCN), Chennai, India, 2017, doi: 10.1109/ICSCN.2017.8085643

[6] M. A. Majeed, R. Sulaiman, Z. Shukur, and M. K. Hasan, "A Review on Text Steganography Techniques," Mathematics, vol. 9, no. 21, p. 2829, Nov. 2021, doi: 10.3390/math9212829

[7] M. H. Kombrink, Z. J. M. H. Geradts, and M. Worring, "Image steganography approaches and their detection strategies: A survey," ACM Computing Surveys, vol. 57, no. 2, 2024, doi: 10.1145/3694965