Information Transmission in Crime Branch Using Steganography

Dr. M. Rahimal Beevi[1], Ms. S. Monisha[2]
[1]*Assistant Professor, Department of MCA,* [2]*Final MCA,*
[1,2] *Mohamed Sathak Engineering College, kilakari.*

***Abstract*—Steganography is the technique of concealing secret information within a digital medium such that its existence remains undetectable. This paper presents a PHP-based image steganography system that employs the Least Significant Bit (LSB) algorithm to embed encrypted text within JPEG images. The proposed system introduces a double-security mechanism requiring two levels of authentication—an encryption key and a validation code—thereby enhancing confidentiality beyond conventional steganographic approaches. A history database is maintained for credential recovery, and the original image quality is fully preserved after embedding. Experimental results demonstrate that the hidden data is imperceptible to the human eye, and the system provides a user-friendly interface for secure covert communication.**

***Keywords*—Steganography, LSB Algorithm, Image Security, PHP, Double Authentication, Data Hiding.**

I. INTRODUCTION

Steganography is the art and science of hiding secret messages within an ordinary digital medium so that only the intended recipient is aware of its existence. Unlike cryptography, which makes data unreadable, steganography conceals the very presence of the communication. In digital images, each pixel is composed of three color channels—Red, Green, and Blue (RGB)—each represented by 8 bits. The Least Significant Bit (LSB) of each channel can be altered to carry hidden information without causing a perceptible change in the image's visual appearance.

This project develops a double-security steganography system using PHP 5.4 as the server-side technology. The system requires two levels of authentication: an encryption key and a validation code, both of which are recorded in a history database for recovery. The safe-hiding approach guarantees that no visible modification occurs to the source image after embedding, and a built-in testing module verifies the integrity of the stego-image.

1.1 Organization Profile

Phoenix Softech was established in 2001 in Madurai, with additional branches in Chennai and Coimbatore. The organization focuses on providing IT strategy consulting and technology solutions across healthcare, pharmaceuticals, logistics, and other verticals. Its mission is to provide market access for state-of-the-art Hi-tech products and services in Information Technology.

1.2 Methodology

The methodology centers on securely embedding secret data within a cover image without causing noticeable changes. The process begins with selecting a PNG or BMP cover image, converting the secret text into binary via ASCII values, and applying the LSB technique pixel by pixel using PHP's GD library. An end-of-message delimiter is appended to facilitate accurate extraction. For retrieval, the stego-image's LSBs are read sequentially and the binary stream is reconstructed into the original message.

II. LITERATURE SURVEY

Recent advancements in the field of information security have significantly focused on techniques such as steganography ancryptography for secure data transmission. Various researchers have explored different methods to improve confidentiality, robustness, and efficiency of hidden communication systems.

Neil F. Johnson and Sushi Jodie (1998) provided one of the earliest comprehensive studies on steganography, explaining its fundamental principles, applications, and limitations. Their work laid the foundation for modern data hiding techniques but mainly focused on theoretical aspects rather than practical implementations.

Chi-Kong Chan and L.M. Cheng (2004) proposed an improved Least Significant Bit (LSB) substitution method that enhances data embedding capacity while maintaining image quality. However, the method

shows vulnerability against statistical and steganalysis attacks.

Jessica Fridrich (2009) introduced advanced steganographic and steganalysis techniques, focusing on improving robustness and detection resistance. Although the approach increases security, it also introduces higher computational complexity, making it less suitable for real-time applications.

Mehdi Kharrazi et al. (2006) concentrated on steganalysis methods used to detect hidden information within digital media. Their work contributed to understanding potential vulnerabilities but did not address secure embedding mechanisms.
In the domain of cryptography, several studies have emphasized combining encryption with steganography to provide an additional layer of security. Hybrid approaches ensure that even if hidden data is detected, it remains protected through encryption techniques.

Despite these advancements, existing systems still face challenges such as limited security layers, lack of efficient key management, and vulnerability to attacks. Therefore, there is a need for a more secure and efficient system that integrates both cryptographic and steganographic techniques.

The proposed system addresses these limitations by implementing a dual-security mechanism using encryption and validation code along with LSB-based image steganography. This approach enhances confidentiality, improves reliability, and ensures secure information transmission.

2.1 EXISTING SYSTEM

Existing data-hiding approaches embed data into digital media using legacy technologies such as ASP with MS-Access. These systems suffer from significant drawbacks in terms of speed, security, and key management. Figure 1 illustrates the architecture and limitations of the existing system.

- Time-consuming processing due to outdated ASP technology.
- Key field assigned as a simple password, reducing overall security.
- No encryption applied before data transmission.

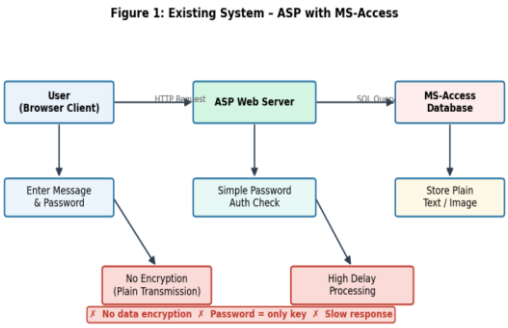

Figure 1: Existing System – ASP with MS-Access Architecture & Limitations

2.2 PURPOSE OF WORK

The primary purpose of this work is to develop a secure and efficient system for transmitting confidential information using a combination of steganography and cryptography techniques. The system aims to hide sensitive data within digital images in such a way that its presence remains undetectable, while also ensuring that the embedded data is protected through encryption. By integrating these two approaches, the proposed system enhances the overall security of data communication and minimizes the risk of unauthorized access.

III. PROPOSED SYSTEM

The proposed system overcomes existing limitations by adopting PHP with MySQL and implementing LSB-based steganography with double-layer authentication. Figure 2 shows the complete architecture of the proposed system including sender, receiver, and database components.

- High security through double-layer authentication (encryption key + validation code).
- No processing delays due to optimized LSB algorithm in PHP.
- Key field managed via a secure history database for recovery.

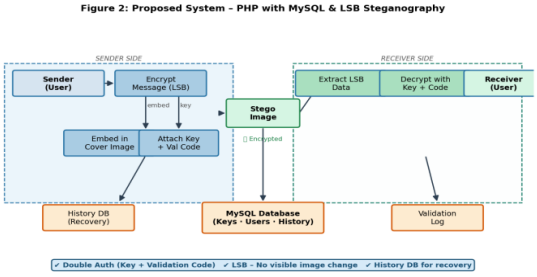

Figure 2: Proposed System – PHP + MySQL with LSB Steganography & Double Authentication

IV. SYSTEM MODULES

The system is organized into the following functional modules:

SENDER SIDE

a) Data Encryption

In this module, the input message is first converted into a secure format before embedding. The text is transformed into binary representation, and encryption is applied to enhance confidentiality. The encrypted data is then prepared for embedding into the image using the Least Significant Bit (LSB) technique.

b) Data Embedding

The encrypted message is embedded into the cover image using the LSB algorithm. Instead of directly inserting plain text, the system modifies the least significant bits of image pixels to store the encrypted data. This approach ensures that there is no noticeable change in the visual quality of the image, thereby maintaining its original appearance.

c) Image Transmission

Once the embedding process is completed, the stego-image is transmitted to the receiver. Along with the image, a validation code and password are provided as additional security parameters. These credentials ensure that only authorized users can access the hidden information.

RECEIVER SIDE

a) Data Extraction

At the receiver end, the system extracts the hidden data from the received stego-image. The least significant bits of the image pixels are analyzed to retrieve the embedded binary data.

b) Data Decryption

After extraction, the encrypted data is decrypted using the corresponding validation code and password. By applying the reverse process of encryption, the original message is reconstructed accurately. The use of secure keys ensures that unauthorized access is prevented.

USER CONFIGURATION

This module manages access control within the system. It defines permissions for different users to send and receive messages. Access rights are assigned based on user roles such as Inspector, Sub-Inspector, and other authorized personnel, ensuring controlled and secure communication.

USER DETAILS

The user details module maintains a record of all registered users within the system. It stores essential information required for authentication and communication, enabling efficient user management.

BRANCH CREATION

This module handles the creation and management of different branches within the system. Each branch is uniquely identified using a branch ID, allowing organized communication across multiple units.

USER CREATION

In this module, new users can register by providing their personal and login details. The information is securely stored in the database. Upon successful registration, users are assigned unique login credentials, which are used for authentication and system access.

5. Data Flow Diagram

The Data Flow Diagram (DFD) in Figure 3 models the complete flow of information through the steganography system, from initial message input by the sender through embedding, transmission, extraction, and final decryption by the receiver. The diagram identifies all external entities (Sender, Receiver, Admin), internal processes (P1–P7), and data stores (D1: MySQL for users and keys; D2: Mailbox/History).

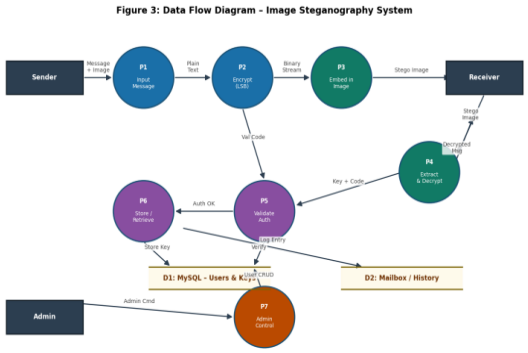

Figure 3: Data Flow Diagram – Image Steganography System (Processes P1–P7)

V. CONCLUSION

In this paper, a secure and efficient image steganography system based on the Least Significant Bit (LSB) algorithm has been successfully developed using PHP. The proposed system effectively hides encrypted text within JPEG images while preserving the original image quality. The implementation of a double-layer security mechanism, consisting of an

encryption key and a validation code, significantly enhances the confidentiality of the hidden data.

The system also provides additional features such as a history database for credential recovery and a user-friendly interface, making it practical and easy to use. Experimental results confirm that the embedded data remains imperceptible to the human eye, ensuring secure covert communication.

Overall, the proposed system demonstrates a reliable and effective approach for secure information transmission, with strong potential for further enhancements and real-world applications.

VI. FUTURE ENHANCEMENTS

While the proposed system ensures secure and imperceptible data embedding, there is still significant scope for further improvements. In future, the system can be enhanced by incorporating advanced encryption techniques to strengthen data security. The implementation of more robust steganographic methods, such as transform-domain algorithms, can improve resistance against various attacks and detection techniques.

Additionally, support for multiple media formats, including PNG images, audio, and video files, can be introduced to increase flexibility and usability. The system can also be extended into a mobile or web-based application, enabling users to access secure communication services more conveniently from different platforms.

Furthermore, integrating artificial intelligence and machine learning techniques can help optimize embedding capacity and improve detection avoidance. Features such as real-time processing, enhanced key management, and multi-user authentication can also be added to make the system more scalable and efficient.

Overall, these enhancements will significantly improve the reliability, security, and adaptability of the system in future applications.

REFERENCES

[1] J. Heather and D. Lundin, "The append-only web bulletin board," in Formal Aspects in Security and Trust, Springer, 2008, pp. 242–256.

[2] T. Jung, J. Han, and X.-Y. Li, "PDA: Semantically secure time-series data analytics with dynamic subgroups," IEEE TDSC, vol. PP, no. 99, pp. 1–1, 2016.

[3] T. Jung and X.-Y. Li, "Collusion-tolerable privacy-preserving sum and product calculation without secure channel," IEEE TDSC, vol. 12, no. 1, pp. 45–57, 2014.

[4] T. Jung et al., "AccountTrade: Accountable protocols for big data trading against dishonest consumers," in Proc. IEEE INFOCOM, 2017, pp. 1–9.

[5] K. Khurana and M. Chandak, "Key frame extraction methodology for video annotation," IJCEIT, vol. 4, no. 2, pp. 221–228, 2013.

[6] J. Kim et al., "Salient region detection via high-dimensional color transform," IEEE Trans. Image Process., vol. 25, no. 1, pp. 9–23, 2016.

[7] D. C. Lee, Q. Ke, and M. Isard, "Partition min-hash for partial duplicate image discovery," in Proc. ECCV, Springer, 2010, pp. 648–662.

[8] J. Leskovec and A. Krevl, "SNAP Datasets: Stanford large network dataset collection," 2014.

[9] J. Leskovec, A. Rajaraman, and J. D. Ullman, Mining of Massive Datasets. Cambridge University Press, 2014.

[10] X.-Y. Li et al., "Graph-based privacy-preserving data publication," in Proc. IEEE INFOCOM, 2016, pp. 1–9.