Professor Gurav P.S., 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

IMGCRYPT: Secrets Hidden Within Ordinary

Professor Gurav P.S.[1], Nirbhay Patil[2], Saksham bansode[3], Sahil Bhujbal[4]
Department of Computer Engineering
TSSM's Bhivarabai Sawant College of Engineering and Reseach

Abstract- In today's digital world, securing sensitive information is very important. Traditional encryption protects data but may attract attention. To overcome this, steganography hides the existence of data itself. This paper presents IMGCRYPT, a system that combines image steganography and encryption to securely hide confidential information inside ordinary images. The proposed system ensures that the hidden data remains invisible and protected even if detected. The approach uses encryption algorithms along with Least Significant Bit (LSB) technique to embed data into images. The system is efficient, secure, and user-friendly, making it suitable for secure communication.

Keywords: Steganography, Image Encryption, Data Security, LSB Technique, Cyber Security.

I. INTRODUCTION

With the rapid growth of internet usage, data security has become a major concern. Sensitive data such as personal messages, passwords, and confidential documents are vulnerable to cyber threats. Traditional methods like encryption convert data into unreadable form, but they do not hide the existence of the data. This may raise suspicion. To solve this issue, steganography is used, which hides the data inside another medium such as images, audio, or video. The project IMGCRYPT focuses on hiding secret data inside images in such a way that it is not noticeable to human eyes. Additionally, encryption is applied to increase security.

The proposed system, IMGCRYPT: Secrets Hidden Within Ordinary, integrates both cryptography and steganography to provide a robust and secure communication mechanism. In this approach, the secret message is first encrypted using a suitable encryption algorithm to ensure confidentiality. The encrypted data is then embedded into an image using the LSB technique, thereby concealing its existence. This dual-layer security approach significantly enhances the overall protection of sensitive information.

The system is designed to be efficient, reliable, and user-friendly, making it suitable for real- world applications. By combining the strengths of both encryption and steganography, IMGCRYPT provides a secure solution for data transmission, minimizing the risk of detection and unauthorized access. This paper presents the design, implementation, and evaluation of the proposed system, highlighting its effectiveness in ensuring secure communication.

II. PROBLEM STATEMENT

Existing security systems mainly rely on encryption, which makes data unreadable but visible. This visibility can attract attackers.

There is a need for a system that:

- Hides the existence of data
- Provides strong security
- Ensures safe transmission

Objectives

- **To develop a system that hides secret data inside images**
- To combine encryption with steganography
- To ensure secure communication
- To make the system simple and user- friendly

III. LITERATURE REVIEW

Many researchers have worked on data security using steganography.

- LSB (Least Significant Bit) is one of the most widely used techniques for image steganography.
- Some systems use only steganography, which is less secure if detected.
- Others use only encryption, which does not hide the presence of data.

IMGCRYPT combines both approaches to provide dual-layer security.

IV. METHODOLOGY

System Overview

The system works in two main phases:

- **Encryption Phase –** The secret data is encrypted
- **Embedding Phase –** The encrypted data is hidden inside an image

Encryption Process

- The message is converted into encrypted format
- Algorithms like AES or simple encoding can be used

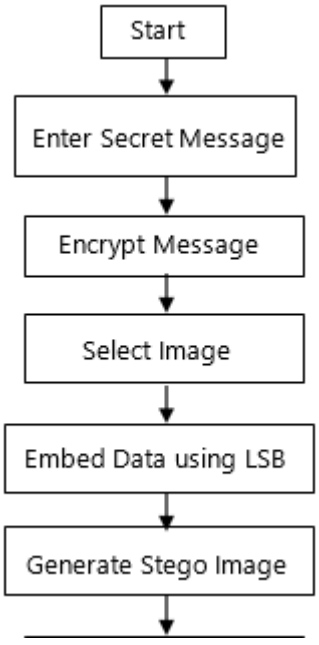
Steganography Process

- The encrypted data is embedded into the image
- LSB technique is used to modify pixel values slightly
- Changes are not visible to human eyes

Extraction Process

- The hidden data is extracted from the image
- Decryption is applied to get the original message

VI. FLOWCHART



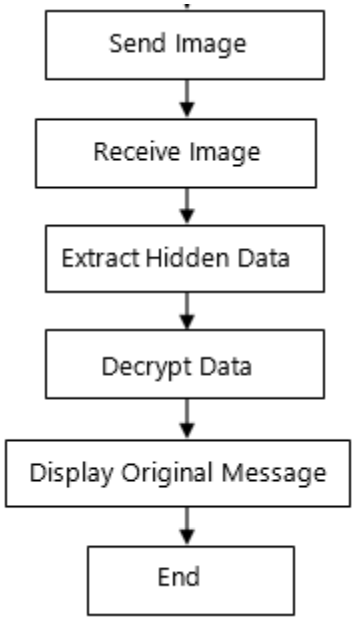


Figure 3 Flowchart of the application

VI. SYSTEM ARCHITECTURE

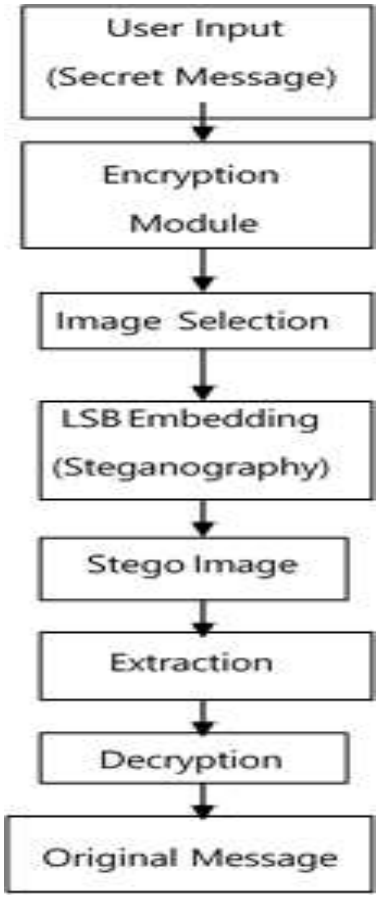


Figure 2 System Architecture of the application

- User inputs secret message
- System encrypts the message
- Image is selected as cover image
- Data is embedded into image
- Stego-image is generated
- Receiver extracts and decrypts data

VII. ADVANTAGES

- High security due to encryption + steganography
- Data remains invisible
- Easy to use
- Suitable for secure communication

Applications

- Military communication
- Secure messaging
- Digital watermarking
- Banking and confidential data transfer

VIII. LIMITATIONS

- Limited data capacity based on image size
- Compression may destroy hidden data
- Requires proper key for decryption

Future Scope

- Use of advanced AI-based steganography
- Support for video and audio files
- Improved encryption algorithms
- Cloud-based secure communication

IX. CONCLUSION

IMGCRYPT provides a secure way to protect sensitive data by combining encryption and steganography. It ensures that the data is both hidden and protected, making it difficult for attackers to detect or access. This system can be widely used in various fields requiring secure communication.

The proposed system is simple to use, efficient in performance, and adaptable to different types of images. It can be effectively used in applications requiring secure communication, such as military operations, banking systems, and confidential data transfer. Despite certain limitations, such as dependency on image size and vulnerability to compression, the system provides a strong foundation for secure data hiding.

Future enhancements can further improve the system by incorporating advanced encryption algorithms, artificial intelligence-based steganography techniques, and support for multimedia formats such as audio and video. Overall, IMGCRYPT demonstrates a practical and reliable solution for enhancing data security in modern communication systems.

REFERENCES

1. "Cryptography and Network Security" by William Stallings
2. Research papers on Image Steganography (IEEE)
3. Online resources on LSB Technique
4. Cyber Security journals