CADT
IDT Institute of Digital Technology

IMAGE STEGANOGRAPHY USING LSB TECHNIQUE

Cryptography Project Report
Generation 10

Lecturer: Mr. Meas Sothearath

Student Name	Soth Vandy
Course	Cryptography
Project Type	Image Steganography - - cover & payload text
Technology	Python, Image Processing
Academic Year	2024 – 205

ABSTRACT

Steganography is a security technique used to conceal secret information inside digital media such that the existence of the information is not noticeable. This project presents the design and implementation of an image steganography system based on the Least Significant Bit (LSB) technique. The system embeds secret textual data within an image by modifying pixel values in a way that preserves visual quality. The proposed method is simple, efficient, and suitable for educational and introductory cybersecurity applications.

1. INTRODUCTION

In the modern digital era, the protection of sensitive information is a major concern. While cryptography secures data by transforming it into an unreadable format, it does not hide the presence of communication. Steganography complements cryptography by concealing the existence of secret information within ordinary digital files such as images. This project focuses on image steganography using the Least Significant Bit (LSB) technique, which alters the lowest bits of pixel values to embed data without producing visible changes.

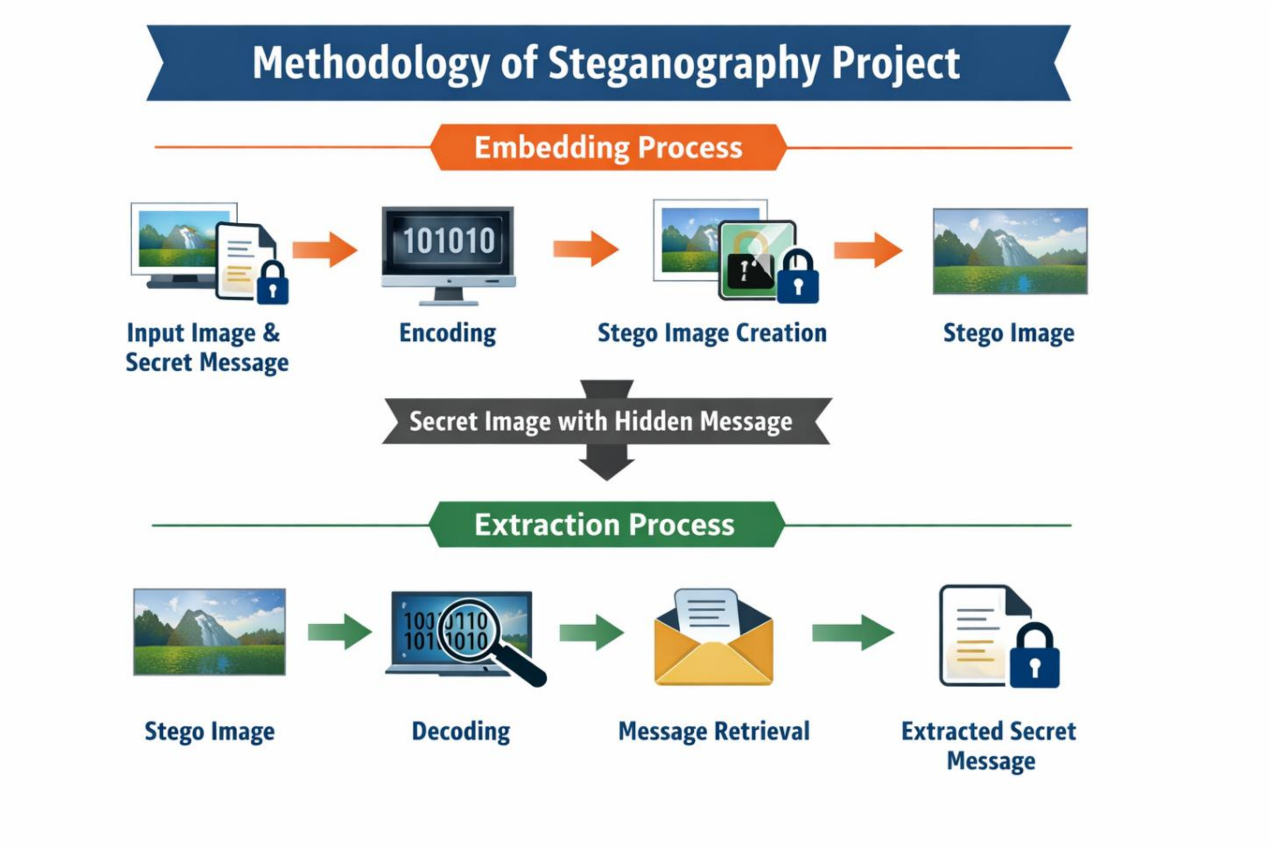
1.1 OBJECTIVES OF THE PROJECT

The primary objectives of this project are:

- To study the concept of image steganography
- To implement LSB-based data hiding using Python
- To embed secret text securely inside an image
- To retrieve the hidden message accurately
- To understand information hiding techniques in cybersecurity

2. METHODOLOGY

The methodology involves converting the input image into RGB format and embedding secret data into the least significant bits of pixel color values. The secret text is first converted into binary form and then embedded sequentially into the image pixels. During extraction, the same process is reversed to reconstruct the hidden message. This approach ensures minimal distortion while maintaining data accuracy.



Methodology of Steganography Project

Embedding Process

Input Image & Secret Message

Encoding

Stego Image Creation

Stego Image

Secret Image with Hidden Message

Extraction Process

Stego Image

Decoding

Message Retrieval

Extracted Secret Message

Input Image + Secret Message
↓
Pre-processing
↓
LSB Encoding
↓
Stego Image Creation
↓
Transmission
↓
LSB Decoding
↓
Secret Message Extraction

3. TOOLS AND TECHNOLOGIES USED

- Programming Language: Python 3
- Image Processing Library: Pillow (PIL)
- Banner Library: Pyfiglet
- Development Environment: Visual Studio Code
- Operating System: Windows / Linux

4. RESULTS AND DISCUSSION

The experimental results demonstrate that the proposed system successfully embeds secret messages within images while preserving visual quality. The steganography images appear visually identical to the original images, confirming the effectiveness of the LSB technique for low-capacity data hiding applications.

5. LIMITATIONS

Despite its simplicity and effectiveness, the system has certain limitations. The lack of encryption makes the hidden data vulnerable if detected. Additionally, the payload capacity depends on the image size, and the technique is susceptible to steganalysis attacks.

6. FUTURE SCOPE

Future enhancements may include encrypting the secret data before embedding, implementing password-based extraction, and extending the system to support audio and video steganography. These improvements would significantly enhance security and robustness.

7. CONCLUSION

This project successfully demonstrates an image steganography system using the Least Significant Bit technique. It provides a practical understanding of information hiding and serves as a strong foundation for further research in cybersecurity and data protection.

8. REFERENCES

https://medium.com/@medoo53111/hidden-messages-with-zero-width-character-97d042119e89