CADT IDT Institute of Digital Technology

IMAGE STEGANOGRAPHY USING COVER & PAYLOAD TEXT 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

Image steganography refers to a method of embedding hidden information in images in a way that does not make the hidden information evident. Compared to traditional cryptography, which merely encrypts data in a message, image steganography hides the message itself. This research study deals with the development of image steganography, embedding text information in an image using Python. This research will make use of the Least Significant Bit method for altering image pixels without contributing any noticeable changes to the image. This will also enable the user to hide information in an image for subsequent recovery. Tests on this method prove that it works effectively since the stego image appears the same as the original image.

1. Introduction

Due to the increase in the usage of digital communication, the concern for securing the data has increased. The sensitive information being transferred through public communication channels can be intercepted and misused. The image steganography technique offers secure communication where the message is concealed in images and the intruder has no knowledge of the message. In this project, an image steganography system is implemented where embedding of cover text as well as payload text is done in an image. The objective is to provide an effective method for the secure hiding of data using images.

2. Background and Literature Review

Steganography has been in existence since the ancient Greek civilization, in which messages were concealed on wax tablets and even on shaved heads. In the computer technology world, the process of steganography has progressed in terms of image, audio, and video steganography. As compared to cryptography, steganography does not draw much attention since the message that has been hidden appears to be embedded in normal files. The most popular form of steganography techniques involves image steganography, which makes use of the redundant data available in images. The Least Significant Bit (LSB) method has been largely favored because it is simple and less prone to visual distortions. Several authors have utilized this LSB-based scheme in text and data hiding, and this technique is applicable to this project.

3. Problem Statement

Conventional methods of encrypting messages will conceal the message content, but the fact that a message may be hidden will not be encrypted. This may attract attackers. There is, however, a need to conceal the secret information in a way that will not be detected. This project will tackle this challenge by hiding text information within an image without modifying its appearance.

4. Objectives of the Project

The project has the following main objectives:

- To develop an image steganography system using the Python Programming Language
- To conceal the cover text and the payload text within the image

- In order to extract the hidden text properly from the stego image, some specific pixels need to be ensured after the image is embedded
- To achieve secure and covert communication

5. Scope of the Project

This project focuses on:

- Text Steganography Based on Digital Images
- LSB Embedding Technique
- Command-line execution with Python
- PNG image format for lossless compression

The project does not involve creating sophisticated encryption algorithms or robustness against all steganalysis attacks.

6. 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

Python

Vscode

7. System Architecture & Design

The system has two major modules including:

Encoding Module

- hides the cover text and the payload text inside an image

Decoding Module

- Extract hidden text from stego image

System Workflow:

- User selects the image
- The User provides Cover Text and Payload Text.
- The text is converted to binary code
- The binary information is embedded into the pixels of the image
- Stego image is created
- Hidden text is extracted through decoding

8. Methodology

8.1 Cover Image Selection

A PNG file is used as it ensures there is no compression loss of quality.

8.2 Cover Text and Payload Text Processing

The input text is first translated to ASCII values and then to binary bits.

8.3 Text Encoding Technique

Every character is represented by an 8-bit value in the form of binary.

8.4 Embedding

The Least Significant Bit of each pixel is altered to encode the binary data. Only one bit per pixel is altered to avoid distortion to the image.

8.5 Stego Image Generation

After embedding every bit, the manipulated image is preserved as the stego image.

8.6 Extraction Process

When decoding, the values of the LSB bits are extracted from the pixels to form characters.

9. Implementation Details

The project involves the use of Python scripts:

main.py #program control functions

Encrypted.py #handles the encoding process

Decrypted.py #decoding process manager

Reveal.py #easy use without the need install a tool (Input Path image in code)

The program supports command-line execution, such as:

```
• py main.py hide "cover text" "payload secret message" image.png output.png
```

10. Encryption and Decryption Process

Encryption:

- Text is translated into binary code
- The LSBs of image pixels hold the binary data
- The End-of-message delimiter is added

Decryption:

- Pixels' least significant bits are extracted
- Binary data is reconstructed
- The original text appears

11. Future Works

- Add a GUI interface
- Support audio and video steganography
- Command-line based (Kali Linux)

12. Conclusion

This project is a successful demonstration of a steganography system for hiding text data, including cover text and payload text, within an image. Because it uses the least significant bit (LSB) method, it hides data while maintaining the integrity of the image. This project shows that steganography on images is a useful practice for stealth communication.

13. References

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