PROJECT DOCUMENTATION

Secure Image Steganography Tool

Title Page

Project Title: Secure Image Steganography Tool

Submitted by: Sultan-56189 | Ch Mubashir-56892

Supervisor: Mr. Syed Yawar Abbas

Course: Information Security

Department: BS/DS-5_1

Table of Contents

Chapter 1 — Introduction

In today's digital era, sensitive information is continuously communicated through online channels. Although cryptography provides a secure way to make data unreadable, the presence of encrypted data can attract attention from attackers. Steganography offers an advanced level of secrecy by concealing the existence of the information itself inside harmless-looking media files.

The Secure Image Steganography Tool combines privacy and confidentiality by hiding text data inside digital images. The message is first encrypted and then embedded inside the pixel data of an image with password protection. Only the user possessing the correct password can extract and decrypt the hidden information.

1.1 Problem Statement

Unauthorized access to private information is increasing rapidly. Even when encrypted data is shared, cyber attackers become aware that a secret message exists. Therefore, there is a need for a system that enables secure communication without revealing the presence of hidden information.

1.2 Objectives

- To provide a secure method of embedding sensitive information inside digital images.
- To implement encryption and password protection for access control.
- To allow message extraction only by authorized users possessing the correct password.
- To ensure that the output image appears visually unchanged to human observation.

1.3 Scope of the Project

This project allows users to:

- Hide secret text messages inside image files.
- Protect the hidden information using a password.
- Extract and decrypt the message only with the correct password.
  This system can be used for personal privacy, research, military communication, academic use, and digital forensics.

Chapter 2 — Literature Review

Steganography is the science of hiding secret information inside a cover medium such as images, audio, or video files. In contrast, cryptography focuses on encrypting information but does not hide the existence of communication. When both techniques are combined, a powerful secure communication model is achieved.

In recent years, image steganography has become the most widely used technique due to the large data capacity and redundancy within image pixels. Researchers have proposed various embedding techniques such as spatial-domain embedding, transform-domain embedding, and hybrid encryption-based embedding. However, most of these methods lack user-friendly tools for practical usage.

The Secure Image Steganography Tool addresses this gap by combining:

- Encrypted message embedding
- Password protection
- A simple and usable interface for non-technical users

Chapter 3 — System Analysis and Design

3.1 Proposed System Workflow

1. User enters secret message
2. User enters password
3. Message is encrypted
4. Encrypted message is embedded inside image pixels
5. Stego image is generated and downloaded
6. To extract, user uploads stego image + password

7. System verifies password → decrypts → displays message

3.2 System Architecture Diagram

User → GUI → Encryption Module → Steganography Encoder → Stego Image Output

↓

Password Verification & Decryption Module ← Steganography Decoder ← User Input

3.3 Data Flow Diagram (DFD – Level 0)

User → [System] → Hide Message → Stego Image

User → [System] → Reveal Message → Secret Text

3.4 DFD — Level 1

User Input → Encryption → Steganography Encoding → Image Generation → Storage/Download

User Input + Password → Authentication → Steganography Decoding → Decryption → Message Output

3.5 Flowchart (Hide & Reveal)

START

↓

Input Message + Password + Image

↓

Encrypt Message

↓

Encode Encrypted Data into Image Pixels

↓

Download Stego Image

↓

(For Extraction)

Upload Stego Image + Password

↓

If Password Wrong → Display Error

Else → Decode Pixels → Decrypt Message

↓

Display Hidden Message

↓

END

Chapter 4 — Implementation and Results

4.1 Technologies Used

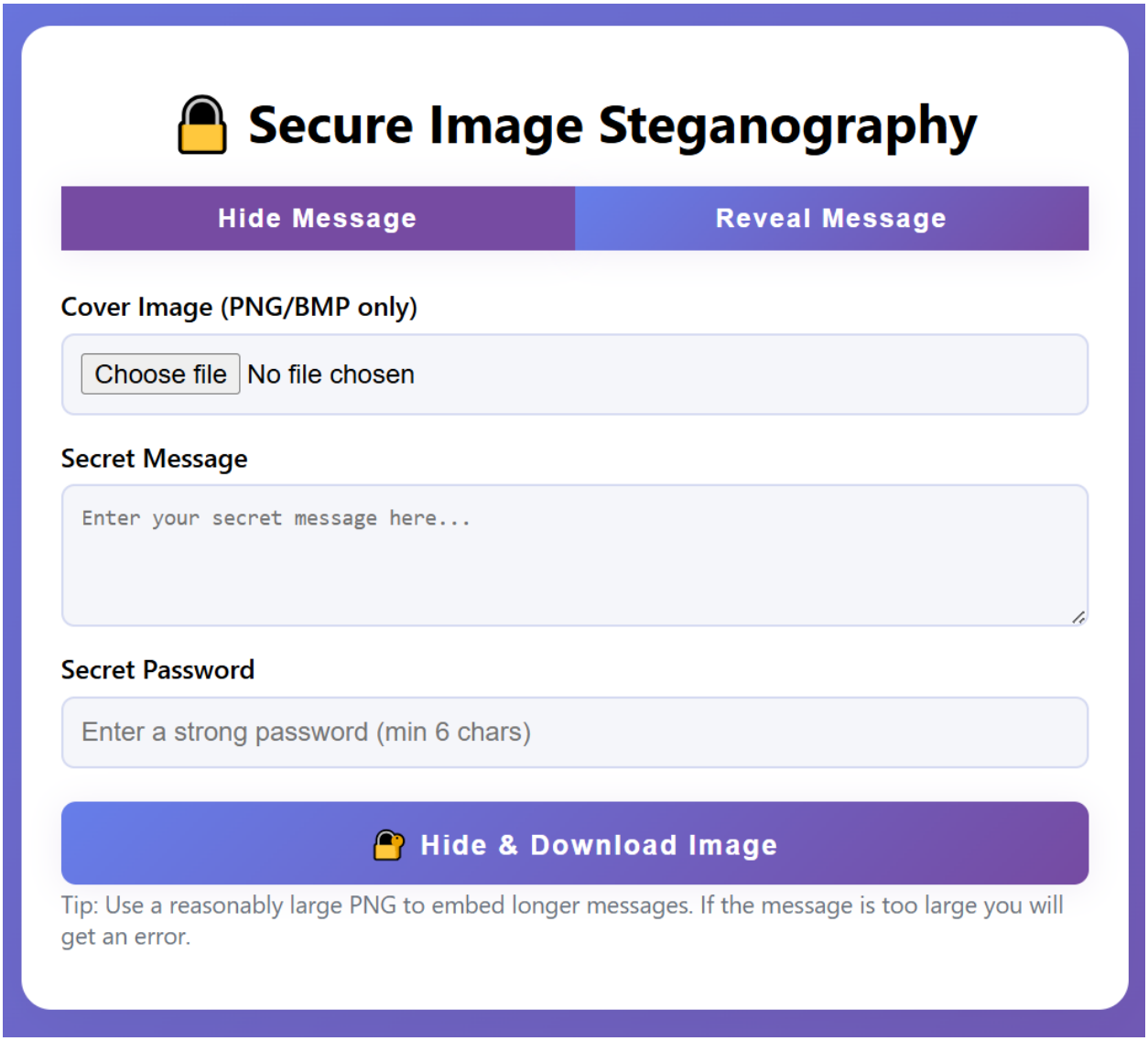
- Python
- Flask Web Framework
- HTML / CSS
- Image Processing Libraries
- Encryption Libraries

4.2 Modules

Module	**Description**
Hide Module	Embeds encrypted message into the image
Reveal Module	Extracts and decrypts hidden message
Password Authentication	Prevents unauthorized extraction
GUI Module	Provides user-friendly interaction

4.3 System Interface (Screenshots)

Home interface of Secure Image Steganography Tool



Message extraction interface requiring password authentication

4.4 Experimental Results

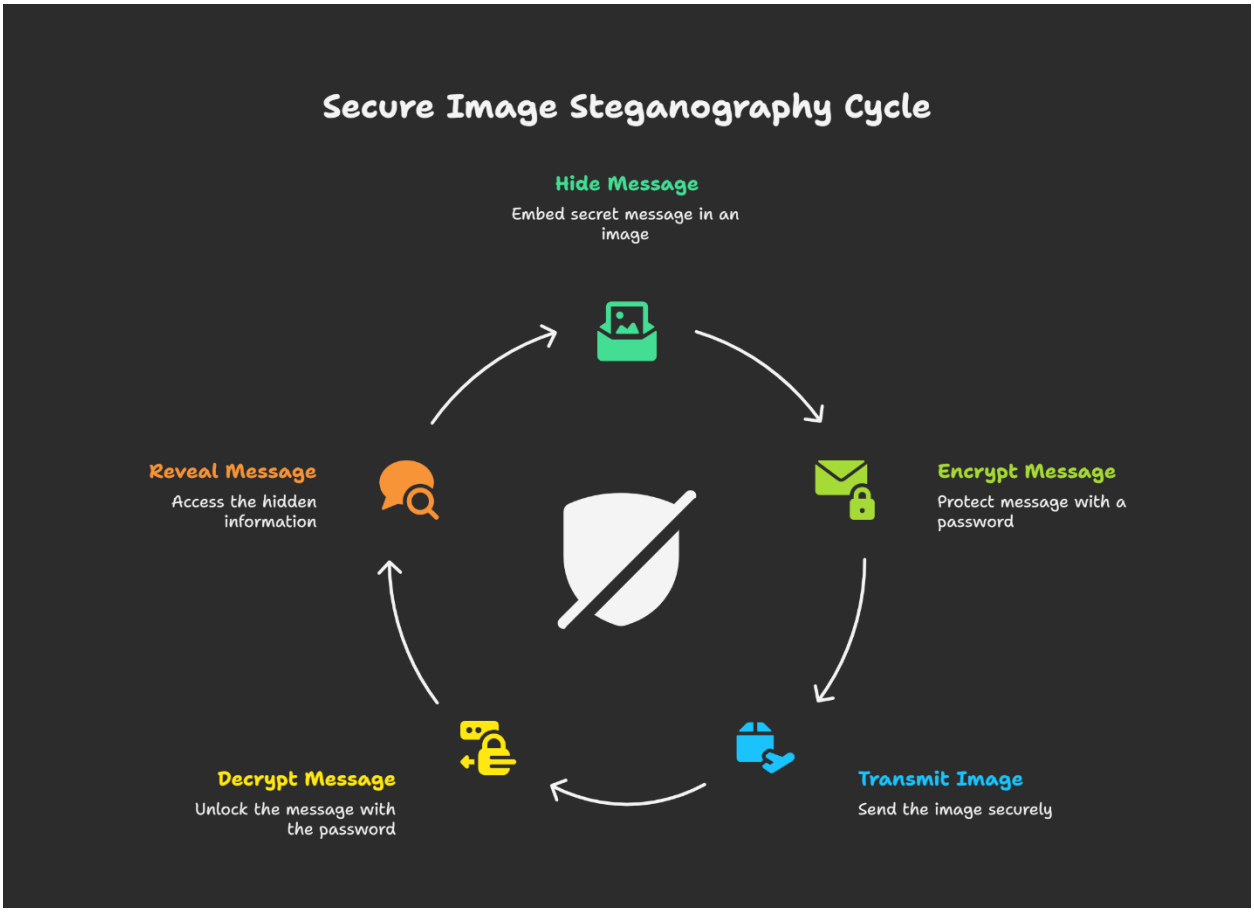
- Image quality remains visually identical after embedding
- Hidden message extraction fails if the password is incorrect
- System successfully hides and retrieves text of any length within allowed capacity

---

Chapter 5 — Conclusion and Future Work

Conclusion

The Secure Image Steganography Tool provides a reliable method for covert communication by combining steganography and encryption. The system ensures that the secret message remains hidden from detection while also protecting access using a password. It successfully enables secure and private transmission of sensitive information.



Future Work Suggestions

- Support for audio/video steganography
- Mobile application version
- Use of biometric authentication instead of a password
- Cloud-based secure message sharing feature