CIPHER SPHERE SHIELD

A
Synopsis Report
of

MAJOR PROJECT (BCA 308)

BACHELOR OF COMPUTER APPLICATION

Batch (2021-2024)

SUBMITTED BY

TISHA KHANIJO (00121402021)
AVI SHARMA (01621402021)

FEBRUARY 2024

DR. HARSHA S RATNANI,
Associate Professor

Jagannath International Management School
Vasant Kunj, New Delhi-110070

(Affiliated to Guru Gobind Singh Indraprastha University, New Delhi)
Recognized u/s 2(f) by UGC & Accredited with 'A+' Grade by NAAC
Participant of UNGC New York and ISO 9001:2015 Quality Certified

Table of Contents

1. INTRODUCTION

1.1 BACKGROUND

Securing the Digital Age with AI-powered Steganography and Cryptography

The digital era's convenience is accompanied by rising data security concerns. As sensitive information transmission surges online, robust protection becomes essential. This project tackles this challenge by introducing an **AI-Integrated Steganography and Cryptography Suite** built with Python.

This suite leverages three powerful technologies:

1. **Steganography:** Concealing messages within ordinary media. Our suite employs various techniques like **Least Significant Bit embedding**, **transform domain techniques**, and **procedural steganography** to seamlessly hide data in images, audio, or video.

2. **Cryptography:** Securing communication through encryption and decryption. We integrate a range of options, including **symmetric algorithms** like the widely used **AES** and **asymmetric algorithms** like **RSA** and **ECC**, allowing users to choose the most suitable protection level.

3. **AI:** AI algorithms analyze hidden data and recommend the most effective methods based on data type, security needs, and cover media properties, ensuring optimal imperceptibility (minimal distortion).

By combining these technologies, our project aims to revolutionize data security, offering an innovative and user-friendly solution for the digital age.

1.2 PROBLEM STATEMENT

The digital age has led to an exponential growth in the transmission of sensitive information online. This information, ranging from personal data and financial records to confidential business communications, requires robust protection to safeguard against unauthorized access and potential misuse.

Current methods for securing data transmission often rely solely on encryption algorithms, which can be computationally expensive and susceptible to evolving attack techniques. Additionally, traditional steganographic techniques might not always offer optimal imperceptibility or security, making it challenging to balance data hiding effectiveness with minimal disruption to the cover media.

Therefore, there is a critical need for a more **comprehensive and user-friendly solution** that addresses these challenges and **enhances the security of data transmission** in the digital landscape

2. OBJECTIVE

This project aims to bridge this gap by developing an **AI-Integrated Steganography and Cryptography Suite**. This suite will combine the strengths of steganography, cryptography, and artificial intelligence (AI) to offer the following:

The primary aim of this project is to design and implement a versatile decryption platform capable of decrypting a diverse range of file formats, including images, audio, text, NFTs, GIFs, video files, and various data file types. This decryption platform will be accessible through a user-friendly website interface, enabling users to effortlessly decrypt their files. Furthermore, the platform will offer seamless encryption functionality for securing sensitive data directly on the website. Integration of AI assistance will be employed to enhance user experience and optimize decryption and encryption processes, ensuring smooth operation and robust security measures. The overarching goal of this project is to deliver a comprehensive decryption and encryption solution.

By addressing these challenges and offering a user-friendly solution, this project aims to contribute significantly to the **development of robust and accessible data security solutions** in the digital era.

3. Tools/Platform and Components

3.1 Hardware

- **Processor:** A modern processor (e.g., Intel Core i5 or equivalent) with sufficient processing power for running the web application and performing AI computations.
- **Memory (RAM):** At least 8GB of RAM is recommended for smooth operation, especially if handling large data files or complex AI models.
- **Storage:** Adequate storage space (e.g., SSD with at least 128GB) to accommodate the application files, libraries, and user data (if applicable).
- **Internet connection:** A reliable internet connection for accessing necessary libraries and documentation, and for potential online user interactions (consider user anonymity if applicable).

3.2 Software

1. **Operating System:** Windows, macOS, or Linux

2. **Libraries and Frameworks:**

   2.1 Web development framework: Flask (lightweight and flexible framework for building web applications)

   2.2 AI libraries:
   1. **TensorFlow or PyTorch:** Open-source libraries for building and deploying AI models.

   2.3 Cryptography libraries:
   1. **PyCryptodome or cryptography:** Provide secure encryption and decryption functionalities.

   2.4 Image processing libraries:
   1. **Pillow (Fork of PIL Fork):** Supports various image formats (JPEG, PNG, etc.) for manipulation and analysis.
   2. **OpenCV:** Powerful library for computer vision tasks, including image processing and analysis (can be used for advanced steganography techniques).

   2.5 Audio processing libraries:
   1. **Librosa:** Open-source library for audio analysis and processing.
   2. **SciPy:** Scientific computing library with functionalities relevant to audio processing.

   2.6 Video processing libraries:
   1. **MoviePy:** Simple and user-friendly library for basic video editing and manipulation.
   2. **OpenCV :** Offers video processing capabilities in addition to image processing.

   2.7 Text processing libraries:
   1. **NLTK (Natural Language Toolkit):** Library for working with human language data (potentially useful for text steganography).

3. **Development Tools:**

   3.1 Programming Language: Python (widely used and versatile for web development and AI applications)

   3.2 Text Editor or IDE: Choose a preferred option (e.g., Visual Studio Code, PyCharm)

3.3 Version Control System: Git (recommended for code versioning and collaboration)

4. SCOPE OF THE PROJECT

4.1 Potential

1. **Enhanced Security:** Combining steganography and cryptography provides double protection for sensitive information.
2. **Improved User Experience:** Web-based interface with AI-powered recommendations simplifies secure data transmission.
3. **Increased Accessibility:** Makes securing data accessible to individuals with varying technical expertise.
4. **Potential Applications:**
    - Secure communication for journalists, activists, businesses, and individuals.
    - Protecting sensitive data in healthcare, finance, and other sectors.

4.2 Market Potential:

The market for secure data transmission solutions is vast and growing due to:

- **Increasing reliance on digital communication:** Sensitive data is frequently transmitted online in various sectors, creating a demand for robust security measures.
- **Rising cyber threats:** Data breaches and cyberattacks are increasingly common, making secure communication essential for individuals and organizations.
- **Growing awareness of privacy concerns:** Individuals and organizations are becoming more aware of the importance of data privacy and seek solutions to protect sensitive information.

4.3 Limitations

- **Complexity of implementation:** Integrating various libraries and ensuring robust

security measures requires careful planning and development expertise.

- **Computational resources:** AI algorithms and encryption/decryption processes may require significant processing power, potentially limiting accessibility for users with low-resource devices.

- **Potential for misuse:** Malicious actors could exploit the functionalities for illegal activities, highlighting the need for responsible usage and safeguards.

- **Ethical considerations:** Steganography raises ethical concerns regarding privacy and potential misuse for spreading misinformation. These need to be addressed through responsible development and use.

1.4 Competitive Advantage:

Several factors differentiate this project from potential competitors:

- **AI-powered recommendations:** Utilizes AI to recommend optimal steganography and encryption methods, enhancing user experience and security effectiveness.

- **Ease of use:** Web-based interface with clear instructions makes the suite accessible to a wider audience compared to complex software solutions.

- **Versatility:** Supports various data types and steganography techniques, offering broader application compared to solutions focused on a single type of data or technique.