JAYPEE INSTITUTE OF INFORMATION TECHNOLOGY, NOIDA
Department of Computer Science and Engineering

Cryptography PBL

Secure Multimedia Data Hiding using Steganography and Cryptography

NAME	BATCH	ENROLL NO.
LAVANYA BHATI	B1	22103007
VANDIT KAUL	B1	22103005
ARYAN SATYAM	B2	22103044

Under the Guidance of:
Dr. Aastha Singh

ABSTRACT

With the rapid growth of digital communication, protecting sensitive multimedia data from unauthorized access has become a key concern. Cyber threats and privacy breaches have made it crucial to secure confidential information transmitted over public networks.

This project, *Secure Multimedia Data Hiding using Steganography and Cryptography*, aims to enhance the confidentiality and security of multimedia data by integrating two powerful techniques: AES (Advanced Encryption Standard) for encryption and LSB (Least Significant Bit) Steganography for data hiding.

In this system, the message is first encrypted using AES encryption to ensure its confidentiality, and then the encrypted data is embedded into a multimedia file such as an image. The embedding process subtly modifies pixel values in such a way that human perception cannot detect any visible change, thus maintaining the image quality.

This hybrid approach ensures data privacy, message integrity, and non-detectability, which are critical for modern secure communication. The proposed model can be used for secure message transfer, digital watermarking, and data authentication in various domains including defense, healthcare, and corporate data exchange.

INTRODUCTION

In today's digital era, data security has become one of the most important challenges. The constant exchange of information through emails, messaging apps, and cloud storage systems exposes sensitive data to risks such as interception, manipulation, and identity theft. Traditional encryption alone protects data but makes the existence of a secret message obvious. On the other hand, steganography hides the existence of the message but does not secure it if discovered.

To overcome these limitations, this project combines both techniques Cryptography and Steganography to build a two-layer security system. Cryptography encrypts the data using strong algorithms like AES, while Steganography conceals it within multimedia files.

The result is a secure and invisible communication channel that ensures privacy and data integrity even over untrusted networks.

LITERATURE REVIEW

Numerous researchers have explored methods for secure communication, particularly focusing on the integration of steganography and cryptography.

- **G. Kaur et al. (2017)** presented a review of various image steganography techniques emphasizing pixel manipulation methods and their effectiveness in data concealment.

- **Cheddad et al. (2010)** analyzed current methods and challenges in digital image steganography and highlighted LSB as one of the most efficient techniques.

- **Stallings (2020)** discussed the fundamental principles of cryptography, focusing on symmetric and asymmetric key encryption methods for secure data transfer.

- **Bandyopadhyay & Sinhababu (2011)** proposed a hybrid model combining cryptography and steganography to improve data confidentiality.

- **Chan & Cheng (2004)** demonstrated the concept of LSB substitution, which involves embedding secret bits into the least significant bits of image pixels without perceptual distortion.

These studies demonstrate that integrating encryption with data hiding significantly enhances the level of protection, making the concealed data almost impossible to detect or decode without the key.

OBJECTIVES AND MOTIVATION

Objectives

The main objectives of this project are:

1. To design a system capable of hiding encrypted text messages within multimedia files.

2. To use AES encryption to ensure strong data confidentiality.

3. To implement LSB-based image steganography for message embedding.

4. To provide a simple user interface for encryption and decryption processes.

5. To verify that image quality remains unaffected after embedding data.

Motivation

Cybersecurity has become a vital part of digital communication. As digital data sharing increases, so does the risk of unauthorized access. Traditional encryption methods alone can draw suspicion since encrypted data is easily noticeable.

Steganography, when combined with encryption, ensures that even if someone intercepts the message, they cannot detect or decode it easily. This dual-layered approach motivated us to implement a secure multimedia hiding system for everyday digital use.

THEORY

Cryptography

Cryptography is the practice of securing communication through mathematical algorithms. It converts plaintext into ciphertext to prevent unauthorized access. We used AES (Advanced Encryption Standard) — a symmetric encryption algorithm that uses 128-bit, 192-bit, or 256-bit keys. AES ensures confidentiality and is computationally efficient for large datasets.

Steps in AES Encryption:

1. Key generation from password input.
2. Conversion of message into binary blocks.
3. Substitution, permutation, and key mixing across multiple rounds.
4. Ciphertext output that cannot be reversed without the key.

Steganography

Steganography is the science of hiding messages in plain sight. It conceals data within an image, audio, or video file without noticeable distortion.

LSB (Least Significant Bit) Method:
The LSB technique modifies the least significant bit of image pixels to embed secret data. For example, if a pixel value is 10110100, changing the last bit to 10110101 has negligible visual effect but embeds a secret bit of information.

METHODOLOGY

The proposed system consists of four key stages:

Step 1: Encryption (Cryptography Layer)

- The user inputs a secret message and a password.
- The password generates an AES key using Python's cryptography library (Fernet).
- The message is encrypted into ciphertext.

Step 2: Embedding (Steganography Layer)

- The ciphertext is converted into binary format.
- Using the LSB technique, each bit of the ciphertext is embedded into the pixel values of an image.
- The modified image (stego image) is visually identical to the original.

Step 3: Transmission

- The stego image is sent to the receiver via email, social media, or any communication medium.

Step 4: Extraction & Decryption

- The receiver extracts the hidden bits from the image.
- The AES key (generated from the same password) decrypts the ciphertext to retrieve the original message.

SYSTEM ARCHITECTURE

The system architecture contains two main modules:

1. **Encryption Module:**
    - Inputs: Message + Password
    - Process: AES encryption using the Fernet library
    - Output: Encrypted binary data
2. **Embedding Module:**
    - Inputs: Encrypted binary + Image file
    - Process: LSB substitution in image pixels
    - Output: Stego image

Architecture Flow Explanation:

User → Message → AES Encryption → Binary Data → LSB Embedding → Stego Image → Transmission → Extraction → AES Decryption → Original Message

IMPLEMENTATION

Technology Stack

Category	Technology
Programming Language	Python
IDE	Visual Studio Code
Cryptography Library	cryptography (Fernet/AES)
Image Processing	Pillow (PIL)
Audio Processing	wave
Algorithm	AES + LSB Steganography

Implementation Steps

Install required libraries using pip install cryptography pillow.

1. Encrypt message using Fernet AES.
2. Open image using PIL, convert to pixel array.
3. Replace LSBs with encrypted data bits.
4. Save the modified image as the stego file.
5. Receiver runs a reverse process to extract and decrypt data.

RESULT AND ANALYSIS

Test Case Example

- Input Message: *"Project completed successfully."*
- Encrypted Message: *Random binary sequence generated by AES.*
- Original Image: *150 KB PNG file*
- Stego Image: *151 KB (visually identical)*
- Output: *Decrypted message matches original input.*

Observations

- Image quality was preserved with no visible changes.
- Encryption and decryption times were under 2 seconds for short text.
- The system resisted brute-force attacks without the correct password.
- Stego files passed unnoticed during normal file transmission.

CONCLUSION

This project successfully demonstrates a secure and efficient method for data hiding using a combination of Cryptography (AES) and Steganography (LSB). The dual protection ensures that even if the stego file is intercepted, the hidden data remains inaccessible without the encryption key.

By merging two powerful technologies, the system not only secures data but also maintains the integrity and visual quality of multimedia files. This approach is highly adaptable for modern digital communication where confidentiality and authenticity are essential.

REFERENCES

1. G. Kaur, S. Rani, and G. Singh, “A review on image steganography techniques,” *ICCCA*, 2017.

2. A. Cheddad, J. Condell, K. Curran, and P. McKevitt, “Digital image steganography: Survey and analysis,” *Signal Processing*, 2010.

3. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th Edition, Pearson, 2020.

4. S. K. Bandyopadhyay and A. K. Sinhababu, “A new framework of combining cryptography and steganography,” *IJCSNS*, 2011.

5. C. K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” *Pattern Recognition*, 2004.