Information Security
(Project)

Submitted by:

Name: Ahmed Mujtaba
Sap id: 26617

Name: Muhammad Yousaf
Sap id: 27014

Submitted too:

Mr. Waqas Ahmad Butt
(Lecturer)

Riphah School of Computing & Innovation
Faculty of Computing
Riphah International University, Lahore
Fall 2024

17 January, 2024

Information Security Project Report

Overview:

Steganography: This is the practice of concealing one piece of information within another in such a way that it is difficult to detect or notice. The term "steganography" is derived from the Greek words "stegnos," meaning "hidden," and "graph," meaning "to write" — hence, it translates to "hidden writing." Unlike cryptography, which focuses on securing communication through encryption, steganography emphasizes hiding the existence of the message.

This Audio Steganography project employs the Least Significant Bit (LSB) encoding technique to embed secret messages within audio files. LSB involves altering the least significant bit of each byte in the audio signal without significantly affecting the perceptual quality of the audio. The project provides an intuitive Graphical User Interface (GUI) using Tkinter for users to encode and decode messages seamlessly.

LSB Algorithm:

The Least Significant Bit (LSB) Algorithm is a common steganographic method. In audio steganography, it involves altering the least significant bit of each audio sample to embed binary data. Since the human ear is less sensitive to minor changes in audio, this method allows for secret message embedding without perceptible alterations.

Embedding Process:

1. **Initialization: WaveGen Class:**

    ➢ The `WaveGen` class initializes default audio parameters such as sample rate, bit depth, frequency, and channels.

2. **Encoding Secret Message:**

    ➢ Bit Conversion: The `bit Message` method converts a string message into a binary string.

    ➢ Encoding: The `encrypt message` method encodes the message using a simple encryption algorithm.

3. **Audio File Construction:**

    ➢ Header Creation: The `WaveGen` class constructs the WAV file header, including RIFF, format, subchunk sizes, and audio format details.

    ➢ Sine Wave Generation: It generates a sine wave signal corresponding to the specified frequency and time.

4. **Embedding:**

    ➢ The secret message bits are embedded in the least significant bits of the audio samples.

5. **Writing to WAV File:**

    ➢ File Output: The generated bitArray is written to a WAV file.

Diagram:
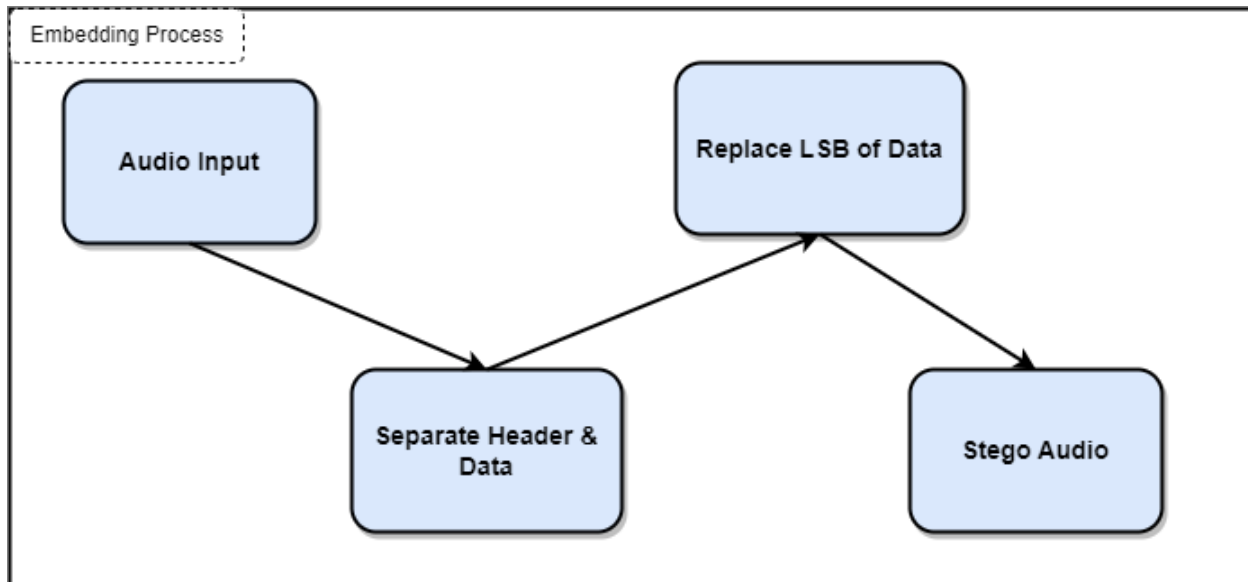

Extracting Process:

1. **Reading WAV File:**

   ➤ Header Extraction: The WAV file's header is read to obtain essential information, such as sample rate.

   ➤ LSB Extraction: The least significant bits of audio samples are extracted.

2. **Decoding Secret Message:**

   ➤ Bit Conversion: The extracted bits are converted into binary strings.

   ➤ Message Decryption: The `decrypt message` method decrypts the binary string using the same encryption.

3. **Validation:**

   If the last 4 characters of the decoded message match '#1991#', the message is considered successfully extracted; otherwise, an error is raised.

Diagram:
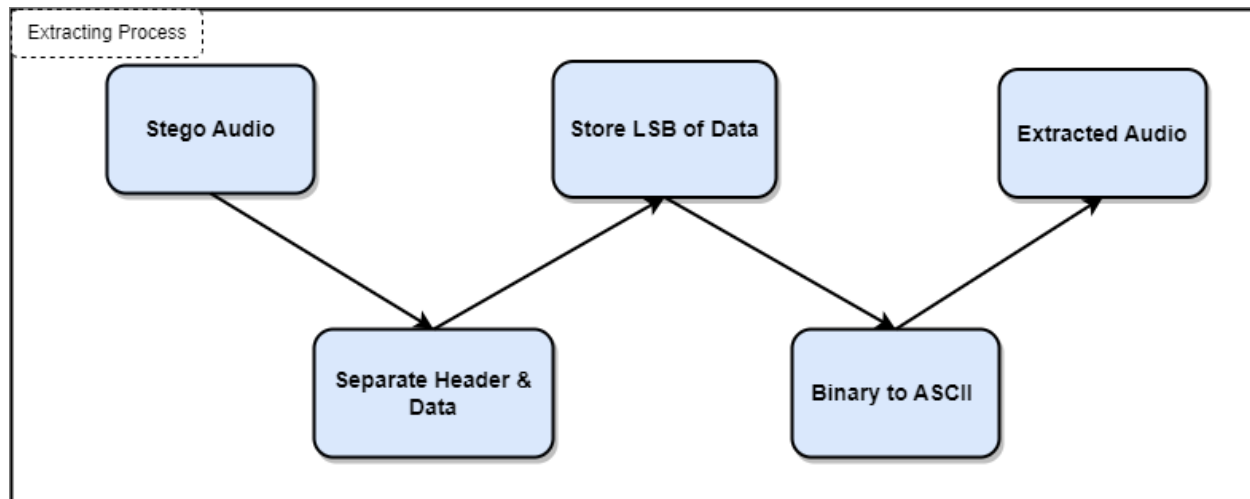
GUI Implementation:

The GUI serves as the front end for users to interact with the Audio Steganography system. It is implemented using Tkinter, a Python GUI library. The GUI consists of two main tabs: Encode and Decode.

Encode Tab

➢ Secret Message Entry: Allows users to input the message they want to encode.

➢ Filename Entry: Enables users to specify the filename for the output audio file.

➢ Password Entry: Provides a password field for additional security.

➢ Encode Button: Triggers the encoding process.

➢ Status Label: Displays the status of the encoding process.

Decode Tab

➢ Filename Entry: Allows users to input the filename of the audio file from which to extract the hidden message.

➢ Password Entry: Provides a password field for decryption.

➢ Decode Button: Initiates the decoding process.

➢ Decoded Message Label: Displays the decoded message.

Conclusion:

Our Audio Steganography project showcases a practical implementation of LSB encryption in audio files, providing a secure and intriguing method for hiding and retrieving secret messages. Steganography remains a valuable tool for safeguarding sensitive information in various applications.