Audio Steganography

Akash Mahale(2015120023), Swapnil Masurekar(2015120025),
Prathamesh Pai(2015120033), Vedanta Pawar(2015120035)

Mentor: Dr. Preetida Jani

Abstract

In todays's world, with growth of internet, there is high demand of data to be tranmsmitted in a secure mannar. Data transmission in public communication system is very less secured because of interception, spoofing and man-in middle attack. So an effective solution for this problem we have proposed is Steganography, which is a way of writing hidden messages in such a way that no one, apart from the sender and intend recipient, suspects the existence of the message. Audio steganography is the scheme of hiding the existence of secret information by hiding it in an audio file.Thus in our work we have proposed a way for audio steganography where the bits of a secret message are hidden into the coefficients of the audio. Each secret bit is embedded into the selected position of a audio coefficient. The position for insertion of a secret bit is selected from the 0th (Least Significant Bit) to 7th LSB based on the upper three MSB (Most Significant Bit). While extracting data at receiver end, a key needs to be entered, which was used for data hiding process. We have used AES encryption process If user gives a wrong key then he/she will not be authenticated. This sche me provides high audio quality,robustness and lossless recovery from the audio.

Keywords: Steganography, RSA (Rivest-Shamir-Adleman),
AES(Advanced Encryption Standards)

1. Introduction

The word steganography is derived from the Greek wo rds stegos meaning cover and grafia meaning writing defining it as covered writing. Steganography and cryptography are closely related. Cryptography scrambles messages

so they cannot be understood. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place.Redundancy can be described as the bits of a media, signal or file that offer accuracy more than needed for the objects use. The redundant bits of an object may also be defined as those bits that can be easily altered without this change being noticed easily. Image, video and audio files in particular fulfill this requirement, while studies have also revealed other file formats that are suitable to be used for information hiding.Initially the secrete message has to encrypted with some standard encryption algorithm with a key supplied by the sender and shared with the receiver. Then the position for insertion inside the sample of the carrier audio file has to be selected based on the decimal value of first 3 M SB bits. Suppose, first 3 MSB bits of a sample are 100 (decimal value is 4), then one bit of the secrete message has to be inserted at the 4th position of the corresponding sample of carrier audio file. After the decimal value for 3 MSB bits are considered for the next sample and similarly the next secrete bit has to be put at the decimal valued position and the process will be repeated for each bit in the secrete message till the full secrete message is hidden.

2. Flow diagram

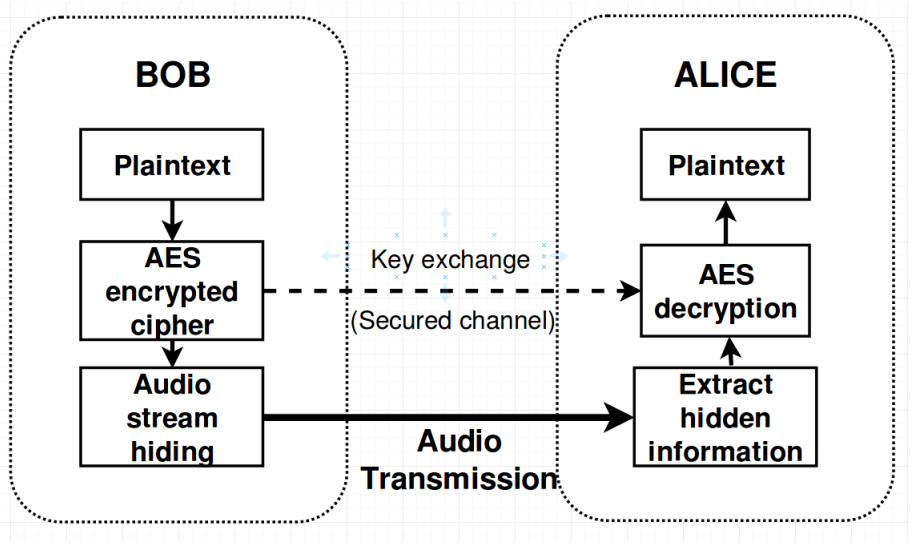

Figure 1: Logical flow of Steganography method

3. Architecture

Input text is taken from the user. This plaintext is encrypted using AES encryption algorithm. Now this encrypted ciphertext is hidden in an audio stream. The position for insertion inside the sample of the carrier audio file has to be selected based on the decimal value of first 3 MSB bits. Now this changed audio stream is transmitted. This changed audio is received at the receiver with bit rate, same as that at the transmission. Considering the first 3 bits, the hidden information is extracted from the audio stream. Now this information is in the form of encrypted text. AES Decryption is used to get the original message.

4. Result

Output of Bob_Hide.py

```
cyclotron3597@cyclotron3597-HP-15-Notebook-PC:~/Desktop/Engineering/SEM7/DCE/Steganography_Batch_B$ python Bob_Hide.py
The Plaintext is: Steganography Batch B-This is the hidden Message
Generating Bob's public and private keypairs for secure channel using RSA......
("Bob's public key is ", (55, 323), " and Bob's private key is ", (199, 323))
Bob's public key written in pkl file
Text Data Encrypted
Steganography: Hiding the text data in the Audio File
(2, 2, 44100, 172363, 'NONE', 'not compressed')
Steganography: Data being hidden successfully in 'Data/2.wav'
Bob's encrypted AES Key is:
116248849181191127181191127211127316101261445051248158127522652 50
Hidden data Audio file sent to Alice and Key Exhanged via secure channel
Bob's encrypted Key written in pkl file
```

Figure 2: Output of Bob_Hide.py

Output of Alice_seek.py

```
cyclotron3597@cyclotron3597-HP-15-Notebook-PC:~/Desktop/Engineering/SEM7/DCE/Steganography_Batch_B$ python Alice_Seek.py
("Bob's public key is being verified, Bob's Public key is", (55, 323))
AES Encryption Key Received
('The AES Key is: ', 'This is a key123', 'Text Length is: ', 48)
Steganography: Seeking Encrypted text from the Audio
(2, 2, 44100, 172362, 'NONE', 'not compressed')
Steganography: Encryped Data being seeked successfully
Data decrypted successfully
The Recovered text is: Steganography Batch B-This is the hidden Message
```

Figure 3: Output of Alice_seek.py

Output of CA.py

```
cyclotron3597@cyclotron3597-HP-15-Notebook-PC:~/Desktop/Engineering/SEM7/DCE/Steganography_Batch_B$ python CA.py
Generating Certificate Authority's public and private keypairs......
("Certificate Authority's public key is ", (263, 323), " and Certificate Authority's private key is ", (311, 323))
CA's public key written in pkl file
Bob's public key certificate written in pkl file
```

Figure 4: Output of CA.py

5. Conclusion

In this method, the embedded message in the audio stream is hidden in such a way that only the known participant can extract the message. Because AES encryption is used, it is very secured and an efficient method to encrypt the information. Since this uses double level of security, it is very difficult to intrude into the system.

6. References

[1] Shweta Vinayakrao Jadhav et al., "A New Audio Steganography with Enhanced Security based on Location Selection Scheme, *"International Journal of Engineering Science(IJESC)*