AUDIO STEGANOGRAPHY USING LSB TECHNIQUE

Jeevesh Pasrija

UG Student
Department of Information Technology,
Maharaja Agrasen Institute of Technology, Rohini, Delhi-110086, India.

Abstract- Steganography is the art of hiding the fact that communication is occurring by concealing data in some other data. A wide range of carrier file formats can be used, yet audio files are one of the most prominent because they are not easy to get caught. For hiding secret information in audio files, there exists a large variety of steganography techniques. This paper addresses the challenges and devises the implementation of LSB technique used for hiding messages inside an audio file.

I. Introduction

It is very important to secure any important information that has to be transferred from a sender to a receiver. Intruders can disclose the information to others, change it to misrepresent an individual or organization, or use it for an attack. This problem can be solved through the use of steganography. Steganography is technique of hiding information in the digital media. In contrast to cryptography, it is not to encrypt the information so that attackers may not get it, but it is used to hide the existence of the information itself. Steganography is an art of concealing information in the ways that prevents detection of hidden information. Steganography includes secret communication methods that hide the information from being seen or discovered. [4]

In Audio Steganography we find a way so that an audio file can be used as a host media to hide textual message without affecting the file structure and content of the audio file. Because of degradation in the perceptual quality of the cover object may leads to a noticeable change in the cover object, may leads to the failure of objective of steganography. The two primary criteria for embedding the covert message are that the stego signal resulting from embedding is indistinguishable from the host audio signal and the message should be correctly received at the receiver side. Audio data hiding method provides the most effective way to protect privacy. [6]

This paper depicts method to implement encryption and decryption technique on the secret information that has to be hidden into audio files which will provide confidentiality to the secret information. Steganography is the technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing hidden information but it is to keep others from thinking that information even exists.

Steganography is art of concealing information in ways that prevents the detection of hidden messages. The growing possibilities of modern communications need special means of security especially on computer network. The network security is important as number of data being exchanged on internet increases. Therefore, confidentiality and data integrity are required to protect against unauthorized access and use. This has resulted in explosive growth of field of information hiding. [8]

The basic steganography model has Audio File, Secret Message. Audio File is also known as cover-audio, inside which secret data is hidden. Thus it serves purpose to hide very existence of secret messages. Secret information is message that sender wants to transmit with confidentiality.
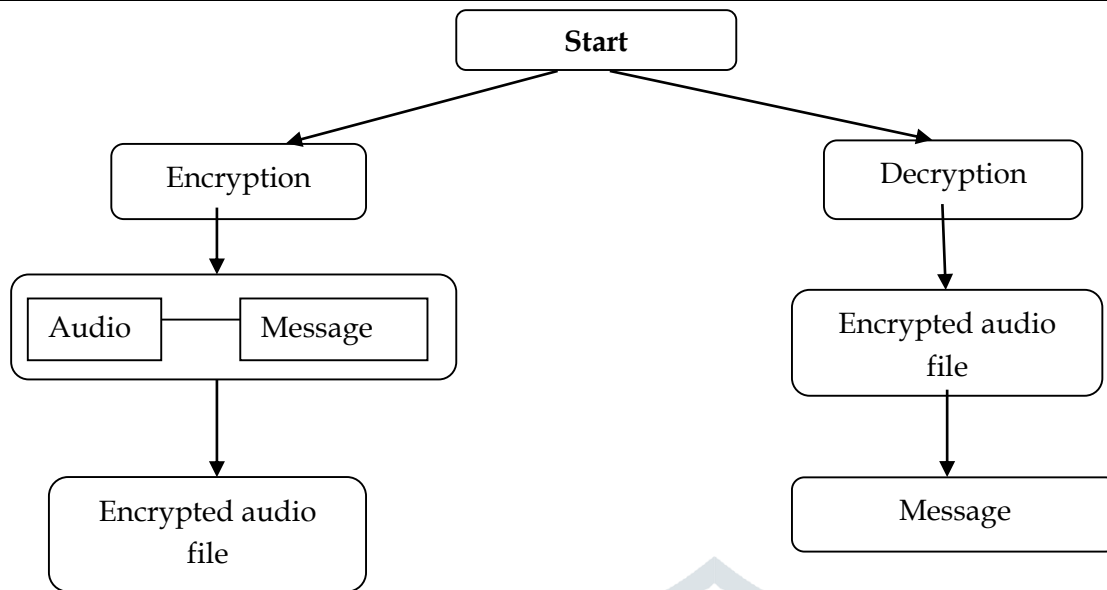
Figure 1: Graphical Representation of Proposed System

II. Related Work

In the year 2015, Ayush Singhal et al [2] proposed that for cover objects, different types of digital media can be used and they used .wav audio as their cover file in the research work. They were able to hide the secret message inside the audio cover file.

In the year 2014, Rohit Tanwar and Monika Bisla [1] advised that one of the most important goal of any audio steganographic technique is that the process should be robust and the audio cover file generated must be resistant to malicious attacks as that is the main aim of the steganography process.

In 2014, Kazem Qazanfari and Reza Safabakhsh [3] proposed an improved version of LSB++ approach. In this improved LSB++ they make distinction between sensitive pixels and allow protecting them from the embedding of extra bits, which results in the lower distortion in co-occurrence matrices.

In the year 2012, M. Baritha Begum and Y. Venkataramani [11] proposed an algorithm that included compression that reduces the redundancy of data. In their audio steganographic technique, dictionary based compression bits were hidden in the least significant bit of audio signals and the signal to noise ratio (SNR) was calculated. This audio Steganography was used to conduct for various compression algorithms with dictionary based compression.

In the year 2009, S. Channalli and A. Jadhav [9] proposed a new LSB based method in which common bit pattern is used to hide data which can be used in audio steganography as well while using the bit patterns with different frequencies of audio signal.

III. Methodology:

In this project, a text file containing the secret information is created. An audio file of WAV format is the chosen as cover medium. Since the contents of the Audio file and text file are different, a function is written to convert the text file into bit stream. [10]

Then the text data is converted to an unrecognizable form. This process is known as Encryption. The encrypted file is then taken and embedded into the audio file. Care is taken throughout the project that the audio file does not suffer from any noise or corruption. [7]

On the receiver side, the audio file is taken and the encrypted file is recovered by De-Steganography. Then the encrypted file is decrypted to reveal the secret information. The contents of the audio file are listened to before and after the techniques have been implemented with the aid of a speaker.

LSB (Least Significant Bit) Algorithm:

LSB algorithm is a classic Steganography method used to conceal the existence of secret data inside a "public" cover. The LSB or "Least Significant Bit", in computing terms, represents the bit at the unit's place in the binary representation of a number. For example, we can represent the decimal number 170 in binary notation as 10101010. The least significant bit, in this case, is 0.

In the simplistic form, LSB algorithm replaces the LSB of each byte in the "carrier" data with one bit from the "secret" message. [5]
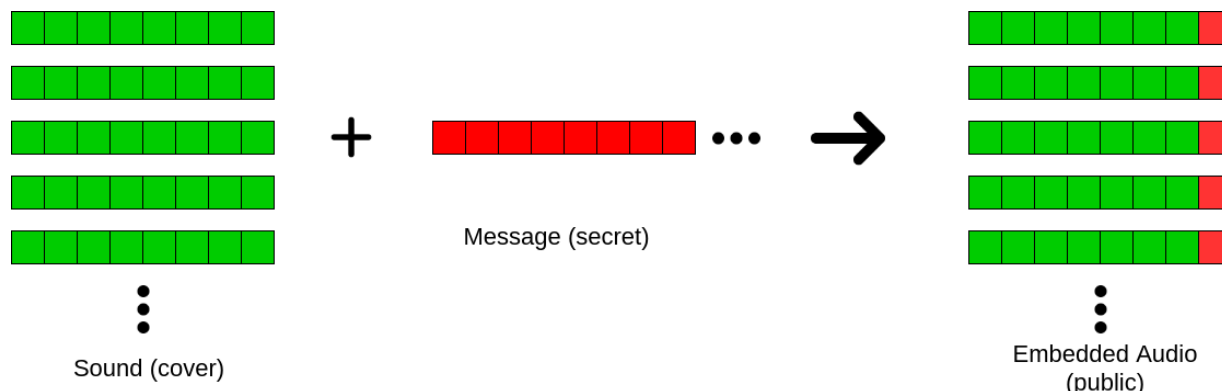

Figure 2: Encryption process

The sender performs "embedding" of the bits of secret messages onto the carrier data byte-by-byte. Whereas the receiver performs the "extraction" procedure by reading LSB bits of each byte of received data, this way the receiver reconstructs the secret message.
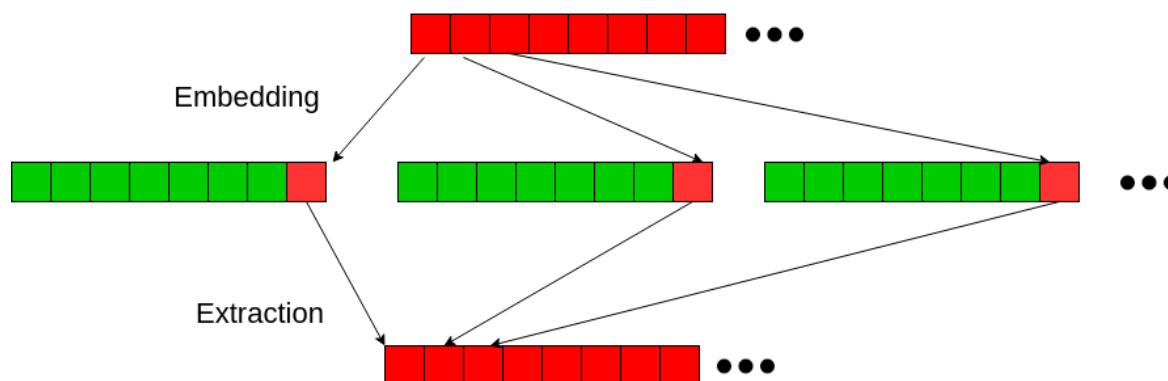

Figure 3: Embedding and Extraction process

IV. Conclusion

The advantage of the LSB technique lies in its ease of implementation and simplicity. The LSB method allows high embedding capacity and uses different frequency levels for more security. Hiding the secret data using Steganography

lowers the chances of the secret data being detected. This LSB technique for audio files work smoothly for .wav audio formats. Using these algorithms (encoding and decoding), one can retrieve secret message exactly as the original data.

V. References

[1]. Rohit Tanwar, Monika Bisla, "Audio Steganography", 2014 International Conference on Reliability Optimization and Information Technology (ICROIT), Feb 2014.

[2]. Ayush Singhal, Nanhay Singh, Mohit Singh Bora, "An Advanced Approach for Implementation of Audio Steganography: Modified LSB Algorithm", International Journal For Science Technology And Engineering, 2015.

[3]. K. Qazanfari and R. Safabakhsh, "A new Steganography Method which Preserves Histogram: Generalization of LSB++", Elsevier International Journal of Information Sciences, Sept. 2014.

[4]. Shivangi Baranawal, Aparna Gupta,Arti Tiwari ,Amit Pratap Singh, "Steganography Using LSB Algorithm", International Journal of Electronics, Electrical and Computational System, 2014.

[5]. https://medium.com/@sumit.arora/audio-steganography-the-art-of-hiding-secrets-within-earshot-part-2-of-2-c76b1be719b3

[6]. R. Darsana, Asha Vijayan, "Audio Steganography Using Modified LSB and PVD", Springer-Verlag Berlin Heidelberg 2011.

[7]. https://www.scribd.com/document/127310687/2849

[8]. B.B. Zaidan, A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, On the Differences between Hiding Information and Cryptography Techniques: An Overview. Journal of Applied Sciences, 2010.

[9]. S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering (IJCSE), 2009.

[10]. https://www.scribd.com/document/424610569/Stegeno

[11]. M. Baritha Begum, Y. Venkataramani, "LSB Based Steganography based on Text Compression", Procedia Engineering, Volume 30, 2012, Pages 703-712.

[12]. Ramadhan J. Mstafa, Christian Bach, "Information Hiding in Images Using Steganographic Techniques", March 2013.