International Journal of Engineering & Technology, 7 (4.15) (2018) 536-538

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Information Hiding Based on Audio Steganography using Least Significant Bit

Fatma Susilawati Mohamad[1]*, Nurul Sahira Mohd Yasin[2]

Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Terengganu, Malaysia
**Corresponding author E-mail: fatma@unisza.edu.my*

Abstract

Steganography is the idea of hiding private or sensitive data or information within something that appears to be nothing out of the normal. A few problems arise especially in securing data and information when the information had been lost or stolen from unauthorized user. Traditionally, we give information manually using paper; it is possible that the information could be stolen by unauthorized user. The main objective of this study is to hide secret information in audio, so that other persons will not notice the presence of the information. The proposed method of this study is by using Least Significant Bit (LSB) algorithm to design an audio steganography. In the proposed method, each audio sample is converted into bits and then the text data is embedded. The expected result of this study will produce a steganography audio that will be able to hide data or information efficiently from unauthorized user, also to ensure the safety of the information in an authorized hand.

Keywords: *Steganography; Audio Steganography; LSB Algorithm.*

1. Introduction

Information security is one of the most challenging problems in today's technological world. This paper is to come up with a technique hiding the presence of secret message which is called steganography. It is also called as "covered writing" because it uses a "cover" of a message for sending any important secret message.
Steganography serves as a means for private, secure and sometimes malicious communication. Steganography is the art to hide the very presence of communication by embedding the secret message into the innocuous looking cover media objects such as images using the human's visual, aural redundancy or media objects' statistical redundancy. Steganography is a powerful tool which increases security in data transferring and archiving. In the steganographic scenario, the secret data is first concealed within another object which is called "cover object", to form "stego object" and then this new object can be transmitted or saved. Embedding secret messages into digital sound is known as Audio Steganography. In this project, the stego-audio will be saved in format audio.wav only.
For any steganography technique to be implemented, it must satisfy three condition:

- Capacity means the amount of secret information can embedded within the host message.
- Transparency evaluates how well a secret information is embedded in the cover audio.
- Robustness measures the ability of secret information to withstand against attacks.

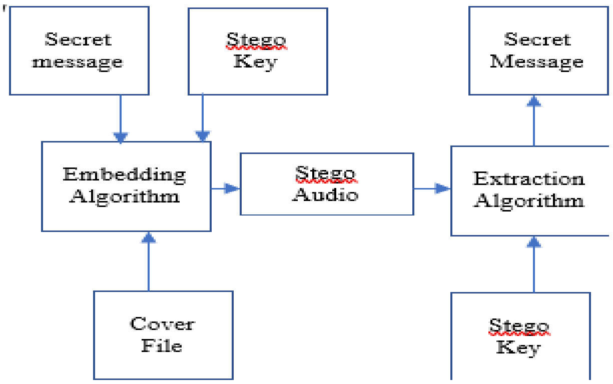

Fig. 1: Block Diagram of Steganography

2. Literature Review

In [12] present an approach for resolving the problem related to the substitution technique of audio steganography. In first level of security, we use RSA algorithm to encrypt message, in the next level, encrypted message is to be encoded in to audio data for this we used genetic algorithm-based substitution method. The basic idea behind this paper is to enhance the security and robustness.

- Advantages: The theory of technique is that simply replacing either a bit or a few bits in each sample will not be noticeable to the human eye or ear depending on the type of file.
- Disadvantages: The main problems of audio substitution steganography algorithm are considerably low robustness. There are two types of attacks to steganography and therefore there are two type of robustness. One type of attacks tries to reveal the hidden message and another type tries to destroy the hidden message.

In [2] proposes a novel approach, where a duel encryption methodology has been implemented. In the first level of encryption, a pattern matching algorithm has been employed to encrypt the text message in terms of their positional value. In second level, the conventional LSB method has been used to embed the positional value in the cover file. Such a duel encryption method will ensure data security in an efficient manner.

- Advantages: Allows a large volume of data given in audio or text format to be encoded and data are found in the receiving end in loss-less format.
- Disadvantages: It is easy for the invaders to identify and destroy the information.

In [13] proposed a novel approach for concealing data. The proposed algorithm is an amalgamation of text encryption, audio steganography and audio encryption. In the first step, the original text message is encrypted using modified Vigenère cipher algorithm. The cipher text gets embedded into the cover audio using LSB encoding in the second step. Further, the audio file is then subjected to transposition making use of Blum Blum Shub pseudo random number generator.

- Advantages: This combination of cryptography steganography ensures that even if the audio file is intercepted by an unauthorized person, the person doesn't discover the secret information.
- Disadvantages: The audio is encrypted only using transposition.

The authors recommend more secure encryption algorithms to be utilized for text encryption, so that data is not easily stolen by an unauthorized party.

In [11] give an overview of two primitive techniques to get an idea of how steganography in audio file works. LSB modification and phase encoding technique are very primitive in steganography. An effective audio steganographic scheme should possess the following three characteristics: Inaudibility of distortion, Data Rate and Robustness. These characteristics are called the magic triangle for data hiding.

- Advantages: This method is easy to implement, but is very susceptible.
- Disadvantages: This method can be used when only a small amount of data needs to be concealed.

In [8, 10] worked with text as the cover medium with the aim of increasing robustness and capacity off hidden data. Elitism was used for the fitness function.

- Advantages: This approach works, achieving effective optimization, security, and robustness.
- Disadvantages: Applicable for text files only.

3. Proposed Work

Least significant bit is algorithm that replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. It allows for large amount of data encoded. The expected result of this study will produce a steganography audio that will be able to hide data or information efficiently from unauthorized user also to ensure the safety of the information in an authorized hand. So, with the algorithm and concept of the project, the system can be a one recommender system for user who want to send the information in more secure way.

4. Methodology

To attain the objective, step-by-step methodology is use in this research work. Figure 2 illustrates the audio steganography process, which is based on least significant bit modification. The flow of the algorithm is given as shown in Figure 2. It is showing the different steps that will be followed in order to encode and decode the secret message.

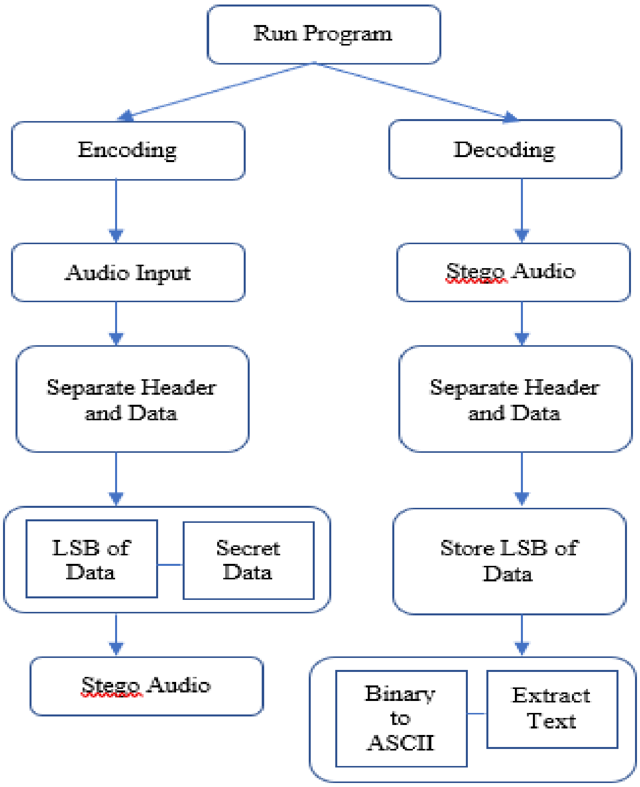

Fig. 2: Flow of LSB Technique for Audio Steganography

4.1. Embedding process (Encoding)

1) Enter audio input
2) Separate the header and data because header in audio file is very sensitive and must not change that
3) Replace the LSB of the data with secret text
4) Finally get stego audio that have secret text

4.2. Extraction Process (Decoding)

1) Receiver receive the stego audio that contain audio and secret data
2) Separate header and the data
3) Store the LSB of the data because LSB contain secret text
4) The LSB will be in binary format, and convert into ASCII format to get the text back

4.3. Least Significant Bit

Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded. In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In some implementations of LSB coding, however, the two least significant bits of a sample are replaced with two message bits. This increases the amount of data that can be encoded, but also increases the amount of resulting noise in the audio file as well. To extract a secret message from an LSB encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process. Normally, the length of the secret message to be encoded is smaller than the total number of samples in a sound file. One must decide then on how to choose the subset of samples that will contain the secret message and communicate that decision to the receiver.

4.4. Example

Character to be embedded – “A”
ASCII value of “A”: 65
8-bit binary representation of the ASCII value: 01000001
8 consecutive audio frames in binary format (consider 8 bit)
10010010 01010101 10010101 11101010 10000100
11110011 10100000 11010101

Table 1: Embedding Process

Each Bit to be Embedded	8 Consecutive Audio Frames	
	Before Embedding	After Embedding
0	10010010	10010010
1	01010101	01010101
0	10010101	10010100
0	11101010	11101010
0	10000100	10000100
0	11110011	11110010
0	10100001	10100000
1	11010101	11010101

5. Results and Discussion

The steganography is one of the safest forms of data transmissions in this digital world. In the proposed method, an audio steganography using least significant bit is proposed and tested. It will produce a steganography audio that will be able to hide data or information efficiently from unauthorized user also to ensure the safety of the information in an authorized hand. In conclusion, by using this method, the text can be embedded into the cover file and it is accepted in the receiving end without any change. So, it is concluded that the integrity and quality of the message are well maintained.

6. Conclusion

Future scope of this paper is the possibilities of improvements in audio steganography system with respect to different technique of data hiding in audio. This paper mainly concentrates on only .wav format of audio files and can extended to a level such that it can be used for the different types of audio wave file formats like .au, .mp3, wma etc., Also, noisy audio files can be considered for making comparisons of SNR and PSNR after embedding message into the same.

Acknowledgement

Special thanks goes to Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin for the support of this work.

References

[1] Kulkarni, S. A., Patil, P. S., & Patil, B. S. (2012). A optimized and secure audio steganography for hiding secret information-review. Journal of Electronics and Communication Engineering, 1, 12-16.

[2] Chowdhury, R., Bhattacharyya, D., Bandyopadhyay, S. K., & Kim, T. H. (2016). A view on LSB based audio steganography. International Journal of Security and Its Applications, 10(2), 51-62.

[3] Adhiya, K. P., & Patil, S. A. (2012). Hiding text in audio using LSB based steganography. Information and Knowledge Management, 2(3), 8-14.

[4] Nehru, G., & Dhar, P. (2012). A detailed look of audio steganography techniques using LSB and genetic algorithm approach. International Journal of Computer Science Issues, 9(1), 402-406.

[5] Rahmani, M. K. I., Arora, K., & Pal, N. (2014). A crypto-steganography: A survey. International Journal of Advanced Computer Science and Application, 5, 149-154.

[6] Kaur, N., & Behal, S. (2014). Audio steganography using LSB edge detection algorithm. Proceedings of the International Conference on Communication, Computing and Systems, pp. 180-183.

[7] Pradhan, K., & Bhoi, C. (2012). Robust audio steganography technique using AES algorithm and MD5 hash. International Journal of Innovative Research in Advanced Engineering, 1(10), 282-287.

[8] Chandrakar, P., Choudhary, M., & Badgaiyan, C. (2013). Enhancement in security of LSB based audio steganography using multiple files. International Journal of Computer Applications, 73(7), 1-4.

[9] Sakthisudhan, K., Prabhu, P., & Thangaraj, P. (2012). Secure audio steganography for hiding secret information. Proceedings of the International Conference on Recent Trends in Computational Methods, Communication and Controls, pp. 33-37.

[10] Chadha, A., & Satam, N. (2013). An efficient method for image and audio steganography using Least Significant Bit (LSB) substitution. International Journal of Computer Applications, 77(13), 37-45.

[11] Bandyopadhyay, S. K. & Banik, B. G. (2012). Multi-level steganographic algorithm for audio steganography using LSB modification and parity encoding technique. International Journal of Emerging Trends and Technology in Computer Science, 1(1), 71-74.

[12] Singh, G., Tiwari, K. & Singh, S. (2014). Audio steganography using RSA algorithm and genetic based substitution method to enhance security. International Journal of Scientific and Engineering Research, 5(5), 703-707.

[13] Sinha, N., Bhowmick, A., & Kishore, B. (2015). Encrypted information hiding using audio steganography and audio cryptography. International Journal of Computer Applications, 112(5), 49-53.