INTERNATIONAL CONFERENCE ON ADVANCES IN TECHNOLOGY AND COMPUTING (ICATC-2021)
Faculty of Computing and Technology (FCT), University of Kelaniya, Sri Lanka
18th December 2021

Index N0: CT-11-74

Audio Steganography using LSB Technique to Embedding Data

Dayanantha Shanmugaradnam (1st Author)
Department of Computer Systems Engineering
University of Kelaniya.
Kelaniya, Sri Lanka
dayanant_ct15009@stu.kln.ac.lk

Dr. Hesiri Dhammika Weerasinghe (2nd Author)
Department of Computer Systems Engineering
University of Kelaniya
Kelaniya, Sri Lanka
hesiri@kln.ac.lk

***Abstract* - Data protection is a major concern on the internet medium. Data needs to be protected from intrusion, penetration, and data theft. Audio steganography is used to hide secret messages in an audio file. This method was intended to secure the secret message. The secret message was protected using the hashing and encryption technique and the Least Significant Bit substitution was performed to hide the data. The Stego audio files were analyzed by Signal-to-Noise Ratio and Mean Opinion Score. The Stego audio files had an 80dB average Signal-to-Noise Ratio and the overall Mean Opinion Score was 4.4 out of 5. It proves that this method helped to improve the robustness and imperceptibility. Using the proposed method higher security can be achieved.**

Keywords — data hiding, audio steganography, lsb

I. INTRODUCTION

Data can be hidden using various methods. Steganography is one of them. In other data hiding methods, the existence of the data can be easily discovered and revealed [1]. Steganography is the art of concealing data. In steganography, only the sender and the receiver know the existence of the hidden data. As a result, steganography has emerged as the most reliable protection method [2].

The basic scheme behind the audio steganography process is to conceal a message secretly on an audio signal called cover audio [3]. The resultant audio after this process is called “stego” audio, which is sent via a protected channel to the recipient. At the receiver’s end, the hidden data will be extracted from the audio by applying a series of pre-defined steps [4].

Audio data concealing is very difficult than other stenographic methods. Because it relies on the human ear's dissimilar sensitiveness to a higher and lower intensity of sounds [5]. In audio steganography, several methods and several techniques were used. The Least Significant Bit coding method is coming under the Spatial Domain Technique [6].

The least significant Bit based audio steganography methods have made a significant contribution. However, because of their lack of robustness, the security of the Least Significant Bit based methods could be quickly violated to obtain the hidden data [7].

Therefore, the hidden or the embedded data needs to be secured. Using Cryptography along with Steganography will increase security.

II. OBJECTIVES

The following objectives were focused on throughout this study.

- A detailed study on Steganography
- Identify the Techniques and Methods
- Study on the Least Significant Bit
- Securing the secret message
- Testing the stego audio

III. METHODS

A. Adapted Technologies

Cryptography

Cryptography is the process of altering the structure of a file before it is sent. Through cryptography, the golden triangle of Confidentiality, Integrity, and Authentication can be achieved [8]. The secure data hashing and the symmetric key encryptions are used in this method.

Audio Signal Processing

Through signal processing, the character of the audio file can be changed. This audio processing can be used for different purposes [9]. Here it is used to enhance the quality of audio, create a new effect, compression and store and transmit data and information.

B. Embedding Process

A key and salt were generated from the password using SHA 256 hashing algorithm. At the same time, the secret message and its length were used to create a formatted message. Then the generated key was encrypted using the fernet symmetric key encryption. Later, a token

was created by encrypting the formatted message using the encrypted key. Finally, the embedding process started in the least significant bit of the cover audio from its offset. The length of the token and salt values was embedded in the first 8 bytes of the cover audio. From the next bytes, the token value string is embedded in the cover audio.

C. *Extraction Process*

In the stego audio from its offset length of the token and the salt were extracted. As the next step token value was extracted using its length. Then the key was generated from the given password and salt using SHA 256 algorithm. Later, the generated key was encrypted using fernet symmetric key encryption. The token was decrypted using the encrypted key to get the formatted message. From the formatted message length of the message was extracted and the secret message was extracted.

Hashing the password and the salt are increasing the security of the embedded message. From this method, Confidentiality, Integrity, and Authentication are archived.

IV. RESULT AND DISCUSSION

The proposed method is tested on four Wav files. And three different secret messages are used to embed. These are evaluated using the Signal to Noise Ratio (SNR) and Mean Opinion Score (MOS).

A. *Signal to Noise Ratio*

The ratio between the cover audio signal and the stego audio signal are used to evaluate the SNR value. The bigger the SNR ratio is better the sound quality.

Table 1. Signal-to-Noise Ratio Values

Cover Audio (.wav)	**Cover audio size (KB)**	**Sampling Frequency (kHz)**	**Time (Sec)**	**SNR (dB)**		
				456 bytes	**796 bytes**	**1480 bytes**
1.Violin	2585	44	15	84.18	79.74	68.89
2.MakeItUp	2585	44	15	85.84	80.56	70.12
3.Takeaway	3446	44	20	89.65	85.49	79.38
4.Believer	3446	44	20	87.37	84.61	77.42

B. *Mean Opinion Score (MOS)*

MOS is commonly used to evaluate the quality of sound. Group of individuals is rated the quality of the stego audio file by listening and compare with the cover audio file.

Table 2. Mean Opinion Score Values

Stego Audio (.wav)	**Mean Opinion Score (scale 1 to 5)**		
	456 bytes	**796 bytes**	**1480 bytes**
1.Violin	4.1	3.7	3.2
2.MakeItUp	4.6	4.6	4.6
3.Takeaway	4.8	4.8	4.7
4.Believer	4.8	4.7	4.8

Experimental study results clearly show the differences between the cover audio file and how the secret message affects the quality of the stego audio file.

The audios 1. Violin and 2. MakeItUp are equal in file size and length. But the SNR values are different with the size of the embedded data. It is because these files have different frequency ranges. The audios 3. Takeaway and 4. Believer are bigger than the previous audio samples and also both are equal in file size and length. These files also have different SNR values. Therefore, it is concluded that the SNR value depends on not only the sampling frequency, length, size, the frequency range of cover audio but also the size and the content of the hidden data. To avoid detection, a user should listen to a stego audio before sending it to a receiver.

The hashing algorithm enhances security. If only the encryption algorithm is used, the encrypted message can be retrieved when the password key is found. But in hashing the hash values has a fixed length and it cannot be reversible. In addition to that, a hash algorithm can be created using the salt and the password. Salt is a randomized number added with the password before the hashing process starts. Even though two people use the same password its hash value will differ because of the salt added. It is the best way to store passwords.

The larger the file size is carrying the larger amount of secret data without any major change. It is proven from the sample audios and the different secret messages.

V. CONCLUSIONS

Information security is very important since information is exchanged on the publicly accessible Internet. Both cryptography and steganography can be used to provide information security. Steganographic techniques allow hiding valuable information in a normal file. While the cryptography technique is used to create confidentiality, integrity and authentication to the hided information.

This proposed method increases the security of the embedded data using encryptions and hashing techniques. The SNR values show the quality of the stego audio file. And the MOS values ensured the quality of the stego audio files. The quality of the audio does not drastically change when a secret message is embedded into the audio by using the proposed solution.

Even though the steganography breaks and the hidden chunk is discovered, it is still useless because it is encrypted using a password. When these two systems are combined, a high level of protection is achieved.

REFERENCES

[1] S. P. Rajput, K. P. Adhiya, and G. K. Patnaik, "Hide Text in Audio," *2017 Int. Conf. Comput. Commun. Control Autom.*, pp. 1–6, 2017.

[2] R. Doshi, P. Jain, and L. Gupta, "Steganography and its Applications in Security," *Int. J. Mod. Eng. Res.*, vol. 2, no. 6, pp. 4634–4638, 2012.

[3] A. Binny, "Hiding Secret Information Using LSB Based Audio Steganography," pp. 1–4, 2014, doi: 10.1109/ISCMI.2014.24.

[4] V. Sharmal, "LSB Modification based Audio Steganography using Trusted Third Party Key Indexing Method," pp. 403–406, 2015.

[5] H. Dudhwal, A. Prof, and J. Boaddh, "A Review of an Extensive Survey on Audio Steganography Based on LSB Method," vol. 7, no. 1, pp. 177–180, 2021.

[6] S. Mishra, V. K. Yadav, M. C. Trivedi, and T. Shrimali, "Audio steganography techniques: A survey," *Adv. Intell. Syst. Comput.*, vol. 554, no. February, pp. 581–589, 2018, doi: 10.1007/978-981-10-3773-3_56.

[7] W. A. Shah, D. Shehzad, A. I. Umar, J. Hussain, and A. Qadir, "Audio Steganography Based on Lsb Msb," vol. 15, no. 6, 2017.

[8] S. K. Moudgil, A. K. Goel, and M. Sharma, "Steganography on Audio Wave Tenth Layer by Using Signal to Noise Ratio Test and Spectrogram Analyses," *Int. J. Appl. Eng. Res.*, vol. 13, no. 4, p. 1931, 2018, doi: 10.37622/ijaer/13.4.2018.1931-1935.

[9] H. Dutta, R. K. Das, S. Nandi, and S. R. M. Prasanna, "An Overview of Digital Audio Steganography," *IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India)*, no. December, 2019, doi: 10.1080/02564602.2019.1699454.