JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-12, Dec 2018 E-ISSN: 2347-2693

A Hybrid Audio Steganography Method

T. Acharjee[1*], A. Choudhury[2], P. Kumar [3]

[1,2,3]Department of Computer Science, Assam University, Silchar, India

[*]Corresponding Author: tapacharjee@gmail.com, Tel.: +91-3842-241271

Available online at: www.ijcseonline.org

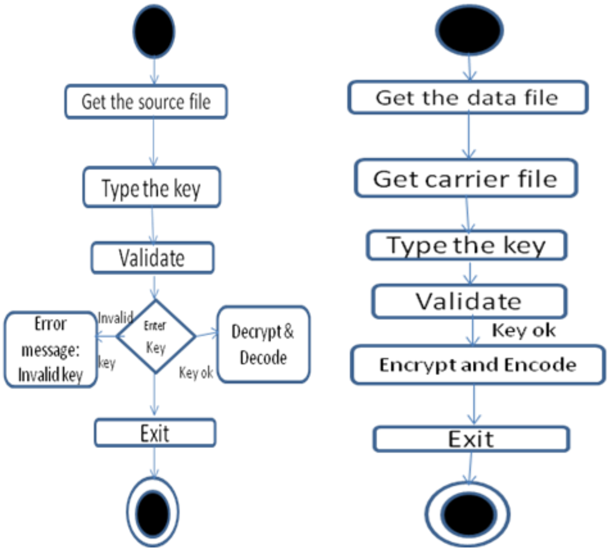
Accepted: 24/Dec/2018, Published: 31/Dec/2018

Abstract— In this era of smartphones and gadgets assisted by high speed internet connectivity, the volume of data transmission and storage have gained a lot. As a result data security and confidentiality has become more important issue than ever. Steganography is one data hiding technique which helps to send some secret message to the receiver by concealing it in a cover file. In this paper, we have focused on the Audio Steganography method. The major challenge in audio steganography is to obtain robust high capacity steganographic systems. This paper presents a secure data transfer technique using Audio Steganography. Here we have proposed a hybrid method combining modified Least Significant Bit (LSB) and spread spectrum based audio steganography methods. We have implemented the proposed method and compared the results with the other methods using two quality measurement techniques, namely, Peak signal to noise ratio (PSNR) and Mean Square Error (MSE).

Keywords— Audio Steganography, confidentiality, Data security, Internet, Peak signal to noise ratio(PSNR), Mean Square Error(MSE)

I. INTRODUCTION

Modern development in technologies has created threats to secure data transmission in digital communication and networking. Cryptography and Steganography are the two techniques which support in attaining security goals. Cryptography involves scrambling of data by using different transformations whereas Steganography mainly deals with concealing the secret data in a cover media in such a way that presence cannot be identified [1]. The word ‘steganography’ is originated from a Greek word meaning covered writing [2]. With Steganography, we can conceal any digital data in any ‘innocent’ looking digital carrier. This secret information can be any simple plain text or cipher text, or even images. The main advantage of Steganography over cryptography is that in Steganography the messages do not invite any attention towards themselves [3]. In digital audio steganographic methods, the secret messages are hidden in digital sound. The secret information may be hidden by making some small changes in the cover sound file. Various audio steganographic software can nowadays support hiding messages in WAV, AU, and even MP3 sound files.



a) Embedding b) Extraction

Figure 1. Activity Diagrams for Embedding and Extraction Process[2]

The terms used in steganography are: i) Cover Signal: A Cover signal is an innocent signal at which the secret information is embedded. The Cover file can be any text, image, audio and video, ii) Stego file: The file which obtained after the secret message is embedded into the cover signal called stego signal, iii) Stego key: The Key is used for providing more security for the secret message. This key is optional during the encryption and decryption process.

In this paper, we are combining the LSB method and Spread Spectrum method in order to acquire high security of sending the texts so that the decoding process will be difficult for the users. Only the sender and receiver will know that it is multi-level approach and how to decode the messages.

Rest of the paper is organized as follows, Section I contains the introduction of steganography and its use in real life along with the basics of audio steganography, different methods of audio steganography is discussed briefly in Section II, Section III contain the proposed method, Section IV contains the results and discussion after the implementation of the proposed method, section V concludes research work with future directions.

II. METHODS OF AUDIO STEGANOGRAPHY

There are many encoding methods for performing audio steganography. The five of the most popular encoding methods for hiding data inside of an audio file are: LSB Coding [5][6][7], Parity Coding [8], Phase Coding [9][10][11], Spread Spectrum [12][13][14], Echo Hiding [15].

Least Significant Bit (LSB) Method

It is a time domain method of audio steganography where the LSB bits of the audio signal may be replaced by the bits of the secret message. The advantage of this method is that it is a simple and easy way of hiding Information with high bit rate. But the main drawback of this method is that sometimes it may be easy to extract and to destroy.

Parity Coding Method

In this method of audio steganography, audio Signal is broken into separate areas of samples and hide the secret message in the parity bit of each sample area. In the case of a mismatch between the secret bit and sample region's parity bit, the LSB of one sample in the region may be flipped. Firstly XOR operation is performed on the LSB, and after that, the LSB of the sample may be modified or not depending on the result of message bit and XOR operation.
The advantage is that more choices in encoding a secret bit. The drawback is that a large amount of data cannot be encoded.

Phase Coding Method

This method operates by replacing the original phase of the signal with a reference phase representing the secret information. The other segments phase is also tuned to synchronize with the relative phase between segments. This method is more robust, but the calculations may be really complicated and ability may be limited.

Spread Spectrum Method

Spread spectrum method is heavily used in communication these days, especially in mobile communications. In audio steganography also the spread spectrum method may be used. Here the secret information is spread over the frequency spectrum of the audio signal. Here the pseudorandom number generator like LFSR (Linear Feedback Shifty Register) may be used to spread the message over the sound file like a random distribution. Spread spectrum method may show better performance compared to LSB coding, phase coding, and parity coding techniques in terms of data transmission rate and robustness [4].

Echo Hiding

Echo hiding technique is another time domain method which hides the secret message in a sound file by using an echo into the discrete signal. When the strong signal disappears it is not capable of hearing with a weak signal. Therefore, the echo is used for embedding the secret message. This method is resilient to lossy data compression algorithms.

III. PROPOSED METHOD

A. Embedding and Extraction Process using Spread Spectrum Method

In Embedding process, we, first of all, take an audio file in .wav format. Then select secret text (.txt). Then convert the secret text ASCII value into binary format, e.g., A = 65 = 01000001). Thereafter we shall generate Pseudo-Random number using LFSR for every character in the message. Then we perform XOR operation between every character with its Pseudo-Random number and it gives an embedded message. We insert that embedded message in the audio file using the LSB method and it generates the stego-audio file. This stego-audio file will be sent to the receiver with the secret keys.
Encoding

Example:

Message: HELLO
We will generate the pseudo random number for each character of (HELLO)
PRN For H= 1 1 0 0 1 0 0 1
PRN For E x= 0 1 1 0 0 1 0 0
PRN For L x=1 0 1 1 0 0 1 0
PRN For L x=0 1 0 1 1 0 0 1
PRN For O x=0 0 1 0 1 1 0 0
First embed H using its respective pseudo random number byperforming XOR operation.

H(72) = 0 1 0 0 1 0 0 0
PRN For (H) = 1 1 0 0 1 0 0 1
Embedded (H)= 1 0 0 0 0 0 0 1
For other letters same procedure is followed:

E(69) = 0 1 0 0 0 1 0 1
PRN For (E) = 0 1 1 0 0 1 0 0
Embedded(E)= 0 0 1 0 0 0 0 1

L(76) = 0 1 0 0 1 1 0 0
PRN For (L) = 1 0 1 1 0 0 1 0
Embedded(L)= 1 1 1 1 1 1 1 0

L(76) = 0 1 0 0 1 1 0 0
PRN For (L) = 0 1 0 1 1 0 0 1
Embedded(L)= 0 0 0 1 0 1 0 1

O(79) = 0 1 0 0 1 1 1 1
PRN For (O) = 0 0 1 0 1 1 0 0
Embedded(O)= 0 1 1 0 0 0 1 1

For extraction, we first select the stego-audio file. Then we will enter the Secret key. Then we will extract the embedded message from stego-audio using LSB extraction algorithm. Lastly, we will perform XOR operation between every character of the embedded message with its Pseudo-Random number by which we get our original message.

Extraction Example:
Embedded (H)= 1 0 0 0 0 0 0 1
Embedded (E)= 0 0 1 0 0 0 0 1
Embedded (L)= 1 1 1 1 1 1 1 0
Embedded (L)= 0 0 0 1 0 1 0 1
Embedded (O)= 0 1 1 0 0 0 1 1

PRN For H= 1 1 0 0 1 0 0 1
PRN For E = 0 1 1 0 0 1 0 0
PRN For L =1 0 1 1 0 0 1 0
PRN For L =0 1 0 1 1 0 0 1
PRN For O =0 0 1 0 1 1 0 0

Then we will extract the original value of H from embedded (H) by performing XOR operation between embedded (H) and PRN of H.
Embedded (H)= 1 0 0 0 0 0 0 1
PRN of (H)= 1 1 0 0 1 0 0 1
Original H(72)= 0 1 0 0 1 0 0 0
Repeat the procedure for other letter also:
Embedded (E)= 0 0 1 0 0 0 0 1
PRN of (E)= 0 1 1 0 0 1 0 0
Original E(69)= 0 1 0 0 0 1 0 1

Embedded (L)= 0 0 0 1 0 1 0 1
PRN of (L)= 0 1 0 1 1 0 0 1
Original H(76)= 0 1 0 0 1 1 0 0

Embedded (O)= 0 1 1 0 0 0 1 1
PRN of (O)= 0 0 1 0 1 1 0 0
Original H(79)= 0 1 0 0 1 1 1 1

B. Embedding and extraction using XOR-LSB Method

After this, we shall use the LSB method in order to acquire high security of sending the texts so that the decoding process will be difficult for the users. Only the sender and receiver will know that it is multi-level approach and how to decode the messages.

Firstly, for embedding, we shall take an audio file as an input so that we can hide the messages. Then we will embed the original secret text message in the input audio file that we have taken with the help of the previous technique. Now we will set the password for embedding the secret message text. Then we will get the stego audio file for the original text Message. Now we will create a duplicate secret text message Now we will embed the duplicate secret message in the resultant stego audio for the original text message with the LSB technique. Then we will set the password for the secret message while embedding. Lastly, we will get our final stego audio

The receiver will extract the final stego audio file with the LSB Technique by entering the password of duplicate secret message. After extracting, the receiver will get the extracted duplicate text message and the stego audio after extracting duplicate text message. Now the receiver will extract that stego-audio with the help of previously mentioned technique by entering the password of original secret message. Then the receiver will get the extracted original text message and original audio file.

IV. Results and Discussion

A. Performance Metrics

Performance Metrics are used to measure the performance of a particular algorithm. It is also used to check whether the algorithm is efficient or not. In this paper, we have considered two performance metrics, namely, Peak Signal to Noise Ratio (PSNR) and Mean Square Error(MSE) [16]. These two metrics are defined below:

PSNR (Peak Signal to Noise Ratio):

The Peak Signal to Noise Ratio (PSNR) depicts the measure of reconstruction of the compressed image. In steganography, this metric may be utilized to differentiate between the cover and stego image. The easy computation is the advantage of this measure. It is formulated as:

$$\text{PSNR} = 10\log 255^2 / \text{MSE}.$$

A low-value PSNR shows that the constructed image is of poor quality.

Mean Square Error (MSE):

Another most widely used quality measurement technique is Mean Square Error (MSE). The MSE can be defined as the measure of the average of the squares of the difference between the intensities of the stego image and the cover image. This technique is popular due to its tractability. It is represented as:

$$MSE = 1/MN \sum_{i=1}^{M} \sum_{j=1}^{N} [f(i,j) - f'(i,j)]^2$$

where f(i,j) is the original image and f'(i,j) is the stego image. A large value for MSE means that the image is of poor quality.

B.Results

Table 1. Results of Modified LSB Method using XOR

Audio File	**Text File**	**Audio sample in KB**	**Ext Sample**	**PSNR**	**MSE**
Audio 1	Text 1	3471	90	70.776	8.7995e-08
Audio 1	Text 2	3471	300	68.246	1.4305e-07
Audio 1	Text 3	3471	1200	54.270	3.6908e-06
Audio 2	Text 1	10,508	90	70.729	8.4823e-08
Audio 2	Text 2	10,508	300	70.385	8.9205e-08
Audio 2	Text 3	10,508	1200	69.692	1.1254e-07

Table 2. Results of Spread Spectrum Method using LFSR

Audio File	**Text File**	**Audio sample in KB**	**Ext Sample**	**PSNR**	**MSE**
Audio 1	Text 1	3471	90	70.512	8.7895e-08
Audio 1	Text 2	3471	300	66.264	2.5065e-07
Audio 1	Text 3	3471	1200	50.471	8.7908e-06
Audio 2	Text 1	10,508	90	70.720	8.5823e-08
Audio 2	Text 2	10,508	300	70.282	9.4505e-08
Audio 2	Text 3	10,508	1200	68.293	1.3654e-07

Table 3. Results of Hybrid Method using LSB and Spread Spectrum

Audio File	**Text File**	**Audio sample in KB**	**Ext Sample**	**PSNR**	**MSE**
Audio 1	Text 1	3471	90	70.512	8.5695e-08
Audio 1	Text 2	3471	300	66.261	2.4835e-07
Audio 1	Text 3	3471	1200	51.025	8.7108e-06
Audio 2	Text 1	10,508	90	70.727	8.2823e-08
Audio 2	Text 2	10,508	300	70.826	9.3105e-08
Audio 2	Text 3	10,508	1200	68.638	1.3154e-07

In the first method of LSB using XOR the PSNR and MSE value is slightly greater than the spread spectrum method and the hybrid method using LSB and the spread spectrum method. But this method is actually less secured compared to the spread spectrum method. In the second method of spread spectrum the PSNR and the MSE value is slightly less than LSB using XOR but it has higher security than the LSB method using XOR because this method is more complex than the first method. But this spread spectrum method is less secured than the hybrid method. In the third method that is the hybrid method using LSB and the spread spectrum the PSNR and MSE value is slightly less than the first method but greater than our second method. But this method is having more security among all of the methods due to its complex nature. So we can conclude from the above tables and the observations that the hybrid method is more reliable to take due to its complex nature having a high value of PSNR and MSE and robust in nature. So after comparing all the three methods in this chapter, we have concluded that Hybrid Method using LSB and Spread Spectrum is the best among all of them.

V. Conclusion and Future Scope

This paper has looked in detail at the major techniques used for data hiding in audio files. We have proposed here a hybrid technique XOR-LSB and Spread Spectrum Technique. In that technique, we combined the modified LSB and spread spectrum by creating a duplicate message so that the attacker will get confused and do not understand which message is to be extracted. Also, this paper checks the performance of the various methods. This work can be extended by improving the performance of the methodology by making it more robust and less complex for the low-frequency audio signal. Also, time consumption for embedding as well as for extraction of the watermark can be reduced.

REFERENCES

[1] M. Zamani, A. B. A. Manaf, R. B. Ahmad, F. Jaryani, H. Taherdoost, A. M. Zeki, "A Secure Audio Steganography Approach", Internet Technology and Secured Transactions, 9-12 Nov. 2009.

[2] G. Nehru, P. Dhar, "A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, PP 1694-0814,2012.

[3] B. G. Kodge, "Information Security: A Review on Steganography with Cryptography for Secured Data Transaction", International Journal of Scientific Research in Network Security and Communication, Volume-5, Issue-6, PP 1-4, 2017.

[4] Sanju, Y. Mamta, "Audio Steganography", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 3, Issue 6, PP 66-70, 2018

[5] N. Cvejic and T. Seppnen, "Increasing the capacity of LSB based audio steganography", In the Proceeding of 5th IEEE International Workshop on Multimedia Signal Processing, pp. 336338, 2002.

[6] S. Roy, A.K. Singh, J. Parida and A. S. Sairam, "Audio Steganography Using LSB Encoding Technique with Increased Capacity and Bit Error Rate Optimization", In the Proceeding of *CCSEIT-12*, India, 2012.

[7] H. Kumar, Anuradha, "Enhanced LSB technique for Audio Steganography", In the Proceeding of ICCCNT'12, India, 2012.

[8] A. Mane, G. Galshetwar and A. Jeyakumar, "Data Hiding Technique: Audio Steganography using LSB Technique", International Journal of Engineering Research and Applications Vol. 2, Issue 3, 2012.

[9] P. P. Balgurgi, S. K. Jagtap, "Audio Steganography Used for Secure Data Transmission," In Proceedings of International Conference on Advances in Computing, pp. 699–706, India, 2012.

[10] K. Geetha, P. V. Muthu, "Implementation of ETAS (embedding text in audio signal) model to ensure secrecy," International Journal on Computer Science and Engineering, vol. 2, no. 4, pp. 1308–1313, 2010.

[11] M. Wakiyama, Y. Hidaka, K. Nozaki, "A Novel Phase Coding Technique for Steganography in Auditive Media", In Proceedings of Sixth International Conference on Availability, Reliability and Security, IEEE 2011.

[12] Z. Kexin, "Audio Steganalysis of Spread Spectrum Hiding Based on Statistical Moment", In Proceedings of 2nd International Conference on Signal Processing Systems (ICSPS-2010), IEEE, vol. 3, pp. 381-384, 2010.

[13] M. Nutzinger, C. Fabian, M. Marschalek, "Secure Hybrid Spread Spectrum System for Steganography in Auditive Media", In Proceedings of Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing ,IEEE, pp. 78-81,2010.

[14] F. Rezaei, T. Ma, M. Hempel, D. Peng, H. Sharif, "An Anti-Steganographic Approach for Removing Secret Information in Digital Audio Data hidden by Spread Spectrum Methods", In Proceedings of IEEE Communication and Information Systems Security Symposium , 2013.

[15] F. Djebbar, B. Ayad, H. Hamam, K. Abed-Meraim, "A view on latest audio steganography techniques," in Proceedings of the 7th International Conference on Innovations in Information Technology (IIT), pp. 409–414, United Arab Emirates, 2011.

[16] R. Kaur, J. Bhatia, H. S. Saini, R. Kumar, "Multilevel Technique to Improve PSNR and MSE in Audio Steganography" International Journal of Computer Applications , Volume 103, No.5,pp 1-4, 2014.

Authors Profile

Dr Tapodhir Acharjee currently is working as an Assistant Professor in the Department of Computer Science & Engineering, Assam University, Silchar, India. He recently completed PhD research from Assam University, Silchar, Assam, India. He is also member of different professional bodies like IEEE, Computer Society of India(CSI), IAENG, Institute of Engineers(India). His areas of interests include Wireless Ad-hoc Networks, Cryptography & Network Security, Artificial Intelligence & Deep Learning etc.

Ms Ananya Choudhury completed her Bachelor of Technology from Assam University, Silchar in the year 2018.

Mr Pawan Kumar completed his Bachelor of Technology from Assam University, Silchar in the year 2018.