Volume 6, Issue 12, December 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Enhanced Audio Steganography Technique

Shital P. Rajput[1], Krishnakant P. Adhiya[2]
[1]PG Student, [2]Associate Professor
[1, 2] Department of Computer Engineering, North Maharashtra University, Jalgaon,
SSBT's COET, Bhambhori, Jalgaon, Maharashtra, India

Abstract— Nowadays keeping information secret is the necessity in every area like business, health centers, military applications etc. Therefore information security is playing an important role and attraction of researchers. Efficient secrecy can be achieved at least in part, by implementing Steganography techniques. The existing LSB based steganography techniques are easy to implement but suffers from low embedding rate and low robustness. This paper proposes the new enhanced audio steganography technique where two bits of secret message are embedded at the time on 0 to 7th LSB position based on the compliments of 3 MSBs of carrier audio. Here in the proposed work, two algorithms have been proposed where in the first algorithm 2 data bits of secret message are embedded at a time on 0 to 7th LSB positions based on the 3 MSBs of carrier audio and in second algorithm those 2 data bits are embedded on 0 to 7th LSB positions based on the compliments of 3 MSBs of carrier audio. Therefore the proposed scheme provides the improved performance by embedding two bits rather than single bit and additional security is provided by using secret key. Without knowing the valid secret key it is difficult to extract the secret message.

Keywords— Embedding, Encryption, Least Significant Bit, Most significant Bit, Security

I. INTRODUCTION

The word steganography is derived from the Greek words grafia means "writing" and "stegos means "Covered or protected" defining it as "covered writing". Steganography is the art and science of hiding information with a secret meaning inside other seemingly innocuous media. Audio steganography is the practice of hiding the very existence of secret data by hiding it into another medium such as audio file. Its primary goal is to hide the fact that a communication is taking place between two parties. Modern techniques of steganography utilize the characteristics of digital media by using them as carriers or cover to hold hidden information. Digital stenography uses a host data or message known as a "Container" or "Carrier" to hide another data or message in it. In steganography technique the sender embeds secret data of any type which can be text, image or audio using a key in a digital cover file to produce a stego file, in such a way that the third parties cannot detect the existence of the hidden message. At the other end, the receiver processes the received stego-file to extract the hidden message. Cryptography's goal is to convert a message in such a way that it is difficult to understand the message directly. Steganography and Cryptography are very similar. As the need of security increases only Cryptography is not sufficient. So steganography is the supplementary to encryption. Both sciences can be combined to produce better protection of the message. In this case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques.

II. LITERATURE REVIEW

A. Background

Information security, sometimes shortened to InfoSec, is the technique of protecting information from unauthorized access, use, disruption, disclosure, modification, perusal, inspection, recording or destruction. The rapid e-communication over the internet has led to the use of three security techniques: cryptography, watermarking, and steganography. In cryptography the content of the messages are mangled. Cryptography can be of two types namely symmetric and asymmetric. Where same secret key is shared between sender and receiver in symmetric cryptography and asymmetric cryptography uses different secret keys for sender and receiver. In watermarking, data are hidden to convey some information such as ownership and copyright. Watermarking can be also of two types like visible and invisible water marking. Visible watermarking is related to the TV logo's or company logos whereas invisible water marking is concerned to authentication copyrighting of image.

Steganography is a practice of hiding of a secret message within another non-secret media so that the presence of the hidden message is undetectable. Based on the types of carrier used steganography can be text steganography, image steganography and audio steganography .Unlike cryptography the message is unaltered in steganography. Here the messages are hidden within a media in such a way so that none can understand the very existence of the message i.e. it cannot be perceived by human. Fig1 shows the tree structure of information security.

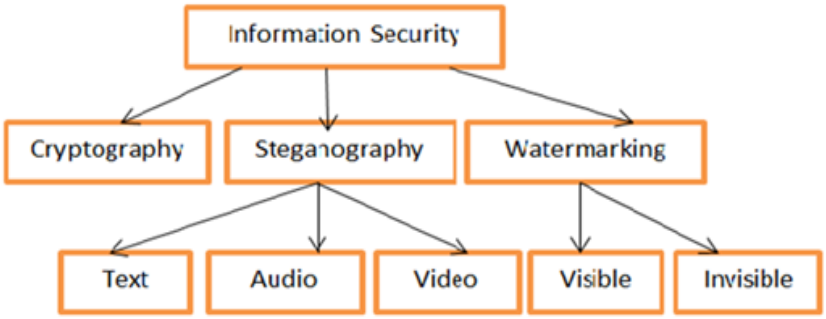

Fig. 1 Information Security

B. Motivation

The particular importance of concealing secret data in audio files results from the prevailing presence of audio signals as information vectors in our human society. It is commendable for steganography that the cover utilized to hide the secret data should not raise any suspicion to opponents. In fact, the popularity and the availability of audio files make them suitable to carry hidden information. The overall study shows that most steganalysis practices are more directed towards digital images leaving audio steganalysis relatively uninvestigated. Some advantages of audio steganography are as follows

- Audio based Steganography has the ability to store more information
- Slight changes in amplitude can store big amounts of information.
- Human hearing can be easily fooled.
- Audio files are generally bigger than images.

C. Overview of Audio Steganography Techniques

- Least Significant Bit Method
  This method is also known as low bit encoding method it is one of the earliest and standard methods used for information hiding. It consists in embedding each bit from the message in the least significant bit of the cover audio. Thus for 10 kbps data minimum of 10 KHz signals is required. This method increases imperceptibility but suffers from the low embedding capacity and low robustness.
- Parity Coding Method
  In this technique instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region.
- Echo Hiding Method
  In echo hiding method, data is embedded in a sound file by introducing an echo into the discrete signal. This technique provides the benefits of high transmission rates and high robustness than the other steganography methods. To hide the data successfully, three parameters of the echo are varied: Decay rate, amplitude and offset (delay time) from the original signal. All these parameters are set lower the human hearing threshold so the echo is not easily resolved which in turns gives high robustness benefit.
- Spread Spectrum Method
  Spread spectrum method distributes secret information across the audio signal's frequency spectrum as much as possible. This method spreads the secret data over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission.
- Phase Coding Method
  This method is based on replacing selected phase components from the original speech spectrum with hidden data. The main advantage of this method is that it is more robust against signal processing manipulation. Phase coding tolerates better signal distortion. Phase modifications are achieved using controlled phase alteration of the host audio.

D. Related Work

In literature many audio steganography methods are provided. The citations presented in this section primarily based on LSB embedding scheme where some of similar works are discussed. There are some advanced LSB methods where encrypted version of the text is embedded in to the cover file for providing better protection.

- In [1], Authors have proposed a new technique of audio steganography with enhanced security where each secret bit of information is inserted into the selected position of a cover audio media and selection is based on upper 3MSB bits of cover media. Additional security is provided using secret key which is known to sender and receiver only.
- In [2], A new method of audio steganography has been proposed by Mohsen Bazyar,Rubita Sudhirman to increase the capacity of data embedding of carrier audio. This method hides the information in variable and

multiple LSBs based on the MSBs of the samples of the carrier audio in comparison of standard LSB technique.2 MSBs of the samples of carrier audio file are checked in this method. The advantage of proposed method is that it has significant increase in carrier audio capacity for embedding additional information without having effects on the signal transparency of the host audio.

- In [3], A new method called "Robust Multi-Layer Audio Steganography" have been proposed by Biswajita Datta, Prithwish Pal and Samir Kumar Bandyopadhyay where LSB embedding is used in multiple layers and also capacity is increased by embedding two bits at a time. Here always two different pairs 01 and 11 are embedded instead of four, made using two bits at a time at the same time increases robustness more. Without knowing the bitwise operation applied here for extraction it is not also very much easy to get the actual data. After embedding flag setting and bit adjustment is done for maintaining the perceptual transparency of stego audio.
- In [4], Authors have proposed a robust audio steganography technique by utilizing the LSB method and Advanced Encryption Standards where robustness is enhanced by randomizing the embedding sequence as proposed and stego files are tested to check the quality of speech over 10 people and found results in either very good or excellent ratings.
- In [5], a new method of Using XORing of LSB's has been proposed by the authors. IN this method XOR operation is performed on the LSBs and then depending on the result of XOR operation and the message bit to be embedded, the LSB of the sample is modified or kept unchanged. From experimental analysis, it is seen that the proposed methods are effective as no difference is found between the original audio signal and the stego audio signal from the listening tests.
- In [6], a new Steganography method based on Genetic algorithms has been proposed by authors to solve the two problems of less robustness against attacks and less robustness against distortion. Authors have provided two solutions respective to the problems where solution to the first problem is provided by making more difficult discovering which bites are embedded by modifying the bits else than LSBs in samples, and selecting the samples to modify privately-not all samples and solution to the second problem is provided by Embedding the message bits in deeper layers and other bits alteration to decrease the amount of the error.
- In [7], authors have proposed a Variants of LSB technique of Audio steganography. The proposed algorithm is composed of two variants of LSB. The replacement of LSB is done at higher LSB layer i.e. 6th layer. The parity of samples of cover audio is checked along with secret message bit and accordingly LSB of sample is modified or unchanged. This method has various advantages like, LSB at higher layer makes it undetectable and unsuspicious secondly capacity has increased since data is hidden at 6th layer and finally Parity method provides efficiency to algorithm since it reduces distortion due to noise and difficult to detect hidden text.
- In [8], authors have proposed an efficient LSB based method which addresses the security issues of traditional LSB algorithms where LSB technique is used by embedding only at specified bit positions which is only known to the sender and receiver. The experimental results shown that the quality of the audio remains same after embedding the secret text and also very less difference between the original audio and steganography audio.

III. PROBLEM DEFINATION

In audio steganography the secret information is hidden in audio so that third person can't know something is hidden in audio file. Only sender and receiver know the decryption methods.

Problems with standard LSB technique of audio steganography is that although it provides the high imperceptibility it suffers from low embedding capacity and low robustness. In traditional LSB method as the no of bits to be embedded increases or number of LSB layers are increases to enhance the security it will reduces the tranceperancy of original signal and which will in turns reduces the robustness of the original audio signal.

IV. PROPOSED WORK

The contribution of this paper is to improve the performance by embedding two bits of secret message at the time on 0 to 7th LSB position based on the compliments of 3 MSBs of carrier audio .Here in the proposed work ,two algorithms have been proposed where in the first algorithm 2 data bits of secret message are embedded at a time on 0 to 7th LSB positions based on the 3 MSBs of carrier audio and in second algorithm those 2 data bits are embedded on 0 to 7th LSB positions based on the compliments of 3 MSBs of carrier audio. Therefore the proposed scheme provides the improved performance by embedding two bits rather than single bit and additional security is provided by using secret key.

A. Proposed Methodology

The steganography technique consists of two basic working modules called Embed and Extract which works as follows:

- Embed Module

  In this module, in first step an input audio file is selected. The selection is made through opening a new dialog box and the path selected is displayed through a text box. The second step is to select an output audio file in which text data or a text file is embedded. The third step is followed by choosing a text file or writing any text message for embedding. Fourth step is progress by selecting a key file. In the fifth step whatever the files that

we have selected are viewed and verification of the path is done. In the sixth step processed data is embedded into the audio file using proposed steganography technique. After embedding the content of both the audio files are played and a listener cannot find any difference between the original audio and stego audio.

- Extract Module

  This module is used to extract the text file from the cover audio file. This module is executed as follows. In first step an encrypted audio file is selected This is the file that a user has to extract information from the output audio. Second step is followed by selecting a new text file to display the embedded message. In proposed algorithm symmetric encryption method is used, so the key selected during the embedding process is used in decryption of the message also. All the steps which have done up till now are displayed using a list box and finally the embedded message can be viewed with the help of a file or in a text box. Finally the performance analysis is done in terms of Peak Signal to noise Ratio (PSNR), Means Square Error (MSE) and Hiding Rate.

B. Proposed Architecture

Architecture of proposed system composed of two blocks namely transmitter and receiver block.

- Transmitter Block

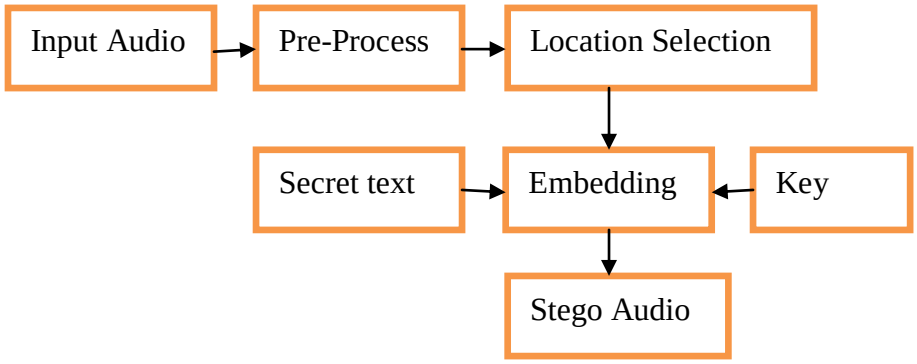

Fig. 2 Transmitter

In the transmitter section the input text file and input audio file are taken as input and then text file is then converted into their ASCII values after that the binary version of text file is taken for insertion into the carrier file and stego audio file is generated as output. Here first the audio file is divided into the samples and in each sample the secret data bits are embedded using proposed technique.

- Receiver Block

  On the Receiver side the reverse procedure is done with the help of the secret key and stego audio the secret data bits are retrieved.

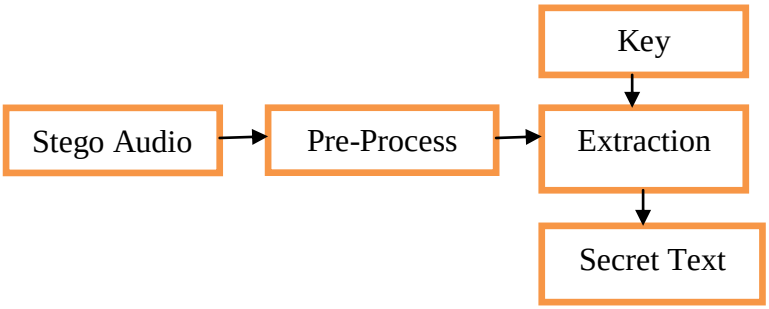

Fig. 3 Receiver

V. CONCLUSION

In this paper a new enhanced audio steganography technique based on LSB and location selection scheme has been presented. The proposed technique provides the advantage of embedding two bits at a time on compliment position of 3MSB's of cover audio samples and additional security is provided by using the secret key.

REFERENCES

[1] Shweta Vinayakarao Jadhav , A.M. Rawate,"A New Audio Steganoghraphy with Enhanced Security based on Location Selection Scheme",IJESC-2016.

[2] Mohsen Bazyar, Rubita Sudhirman, "A New Method to Increase the capacity of Audio Steganography Based on the LSB algorithm", Journal Teknologi Science and Engineering, 74:6 (2015), 49-53.

[3] Biswajita Datta, Prithwish Pal and Samir Kumar Bandyopadhyay, "Robust Multi-Layer Audio Steganography", IEEE-2015.

[4] Aniruddha Kanhe, G.Aghila,"Robust Audio Steganoghraphy based on Advanced Encryption Standards in Temporal Domain", IEEE-2015.

[5] H.B.Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale, Information Hiding in Audio Signals, International Journal of Computer Applications (0975 – 8887) Volume 7– No.9, October 2010.

[6] Mazdak Zamani, Azizah A. Manaf, Rabiah B. Ahmad, Akram M. Zeki, and Shahidan Abdullah, A Genetic-Algorithm-Based Approach for Audio Steganography World Academy of Science, Engineering and Technology 54 2009.

[7] Jyoti Bahl, Dr. R. Ramakishore," Audio Steganography using Parity Method at higher LSB layer as a variant of LSB Technique", IJIRCCE-Vol. 3, Issue 7, July 2015.

[8] P. Rameshkumar, M. Monisha and B. Santhi," Enhancement of Information Hiding in Audio Signals with Efficient LSB based Methods", Indian Journal of Science and Technology- Vol. 7(S4), 80–85, April 2014.

