A Survey on Audio Steganography with It's Techniques

Surbhi D. Tiwari[1], Prof. Krunal J. Panchal[2]

[1]*Research Scholar, Computer Engineering Department, L.J Institute of Engineering and Technology, Gujarat, India*
[2]*Assistant Professor, PG Department (Computer Engineering), L.J Institute of Engineering and Technology, Gujarat, India*

ABSTRACT

In the current internet scenario, secure data transmission is limited due to its attack, interception and manipulation by eavesdropper. So the attractive solution for this problem is steganography, which is the art and science of writing hidden messages in such a way that no one apart, from the sender and receiver suspects the existence of the hidden message. The primary goal of steganography is to provide confidentiality of information, where information can be hidden in carriers such as image, text, video and audio. Audio steganography hides the secret message in a cover audio signal in a completely undetectable manner. In this paper, we mainly discuss different types of audio steganography techniques, application, advantages and disadvantages.

Keyword: - *Steganography, Audio Steganography, Least Significant Bit*

1. INTRODUCTION

The rapid growth of digital communication emphasizes the need of secret communication. Data security is one of great concern due to the interception and manipulation by eavesdropper. So there are two common approaches use to ensure information secrecy: Cryptography and Steganography [8]. Cryptography is a method for storing and transmitting data in an encrypted form so that only intended users have access. It is often done by scrambling the plaintext into the ciphertext using an encryption process and decrypt using a decryption process.

The word steganography comes from two greek words "stegano" and "graphy". Stegano means secret and graphy means writing. So steganography literally means secret writing. Steganography is the art and science of covered writing and its aims to secure communication in a completely undetectable manner [8]. It means concealing data into text message, image, audio and video in such a way that other cannot detect the presence of hidden information.

1.1 Audio Steganography:

Audio Steganography is the type of steganography, where we can embed the secret message into digital sound. It is more complex process as compared to embedding messages in other media like video and image due to the characteristics of Human Auditory System(HAS) any slight change in the audio can easily detected by the human ears. This steganography method can embed messages in WAV, AU and even MP3 sound files [10].

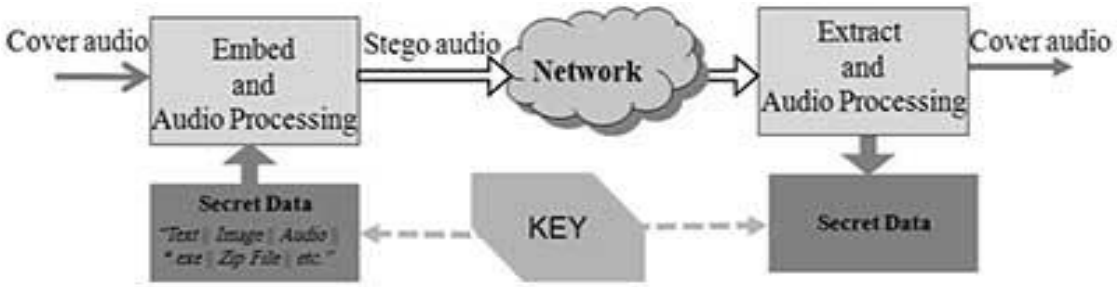

Fig -1: Basic Diagram of Audio Steganography [11]

Audio Steganographic techniques must be satisfied by three conditions [8]:
Capacity: It means the amount of secret information that can be embedded within the host audio without affecting the perceptual quality of audio.
Transparency: It evaluates how well a secret message is embedded in the cover audio. The difference between audio after hiding and audio before hiding should remain negligible.
Robustness: It indicates the ability of secret message to withstand against attacks.

1.2 Merits and applications:

- **Merits:** Potential to conceal more information and has an ability to combine with existing cryptographic technologies. Flexibility of audio stegnography is very powerful and greater amount of information can be embedding without any audible degradation.
- **Applications of audio steganography:** It is used to improve the quality of telephone speech, Used in navigation system where acoustic data are embedded in background music to indicate the location of receiver, used in data storage (means it could be seen in subtitled movies. Actors speech, film, music, background sounds could be used to embed the text needed for translation), For Protection of copyrighted digital media (CD or in music) and government information system security, Used in military system and satellite communications for transferring sensitive data and also used in forensic application [4].

2. AUDIO STEGANOGRAPHY TECHNIQUES:

There are two types of audio steganography techniques 1) Spatial domain and 2) Temporal domain

2.1 Spatial Domain Audio Steganography
These methods hide information on the basis of geometric characteristics of audio signal. Least Significant Bit and Echo Hiding methods are fall in category of spatial domain.

1. Least Significant Bit
Also known as a Low Bit Encoding. It is simplest audio steganography techniques providing high capacity. This technique based on embedding each bit from the message in the least significant bit of the cover audio in a deterministic way. As for example, let us consider we want to hide the letter "a" (ASCII code of 'a' is 97, which is 01100001 in binary) inside 16 bit CD quality sample. First the secret message 'a' and the audio file are converted into bit stream. The least significant column of the audio file is replaced by the bit stream of secret information 'a'. The resulting file after embedding secret information 'a' is called stego-file [5, 4].

2. Echo Hiding
Echo hiding used to embeds secret data into audio signals by introducing a short echo to the host signal. It provides a high transmission rate and excellent robustness but low embedding rate and security. Since only one bit of information can be stored is an echo, the original signal is broken down into blocks to produce numerous echos and later joined back to the original signal. One offset value represents a binary one and second offset value represents a binary zero. If only one echo was produced from the original audio, only one bit of message could be encoded. The original signal is broken down into blocks. Once the encoding process is done, the blocks are concatenated back together to create final signal [9, 5].

2.2 Transform Domain Audio Steganography
These methods hide information along the frequency distribution of the carrier signal. Various methods of transform domain are used for hiding data.

1. Spread Spectrum
In spread spectrum technique, spreads the secret information over the frequency spectrum of the audio signal using a code which is independent of the audio sample. This technique produces redundant copies of the data signal. Actually, multiple copies of data are produced using M sequence code which is known to both sender as well as receiver. Once multiple copies are produced they are embedded in audio carrier. Hence, if some values get corrupted, there will still be copies of the values which would be used to recover the hidden information [9, 5].

2. Phase coding
In this method, the initial phase of the audio segment is replaced with the reference phase of the secret message. The subsequent segment's phases are altered in accordance. Phase shifts between adjacent segments can be easily

detected. Hence the relative phase difference between them must be maintained. During extraction of the message, the receiver uses the length of the segment to get the output. Phase Coding is based on the fact that phase components of sound are not as perceptible to human ear as noise is. The disadvantage of phase coding is low transmission rate because the secret message is embedded only in the first signal segment. This technique encodes the secret message as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio [9, 5].

3. Discrete Wavelet Transform

Wavelet usually refers to small waves. The technique is used to hide data in transform coefficients of the audio signal. It is actually decomposed with different resolutions sub-bands so as to find the most suitable sub-band for embedding bits of secret message. It provides with a high embedding rate but a possibility of inaccuracy in recovering the hidden data [9, 5].

4. Tone insertion

This technique makes use of auditory masking. Psycho acoustical or auditory masking is actually the characteristic of human auditory system HAS where the presence of stronger tone renders the weaker tone in its spectral domain. The masked sound becomes inaudible in presence of another louder sound. However, the masked signal is still present. This method is strong in terms of low- pass filtering and bit truncation attacks but it offers low embedding capacity and security [9, 5].

3. Related Works:

3.1 LSB Based Audio Steganography Based on Text Compression

Authors [1] have proposed a new dictionary based text compression technique for ASCII texts for the purpose of obtaining good performance on various document sizes. In order to increase the secrecy of the text message compressed by dictionary based compression, it is hidden in the audio file. If the text message is hidden using stenographic system, it may be detected by attackers. To avoid this, the input message may be converted into highly redundant code and then hidden .This method will help maintain secrecy. This approach achieves better value of signal to noise ratio.

3.2 Highly Secure DNA- based Audio Steganography

Authors [2] have proposed an approach uses a three leveled security. The three levels are Encryption, DNA steganography and audio steganography. For encrypting the text file the proposed method uses a DNA based playfair encryption algorithm. In the second level, the encrypted secret file is hidden in a randomly generated DNA sequence. In the third level the DNA sequence which is embedded with encrypted file is hidden inside an audio file using least significant bit modification technique. The main objective of this paper is to come up with an efficient method to preserve security of secret messages in a text file against unauthorized access by hiding the presence of text file.

3.3 A New Audio Steganography Scheme Based on Location Selection with Enhanced Security

Authors [3] proposed a new scheme for audio steganography is presented where the bits of a secret message are embedded into the coefficients of a cover audio. Each secret bit is embedded into the selected position of a cover coefficient. The position for insertion of a secret bit is selected from the 0th (Least Significant Bit) to 7th LSB based on the upper three MSB (Most Significant Bit). This scheme provides high audio quality, robustness and lossless recovery from the cover audio.

3.4 An approach for enhancing the message security in Audio Steganography

In this paper [4] author proposed a method that uses parity of audio sample to choose whether message bit is embedded in right or left channel of audio signal. Along with this 4 bit stego-key is used for each 16 bit sample. Decimal value of stego-key represents a bit in audio sample. XOR operation is performed between stego-key value and message bit. Modification of LSB depends on the result of XOR operation. This method provides robustness but requires 4 bit key for each sample requires large amount of space.

3.5 Multi Agent Based Audio Steganography

In this paper [6] author present a trusted communication platform for multi-agents that are able to hide the confidential message in the cover audio stream according to the user request and retrieve the hidden information

from the stego audio file. This system provides high availability and flexibility in this context and a more feasible way to trust the message transmission. This paper works on two parameters PSNR (peak signal to noise ratio) and MSE (mean square error).

3.6 A Proposed Implementation Method of an Audio Steganography Technique

In this paper [7] author present an implementation of an audio steganography using two cards of arduino due applying successfully the Least Significant Bit (LSB) technique on a pure communication channel. The proposed method is applied to various audio files such as speech and music envelope signals. These audio files were used as covers and secret messages and it all giving remarkable results on steganography concept. This paper works on two parameters PSNR (peak signal to noise ratio) and MSE (mean square error).

4. COMPARATIVE TABLE

Table -1: Comparative Table

Sr. No	Paper Title	Techniques	Advantages	Disadvantages
1	LSB Based Audio SteganographyBased on Text Compression	Dictionary Based Encoding (DBE) approach using LSB insertion method	Maintain secrecy and achieves good compression ratio, reduces bits per character	Size of input text
2	Highly Secure DNA- based Audio Steganography	Single level encryption and two level of steganography	Not attract with unwanted attention , better security	Low embedded rate
3	A New Audio Steganography Scheme Based on Location Selection with Enhanced Security	Standard Encryption algorithm using LSB method	Insertion position is totally unknown	Large size of audio signal
4	An approach for enhancing the message security in Audio Steganography	Stego-key and parity concept based LSB method	Increase robustness	Addition of noise
5	Multi Agent Based Audio Steganography	Encryption and decryption technique using random key (LSB method)	1) Robustness 2) provide secure communication between selected agents	Optimal message size
6	A Proposed Implementation Method of an Audio Steganography Technique	Using Cards of arduino applying Successfully the LSB technique	Quality of sound	Noisy communication channel

5. CONCLUSIONS

The steganography is one of the safe ways of secret data transmissions in today's digital world. In this paper we surveyed various types of audio steganography techniques with their own advantages and disadvantages. From our point of view, various audio steganography techniques expand application possibilities and its requirement to provide hiding capacity, high level of data security, data embedding rate, data extraction rate and various others factors.

6. ACKNOWLEDGEMENT

The authors are very much grateful to Department of Computer Engineering, L.J Institute of Engineering & Technology, Ahmedabad, from Gujarat Technological University; for giving opportunity to do research work in Audio Steganography. Two authors Surbhi Tiwari and Prof. Krunal J. Panchal are also grateful to management team of L.J Institute of Engineering & Technology, Ahmedabad, from Gujarat Technological University; for giving constant encouragement to do research work in the Department.

7. REFERENCES

[1]. M.Baritha Beguma, Y.Venkataramanib "LSB Based Audio Steganography Based on Text Compression" Science direct International Conference on Communication Technology and System Design, March 2012, doi:10.1016/j.proeng.2012.01.917, pp. 703-710.

[2]. Shyamasree CM, Sheena Anees "Highly secure DNA- based Audio Steganography" IEEE International Conference on Recent Trends in Information Technology (ICRTIT), July 2013, DOI-10.1109/ICRTIT.2013.6844257 , pp. 519-524.

[3]. Pratik Pathak, Arup Kr. Chattopadhyay, Amitava Nag "A New Audio Steganography Scheme based on Location Selection with Enhanced Security" IEEE International Conference on Automation, Control, Energy and Systems(ACES), Feb 2014 , DOI: 10.1109/ACES.2014.6807979, pp. 1- 4.

[4]. Ashis Kumar Mandal, Mohammed Kaosar, Md. Olioul Islam, Md. Delowar Hossain "An Approach for Enhancing Message Security in Audio Steganography" IEEE International Conference Computer and Information Technology, March 2014, ISBN - 978-1-4799-3497-3/13, pp. 383- 388.

[5]. Ifra Bilal, Mahendra Singh Roj, Rajiv Kumar and P K Mishra, "Recent Advancement in Audio Steganography" IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Dec 2014, pp. 402-405

[6]. T. Kartheeswaran, V.Senthooran, T D D L Pemadasa "Multi Agent Based Audio Steganography" IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Dec 2015, ISBN - 978-1-4799-7849-6/15, pp. 1- 4.

[7]. Mazhar Tayel, Ahmed Gamal, Hamed Shawky "A Proposed Implementation Method of an Audio Steganography Technique" IEEE International Conference on Advanced Communication Technology (ICACT), Feb 2016, ISBN - 978-89-968650-6-3, pp. 180 - 184.

[8]. Jithu Vimal , Ann Mary Alex "Audio Steganography Using Dual Randomness LSB method" IEEE International Conference on Control, Instrumentation Communication and Computational Technologies(ICCCICCT), July 2014, ISBN - 978-1-4799-4190-2/14 , pp. 941 - 944.

[9]. Namrata Singh "A Survey Paper on Audio Steganography and its Applications" International journal of Innovative Research in Science, Engineering and Technology, Feb 2017, DOI: 10.15680/IJIRSET.2017.0602120, pp. 2648- 2656.

[10]. Navneet Kaur, Sunny Behal "Audio Steganography Techniques- A Survey" International Journal of Engineering Research and Applications, June 2014, ISBN – 2248- 9622, pp. 90- 100.

[11]. https: // encrypted-tbn2.gstatic.com/ images? q=tbn: ANd9GcQ4vNaFmQDIfF6YEAvXxFypn2fv17vCZ83H-2fdmOh5-GN9qy, time – 00:12.

[12]. https: //en.m.wikipedia.org/wiki/steganography, time – 00:12.