International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), Nov 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

A Review on various Techniques for Audio Steganography

Kirandeep Kaur[1],Vijay Laxmi[2]

[1]*M.Phil Scholar Guru Kashi University, Talwandi Sabo, (India)*

[2]*Professor in Computer Application, Guru Kashi University, Talwandi Sabo, (India)*

ABSTRACT

Steganography is process to hide the secret data within a cover media such as digital images, sound files, video files in such a way that the existence of the message could not be noticeable. Audio steganography is a process to hide the secret data such as text or images in the audio signals. In this paper we gives a review on various techniques for audio steganography. The main challenge in audio steganography is to increase the capacity of steganographic system and to hide the data in such a way that nobody can extract the secret data from the audio signal.

Keywords—Steganography; Audio steganography techniques; data hiding

I. INTRODUCTION

Steganography is the art and science of covered writing (hide in plain sight) and its techniques are in use from hundreds of years. Digital Steganography is the technique of securing digitized data by hiding it into another piece of data. Today, in digital age the easy access to any form of data such as audio, videos, images and text make it vulnerable to many threats [1]. The data can be copied for purpose of copyright violation, tampered with or illegally accessed without the knowledge of owner. Therefore, the need of hiding secret identification inside different types of digital data is required such that owner can prove copyright ownership; identify attempts to tamper with sensitive data and to embed annotations. The main task of the field of steganography is the storing, hiding, and embedding of secret data in all types of digital data. The main goal of steganography is to communicate securely in a completely undetectable manner [2] such that no one can suspect that it exist some secret information. Unlike cryptography, which secures data by transforming it into another unreadable format, steganography makes data invisible by hiding (or embedding) them in another piece of data [3]. Thus cryptography is science of overt secret writing while steganography as covert secret writing. The cover, host or the carrier is the target media in which information is hidden so that other person will not notice the presence of the information. The modified cover, including the hidden data, is referred to as a stego-object which can be stored or transmitted as a message [4]. The secret information can be embedded in various types of cover. If information is embedded in cover text file, the result is stego-text object. It is possible to have cover audio, video and image for embedding which result in stego-audio, stego-video, stego- image Nowadays, the combinations of steganography and cryptography methods are also used to ensure data confidentiality [5] and to improve the information security.

II. AUDIO STEGANOGRAPHY

In this type of steganography we can embed secret messages into digital sound in audio steganography. It is more complex process as compare to embedding messages in other media. This steganography method can embed messages in WAV, AU And even MP3 sound files [6]. The audio steganography consists of Carrier or Audio file, Message and Password. Carrier is also known as a cover-file, which conceals the secret information. In steganography model the secret message that the sender sends wants to remain it secret. Message can be of any type may be text, image, audio or any type of file, in secret stego key which only the receiver knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file.

III. LITERATURE SURVEY

Prashant Johri[1] ,In this paper authors are considering audio file as cover media and text message as secret information. The secret information is embedded in a cover media as noise as the HAS cannot detect the sound less than 20Hz or greater than 20000Hz. Generally LSB algorithm is used to embed the secret information within a cover media. Here authors are using genetic programming to increase the robustness of the data so that the secret data could not be noticeable as far as possible. In the proposed approach the secret message is inserted in the audio file in the form of noise and GA is basically used for optimization purpose. So GA may be a successful approach to decrease the dissimilarity between the original cover file and stego file.

Yugeshwari Kakde [2], In this paper authors are working on audio-video steganography which is the combination of Audio

steganography and Image steganography, in this authors are using computer forensics technique for authentication purpose. In this paper the aim is to hide secret information behind audio

and image of video file. video is the combination of many still frames of images and audio. System can select any frame of video and audio for hiding our secret data. This paper proposed an algorithm for hiding image in selected video sequence is an image-hiding technique based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) and random LSB (Least Significant Bit) audio steganography method for hiding secret text information inside audio of the audio-video file, it reduce embedding distortion of the host audio. This paper focuses the idea of computer forensics technique which is use as a tool for authentication and data security purpose and its use in video steganography in security manner.

Neha Gupta[3], In this paper author specify that Steganography is a fascinating and effective method of hiding data that has been used throughout history. Methods that can be employed to uncover such devious tactics, but the first step

are awareness that such methods even exist. There are many good reasons as well to use this type of data hiding, including

watermarking or a more secure central storage method for such things as passwords, or key processes. Regardless, the technology is easy to use and difficult to detect. Researchers and scientists have made a lot of research work to solve this problem and to find an effective method for image hiding . The proposed system aims to provide improved robustness, security by using the concept of DWT (Discrete Wavelet Transform) and

LSB (Least Significant Bit) proposed a new method of Audio Steganography. The emphasize will be on the proposed scheme of image hiding in audio and its comparison with simple Least Significant Bit insertion method for data hiding in audio.

Harish Kumar[4], The idea of this paper is to invent a new strategy in Steganography to get the minimum effect in audio which is used to hide data into it . "Progress always involves risk" Fredrick Wilcox observed that technological progress of computer science and the Internet altered the way we lived, and will continue to cast our Iife. In this paper authors have presented a Steganography method of embedding text data in an audio file. The basic approach behind this paper is to provide a good, well-organized method for hiding the data and sent to the destination in safer manner. In the proposed technique fIrst the audio file is sampled and then appropriate bit is modified . In selected sample one bit is modified at least significant bit .The remaining bits may be used but it may be cause noise. Authors have attempted to provide an overview, theoretical framework about audio Steganography techniques and a novel approach to hide data in an audio using least significant bit (LSB).

Fatiha Djebbar[5], In this paper a novel and versatile audio steganographic methods have been proposed. A perfect audio Steganographic technique aim at embedding data in an imperceptible, robust and secure way and then extracting it by authorized people. Hence, up to date the main challenge in digital audio steganography is to obtain robust high capacity steganographic systems. Leaning towards designing a system that ensures high capacity or robustness and security of embedded data has led to great diversity in the existing steganographic techniques. In this paper, we present a current state of art literature in digital audio steganographic techniques.Authors explore their potentials and limitations to ensure secure communication. A comparison and an evaluation for the reviewed techniques is also presented in this paper.

Ms. Manisha[6],In this paper, authors have presented different types of steganography techniques. The different categories of steganography have been discussed in brief and main focus is put on audio steganography technique. Initially, we have surveyed about text steganography and then move to another steganography technique i.e. image steganographyand its techniques are discussed in brief. During image steganography, Least Significant Bits, Masking and filtering and Transformations will be subjected. Finally, audio steganography which contains LSB Coding, Phase Coding, Spread Spectrum and Echo Hiding techniques is described.

IV. DRAWBACKS OF THE EXISTING TECHNIQUES

Now days, multiple techniques of steganography are present but are in scattered format. For example text to audio steganography, image to audio steganography, audio to audio steganography. Maximum audio steganographic algorithms basically work with LSB insertion method. But these techniques are having many drawbacks as specified below:

- These systems are less secure as Algorithms used in LSB insertion method are easily decryptable.
- Steganographic systems may suffer from vulnerability attacks.
- LSB insertion method adds the noise to cover data.
- Sometimes the audio file may get corrupted.
- At a time only one technique can be used i.e. either text to audio or image to audio or audio to audio steganography.

V. PROPERTIES OF AUDIO STEGNIGRAPHY TECHNIQUES

A. *Secrecy*

No one should be able to extract message from the host medium without the knowledge of the proper secret key used in the extraction procedure.

B. Imperceptibility

The stego file should be indiscernible from the original cover file. One should not become suspicious of the existence of the secret message within the cover file.

C. High capacity

The maximum length of the secret message that can be embedded in a cover file without affecting its quality as much as possible.

D. Resistance

The secret message should be able to survive when the host medium is manipulated, e.g. Lossy compression scheme.

E. Accurate extraction

When the secret message extracted at intended receiver side the secret message should be accurate and reliable.

VI. APPLICATIONS OF AUDIO STEGNOGRAPHY

Audio steganography is use in wide range of applications.

Few applications are discussed below:

F. Secret Communication

To maintain patient's medical records secrecy, proposed multilevel-access control audio steganography system to telemedicine users for secure transmission of medical images. The system embeds medical images in audio files which is send to different recipients such as doctors' in-charge of the corresponding patient. For more security, only intended recipients having the knowledge of a key will be able to extract the medical images.

G. Data Storage

Audio Steganography could be used in subtitled movies where actors' speech, film music, background sounds could be used to embed the text needed for translation

VII. TYPES OF AUDIO STEGNOGRAPHY TECHNIQUES

H. Insertion-Based

In this type we can store the information that we want to hide in those sections of a file which are ignored by processing application. Due to this we avoid modifying those file bits that are relevant to an end-user. For example, with some files there is an EOF or end-of-file marker. This flag signifies to the application that is reading the file that it has reached the end of the file and the application can stop processing the file. Hidden information can then be inserted after the EOF marker. The end-user may not even realize that the file contains additional hidden information. We can use a injection method which changes file size with amount of data hidden in file and if the file size large, it may arouse suspicion.

I. Substitution-Based

In substitution we can replace the least significant bits of data that makes the meaningful content of the cover file with new information which makes the less amount of distortion. In this the cover file size does not change after the execution of the algorithm. Limited amount of data we can hide with this approach as there is a limited amount of insignificant data in any given file.

J. Generation-Based

In insertion and substitution, this type does not require any existing cover file. In this it generates a cover file for the sole purpose of hiding the message. The main drawback of the insertion and substitution is the comparison of the stego file with any pre-existing copy of the cover file (which is supposed to be the same file) and find differences between the both. You won't have that problem when using a generation approach, in this the result is an original cover file and is immune to comparison tests.

VIII. EXISTING TECHNIQUES FOR AUDIO STEGNOGRAPHY

The following are some of the techniques for audio steganography:

K. Echo Hiding

Echo hiding used to embeds secret data in a audio file by pass an echo into the discrete signal. This technique has advantages of providing a high data transmission rate and robustness when we make comparison of echo hiding to other methods. One bit of secret data could be encoded if one echo was produced from the original signal; before the encoding process starts the original signal is broken down into blocks. Once the encoding process is done, the blocks are concatenated back together to create the final signal.

L. Phase Coding

Phase coding exploits HAS insensitivity to relative phase of different spectral components. In this method we can replace selected phase components from the original sound signal spectrum with hidden information .due to in audibility of information, phase components medication should be kept small. It is very effective coding methods in terms of the SNR ratio. When the phase relation between each frequency component is changed, phase dispersion will occur. The modification of the phase is sufficiently small (sufficiently small depends on the observer; professionals in broadcast radio can detect modifications that are unperceivable to an average observer), an inaudible coding can be achieved.

M. Parity Coding

This technique is one of the robust audio steganographic techniques. Instead of breaking a signal into individual samples, it breaks a signal into separate samples sections and embeds each bit of the secret message information from a parity bit. If the of a selected parity bit region does not match the secret message bit to be encoded, the process inverts the LSB of one of the section in the region. Then the sender has many choices for encoding the secret bit.

N. Spread Spectrum

In this technique spread out the encoded information across the available frequencies. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. This method spreads the secret data over the audio file frequency spectrum which using a code that is

independent of the original signal. The final signal occupies a bandwidth in excess of what is actually required for transmission at end. The sampling is used in chip rate for the sound signal communication. This method is the most secure way to send hidden secret messages in sound, but it can introduce random noise to the audio which prevents the problem of data loss

Advantage: It maintains a high level of robustness.

Disadvantage: Quality of file is being effected due to presence of noise in audio file.

O. Tone insertion

Tone insertion used on the inaudibility of lower power tones in the presence of significantly higher ones. This method used resist to attacks such as low-pass filtering and bit truncation. In cyba addition to less embedding capacity, embedded information could be maliciously extracted when inserted.

P. LSB (Least Significant Bit)

In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In LSB coding, two least significant bits of a data is replaced with two message bits. If we increase the amount of information encoded will also increase the noise in the sound file. Like, a sound file that was recorded in a bustling subway station would mask low-bit encoding noise.In secret message extraction from an LSB encoded audio file, the recipient needs access to the sequence of sample indices used in the embedding process. The length of the secret message to be encoded is smaller than the total number of section in audio file. We also know about how to choose the subset of samples which contain the secret message or information and communicate that decision to the recipient. One trivial it is to start at the beginning of the audio file and perform LSB coding upto message completely embedded, leaving the remaining sections unchanged. But it creates a problem like in the first part of the audio file will have different statistical properties than the second part of the audio file which was not modified. Solution to this problem is to pad the secret message with random bits so that the length of the message is equal to the total number of samples. LSB (Least Significant Bit), this method is one of the important and easiest methods used for data hiding [11]. Traditionally, it is based on embedding each bit from the message in the least significant bit of the cover audio in a deterministic way The LSB method allows more embedding capacity for information and easy to implement or to combine with other hiding methods. It characterizes by less robustness to noise addition which reduces its security performance since it becomes vulnerable even to simple attacks.

IX. CONCLUSION

This paper provides literature review on Audio steganography techniques. As steganography becomes widely used in computing, there are some issues are there that need to be resolved. There is a large variety of different techniques with their own advantages and disadvantages. We surveyed various types of audio steganography in this paper. It is concluded that a more robust audio steganography technique is required to hide the secret data into audio signals.

REFERENCES

[1] Prashant Johri, Arun Kumar, Amba,"Review Paper On Text And Audio Steganography Using GA", International Conference on Computing, Communication and Automation (ICCCA2015)

[2] Yugeshwari Kakde, Priyanka Gonnade, Prashant Dahiwale, "Audio-Video steganography", IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15

[3] Neha Gupta, Ms. Nidhi Sharma, "Dwt and Lsb Based Audio Steganography", 2014 International Conference on Reliability, Optimization and Information Technology - ICROIT 2014, India, Feb 6-8 2014

[4] Harish Kumar, Anuradha, "Enhanced LSB technique for Audio Steganography", IEEE-20180

[5] Fatiha Djebbar, Beghdad Ayady, Habib Hamamzand Karim Abed-Meraim , "A view on latest audio steganography techniques", 2011

[6] Ms. Manisha, Ms. Maneela,"A Survey on Various Methods of Audio Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, May 2014G. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (*references*)

[7] Ruby Garg,Vijay Laxmi,"A REVIEW ON VARIOUS AUDIO STEGANOGRAPHY TECHNIQUES FOR AUDIO SIGNAL",International journal of engineering sciences and research technology, oct.2016

[8] Sara Khosravi, MashallahAbbasiDezfoli, Mohammad HosseinYektaie, " A new steganography method based HIOP (Higher Intensity Of Pixel)algorithm and Strassen's matrix multiplication" , Journal of Global Research in Computer Science, Vol. 2, No. 1, 2011.

[9] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA,2000.

[10] ShashikalaChannalli et al ," Steganography An Art of Hiding Data ",International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.

[11] Gruhl D, Lu A, Bender W. Echo hiding. Lecture Notes inComputer Science, 1996, 1174: 295-315.

[12] Xu Chansheng, Wu Jiankang, Sun Quibin, et al. Applications of digital watermarking technology in audio signals. Journal of Audio Engineering Society, 1999, 47(10): 805-812.

[13] Garcia R A. Digital watermarking of audio signals using a psychoacoustic auditory model and spread spectrum theory. In: 107th AES Convention. New York, USA, 1999:2713-2720.

[14] XU Shuzheng, ZHANG Peng, WANG Pengjun, YANG Huazhong, "Performance Analysis of Data Hiding in MPEG-4 AAC Audio" TSINGHUA SCIENCE AND TECHNOLOGY Volume 14, Number 1, February 2009..