ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

An Analysis of Various Techniques in Audio Steganography

B.Ramapriya[1], K.Bhuvanasundari[2], D.Bharathi[3]

Assistant Professor, Dept. of Computer Science, Sri Akilandeswari Women's College, Wandiwash, Tamil Nadu, India[1]

PG Student, Dept. of Computer Science, Sri Akilandeswari Women's College, Wandiwash, Tamil Nadu, India[2]

PG Student, Dept. of Computer Science, Sri Akilandeswari Women's College, Wandiwash, Tamil Nadu, India[3]

ABSTRACT: Nowadays large requirement of internet applications needed a data to be transmitted in a protected manner. Data communication in public system is not safe because of interception and improper manipulation. We can converse with each other by sharing messages which is not safe, but we make a communication by embedding the message into carrier or by special tools such as invisible ink, microdots etc. In digital era, new techniques of trouncing the data inside the carrier are invented which are known as digital Steganography. Which is the art and science of writing hidden messages in such a way that no one, apart from the sender and intend recipient, suspects the existence of the message The message can be an image, audio, video or a text file. Audio Steganography is the scheme of hiding the survival of covert information by concealing it into another medium. In this paper we mainly discuss different types of audio steganographic methods enhance the security level in audio Steganography.

KEYWORDS: Cryptography, Audio Steganography**,** Echo Hiding, Phase Coding, Parity Coding, Spread Spectrum, LSB

I. INTRODUCTION

Steganography is the art and science of covered writing of digital documents. Digital Steganography is the technique of securing data by hiding it into another piece of data. The trouble-free access of data such as audio, videos, images and text make it exposed to many threats [1]. In cryptography, the arrangement of a message is worthless unless the decryption key is available. It makes no attempt to mask the message. It offers the ability of transmitting information between people in a way that prevents a third party from understanding it. Cryptography can also provide validation for verifying the uniqueness of someone [2].In Steganography does not alter the secret message, but hides it inside a cover image so that it cannot visible. A communication in a cipher text which might stimulate doubt on the part of the recipient while an unseen message formed with steganographic methods will not. The data may be copied for purpose of copyright violation, illicitly accessed without the acquaintance of holder. Therefore, the want of hiding secret recognition inside different types of digital data is required such that owner can prove copyright ownership. The main task of Steganography is to communicate secretly in an undetectable manner [3].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

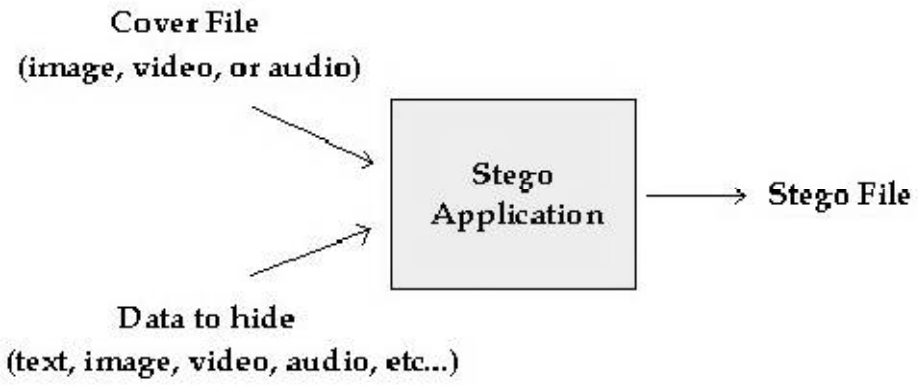

Fig.1 Stego-file of Audio cover file

Thus cryptography is science of explicit secret writing while Steganography as hidden secret writing. The cover is the target media in which information is hidden. The personalized cover which includes the hidden data is referred to as a *stego-object* [4]. The secret information can be embedded in different types of cover. If message is entrenched in cover text file then the result is stego-text object. The Steganography application hides different types of data within a cover file. The resulting stego also contains hidden message. Steganography essentially does is exploit human perception. Human senses are not educated to look for files that have information hidden inside of them; although we have many programs available are called Steganalysis. It is possible to have cover audio, video and image. The combinations of Steganography and Cryptography techniques are used to ensure data secrecy [5].

II. AUDIO STEGANOGRAPHY

Steganography is the art and science of hitting secret information in a cover file such that only sender and receiver can sense the survival of the secret information [3]. Surreptitious information is encoded in a manner such that the very existence of the information is concealed. The main goal of Steganography is to communicate steadily in an absolutely untraceable manner [4]. If a Steganography method causes someone to imagine there is undisclosed information in a carrier medium, then the method has unsuccessful [6, 8]. In this type of Steganography we can embed covert messages into digital sound in audio Steganography. It is more composite process as compare to embedding messages in other media. This Steganography method can embed messages in WAV, AU And even MP3 resonance files [9]. 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 subsequent 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 [10].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

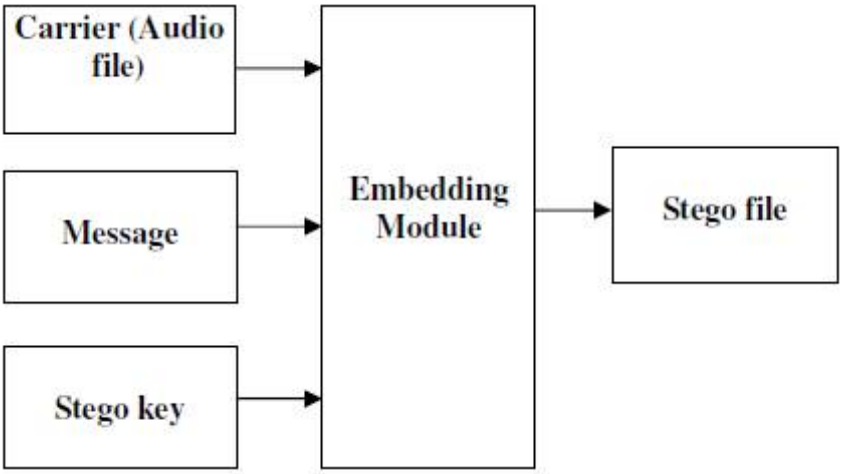

Figure 2: Audio Steganographic Model

Covering process is consists of two steps [8].In first, the Identification of superfluous bits in a cover- file. Redundant bits are those bit that can be modified without corrupting the quality of the cover-file. In second step wrapping the secret information in the cover file, the redundant bits in the cover file is replaced by the bits of the secret data. We can modify audio files in such a way that they contain secreted data. Similar to copyrighted data, we can modify data in such a way that it doesn't destroy the signal. In audio Steganography we can hide data in audio files with the help of Human Auditory System (HAS). The HAS perceives the additive random noise and the perturbations in an audio file can also be detected. But there are some holes. The digital sound is obtained from by converting it to digital domain. The renowned file formats of sounds are the Windows Audio-Visual (WAV) and the Audio Interchange File Format (AIFF). While implementing this process, we can first check environments of the sound signal will travel between encoding and decoding. In storage environment or digital signal, other is transmission path of the signal may travel [11][12]. After secret messages hide successfully some methods are used for embedding data in digital audio.

III. AUDIO STEGANOGRAPHIC METHODS

There have been many techniques for hiding information or messages in audio in such a manner,
That the modification made to the audio file is perceptually not dissemble.

A. LSB coding

The LSB (Least Significant Bit) algorithm, which replaces the least significant bit in some bytes of the cover file to cover a series of bytes containing the hidden data. That's usually a valuable technique. The LSB substitution doesn't cause significant quality degradation, such as in 24-bit bitmaps. In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the principle in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) location.

For example, to hide the letter "b" (ASCII code 98, which is 01100010) inside eight bytes of a cover, you can set the LSB of each byte like this:
1001001**0**
0101001**1**
1001101**1**

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

11010010
10001010
00000010
01110011
00101010
Using this technique, you hide a byte every eight bytes of the cover. Note that there's a fifty percent chance that the bit you're replacing is the same as its replacement,

B. Parity Coding

Parity coding is one of the robust audio steganographic techniques. This method breaks a signal into separate samples and embeds each bit of the secret message from a parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process inverts the LSB of one of the samples in the region. Therefore, the sender has more of an option in encoding the surreptitious bit.

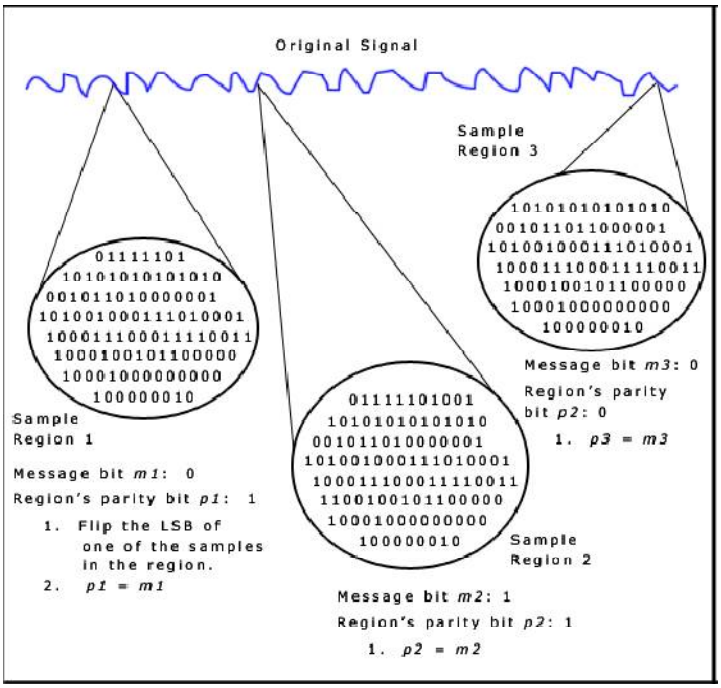

Fig.3 Parity coding procedure.

C. Phase Coding

The phase coding technique works by replacing the phase of an initial audio segment with a reference phase that represents the secret information. The remaining segments phase is adjusted in order to preserve the relative phase between segments.

Phase coding is explained in the following procedure:
a. Divide an original sound signal into smaller segments such that lengths are of the same size as the size of the message to be encoded.
b. Matrix of the phases is created by applying Discrete Fourier Transform (DFT).
c. Calculate the Phase differences between adjacent segments.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

d. Phase shifts between adjacent segments are easily measurable. It means, we can change the absolute phases of the segments but the relative phase differences between adjacent segments must be preserved.
e. Using the new phase of the first segment a new phase matrix is created and the original phase differences.
f. The sound signal is reconstructed by applying the inverse Discrete Fourier Transform using the new phase matrix and then original matrix is obtained by concatenating the sound segments back together.

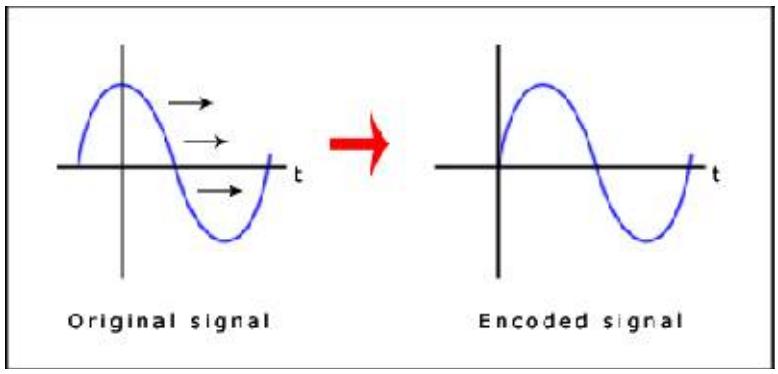

Fig. 4 Phase coding

D. Spread Spectrum

The basic spread spectrum (SS) method attempts to stretch secret information across the frequency spectrum of the audio signal. The Spread Spectrum method spreads the secret information over the frequency spectrum of the sound file using a code which is independent of the actual signal [14]. The Spread Spectrum method is capable of contributing a better performance that it offers a moderate data transmission rate and high level of robustness against exclusion techniques.

E. Echo Hiding

Echo hiding technique embeds secret information in a sound file by adding an echo into the
Discrete signal. Echo hiding has advantages of providing a high data transmission rate and superior robustness. Only one bit of secret information could be encoded if only one echo was produced from the original signal. Once the encoding process is done, the blocks are concatenated back jointly to build the final signal [13].

IV. PROPOSED METHODOLOGY

We have proposed a method to increase the security level of Steganography more secure not in favor of attacks. We first select any input cover image then select encryption type which may be text or image and then message is converted into binary. After conversion, data is hide to cover image by LSB based encryption using edges. Then select a cover audio file which in turn converted into binary. Then embed the image file into audio file by bitwise embedding. In Extraction Process end, after embedding we can extract image file from audio file by Bitwise Extraction and then convert into binary. Original message extracted from cover image by LSB based decryption using edge pixels.

Steps to hide secret information using LSB are:
a. Covert the audio file into bit stream.
b. Convert each character in the secret information into bit stream.
c. Replace the LSB bit of audio file with the LSB bit of character in the secret information.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

V. AUDIO STEGANOGRAPHIC APPLICATIONS

Audio data hiding can be used for many reasons to hide data. The most important is to prevent unauthorized persons conscious of the existence of a secret message. In the business world, Audio data thrashing can be used to hide plans for a new invention. Terrorists can also use Audio data hiding to keep their exchanges secret and to coordinate attacks. In the project ARTUS1 which aims to embed animation parameters into audio and video contents [10]. Data hiding in video and audio is of interest for the protection of copyrighted digital media, and to the government for information systems security and for covert communications. It can also be used in forensic applications for inserting hidden data into audio files for the verification of spoken words and other sounds.

VI. CONCLUSION

This paper provides analysis of Audio Steganography techniques. Steganography becomes widely used in computing, there are some issues which to be resolved. There are different techniques with their own advantages and disadvantages. We analyzed various types of audio Steganography in this paper. We proposed a method to improve the security of communication. Thus we conclude that audio data hiding techniques can be used for a number of purposes other than secret communication

REFERENCES

[1] Artz, Donovan. "*Digital steganography: hiding data within data.*" internet computing, IEEE 5.3 (2001): 75-80.
[2] Robert Krenn, "Steganography and steganalysis", An Article, January 2004.
[3] Amin, Muhalim Mohamed, et al. *"Information hiding using steganography."* Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on. IEEE, 2003
[4] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An *overview of image steganography*." ISSA. 2005.
[5] Yuk Ying Chung, fang Fei Xu , *"Development of video watermarking for MPEG2 video"* City university of Hong Kong ,IEEE 2006.
[6] Nedeljko Cvejic, Tapio Seppben "Increasing the capacity of LSB-based audio steganography " FIN-90014 University of Oulu, Finland ,2002.
[7] Neil F.Johnson, Z.Duric and S.Jajodia. "Information Hiding Steganography and Watermarking-Attacksand Countermeasures",Kluwer Academic Publishers, 2001
[8] Min Wu, Bede Liu. "Multimedia Data Hiding", Springer- Verlag New York, 2003
[9] Prof. Samir Kumar, Bandyopadhyay Barnali, Gupta Banik," *LSB Modification and Phase encoding Technique of Audio Steganography Revisited*". Vol.1 (4) IJARCCE 2012.
[10] Chandrakar, Pooja, Minu Choudhary, and Chandrakant Badgaiyan. *"Enhancement in Security of LSB based Audio Steganography using Multiple Files*." International Journal of Computer Applications 73 (2013).
[11] R.Anderson, F.Petitcolas: *On the limits of the steganography*, IEEE Journal Selected Areas in Communications, VOL .16, NO. 4, MAY 1998.
[12] Sridevi, R., A. Damodaram, and S. V. L. Narasimham. "*Efficient method of Audio steganography by modified LSB algorithm and strong encryption key with enhanced security*". Journal of Theoretical & Applied Information Technology 5.6 (2009).
[13] V. Vapnik, "Statistical Learning Theory", John Wiley, 2008.
[14] Mengyu Qiao, Andrew H. Sung , Qingzhong Liu "Feature Mining and Intelligent Computing for MP3 Steganalysis" International Joint Conference on Bioinformatics, Systems Biology and Intelligent Computing 2009.