A Comparative Study of Audio Steganography Techniques

Palwinder Singh[1],

[1]*Assistant Professor,*
Guru Nanak Dev University, Amritsar- 143001, India
E-mail: palwinder_gndu@yahoo.com

Abstract: *The emerging growth in use of digital data recommended the need of effective measure to ensure security of digital data. The goal of steganography is to hide information by concealing it into some other medium like image, audio or video so that only sender and intended recipient knows existence of information in communication. We have focused in this paper on some emerging concepts and recent techniques like Parity Coding, Least Significant Bit Coding (LSB), Phase Coding, Echo Data Hiding, Spread Spectrum about audio steganography. We also evaluate performance of recent audio steganography techniques on the basis of strengths, weaknesses and hiding rate. We have also discussed some advancement like Genetic Algorithm based Audio Steganography.*

Keywords: Steganography, data hiding, parity, coding, audio

1. INTRODUCTION

The rapid growth in use of data communication realized the need of secure data transfer. The word steganography or data hiding came from Greek origin and its meaning is "concealed writing" and the Greek words “stegano” means "Secret or hidden", and “graphy” means "writing"[1]. The Technique of Steganography is the art and science of concealed hiding messages (or data) within data in such a way that no one apart from sender and intended recipient, suspects the existence of message, a form of security through obscurity i.e. Steganography is changing the audio file in such a way that observer cannot detect the existence of hidden information. The steganography techniques which uses image or video as a cover depend on the limited human visual system where as techniques which use audio file as a cover exploits human auditory system. The idea of steganography was first introduced in 1983 by Simmons [2]. Audio based steganography has more potential to conceal information because audio files are larger than images and small change in amplitude can store huge amount of information. In steganography, the cover message which is used to make a message secret is called host message. The content of host message or cover message when modified, the resultant message is called stego-message. Stego-message is a combination of host message and secret message. Figure 1 demonstrated the general steganography system as:

1. Write a cover message which is non-secret.
2. The stego-message is produced by hiding a secret message embedded on the cover message by using a stego-key.
3. The stego-message is sent over the insecure channel to the receiver.
4. On receiving the stego-message, at the receiver end the intended receiver extracts the secret embedded message from the stego- message by using a pre agreed stego-key.

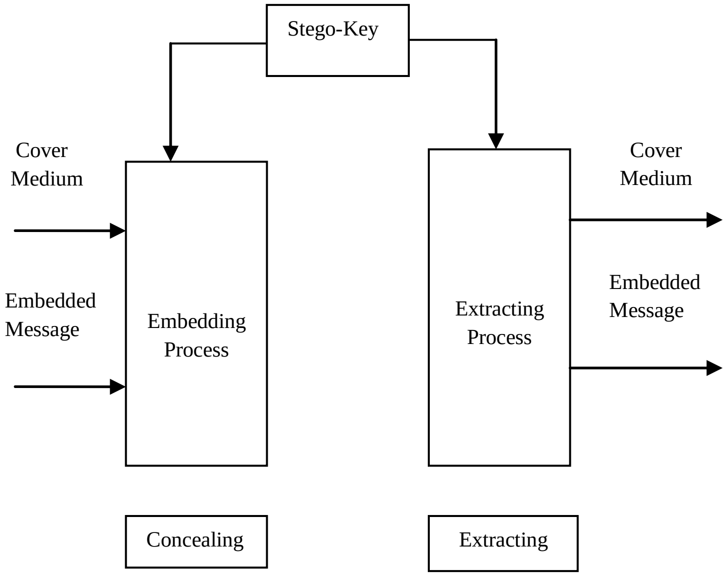


Fig 1: The General Steganography System

2. TYPES OF STEGANOGRAPHY

2.1 Steganography in Images: Image steganography is very effective, efficient and can serve a variety of purposes included authentication, concealing of messages etc. The hidden messages will change the last bit of byte in an image in Least significant bit method[3]. So by doing this, there will be relatively no change within the carrier image.

2.2 Steganography in Audio: In audio Steganography system, secret messages are embedded into digitized audio signal which results into altering binary sequence of corresponding audio files.

2.3 Steganography in Video: Steganography in Videos basically deals with hiding of information in each frame of video. This type reveals more information instead of hiding.

2.4 Steganography in Text: Encoding secret messages in text can be a very challenging task. This is because text files contain redundant data to replace with a secret message. Another cons is the ease of which text based Steganography can be altered by an unwanted parties by just changing the text itself or reformatting the text to some other form (from .TXT to .PDF, etc.).

3. COMPARISON OF SECRET COMMUNICATION TECHNIQUES

Secret Communication Techniques	Encryption	Digital Signatures	Steganography
Unremovability	Yes	No	Yes
Integrity	No	Yes	Yes/No
Confidentiality	Yes	No	Yes/No

Table 1: Comparison of secret communication techniques

4. AUDIO STEGANOGRAPHY

The technique which embeds secret messages into digital sound is called Audio Steganography. The process is usually a more difficult than embedding messages in other media[4]. Audio Steganography methods can embed any messages in WAV, and even MP3 sound files. In Audio Steganography system, secret messages are embedded into digitized audio signal which results into altering binary sequence of corresponding audio files. Audio steganography techniques are lesser prone to malicious attacks because many attacks which are malicious against image steganography algorithms like geometrical distortion, spatial scaling cannot be implemented against audio steganography schemes. Audio steganography in particular addresses key issues brought about by the the P2P software, MP3 format, and the need for a secure broadcasting scheme that can maintain the secrecy of the transmitted information, even when passing through insecure channels.

5. MODEL OF AUDIO STEGANOGRAPHY:

The basic model of Audio steganography consists of Carrier file, given Message and Password which is kown as stego- key. Carrier is also known as a cover-file, which hides the secret information [5].

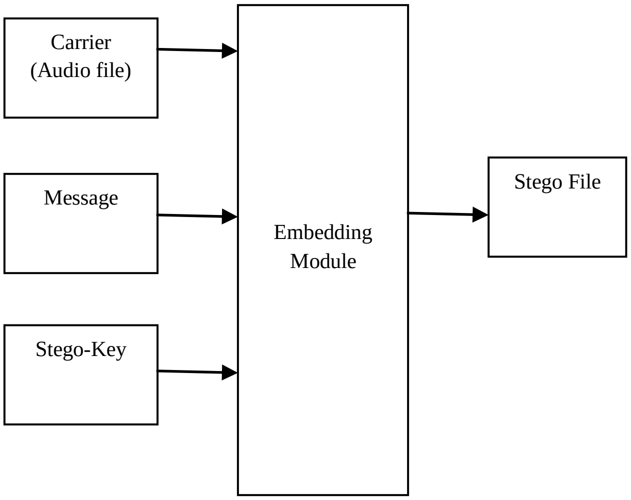


Fig 2: Basic Audio Steganographic Model

Message is any data that the sender wants to remain it confidential. Message can be plain text, image, audio or any type of file. The password is known as a stego-key, which ensures that only the recipient who 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.

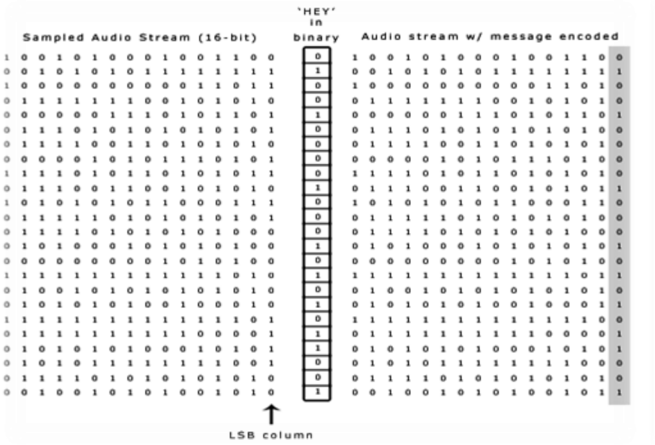
The information hiding process consists of following two steps:

I. Firstly, redundant bits in a cover-file are identified. Redundant bits are those bits that can be altered without destroying the integrity and exploiting the quality of the cover file.

II. To embed the secret information (or data) in the cover file, the redundant bits present in the cover file is replaced by the bits of the secret information.

6. AUDIO STEGANOGRAPHY TECHNIQUES

6.1 Least Significant Bit Coding: Least significant bit (LSB) coding is the simple, fast and popular methodology to embed information in a digital audio file[6]. In this technique, LSB of binary sequences of each sample of digitized audio file is replaced with binary equivalent of secret message. LSB coding allows for a large amount of data to be encoded. Example is given below.



Sampled Audio Stream (16-bit)	'HEY' in binary	Audio stream w/ message encoded
1 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0	0	1 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0
0 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1	1	0 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1
1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 1	0	1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0
0 1 1 1 1 1 1 1 0 0 1 0 1 0 1 0	0	0 1 1 1 1 1 1 1 0 0 1 0 1 0 1 0
0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1	1	0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1
0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 1	0	0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 0
0 1 1 1 1 0 0 1 1 0 1 0 1 0 1 0	0	0 1 1 1 1 0 0 1 1 0 1 0 1 0 1 0
0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 1	0	0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 0
1 1 1 1 0 1 0 1 1 0 1 0 1 0 1 1	0	1 1 1 1 0 1 0 1 1 0 1 0 1 0 1 0
0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 0	1	0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 1
1 0 1 0 1 0 1 0 1 1 0 0 0 1 1 1	0	1 0 1 0 1 0 1 0 1 1 0 0 0 1 1 0
0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 1	0	0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 0
0 1 1 1 1 0 1 0 1 0 1 0 1 0 0 0	0	0 1 1 1 1 0 1 0 1 0 1 0 1 0 0 0
0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 0	1	0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 1
0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0	0	0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0
1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0	1	1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1
0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0	0	0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0
0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 0	1	0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1	0	1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0
0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1	1	0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1
0 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1	1	0 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1
0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 1	0	0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 0
0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0	0	0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0
0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 0	1	0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 1

Fig. 3: LSB coding example

This figure illustrates that how the message "HEY" is encoded in a 16- bit CD quality samples using the LSB method. In this, the secret information is 'HEY' and the cover file is audio file. HEY is to be embedded inside the audio file. For this conversion of the secret information 'HEY' and the audio file into bit stream are needed. The least significant column of the audio file is replaced by the bit stream of secret information 'HEY'. The resulting file after embedding secret information 'HEY' is called Stego-file.

6.2 Phase Coding : Phase coding addresses the disadvantages of the noise-inducing methods of audio Steganography. Phase Coding works by substituting the phase of an initial audio segment with a reference phase that represents the data[7]. This technique relies on the fact that the phase components of sound are not as distinguishable to the human ear as noise is. Rather than introducing perturbations, the technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio (SPNR).

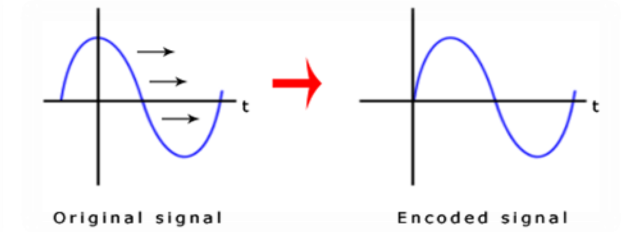


Fig. 4: Phase coding Method

6.3 Parity Coding[7]: Parity coding is one of the robust audio Steganographic techniques. Instead of breaking a signal into individual samples, this method breaks an original 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. Thus, the sender has more of a choice in encoding the secret bit.

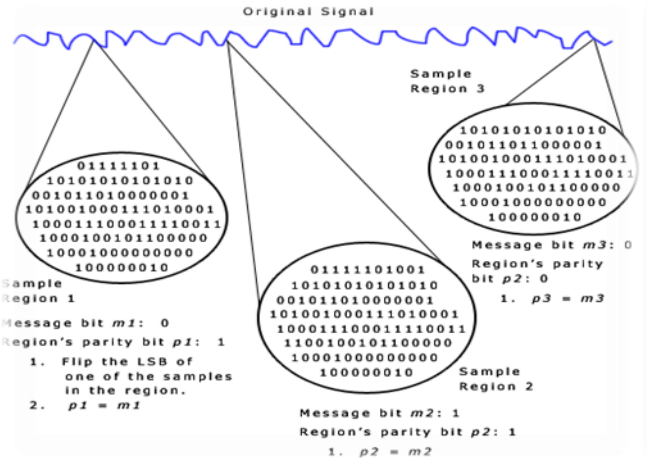


Fig. 5: Parity Coding Method

6.4 Echo data hiding[6]: Echo data hiding deals with embedding of text (or data) in audio file by introducing an echo to the original signal . The data then hidden by varying three parameters of the echo:

I. Initial amplitude,
II. Decay rate, and
III. Offset

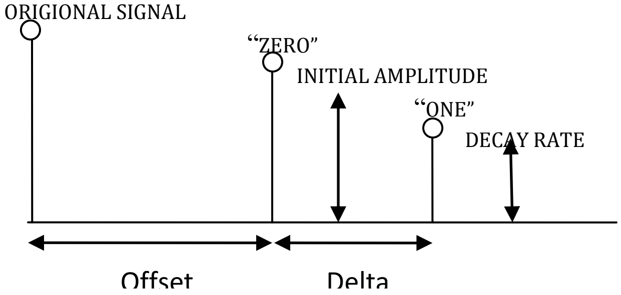


Fig.6: Adjustable parameters

One offset value represents a binary one, and a second offset value represents a binary zero.

6.5 Spread Spectrum: In audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the frequency spectrum of the audio signal using a code which is independent of the actual signal[6].

Two versions of Spread Spectrum can be used in audio Steganography:

Direct-sequence: Direct-sequence SS attempts to spread out the secret message by a constant called the chip rate and then modulated with a pseudorandom signal and interleaved with the cover-signal[7].

Frequency-hopping schemes. In frequency-hopping SS, the frequency spectrum of audio files is changed so that it hops rapidly between frequencies. Steps of spread spectrum are given below

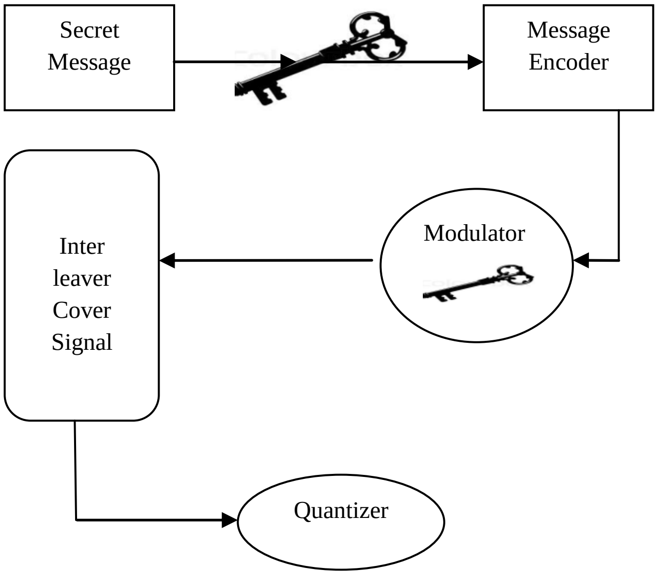


Fig 7: Spread spectrum Steps

The figure 7 demonstrates the steps of spread spectrum as:

a. The secret message is encrypted using a symmetric key k1.
b. Then encode encrypted message using a low rate error correcting code that increase overall robustness of the system.
c. The encoded message is then modulated with a pseudorandom signal that was generated using a second symmetric key.
d. The resulting random signal that contains the message is interleaved with cover signal.
e. The final signal is quantized to create a new digital audio file that contains the message.
f. This process is reversed for message extraction.

How Least Significant Bit (LSB) stegano works?

Least significant bit (LSB) steganography is the simple, fast and popular methodology to embed information in a digital audio file

The algorithm for LSB modification as shown in figure 8:

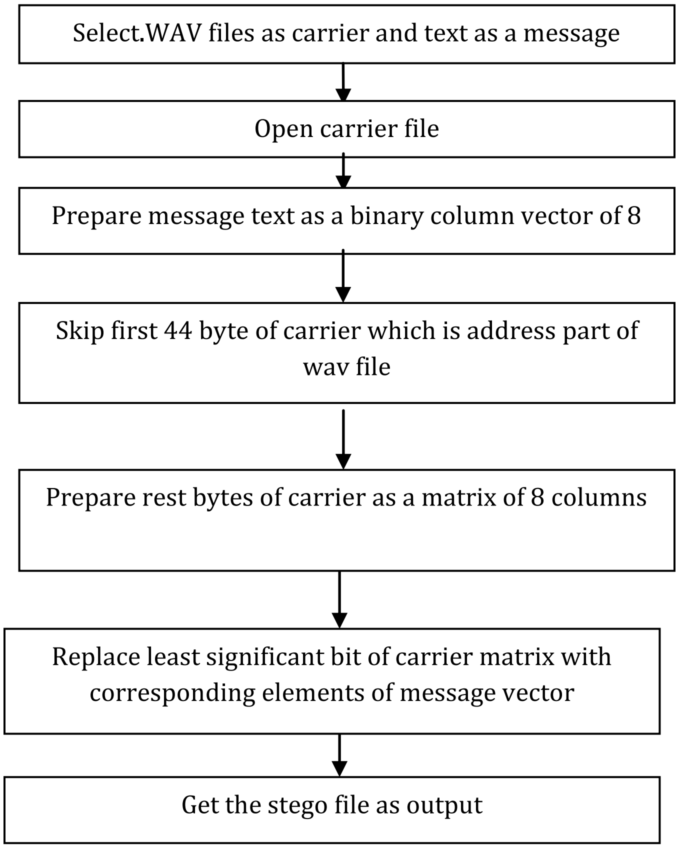
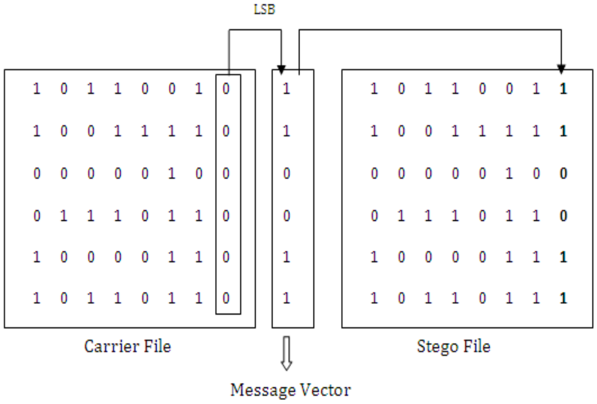

Select.WAV files as carrier and text as a message
Open carrier file
Prepare message text as a binary column vector of 8
Skip first 44 byte of carrier which is address part of wav file
Prepare rest bytes of carrier as a matrix of 8 columns
Replace least significant bit of carrier matrix with corresponding elements of message vector
Get the stego file as output

Fig 8: Flowchart of LSB modification Technique for Audio Steganography

For Example



1	0	1	1	0	0	1	0	1	1	0	1	1	0	0	1	1
1	0	0	1	1	1	1	0	1	1	0	0	1	1	1	1	1
0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0
0	1	1	1	0	1	1	0	0	0	1	1	1	0	1	1	0
1	0	0	0	0	1	1	0	1	1	0	0	0	0	1	1	1
1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1

Figure 9: LSB modification procedure for Audio Steganography

6.6 Increasing Robustness of LSB Audio Steganography: The basic idea of the proposed LSB algorithm is watermark embedding that causes minimal embedding distortion of the host audio[8]. Using the proposed two-step algorithm, watermark bits are embedded into higher LSB layers, resulting in increased robustness against noise addition or MPEG compression. Discrimination values and mean opinion scores in the case of the proposed algorithm embedding in the 6th LSB layer are practically the same as in the case of the standard algorithm embedding in the 4th LSB layer. This confirms that the described algorithm succeeds in increasing the depth of the embedding layer from 4th to 6th LSB layer without affecting the perceptual transparency of the watermarked audio signal [9].

6.7 GA (Genetic Algorithm) based Audio Steganography: A new approach is proposed to resolve two problems of substitution technique of audio Steganography. First problem is having low robustness against attacks which try to reveal the hidden message and second one is having low robustness against distortions with high average power[10]. Proposed solution is using GA. An intelligent algorithm will try to embed the message bits in the deeper layers of samples and alter other bits to decrease the error and if alteration is not possible for any samples it will ignore them. Using the proposed genetic algorithm, message bits could be embedded into multiple, vague and deeper layers to achieve higher capacity and robustness. Presented solutions are as follow [11]:

a. The solution for first problem: 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[12].

b. The solution for second problem: Embedding the message bits in deeper layers and other bits alteration to decrease the amount of the error.

7. COMPARISON OF AUDIO STEGANOGRAPHY TEQNIQUES

Methods	Embedding Techniques	Strengths	Weakness	Hiding Rate
Least Significant Bit	LSB of each sample in the audio is replaced by one bit of hidden information	Simple and easy way of hiding Information with high bit rate	Easy to extract and to destroy	16 Kbps
Echo Hiding	Embeds data by introducing echo in the cover signal	Resilient to lossy data compression algorithms	Low security and capacity	40-50 Bps
Phase Coding	Modulate the phase of the cover signal	Robust against signal processing manipulation and data retrieval needs the original signal	Low capacity	333 Bps
Parity Coding	Break the signal into separate samples and embeds each bit from secret message in sample region parity bit	Sender has more of a choice in encoding the secret bit.	Not Robust	320bps
Spread Spectrum	Spread the data over all signal frequencies	Provide better robustness	Vulnerable to time scale modification	20 Bps

Table 2: Comparison of audio steganography

8. CONCLUSION:

In order to provide better protection to data over network many steganography techniques have been developed by researchers. The availability and popularity of digital audio signals have made them a preferred choice of researchers to convey secret data. So in this paper comparative study of different audio steganography techniques and their approaches is presented. The different techniques on the basis of some parameters like strengths, weaknesses, Embedding technique, hiding rate have been discussed in the Table 2 given above. Audio steganography techniques can also be combined with existing cryptography methods so along with encryption information can also be made hidden. The advantage of one technique over other depends upon the type of application and its requirements.

REFERENCES:

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

[2] G. J. Simmons, "The prisoners' problem and the subliminal channel" in Proc. Advances in Cryptology (CRYPTO '83), pp. 51-67.Berglund, J.F.and K.H. Hofmann, 1967. Compact semitopological semigroups and weakly almost periodic functions. Lecture Notes in Mathematics, No. 42, Springer-Verlag, Berlin-New York.

[3] Masoud Nosrati, Ronak Karimi, Mehdi Hariri, "An introduction to steganography methods", World Applied Programming, Vol (1), No (3),August 2011. 191-195.

[4] Min Wu, Bede Liu, "Multimedia Data hiding", Springer-Verlag New York, 2003

[5] Nedeljko Cvej, "Algorithms for audio watermarking and steganography", Oulu 2004, ISBN: 9514273842.

[6] Bender W, Gruhl D & Morimoto N (1996) "Techniques for data hiding". IBM Systems Journal 35(3): p 313–336.

[7] "audio steg: methods", Internet publication on www.snotmonkey.com"http://www.snotmonkey.com /work/school/405/methods.html"

[8] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, "A Tutorial Review on steganography"

[9] R Sridevi, A damodram, Svl Narsimham,"efficient Methods of audio Steganography by modified LSB Algorithm and strong encryption key with enhanced security", Journal of Theoretical and applied information technology, pp. 771-778,2009.

[10] Nedeljko Cvejic, Tapio Seppänen, "Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04).

[11] 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.

[12] Sos S. Agaian, David Akopian, Sunil A. D'Souza1, "Two algorithms in digital audio steganography using quantized frequency domain embedding and reversible integer transforms", USA.