Audio Steganography

Rohit Tanwar
IT Department, ManavRachna College of
Engg, Faridabad, India
rohit.mrce@mrei.ac.in

Monika Bisla
M.Tech (CS), ManavRachna College of
Engg, Faridabad, India
monikabisla5@gmail.com

Abstract—**Drastic increase in the usage of electronic communication needed security of data being transmitted. Steganography is one such technique of hiding the message in a chosen carrier such that no one except the intended receiver is aware of its existence and hence prevents unauthorized access. The goal of Audio steganographic technique is to embed data in audio cover file that must be robust and resistant to malicious attacks. This paper presents various audio steganographic methods like LSB, echo hiding, spread spectrum etc. Merits and demerits of each method are described.**

Key Words **— Audio steganography, steganalysis, HVS, HAS, embedding capacity, robustness**

I. INTRODUCTION

Rapid and sudden increase in the Transmission of digital data over the Internet forced researchers for enhancement in the security system. Various alternatives are presented in this regard like cryptography, watermarking. But steganography has gained much importance in this context. Steganography is the art of 'secret writing'. It conceals the existence of hidden message and allows it to be only extracted by intended recipient. It adds two-layer protection against cryptography because cryptography only changes the message form but its existence is not hidden, while steganography even hides its presence [1]. The sender produces a stego file by embedding the secret message using a key in the digital cover so that an intruder cannot feel the presence of hidden message. The recipient of the message then extracts the hidden message by processing the stego file [3]. Thus, the host message is the one which embeds secret data in it. There are various options which can be used as a cover signal like images, audio signal, video files etc. Embedding secret data in digital audio cover is more challenging than using digital images as a cover since human visual system(HVS) is less sensitive in comparison to human auditory system(HAS) [2].

Figure 1 shows an example of audio steganography, here audio cover file is being used to hide secret data.

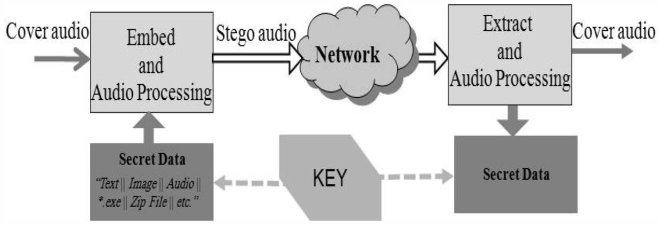

Cover audio
Embed and Audio Processing
Stego audio
Network
Extract and Audio Processing
Cover audio
Secret Data
"Text || Image || Audio || *.exe || Zip File || etc."
KEY
Secret Data

Fig. 1Block diagram for audio steganography[9]

There are three major parameters of audio steganography technique as shown in figure 2:

Perceptual Transparency: the cover file containing secret data i.e. stego file must be perceptually indistinguishable [4].

Robustness: measures the capability of embedded data how it can face intentional or unintentional attacks. Unintentional attacks could be like conversion from analog to digital format, re-sampling etc. and intentional attack could cover cropping, resizing etc in case of image steganography schemes [5].

Capacity can be defined as the amount of data that can be embedded in the information hiding scheme thereby not disturbing the perceptual transparency so that an observer cannot detect the presence of secret data. In case of audio cover file it measures the amount of data that can be hidden in the cover audio signal. Capacity is measured in terms of percent (%) and even in bits per second audio signal [6].

In this review audio file is used as a cover for secure communication between two parties and various audio steganographic methods have been illustrated in the later sections.

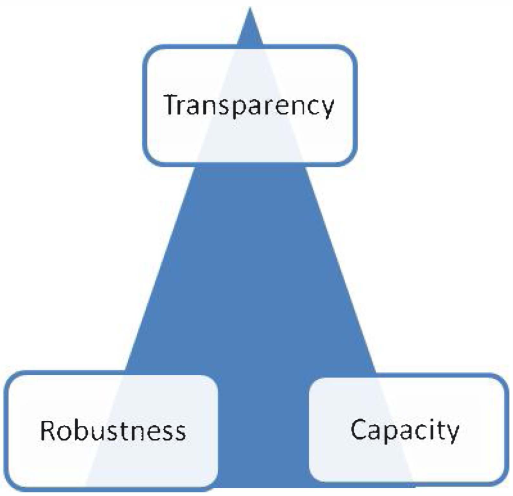


Fig. 2 Magic Triangle

978-1-4799-2995-5/14/$31.00©2014 IEEE

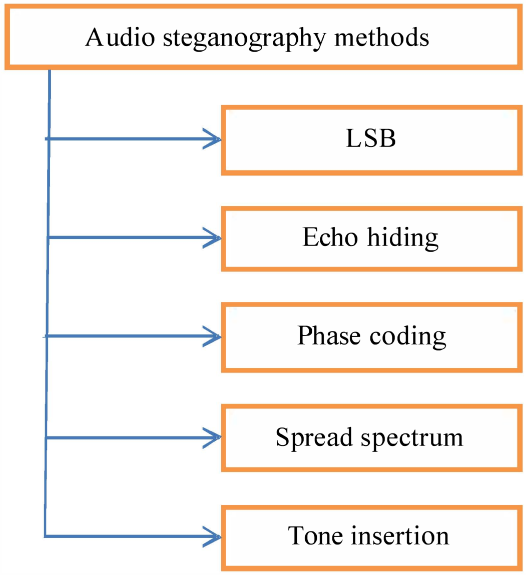


Fig. 3 Audio steganography methods

II. LOW BIT ENCODING

It is the earliest method used for information hiding [3]. It is a simple method too. LSB is the common name used for it which stands for least significant bit. It works by embedding each bit of the secret message in least significant bit of the cover audio samples. The weightage of LSBs is very small as compared to the weightage of the whole audio sample. Obviously when LSB is changed some noise will be induced but if the induced noise is less than the detectable threshold value then audio steganography can be performed successfully. If induced noise is above the threshold value and detectable by some steganalysis method, audio steganography fails in that case. If embedding capacity is increased then it will result in decreased transparency. On contrary, if less LSBs per sample are used it will result in increased transparency but decrease in capacity [6]. Robustness and capacity, these two parameters hardly co-exist together.

The figure 4 illustrates how LSB method is used to embed “HEY” message in 16 bit CD sample [7].

Advantage: Capacity for hiding data is significant in LSB method.

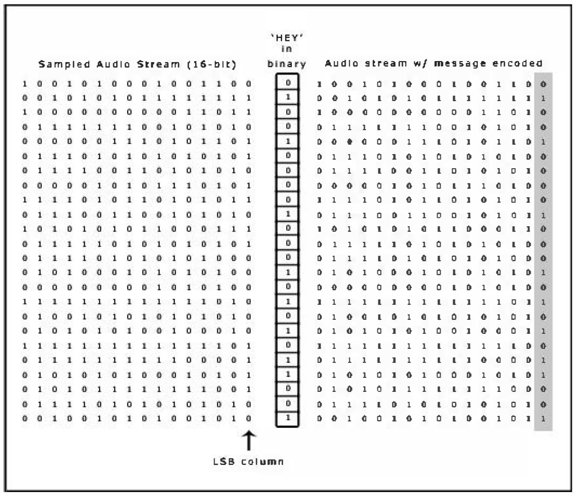
Disadvantage: In addition to low robustness, it is also not immune to manipulation. Message can be extracted easily.

III. ECHO HIDING

In order to embed data in the audio signal a short echo is introduced to the audio signal. It exploits human perception by adding echo to parts of cover audio signal. In echo hiding method there are three parameters that are to be manipulated for hiding data in the echo signal and these are: decay rate, offset and amplitude so that echo is inaudible [8]. If the delay between echo and the original signal is up to 1ms then the effect will not be noticed. All the parameters should take on the values that are below the human ear hearing threshold such that existence of echo does not get resolved. The parameter offset is varied which represents the message (binary) that is to be encoded. One value of offset denotes a binary zero whereas the another value of offset denotes a binary one [10]. Before the encoding procedure begins the original signal is decomposed into blocks and the blocks are merged when encoding procedure stops so that final signal is obtained [11].

Advantage: HAS is not easily able to detect the presence of additional data.

Disadvantage: Embedding capacity is less and this method is less secure too. Therefore, this method is not much used in recent researches.



```
                                                 'HEY'
                                                  in
Sampled Audio Stream (16-bit)                   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
                              ↑
                          LSB column
```

Fig. 4LSB Coding method [7]

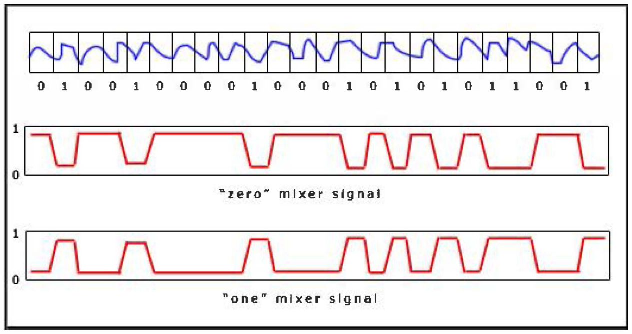


Fig. 5 Echo hiding [7]

IV. PHASE CODING

This method is based on selecting the phase components within the original speech spectrum and replacing the components by the data to be hidden.

Phase components modification must be kept small to ensure inaudibility [12]-[15]. This method is resistant to signal distortion as compared to other data hiding techniques [3]. Authors in [12] have used a strategy known as multiband phase modulation to insert data within phase components. In the strategy, phase modifications are obtained that are inaudible by

Phase components modification must be kept small to ensure inaudibility [12]-[15]. This method is resistant to signal distortion as compared to other data hiding techniques [3]. Authors in [12] have used a strategy known as multiband phase modulation to insert data within phase components. In the strategy, phase modifications are obtained that are inaudible by controlling phase alteration to the cover audio. The method known as quantization index modulation (QIM) is used on phase components where phase value of frequency bin is substituted with the closest x point to conceal '1'or o point in order to conceal '0' as described by figure 6.

Advantage: Tolerates better signal distortion. Resistant to compression.

Disadvantage: Not immune to low-pass filtering and low capacity.

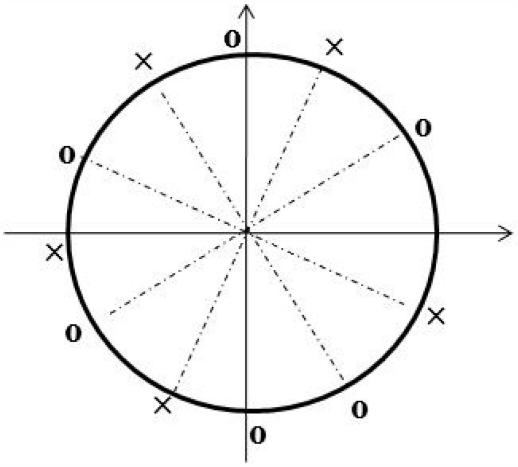


Fig. 6QIM [18]

V. SPREAD SPECTRUM

Spread spectrum method makes use of a code which does not depend on the original signal and spreads the secret message along the frequency spectrum of the audio signal [9]. Even if there is interference on some frequencies this method permits signal reception. Spread spectrum is of two types namely, frequency hopping spread spectrum and direct sequence spread spectrum and audio steganography can use both of these [16]. In case of frequency hopping method the frequency spectrum of the audio signal can be altered in order to rapidly hop between frequencies [17]. The DSSS spreads the secret signal by multiplying it with the chip and then modulating the message with pseudorandom signal which is interleaved with the cover audio.

Advantage: Provides better robustness.

Disadvantage:Vulnerable to time scale modification.

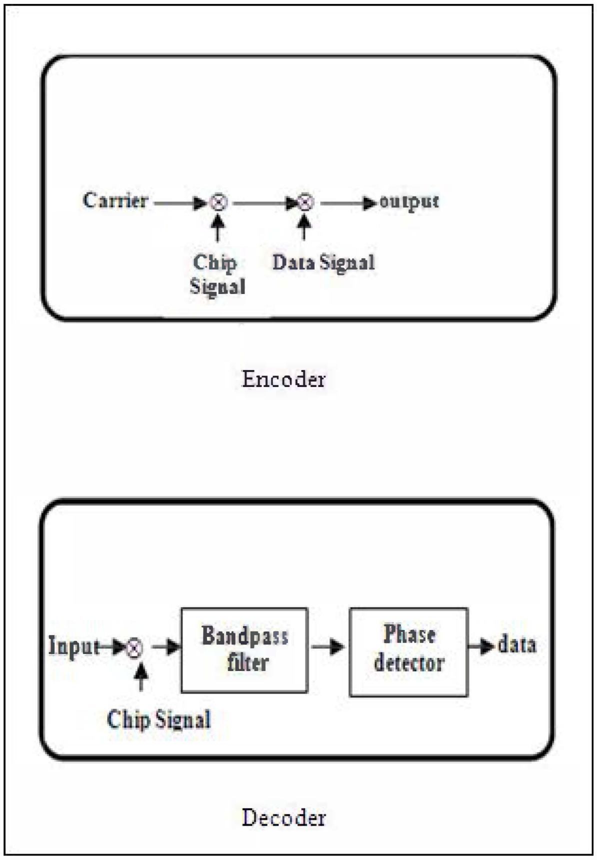


Fig. 7 Spread spectrum method[7]

VI. TONE INSERTION

Tone insertion method takes advantage of limitations in human auditory system, i.e. low power tones are inaudible in light of louder ones [19]. This audio steganographic method operates by inserting the weak power tones in presence of higher tones such that the lower power tones cannot be heard [7].

Advantage: Concealed data is not easily perceivable.

Disadvantage: It is less secured technique.

VII. CONCLUSION

Audio steganography addresses the issue related to security. Forwarding of secret data across the insecure network is more prone to attacks. Audio steganography is a much more challenging technique as compared to image steganography as already mentioned that the human visual system is less sensitive if compared to human auditory system. This paper illustrates some of the methods of digital audio steganography technique. Potentials and weaknesses of each method have also been defined in the paper.

REFERENCES

[1] KaliappanGopalan, "A Unified Audio and Image Steganography by Spectrum Modification",International Conference on Industrial Technology, 2009, Page(s): 1 - 5.

[2] Zamani M., Manaf A. A., Ahmad R.B., Zeki A. M., and Abdullah S., “A Genetic-Algorithm-Based Approach for Audio Steganography”, World Academy of Science, Engineering and Technology 54, 2009.

[3] Walter Bender, Daniel Gruhl, Norishige Morimoto, Anthony Lu,”Techniques for Data Hiding”, IBM Systems Journal, vol. 35, no. 3 and 4, pp. 313-336, 1996.

[4] Petitcolas, R.J. Anderson, and M.G. Kuhn, “Information Hiding—ASurvey,” Proc. IEEE, 1999, pp.1062–1078.

[5] Cvejic N. and Seppänen T. ”Increasing the capacity of LSB based audio steganography”, Proc. 5th IEEE International Workshop on MultimediaSignal Processing, St. Thomas, VI, December 2002, pp.336- 338.

[6] Muhammad Asad, JunaidGilani, Adnan Khalid, “An Enhanced Least Significant Bit Modification Technique for Audio Steganography”,978-1- 61284-941 6/111$26.00©2011 IEEE.

[7] Pooja P. Balgurgi, PG Student, Prof. SonalK. Jagtap, Asst. Professor,”Intelligent Processing : An Approach of Audio Steganograph” 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 1920, Mumbai,India.

[8] D. Gruhl, W. Bender, ”Echo hiding”, Proceeding of Inforomation Hiding Workshop ,pp. 295315, 1996.

[9] FatihaDjebbar_, BeghdadAyady, Habib Hamamzand Karim AbedMeraimx,”A view on latest audio steganography techniques”,2011International Conference on Innovations in Information Technology

[10] P.K.Singh, R.K.Aggrawal,” Enhancement of LSB based Steganography for Hiding Image in Audio”, International Journal on Computer Science and Engineering, Vol. 02, No. 05, 2010.

[11] K.Geetha And P.VanithaMuthu,” Implementation of ETAS (Embedding Text in Audio Signal) Model to Ensure Secrecy”, International Journal on Computer Science and Engineering, Vol. 02, No. 04, 2010.

[12] Gang. L, A.N. Akansu, M. Ramkumar, ”MP3 resistant oblivioussteganography”, Proceedings of IEEE International Conference onAcoustics, Speech, and Signal Processing, Salt Lake City, UT, Vol.3,pp.1365-1368, 7-11 May 2001.

[13] X. Dong, M. Bocko, Z. Ignjatovic, ”Data hiding via phase manipulationof audio signals”, IEEE International Conference on Acoustics, Speech,and Signal Processing (ICASSP), vol. 5, pp. 377-380, 17-21 May 2004.

[14] R. Ansari, H. Malik, and A. Khokhar, ”Data-hiding in audio usingfrequency-selective phase alteration”, IEEE International Conference onAcoustics, Speech, and Signal Processing, (ICASSP'04), pp. 389-392,Montreal, Quebec, Canada, May 2004

[15] H. M. A. Malik, R. Ansari, and A. A. Khokhar, ”Robust Data Hidingin Audio Using Allpass Filters”, IEEE Transactions on Audio, Speechand Language Processing, vol. 15, no. 4, pp. 1296 - 1304, May 2007.

[16] P.Dutta1, D.Bhattacharyya, and T.Kim,” Data Hiding in Audio Signal:A Review”, International Journal of Database Theory andApplication,Vol. 2, No. 2, June 2009.

[17] S.K.Bandyopadhyay, D.Bhattacharyya, D.Ganguly, S.MukherjeeandP.Das,” A Tutorial Review on Steganography”, 1Computer Science and Engineering Department, Heritage Institute of Technology, Anandapur, Kolkata – 700107.

[18] Gang. L, A.N. Akansu, M. Ramkumar, ”MP3 resistant oblivious steganography”, Proceedings of IEEE International Conference Acoustics,Speech,andSignalProcessing,SaltLakeCity,UT,Vol.3, pp.1365-1368,7-11May2001.

[19] B. Paillard, P. Mabilleau, S. Morissette, J. Soumagne, ”PERCEVAL:Perceptual Evaluation of the Quality of Audio Signals”, journal of Audio Engeneering Society, vol. 40, pp 21-31, February 1992.