RESEARCH ARTICLE OPEN ACCESS

Audio Steganography Techniques-A Survey

Navneet Kaur*, Sunny Behal**
(Department of Computer Science, SBSSTC, India)
(Department of Information Technology, SBSSTC, India)

ABSTRACT
we can communicate with each other by passing messages which is not secure, but we make a communication be kept secret by embedding the message into carrier or by special tools such as invisible ink, microdots etc. Steganography is the science that involves communicating secret data in an appropriate carrier which is used from hundreds of years. In digital age new techniques of hiding the data inside the carrier are invented which are known as digital steganography. Nowadays, the carrier of the message can be an image, audio, video or a text file. In this paper we have purposed a method to enhance the security level in audio steganography and also improve the quality by making 2-level steganography.

Keywords **-** Steganography, Audio steganography and its technique**,** Echo Hiding, Phase Coding, Parity Coding, Spread Spectrum, Tone insertion, LSB

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-vedio, 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 [7].

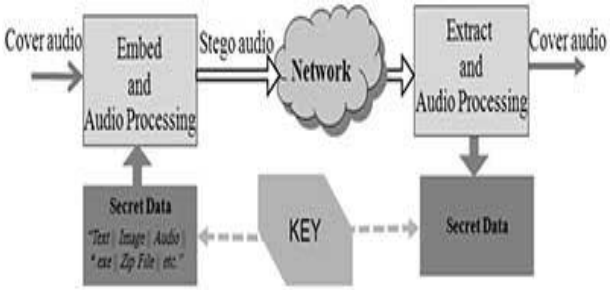

Fig 1: Basic Audio Steganographic Model

Hiding process is consists of two steps [8][9]In first steps Identification of redundant bits in a cover-

file. Redundant bits are those bit that can he modified without corrupting the quality or destroying the integrity of the cover-file. In second step embedding the secret data in the cover file, the redundant bits in the cover file is replaced by the bits of the secret data. As same as in document images, we can modify sound files in such a way that they contain hidden data, like copyright data, we can make data modified in such a way to not destroy the signal. In audio steganography we can embed information in sound files with the help of Human Auditory System (HAS). The HAS perceives the additive random noise and also the perturbations in a sound file can also be detected. But there are some ―holes‖. The digital sound is obtained from the analog sound by converting it to digital domain. The famous file formats for sounds are the Windows Audio-Visual (WAV) and the Audio Interchange File Format (AIFF). There are also compression algorithms such as the International Standards Organization Motion Pictures Expert Group-Audio (ISO MPEG-AUDIO). While implement data hiding method for audio, we can first check a environments of the sound signal will travel between encoding and decoding. Modification will take place in 2 types of area which we consider. In storage environment or digital signal, other is transmission path of the signal may travel [11][12]. After secret messages conceal successfully some methods are used for embedding data in digital audio These methods range embed information in the form of signal noise to more powerful methods that makes a secure or powerful signal processing techniques to hide data.. [10]

III. TECHNIQUES OF AUDIO STEGANOGRAPHY

1. HIDING METHODS:

1.1) 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

1.2) 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

1.3) 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. [13][14][15][16]

2) AUDIO STEGANOGRAPHYTECHNIQUES

2.1) 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 [17][18][19][20][21]

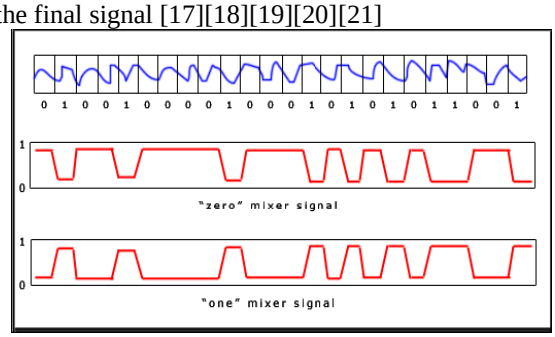

Fig2. Echo hiding

2.2) 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. Phase coding is explained in the following procedure:

2.2.1)The original signal is dividing into smaller sections whose lengths equal the size of the message to be encoded.

2.2.2) A Discrete Fourier Transform (DFT) is applied to each segment sections to create a matrix of the phases and Fourier transforms magnitudes.

2.2.3) Calculate the adjacent difference between phases

2.2.4) Phase shifts between consecutive segments are easily detected. Therefore the secret message is only inserted in the phase vector of the first signal segment as follows:

$$Phase_{new} = \begin{cases} \frac{\pi}{2} & if\ message\ bit = 0 \\ \frac{-\pi}{2} & if\ message\ bit = 1 \end{cases}$$

2.2.5) A new matrix phase is made by using the new phase of the first segment section and the original phase differences [22].

2.3) 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.

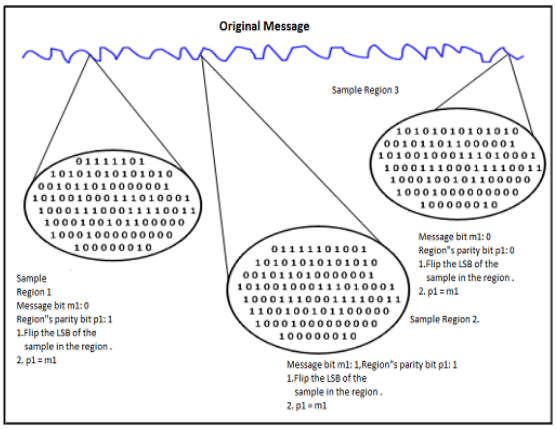

Fig 3. Parity coding

2.4) 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 [17] [18][19][20][21].

2.5) 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. [13][22].

2.6) 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 unto 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 [10]. 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.

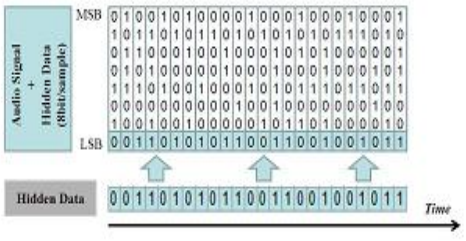

Fig: 4 LSB in 8 bits per sample signal is over written by one bit of the hidden data.

To improve the robustness of LSB method against distortion and noise addition, have increased the depth of the embedding layer from 4th to 6th and to 8th LSB layers without affecting the perceptual transparency of the stego audio signal. In, only bits at the sixth position of each 16 bits sample of the original host signal are replaced with bits from the message. For low embedding error, the other bits can be flipped in order to have a new sample that is closer to the original one And in other side has shifted the LSB embedding to the eighth layer and has avoided hiding in silent periods or near silent points of the host signal. The present steganography techniques take help of well known cryptography algorithm to increase security level

IV. PROPOSED METHODOLOGY

We have purposed a method to make the security level of steganography more secure against attacks. Purposed method is consisting of 2-Level Security Process. In this first we select any input cover image then select encryption type which may be text or image and then message converted into binary. After conversion message hide to cover image by LSB based encryption using edges. Then select a cover audio file, then convert audio file into binary, then embed image file into audio file by Bitwise embedding. In Extraction Process: After embedding we can extract image file from audio file by Bitwise Extraction and then convert into binary. After converting original message extracted from cover image which may be text/image by LSB based decryption using edge pixels. The flow chart of purposed methodology is given below:

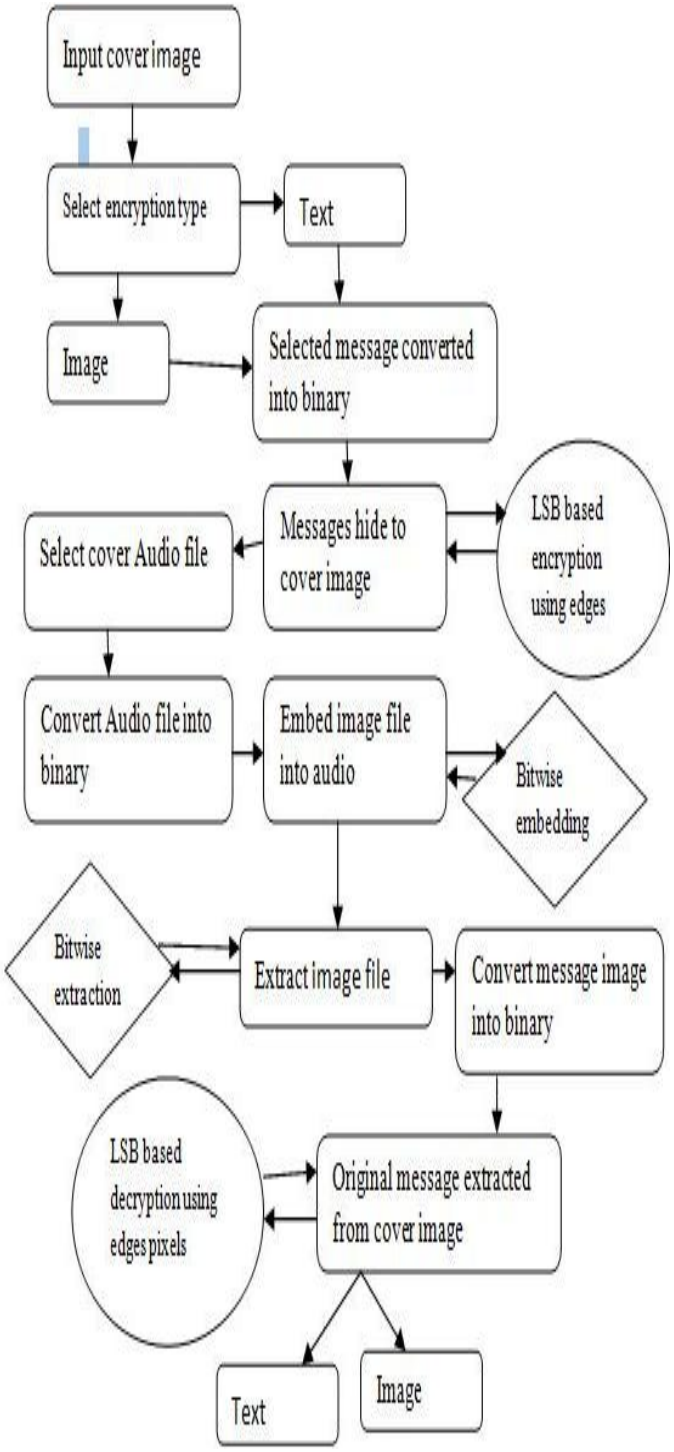

Fig 5. Shows the Purposed Methodology chart

V. COMPARISON OF VARIOUS TECHNIQUES:

Paper Name	Author	Year of Publication	Results
LSB Audio Steganography On Text Compression	M. Baritha Begum , Y. Venkataramani	2013	Audio Steganography based text compression achieves better SNR value.
A Steganography Algorithm for hiding image in image by improved LSB substitution by minimize	Vijay kumar Sharma, Vishal shrivastava	2012	quality of the stego-image can be greatly improved with low extra computational complexity. a good balance between the security and the image quality is achieved.
Information hiding using Audio steganography	Jayaram P, Ranganatha H R, Anupama H	2011	data hiding techniques used for a number of covert communication or deniable data storage, information tracing and finger printing, tamper detection.
Information Hiding in Audio Signals	H.B.Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale	2010	increases the capacity of the cover audio by as much as 8 times and also provides robust encryption. This will give great security and the embedded message cannot be extracted without the knowledge of the embedding process.
On Embedding of Text in Audio – A case of Steganography	Pramatha Nath Basu, Tanmay Bhowmik	2010	The main goal of this research work was embedding of text into audio as a case of steganography. the stego signal resulting from embedding is indistinguishable from the host audio signal, and the embedded message is recovered correctly at the receiver.
Audio Steganography using Bit Modification – A Tradeoff on Perceptibility and Data Robustness for Large Payload Audio Embedding	Kaliappan Gopalan, Qidong Shi	2010	. The study demonstrated the capability of the technique for hiding a potentially large payload of data with robustness using high bit indices for embedding. A tradeoff between noise tolerance and payload, both of which depend on higher bit indices, is needed for a reasonably imperceptible embedding
A Survey on Steganography in Audio	Pradeep Kumar Singh, Hitesh Singh and Kriti Saroha	2009	the storage environments, or digital representation of the signal that will be used in encoding and decoding,.
A Secure Audio Steganography Approach	Mazdak Zamani, Azizah Bt Abdul Manaf, Rabiah Bt Ahmad, Farhang Jaryani	2009	An algorithm 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. the proposed genetic algorithm, message bits could be embedded into multiple, vague and deeper layers to achieve higher capacity and robustness

I. 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. We purposed a method to improve the security of secret communication and quality of file.

II. ACKNOWLEDGMENT

This is to express my sincere gratitude to Mr. Sunny Behal, Assistant Professor, Department of Computer Science & Engineering, SBS State Technical Campus, Ferozepur (Punjab), India, for sparking in me the enthusiasm and initiative to discover and learn. I am truly thankful to him for guiding me through the entire paper and being my mentor and guide in this learning curve.

REFERENCES

[1] Artz, Donovan. "*Digital steganography: hiding data within data."* internet computing, IEEE 5.3 (2001): 75-80.

[2] Amin, Muhalim Mohamed, et al. *"Information hiding using steganography."* Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on. IEEE, 2003.

[3] Shashikala Channalli, Ajay Jadhav, *"Steganography An Art of Hiding Data*" International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141

[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] Prof. Samir Kumar, Bandyopadhyay Barnali, Gupta Banik," *LSB Modification and Phase encoding Technique of Audio Steganography Revisited*". Vol.1 (4) IJARCCE 2012.

[7] 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).

[8] N. Taraghi-Delgarm, "*Speech Watermarking*", M.Sc. Thesis, Comptuer Engineering Department, Sharif University of Technology, Tehran, IRAN, May 2006

[9] [9] M. Pooyan, A. Delforouzi, *"LSB-based Audio Steganography Method Based on Lifting WaveletTransform",* in Proc. 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'07), December 2007, Egypt.

[10] Singh, Pradeep Kumar, Hitesh Singh, and Kriti Saroha. "*A survey on Steganography in Audio* ." National Conference on Computing for Nation Development, Indiacom. 2009.

[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] Pramatha Nath Basu, Tanmay Bhowmik,'On Embedding of Text in Audio – A case of Steganography' International Conference on Recent Trends in Information, Telecommunication and Computing

[14] [14]Kumar, H.; Anuradha "Enhanced LSB technique for audio steganography". Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference o*n*, On page(s): 1 - 4

[15] Keeping Secrets Secret: Steganography with .NET – http://www.devx.com/dotnet/Article/22667

[16] Cole, Eric. - "Hiding in Plain Sight: Steganography and the Art of Covert Communication".

[17] HS, Anupama. "*INFORMATION HIDING USING AUDIO STEGANOGRAPHY--A SURVEY*." International Journal of Multimedia & Its Applications 3.3 (2011).

[18] Mat Kiah, M. L., et al. *"A review of audio based steganography and digital watermarking*." International Journal of Physical Sciences 6.16 (2011): 3837-3850.

[19] Malviya, Swati, Manish Saxena, and Dr Anubhuti Khare. *"Audio Steganography by Different Methods"*. International Journal of Emerging Technology and Advanced Engineering [20] Website: www. ijetae.com (ISSN 2250-2459, Volume 2, Issue 7 (2012) .

[20] Dutta, Poulami, Debnath Bhattacharyya and Tai-hoon Kim. *"Data hiding in audio signal: A review*." International journal of database theory and application2.2 (2009): 1-8

[21] H.B.kekre , Archana Athawale , *"Information Hiding In Audio Signal"*.Intertional Journal of Computer Application volume 7-No.9 October 2010.