A Survey on Digital Audio Steganography Techniques Used for Secure Transmission of Data

[1] Hinal Somani, [2] Kaushal M. Madhu
[1]Student, [2]Assistant Professor
[1 2]Department of Computer Engineering,
[1 2] L. J. Institutes of Engineering and Technology, Gujarat Technological University
Ahmedabad, Gujarat, India

***Abstract* - In era of digital communication, to enforce data security new technique has been proposed is Steganography. Audio Steganography is a method of hiding information in order for data in an audio file to remain safe in such a manner that existence of secret message is concealed from third party. To achieve this, message bits are embedded in random and higher Least Significant Bit (LSB) layer that increases robustness against noise addition and appropriate modification of bits in audio sample is performed to reduce the distortion.**

***Keywords* - Audio Steganography, Least Significant Bit (LSB), Information Hiding, Robustness**

I. INTRODUCTION

In present day to day life, the demands of internet application have increased the possibility of attacks. For secure transmission of data, mainly two approaches can be used e.g. Cryptography and Steganography. Cryptography is defined as protecting the information by encrypting it into unrecognizable format. It doesn't hide the existence of the message from the attacker instead it renders the content of the message garbled to unauthorized people [1].

Steganography is related to information hiding. Steganography is one of the best techniques employed for ensuring data security. Steganography hides the information in such a way that the existence of information is undetectable [1].This is usually done by embedding the secrete message into a cover medium. On the basis of system's requirement, both the secret message and the cover medium can be of any data format, including text, image, audio, and video [2].

These days, most commercial organizations use the steganography approach by means of communication with respect to transmission of secure information such as transaction information, business dealing, etc. But sometimes, these information hiding schemes are not enough to provide security for the aforementioned confidential information. The enormous use of electronic communication and huge availability of different free data hiding software makes the situation more critical. The correctness of information sometimes suffers by the data hiding scheme as the information loss its originality during different types of transformations [3].

To solve the above issues, the use of audio steganography is quite successful up to a certain extend as it provides better security of information and robustness [3]. Data hiding in audio files is especially challenging because of the sensitivity of the Human Auditory System (HAS). However, HAS still tolerates common alterations in small differential ranges. For example, loud sounds tend to mask out quiet sounds. Additionally, there are some common environmental distortions which may be ignored by listeners in most cases. These properties have led researchers to explore the utilization of audio signals as carriers to hide secret data [4].

In this paper, Section II describes parameters that need to be satisfied by audio steganography technique and various techniques used for audio steganography. Section III describes related work for Least Significant Bit (LSB) method. Section IV describes comparative study of techniques which have been used to hide secret data in audio file. Proposed work and Conclusion is presented in Section V and VI respectively.

II. AUDIO STEGANOGRAPHY

To perform audio steganography successfully, the adopted technique should work against HAS. For any audio steganography technique to be implementable, it needs to satisfy three conditions; capability, transparency and robustness [5].

Capacity: Capacity refers to the amount of secret information that can be embedded within the host audio without affecting the perceptual quality of audio [6].

Transparency: Transparency evaluates how well a secret message is embedded in the cover audio. The difference between audio after hiding and audio before hiding should remain negligible [6].

Robustness: Robustness measures the ability of embedded data or watermark to withstand against intentional and unintentional attacks. Unintentional attacks generally include common data manipulations such as lossy compression, digital-to-analog conversion, re-sampling, requantization , etc. whereas intentional attacks cover a broad range of media degradations which include addition white and colour noise, rescaling, resizing, cropping, random chopping, and filtering attacks [7].

In audio steganography data embedding approaches are broadly classified into spatial domain and transform domain.

2.1 Spatial Domain Audio Steganography

These methods hide information on the basis of geometric characteristics of audio signal [1]. Low Bit Encoding and Echo Hiding methods are fall in category of spatial domain.

1. Low Bit Encoding

The Low Bit Encoding modification is one of the simplest audio steganography techniques providing high capacity. In this technique, data is being hidden in least significant bit(s) of audio samples. The weightage of LSBs in comparison with the combined weightage of whole sample is very small. However, changing the LSBs will induce some noise but as long as the noise induced is below detectable threshold, audio steganography is possible. Increasing the number of altered LSBs will induce more noise. If noise increases above the threshold and becomes detectable through any of the steganalysis methods, audio steganography technique fails. Using more LSBs per sample increases the capacity and decreases the transparency. On the other hand, using less LSBs per sample will decrease the capacity and increase the transparency. So, there is always a trade-off between both these parameters [5].

2. Echo Hiding

This method introduces a short echo to the host signal and then embeds data in it. After addition of echo in the carrier file, the stego signal must retain the same statistical characteristics. Three parameters of echo signal are manipulated for hiding data: initial amplitude, the offset (delay) and the decay rate (for the inaudible echo). The effect is indistinguishable for delay up to 1ms between original signal and echo. The drawback of this method is low embedding rate and security [1].

2.2 Transform Domain Audio Steganography

These methods hide information along the frequency distribution of the carrier signal. Various methods of transform domain are used for hiding data.

1. Spread Spectrum

In spread spectrum technique, the hidden information is distributed over a frequency spectrum of audio signal. This technique produces redundant copies of the data signal. Actually, multiple copies of data are produced using M sequence code which is known to both sender as well as receiver. Once multiple copies are produced they are embedded in audio carrier. Hence, if some values get corrupted, there will still be copies of the values which would be used to recover the hidden information [1].

2. Discrete Wavelet Transform

Wavelet usually refers to small waves. The technique is used to hide data in transform coefficients of the audio signal. DWT was developed as an alternative to short time Fourier transforms. DWT actually decomposes the audio signal into many multi resolution sub-bands, which in turn helps to locate the most appropriate sub-bands for embedding bits of secret message. Data hiding in wavelet domain attempts to obtain high embedding rate but the extraction of data at the receiver might be inaccurate [1].

3. Phase coding

Phase Coding is based on the fact that phase components of sound are not as perceptible to human ear as noise is. This technique encodes the secret message as phase shifts in the spectrum of a digital signal. The disadvantage of phase coding is low transmission rate because the secret message is embedded only in the first signal segment. We can increase the transmission rate by increasing the length of the signal segment but this would also change phase relations between each frequency component of a segment more drastically, which will make embedding easier to detect [1].

4. Tone Insertion

It is the indirect exploitation of the psychoacoustic masking phenomenon. Psycho acoustical or auditory masking is actually the characteristic of human auditory system HAS where the presence of stronger tone renders the weaker tone in its spectral domain. The masked sound becomes inaudible in presence of another louder sound. However, the masked signal is still present. The method is resistant to attacks of low-pass filtering and bit truncation. Tone insertion method has low embedding capacity. Also, the embedded data can be easily extracted since inserted tones are easy to detect [1]

III. RELATED WORK

3.1 Audio Steganography using GA

Authors [8] have proposed an approach that uses most powerful encryption algorithm (RSA) to encrypt message in the first level of security, which is very complex to break. In the second level, they use a more powerful GA (Genetic Algorithm) based LSB (Least Significant Bit) Algorithm to encode the encrypted message into audio data. Here encrypted message bits are embedded into random and higher LSB layers, resulting in increased robustness against noise addition. On the other hand, GA operators are used to reduce the distortion.

3.2 An audio steganography by a low-bit coding method with wave files

In this method [9] data is embedded based on predefined threshold. If range of audio is 0-255 and if at a middle range 128 the sound is silent then data cannot be embedded. Based on this, two amplitude threshold are decided. If amplitude range is less than threshold 1, then data is not embedded. If amplitude range is between threshold 1 and 2 then one bit is embedded and if range is greater than threshold 2 then two bits are embedded. So by using this technique capacity of audio signal is increased.

3.3 Increasing the capacity of cover audio signal by using multiple LSBs for Information Hiding

Authors [10] have proposed method to increase capacity of audio signal based on their MSB. If MSB of audio signal is 0 then 6 bits are embedded and if MSB of audio signal is 1 then 7 message bits are embedded in an audio sample. This method increases capacity but introduces higher distortion result in a poor robustness.

3.4 Intelligent Processing: An approach of audio steganography

In this paper [11] author discussed methods are being used earlier for embedding data at LSB. In conventional LSB message bits are embedded in LSB .This method is more vulnerable to attack. So they proposed a technique by performing XOR operation on last two significant bits. Modification of LSB depends on the result of XOR operation. This technique enhancing the security but addition of noise can destroy data.

3.5 Lossles Audio Steganography in Spatial Domain

In this paper [4] authors devised a hash function in order to generate pseudorandom position for insertion and extraction of secret message bits from an audio sample. In each audio sample, secret bits are embedded in (0-4) LSBs based on pseudorandom position generated .This technique supports text, image and audio as a secret message.

3.6 Safe transmission of text files through a new audio steganography technique

Authors [12] have proposed a method in which text or information is embedded in an audio file based on sample quality and sample rate in such a way that embedded information should only be extractable if the extracting entity has the original file. To add another level of security they have used password guessing algorithm. Disadvantage of this method is that it is based on speech recognition of receiver. If in any case the voice of receiver is changed then this algorithm do not work properly.

3.7 Dynamic approach in substitution based audio steganography

Authors [7] have proposed a method for embedding bits in deeper LSB layers of an audio sample. Embedding bit position is decided by parity of that sample. In this XOR operation is performed between parity bit and message bit and the result of XOR operation decides the embedding position in audio sample. This method provides robustness by embedding bits based on parity of audio sample, but embedding in deeper layer introduces higher distortion.

3.8 An approach for enhancing the message security in Audio Steganography

In this paper [2] author proposed a method that uses parity of audio sample to choose whether message bit is embedded in right or left channel of audio signal. Along with this 4 bit stego-key is used for each 16 bit sample. Decimal value of stego-key represents a bit in audio sample. XOR operation is performed between stego-key value and message bit. Modification of LSB depends on the result of XOR operation. This method provides robustness but requires 4 bit key for each sample requires large amount of space.

3.9 Audio Steganography using dual randomness LSB method

Authors [6] proposed dual randomness LSB method to increase the security. To achieve this, dual layer randomization approach is used. First layer of randomization is achieved by randomly selecting the byte number or samples. An additional layer of security is provided by randomly selecting the bit position at which embedding is done in the selected samples. Using this proposed algorithm the transparency and robustness of the steganographic technique is increased.

IV. COMPARATIVE STUDY

Table: I Comparison between different Audio Steganography techniques invented in LSB coding

No	Technique Used	Strong Points	Weak points
1	Genetic Algorithm based on LSB	More Secure embedding method Increased robustness due to higher random LSB layer	Computational Complexity is high
2	Variable Low bit coding	Increased embedding capacity	Some amount of distortion introduced
3	Embedding bits based on MSB	Increased capacity	Distortion increased because 6 or 7 bits of samples are used for embedding
4	XORing of LSB	Easy to implement	Addition of noise can destroy the data
5	Embedding at Pseudorandom position of LSB	Increased robustness due to random LSB layer	Additional queue is required which consumes more space
6	Amplitude Modifying method	Password guessing algorithm provides more security	Only text data supported
7	Parity and XORing method	More security due to deeper LSB layer	Distortion is high
8	Stego-key based LSB method	This method increases robustness by using Stego-key	Addition of noise because data is embedded at LSB
9	Dual randomness LSB method	Increases robustness and confidentiality	Low Capacity

V. PROPOSED WORK

As seen all the methods that are invented in LSB, most of the method suffers through about the capacity and distortion created by embedding bit into audio file. In order to enhance the capacity with maintaining perceptual transparency, a new audio steganographic technique has been proposed and following are the steps.

Step 1: Read the Secret message.
Step 2: Convert each character of secret message into bits using Huffman Coding.
Step 3: Convert that bits into hexadecimal digits.
Step 4: AES Encryption Algorithm is performed on hexadecimal digits.
Step 5: Read the audio file and convert into 8 bits samples using sampling.
Step 6: Store the length of ciphertext using standard LSB technique.
Step 7: Select the binary samples of audio randomly based on MSB of an audio sample
Step 8: Hide two consecutive bits of ciphertext into selected 8 bits sample at randomly selected LSB layers based on MSB of the selected sample
Step 9: Convert the binary audio samples into same audio format, such as the input audio file.

VI. CONCLUSION

To enforce security of digital information, various techniques are presented in recent research work. Audio Steganography addresses issues related to integrity of hidden data. This paper presents review of techniques and research work has been done in Low-bit encoding method along with their potentials and limitation in ensuring secure communication. Low-bit encoding provides high capacity along with successful retrieval of data. So there is requirement of new technique that provides high capacity and robustness against intentional and unintentional attacks. In future this can be achieved by embedding multiple bits in selected sample randomly and appropriate modification will be performed to reduce the distortion and increases robustness.

REFERENCES

[1] Ifra Bilal, Mahendra Singh Roj, Rajiv Kumar and P K Mishra, "Recent Advancement in Audio Steganography" IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC) , Solan , Dec 2014, pp 402-405
[2] Ashis Kumar Mandal, Md. Olioul Islam, Mohammed Kaosar and Md. Delowar Hossain, "An Approach for Enhancing Message Security in Audio Steganography",IEEE International Conference on Computer and Information Technology, Kulna , March 2014, pp 383-388.
[3] Lukman Bin Ab. Rahim, Shiladitya Bhattacharjee and Izzatdin B A Aziz, "An Audio Steganography Technique to Maximize Data Hiding Capacity along with Least Modification of Host," Springer Proceedings of the First International Conference on Advanced Data and Information Engineering (DaEng-2013), Lecture Notes in Electrical Engineering, 2014, pp. 277-289.
[4] Dipankar Pal, Anirban Goswami and Nabin Ghoshal, "Lossless Audio Steganography in Spatial Domain (LASSD)," Springer Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), Advances in Intelligent Systems and Computing, vol. 199, 2013, pp. 575-582.
[5] Muhammad Asad, Junaid Gilani, and Adnan Khalid, "An Enhanced Least Significant Bit Modification", IEEE, International Conference on Computer Networks and Information Technology (ICCNIT), Abbottabad, July 2011, pp 143-147
[6] Jithu Vimal and Ann Mary Anex, "Audio Steganography Using Dual Randomness LSB Method" ,IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kanyakumari, 10-11 July 2014 ,pp 941-944
[7] Anupam Kumar Bairagi, Saikat Mondal and Amit Kumar Mondal , "A Dynamic Approach In Substitution Based Audio Steganography", IEEE International Conference on Informatics, Electronics & Vision (ICIEV), Dhaka, 18-19 May 2012,pp 501-504
[8] Krishna Bhowal, Anindya Jyoti Pal, Geetam S. Tomar and P. P. Sarkar, "Audio Steganography using GA", IEEE International Conference on Computational Intelligence and Communication Networks (CICN), Bhopal, 26-28 Nov. 2010, pp 449 - 453
[9] Masahiro Wakiyama, Yasunobu Hidaka, Koichi Nozaki, "An audio steganography by a low-bit coding method with wave files", IEEE Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Darmstadt ,15-17 Oct. 2010, pp 530 – 533
[10] Dr H.B Kekre , Archna Athawale , B.Swarnalata Rao and Uttara Athawale, "Increasing the Capacity of the Cover Audio Signal by using Multiple LSBs for Information Hiding", IEEE 3rd International Conference on Emerging Trends in Engineering and Technology (ICETET), Goa , 19-21 Nov. 2010, pp 196 - 201
[11] Pooja P. Balgurgi and Prof. Sonal K. Jagtap, "Intelligent processing: An approach of audio steganography", IEEE International Conference on Communication, Information & Computing Technology (ICCICT), Mumbai , 19-20 Oct. 2012 ,pp 1-6
[12] Mayank Punetha, Neelam Jain, Ravi Kumar and Mohit Gawande, "Safe Transmission of text files through a new Audio Steganography Technique", IEEE 2nd International Symposium on Computational and Business Intelligence (ISCBI), New Delhi , 7-8 Dec. 2014 ,pp 58 - 62