Threshold Based LSB Audio Steganography

Abdul Hakeem, Noor Ul Amin, Mohsin Shah, Zakir Khan, and Abdul Qadi

***Abstract*----**Audio steganography is the technique of hiding secret information into the samples of an audio signal. A number of audio steganographic techniques are available in literature. All the available techniques emphasis on the security of the technique and the payload. Not a single technique promises good security and high payload at the same time. In this work a new least significant bit (LSB) audio steganographic technique is introduced. In this technique secret information is embedded in audio samples based on the amplitude of the sample. The idea is taken from the fact that high amplitude audio samples over run low amplitude samples which means that more information bits can be embedded in low amplitude samples and vice versa. A threshold is set to decide what number of bits to be embeddedin which amplitude sample. This threshold works as a secret key for the information hidden in the audio samples.The proposed technique does not affect the quality of the resultant audio signal and is more secure than the conventional LSB technique.

***Keywords*---**Audio Steganography; Least Significant Bit (LSB) technique, Threshold, Secret information, MSE (mean square error), RMSE (root mean square error), MAE (mean absolute error),NAE(normalized absolute error), AD (Average difference) and MD (maximum difference)

I. Introduction

THE fast improvement of the Internet and the digital information revolution caused major changes in the overall culture. Flexible and simple-to-use software and decreasing prices of digital devices (e.g. portable CD and MP3players, DVD players, CD and DVD recorders, laptops, PDAs) have made it feasible for consumers from all over the world to create, edit and exchange multimedia data. Broadband Internet connections almost an errorless transmission of data helps people to distribute large multimedia files and makes identical digital copies of them [1]. In modern communication system data hiding is most essential for network security issue. Sending sensitive messages and files over the Internet are transmitted in an unsecured form but everyone has got something to keep in secret. Three main methods are being used: encryption, watermarking, and steganography. In this developing technology electronic communication has become integral and significant part of every one's life because it is easy, quick and more secure. It is necessary to transmit data securely to the receiver. Steganography originated from the word "steganos" which means covered, concealed or protected. Steganography is a branch of science that deals with embedding a message on the transmitter side and retrieving it on the receiver side. It may be for copyright protection to prevent piracy or private personal communication. The message used to hide user's message is called "host" or "cover message"Stego-messageis the combination of host message and user's message**. [2]**

An audio steganographic system has the following components:

Message signal (Secret information).

- Cover signal (Audio signal in which secret information is to be embedded).
- Encoding algorithm
- Stego signal (The resultant audio signal after information embedding).
- Decoding algorithm

The primary goal of steganography is to hide the fact that communication takes place between two parties and keep any third party unaware of.[3] There are four main categories of audio Steganography those are commonly used to hide information into auditory data: least significant bit coding, echo coding, phase coding and spread spectrum coding. Each method varies in implementation, bandwidth, and covertness. They all have advantages and disadvantages and are typically used for differing applications.

Least Significant Bit Encoding

As the name implies least significant bit coding (LSB encoding) deals with modifying the least significant bit of each audio frame in order to encode binary information. This is an inherently simple task and has the advantage of embedding high payload in audio cover file but with less security. Small format changes that occur during file conversion, compression, or through preventative techniques, can easily contaminate the hidden data [4].

Echo Hiding

Echo hiding exploits human perception by adding one of two different kinds of sub-perceptible echoes to segments of the cover audio. For data hiding three parameters of echoes are varied: amplitude, decay rate, and offset (delay time) from

Abdul Hakeem, Noor Ul Amin, Zakir Khan, and Abdul Qadi, are with Department of Information Technology, Hazara University Mansehra, Pakistan.

Mohsin Shah, is with Optical Engineering, School of Optoelectronics, Beijing Institute of Technology, China.

http://dx.doi.org/10.15242/IIE.E1114031

the original signal [5]. All the parameters are set below the human hearing threshold so the echo is not easily resolved. The offset is varied to represent the binary message to be encoded. One offset value represents a binary one, and a second offset value represents a binary zero [6]. If only one echo was produced from the original signal, only one bit of information could be encoded. Therefore, the original signal is broken down into blocks before the encoding process begins and once the encoding process is completed, the blocks are concatenated back together to create the final signal [7]. When it is compared with the noise inducing methods, it allows for a high data transmission rate and provides superior robustness. The limitation of echo hiding technique is the low hiding capacity as it would be computationally intensive to insert echo for every bit to hide.

Phase Coding

Phase coding depends on replacing selected phase components from the original speech spectrum with hidden data. It is based on the fact that the phase components of sound are not as perceptible to the human ear as noise is. This leads to inaudible encoding in terms of the signal to perceived noise ratio (SPNR) and the secret message gets camouflaged in the audio signal, not detectable by the steganalysis methods based on SPNR [5]. Thus, phase coding addresses the disadvantages of the noise inducing methods of audio steganography [10]. In this approach, imperceptible phase modifications are achieved using controlled phase alteration of the host audio.

Spread Spectrum

The basic spread spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum using a code that is independent of actual signal [5]. So the final signal occupies bandwidth in excess of what is actually required for transmission. Two versions of SS can be used in audio steganography: the direct sequence and frequency hopping schemes [10]. In direct sequence spread spectrum, the secret message is spread out by a constant called the chip rate and then modulated with the pseudorandom signal and interleaved with the cover signal. In frequency hopping SS, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies [11]. The advantage of Spread Spectrum method is its speed in covering data; however, its drawback is that it introduces noise and distortions to the audio file.

Data embedding methods in LSB

There are several methods used for data hiding in LSB technique.

Parity Coding

In parity coding method, sample region's parity bit is used for data embedding [8]. In this case signal breaks down into separate region of samples instead of individual samples. If the secret bit to be encoded does not match with the sample region's parity bit then process flips the LSB of one of the samples in the region [9]. Therefore the sender has more of a choice in encoding the secret bit.

XORing Method

Using XORing of LSB's method performs XOR operation on the LSBs and then depending on the result of XOR operation and the message bit to be embedded, the LSB of the sample is modified or kept unchanged. Also, this approach increases the capacity of the cover audio by as much as 8 times and provides robust encryption [12].

Bit Selection

In this method the different bits in every sample is selected to hide the secret data. For this purpose the 1st two MSB bits of a sample are used for bit selection of that sample but only 1st three LSB's are used for data embedding. The merits of this technique are randomness in bits is generated to confuse the intruder [13]. If 1st two MSB's of the sample are 00, then 3rd LSB is used for data hiding and so on.

Sample Selection

In this method instead of using all the samples only few samples are used for data hiding purpose. Thus here randomness is generated in sample numbers and it is controlled by 1st three MSB's. If current sample is i, then last column indicates the next sample that will contain the secret message bit. The number of samples skipped between two consecutive secret message bits is equal to one more than the decimal value of 1st three bits [13].

Lowest Bit Coding

As the name suggests this method embeds the data in the least significant bit (LSB). This method shows how the wave data is embedded using lowest bit method. The wave data and secret data are in binary format and the low bit of wave data is replaced with the secret data one by one [10]. This method minimizes the transition and gives embedding capacity up to 12.5% of the wave file.

Variable Low Bit Coding

This method is advance version of lowest bit coding method and gives increased embedding capacity. Suppose that the range of audio data is 0 to 255 and the middle range is 128 at which sound is silent [10]. So the data can`t be embedded in the middle range so using this calculating the standard level and two thresholds 1and 2. If amplitude range is less than

http://dx.doi.org/10.15242/IIE.E1114031

threshold 1 then secret data is not embedded. If amplitude range is between threshold 1 and 2 then one bit is used for data embedding and if amplitude range is beyond threshold 2 then two bits are used for data embedding.

Average Amplitude Method

In this method the average amplitude data of surrounding audio data is used as threshold. This method shows the level of amplitude at each time. The average of an amplitude level for audio data is calculated by 10 audio data about before and after 5 audio data except for own audio data. If amplitude level is greater than average value, then 2 binary digits are Used for embedding otherwise binary digits are not used for embedding. The number of embedding binary digits is limited to 2 bits [10].

II. Proposed Method

In this proposed technique every kind of audio whether are channel or other is included. The technique proposes the hiding of data in audio samples. Every audio sample includes 16bits. First bit is either plus or minus rest of the 15bits are divided into two groups. The first division has 7bits known MSB while the other division includes 8bits known as LSB. In this way the signals are interrupted and data cannot be conveyed secure. For proper and secure conveyance the payload is increased and signals are improved.

Data Embedding

The signal value is important in embedding of data. Figure1 states that 1 bit is embedded inthe least significant bits of the sample audio the range is between 0 and 255.

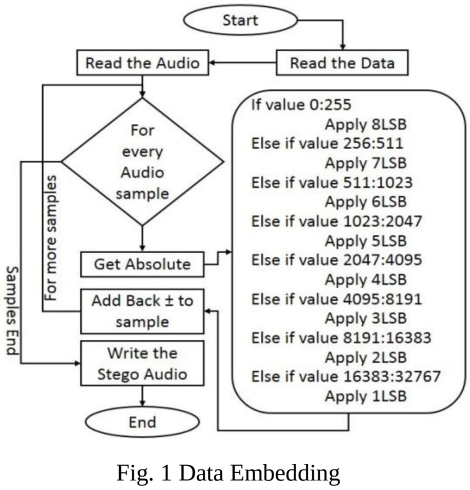

Fig. 1 Data Embedding

Similarly, 2 bits are embedded when the range is from 256 to 511, 3bits are embedded when the range is 512 to 1023, 4bits are embedded when the range is 1024 to 2047, 5bits are embedded when the range is 2048 to 4095, 6bits are embedded when the range is 4096 to 8191, 7bits are embedded when the range is 8192 to 16383, and 8 bits are added for the sample audio falling in the range 16384 to 32768.

Data extraction

Figure 2 show the flowchart for the algorithm of secret message extraction. The decoding algorithm reads the Audio Sample and decodes the bits according to the range of threshold. This procedure gives back the secret message.

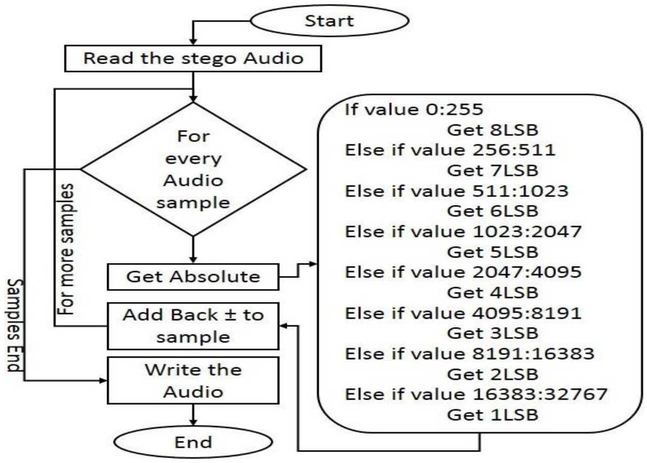

Fig. 2 Extraction of secret information

Experimental Results

For the implementation of the proposed technique, we used standard matlab audio shown in figure 3 with following specification before implementation of proposed technique.

Audio Length = 8 sec,   Original Audio Size= 142 KB

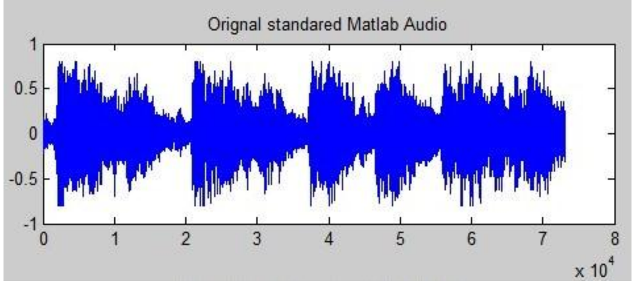

Fig. 3 Standard Matlab audio

MATLAB is used to implement the proposed technique for producing the Stego audioto represent in Figure 4.

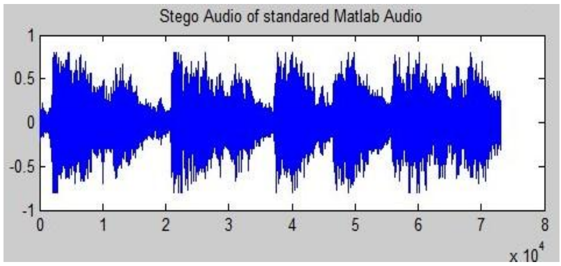

Fig. 4 Stego Audio

The quality of produced Stego audio is high and human eye cannot detect the changes between standard MATLAB audio and Stego audio. The difference between the standard audio and Stego audio is shown in figure 5.

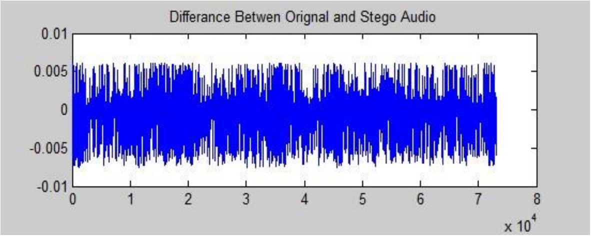

Fig. 5 difference between Stego and original audio

And results are shown in table 1.

TABLE I

STANDARD AUDIO

MSE	0.00000
RMSE	0.00092
MAE	0.00037
AD	$6.6222*10^{-5}$
MD	0.0061
NAE	0.1475
Payload	35 KB
Audio Length	8 sec
Original Audio Size	142 KB
Stego Audio Size	142 KB

Results obtained from implementation will be analyzed for the expected results and also compared with the results of existing LSB techniques. This shows that the proposed technique hides a high capacity of information in the standard audio with very minor changes in the standard audio.

III. CONCLUSION

Variable Low bit coding technique is most simple and efficient. This proposed technique does not affect the quality of the resultant audio signal and is more secure than the conventional LSB technique.This technique lowers the audio quality of Stego audio file and the embedded secret information can be recovered easily. It is a known fact that high amplitude samples run over low amplitude samples of an audio signals. Means more secret information bits can be embedded in low amplitude samples and less bits in high amplitude samples.A threshold is set to embed variable number of bits in different amplitude samples of the cover audio file.

REFERENCES

[1] J. Johnston and K. Brandenburg, 1992, "Wideband Coding Perceptual Consideration for Speech and Music". Advances in Speech Signal Processing, S. Furoi and M. Sondhi, Eds. New York: Marcel Dekker.

[2] Asad, M. ; Telecommun. Eng. Dept., Univ. of Eng. & Technol. Taxila, Rawalpindi, Pakistan ; Gilani, J. ; Khalid, A." An enhanced least significant bit modification technique for audio Steganography"

[3] Pooja P. Balgurgi, PG Student Elec. & Telecommunication department SKN College of Engineering Vadgaon Bk. Pune, India "*Intelligent Processing : An Approach of Audio Steganography*".

[4] Ishaque, M. Qudus Khan, F. Abdul Sattar, S. Investigation of Steganalysis Algorithms for Multiple Cover Media. October 2011, Ubiquitous Computing and Communication Journal. Vol 6, no 5.

[5] F.Djebbar, B.Ayady, H.K.Abed Meraimx, 2011," A view on latest audio steganography techniques", International Conference on Innovations in Information Technology.

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

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

[8] H.B.Kekre, A.Athawale, S.Rao, U.Athawale, October 2010 " Information Hiding in Audio Signals" ,International Journal of Computer Applications, (0975 – 8887)Volume 7– No.9.

[9] M.Wakiyama, Y.Hidaka, K.Nozaki, 2010, " An audio steganography by a low- bit coding method with wave files", Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processinghttp://dx.doi.org/10.1109/IIHMSP.2010.135
http://dx.doi.org/10.1109/IIHMSP.2010.135.

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

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

[12] H.B.Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale, October 2010, Information Hiding in Audio Signals, International Journal of Computer Applications (0975 – 8887) Volume 7– No.9.

[13] M.Asad, J.Gilani, A.Khalid, 2011, " An Enhanced Least Significant Bit Modification Technique for Audio Steganography", IEEE978-1-61284-941-6/111$26.00 .

Abdul Hakeem has done his Bachelor of Computer Science from Peshawar University, KPK, Pakistan in 2012 and is currently enrolled for his Master in Computer Science at the Department of Information Technology Hazara University, Pakistan. His Research interests include audio steganography, and computer Networks.

Zakir Khan has done his bechlor of computer science from Hazara University Mansehra, Pakistan 2012 and his currently enrolled for his Master in computer science at the department of information technology hazara university, Pakistan. He is a skilled programmer and his research interests include image processing, optical fiber communication and computer networks.

Mohsin Shah have been serving as Lecturer at the Department of Information Technology Hazara University Mansehra, Pakistan. He has done his B.Sc Telecommunication Engineering from University of Engineering and Technology Peshawar, Pakistan in 2007 and M.Sc. Telecommunication Engineering from University of Engineering and Technology Taxila, Pakistan in 2012. Recently he is admitted for his PhD in Optical Engineering at Beijing Institute of Technology China. He has 2 years of diversified experience in the field of cellular mobile communication systems. His research interests include Optics and Photonics, Network Security and Image Processing.

Noor ul Amin have been serving as head of the department and is Assistant Professor at the Department of Information Technology Hazara University Mansehra, Pakistan. He got his MS from Islamic University, Islamabad. He is pursuing his Ph.D. in sensor networks from the Department of Information Technology Hazara University Mansehra, Pakistan. His research interests include Sensor Networks, Network Security and Steganography.

Abdul Qadir has done his master of Computer Science from Comsats institute abbottabad, Pakistan in 2004 and is currently enrolled for his MS Computer Science at the Department of Information Technology Hazara University, Pakistan. He is a skilled programmer and his Research interests include Image processing, Cryptography and computer networks.

.

http://dx.doi.org/10.15242/IIE.E1114031