An Efficient Secure Data Hiding Algorithm Using Audio Steganography

Surbhi Tiwari[1], Krunal J. Panchal[2]

[1] Student LJIET, Ahmedabad, Gujarat, India
[2]Assistant Professor, Department of Computer Engineering, LJIET, Ahmedabad, Gujarat, India
[1]Computer Engineering,
[1]LJIET, Ahmedabad, India

Abstract: *In the current internet scenario, secure data transmission is limited due to its attack, interception and manipulation by eavesdropper. So more robust methods are required to ensure data transmission. One solution to the above problem is steganography, which is the art and science of writing message in such a way that no one can detect the existence of the hidden message. Audio steganography hide the secret message in cover audio file in an undetectable way. This paper proposes a method MAES (Modified Advance Encyption Standard) advance 3 levels LSB embedding technique with secret data. The main objective of the proposed system is to provide high audio quality, robustness, high embedded bit rate and computed using PSNR, MSE values for various audio signals.*

IndexTerms – Steganography, Audio Steganography, Least Significant Bit

I. INTRODUCTION

Due to the rapid growth of digital communication emphasizes the need of secret communication. Data security is one of the most important concerns due to the interception and manipulation by eavesdropper .So there are three common approaches use to make sure data secrecy: Cryptography, Watermarking and Steganography [8]. Cryptography may be a methodology for storing and transmitting data in encrypted form in such a way that only intended users have access.

The word steganography comes from two greek words "stegano" and "graphy". Stegano means that secret and graphy means that writing. So steganography virtually means that secret writing. Steganography, which is the art and science of writing hidden messages in such a way that nobody apart, from the sender and receiver suspects the existence of the hidden message. The primary goal of steganography is to provide a confidentiality of information, wherever data is hidden in carriers like image, text, video and audio.

Nowadays, most of the business organizations use the steganography approach by means that of communication with relevance transmission of secure data like transaction information, business dealing, etc. But, sometimes these information hiding schemes are not enough for the aforementioned confidential information. The enormous use of electronic communication and huge availability of different free data hiding software makes situation more critical. The correctness of data generally suffers by the information concealing theme because the information loss is originality throughout differing kinds of transformations [8].

To solve the above issues, the use of audio steganography is quiet successful up to certain extend as it provides a better security [11]. Data hiding in audio steganography is quiet difficult or challenging because of the sensitivity of the Human Auditory System (HAS). However, HAS tolerates common alterations in small differential ranges. For example, loud sound tends to mask out quiet sounds. These properties have lead researches to explore the utilization of audio signals as carriers to hide secret data [11].

In this paper, section 2 describes the conditions that need to be satisfied by audio steganographic technique. Section 3 describes related work for least significant method (LSB). Proposed work and experimental results is presented in section 4 and 5 respectively.

II. AUDIO STEGANOGRAPHY

Audio Steganography embeds the key message in audio file, known as cover audio and generated audio file is called as stego signal. While performing this method, following three parameters are to be maintained:

Capacity: It means the number of secret data that may be embedded among the host audio without affecting the perceptual quality of audio [8].

Transparency: It evaluates how well secret message is embedded in the cover audio. The difference between audio after hiding and audio before hiding should remain negligible [8].

Robustness: It indicates the flexibility of secret message to face up to against attacks [8].
Audio steganography is an active research area these days. Different techniques have been used to achieve the same goal:

- Least Significant Bit (LSB) Modification: Replacing least significant bits of audio signal with bits of secret message [9].
- Parity Coding: The parity coding method breaks a signal down into separate regions and encodes each bit from the secret message in the sample region's parity bit [9].
- Phase Coding: The phase of an initial audio segment is substituted with a reference phase that represents the data.
- Spread Spectrum: Secret information is spread across frequency spectrum [10].
- Echo Data Hiding: Introducing an echo to the original signal and then the data is hidden by varied three parameters of the echo: initial amplitude, decay rate, and offset [10].

III. Related Work

Authors [1] have proposed a new dictionary based text compression technique for ASCII texts for the purpose of obtaining good performance and secrecy of the text message on various document sizes. For high leveled security [2], the encrypting method is done by DNA based playfair encryption algorithm and in the second level; encrypted secret file is hidden in a randomly generated DNA sequence. In the third level the DNA sequence which is embedded with encrypted file is hidden inside an audio file using least significant bit modification technique. The main objective of this paper is to come up with an efficient method to preserve security of secret messages.

Implementing a new scheme for audio steganography [3], wherever bits of a secret message are embedded into the coefficients of a cover audio file. The main objective of this paper is to produce high audio quality, robustness and lossless recovery from the cover audio. In this paper [4] author proposed a method that uses parity of audio sample to decide on whether or not message bit is embedded in right or left channel of audio signal. XOR operation is performed between stego-key value and message bit in order to achieve robustness.

Implementing a trusted communication platform for multi- agents [6], where confidential data is hiding in the cover audio stream according to the user request and retrieves the hidden information from the stego –audio file. This system provides high availability and flexibility in this context and a more feasible way to trust the message transmission. In this paper [7], present an implementation of audio steganography using two cards of arduino due applying with success within the (LSB) technique on a pure communication channel.

IV. Proposed System

In planned technique, pre-processing is applied on secret message. In pre-processing secret message is converted into variant size of bits using Huffman coding. Then these bits are converted into hexadecimal digits. Hexadecimal digits are encrypted by using faster and less computational MAES (Modified Advanced Encryption Standard) algorithm. Generated ciphertext is converted into binary and concates this binary bits form a binary string of message that is embedded in an audio file using modified dual randomness LSB method.

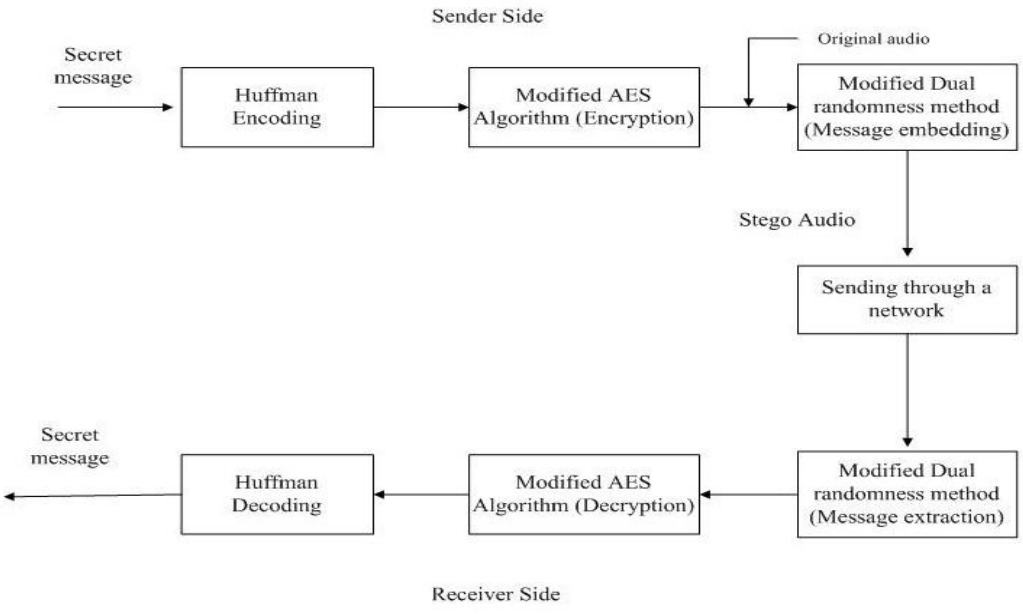


Figure 1: Proposed System

4.1 Huffman Coding:

Character coding is employed to map characters to bits and bits to characters within the reverse operation. On the opposite aspect, the secret message is within the type of characters. These characters embedded into bits before they embedded in the cover audio.

4.2 Modified Advanced Encryption Standard:

It is the advance version of AES algorithm. In MAES encryption and decryption process resembles to that of AES, in account of range of rounds, data and key-size. The main objective of the MAES is to provide less computation and higher security for information. The modify AES algorithm adjusts to produce high encryption speed.

4.3 Modified Dual randomness LSB method:

Data embedding dual randomness LSB method is given below. Secret message bits are embedded using this method.

Let the current sample i

if first 3 MSB of i =000 then
Next sample i+2
Secret message bit 4th and 1st LSBs

else if first 3 MSB of i =001 then
Next sample i+2
Secret message bit 4th and 1st LSBs

else if first 3 MSB of i =010 then
Next sample i+3
Secret message bit 3rd and 1st LSBs

else if first 3 MSB of i =011 then
Next sample i+4
Secret message bit 3rd and 1st LSBs

else if first 3 MSB of i =100 then
Next sample i+5
Secret message bit 2nd and 1st LSBs

else if first 3 MSB of i =101 then
Next sample i+6
Secret message bit 2nd and 1st LSBs

else if first 3 MSB of i = 110 then
Next sample i+7
Secret message bit 2nd and 1st LSBs

else
Next sample i+8
Secret message bit 2nd and 1st LSBs
End

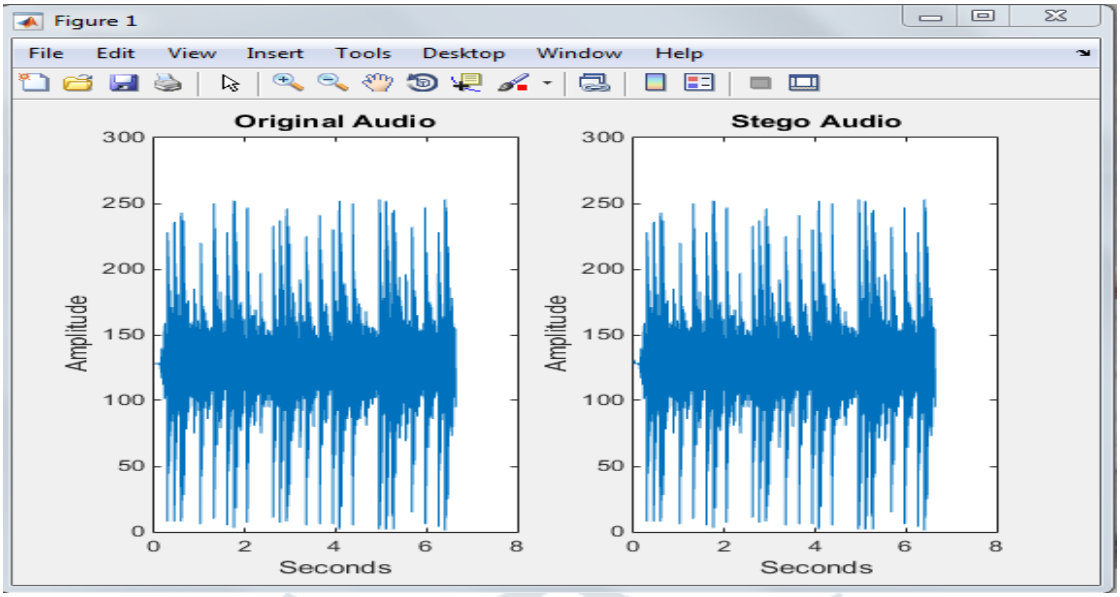
V. ALGORITHM

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 every characters of secret message into bits form by using Huffman Coding.
Step 3: Convert that bits on hexadecimal form.
Step 4: MAES Encryption Algorithm is performed on hexadecimal digits.
Step 5: Scan the audio file and convert into eight bits sample using sampling.
Step 6: Store the length of the ciphertext.
Step 7: Choose 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 randomly which is based on MSB of the selected sample.
Step 9: Convert binary audio samples into same audio format, like input audio file.

VI. EXPERIMENTAL RESULTS

The proposed scheme has been experimented with CD quality mono audio signal. The signal is sampled at a rate of 44.1 KHz with 16 bit resolution. Fig. 2 shows sample audio signal (both original and stego) involved in the experimentation. The initial audio signal is: Fig 2a – Best_EDM_Tone.wav and Stego audio signal is: Fig 2b- Stego_EDM.wav. Fig 2 shows histogram results of each original and stego audio signals.



(a) **(b)**

Figure 2: Histogram results of original and Stego audio signals

6.1 Experimental Results

Completely different sizes of audio signals are tested below this proposed system and table given below shows experimental results among PSNR and MSE parameters.

Table 4.1: Metric values of Audio Signals

Source Audio	MSE (proposed Method)	PSNR(Proposed method)
Best_EDM_Tone.wav	6.9666	79.7006
1.wav	6. 6314	82.5300
Mahadev_Theme	6.8037	74.3949

V. CONCLUSIONS

To enforce security of digital information, varied techniques are presented in recent research work. We have got seen review of techniques and analysis work has been done in Low Significant bit method along with their potentials and limitation in making certain secure communication. Low significant bit provides high capacity along with successful retrieval of information. So there is requirement of new technique that provides high capacity and robustness and overcome from noisy communication channel.

REFERENCES

[1] M.Baritha Beguma, Y.Venkataramanib "LSB Based Audio Steganography Based on Text Compression" Science direct International Conference on Communication Technology and System Design, March 2012, doi:10.1016/j.proeng.2012.01.917, pp. 703-710.

[2] Shyamasree CM, Sheena Anees "Highly secure DNA- based Audio Steganography" IEEE International Conference on Recent Trends in Information Technology (ICRTIT), July 2013, DOI- 10.1109/ICRTIT.2013.6844257 , pp. 519-524.

[3] Pratik Pathak, Arup Kr. Chattopadhyay, Amitava Nag "A New Audio Steganography Scheme based on Location Selection with Enhanced Security" IEEE International Conference on Automation, Control, Energy and Systems(ACES), Feb 2014 , DOI: 10.1109/ACES.2014.6807979, pp. 1- 4.

[4] Ashis Kumar Mandal, Mohammed Kaosar, Md. Olioul Islam, Md. Delowar Hossain "An Approach for Enhancing Message Security in Audio Steganography" IEEE International Conference Computer and Information Technology, March 2014, ISBN - 978-1-4799-3497-3/13, pp. 383- 388.

[5] 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

[6] T. Kartheeswaran, V.Senthooran, T D D L Pemadasa "Multi Agent Based Audio Steganography" IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Dec 2015, ISBN - 978- 1-4799-7849-6/15, pp. 1- 4.

[7] Mazhar Tayel, Ahmed Gamal, Hamed Shawky "A Proposed Implementation Method of an Audio Steganography Technique" IEEE International Conference on Advanced Communication Technology (ICACT), Feb 2016, ISBN - 978-89-968650-6-3, pp. 180 - 184.

[8] Jithu Vimal , Ann Mary Alex "Audio Steganography Using Dual Randomness LSB method" IEEE International Conference on Control, Instrumentation Communication and Computational Technologies(ICCCICCT), July 2014, ISBN - 978-1-4799-4190-2/14 , pp. 941 - 944.

[9] Namrata Singh "A Survey Paper on Audio Steganography and its Applications" International journal of Innovative Research in Science, Engineering and Technology, Feb 2017, DOI: 10.15680/IJIRSET.2017.0602120, pp. 2648- 2656.

[10] Navneet Kaur, Sunny Behal "Audio Steganography Techniques- A Survey" International Journal of Engineering Research and Applications, June 2014, ISBN – 2248- 9622, pp. 90- 100.

[11] 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.

[12] Https: // encrypted-tbn2.gstatic.com/ images? q=tbn: ANd9GcQ4vNaFmQDIfF6YEAvXxFypn2fv17vCZ83H- 2fdmOh5-GN9qy, time – 00:12.

[13] Https: //en.m.wikipedia.org/wiki/steganography, time – 00:12.