Robust and High Capacity Audio Steganography using Modified Dual Randomness LSB method

[1] Hinal Somani, [2] Kaushal M. Madhu
[1] Department of Computer Engineering,LJIET, Ahmedabad, Gujarat, India
[2]Assistant Professor, Department of Computer Engineering,LJIET, Ahmedabad, Gujarat, India
[1]hinal_somani93@yahoo.com, [2]kaushalmadhu.cse@gmail.com

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. A perfect audio Steganographic technique aim at embedding data in an imperceptible, robust and secure way and then extracting it by authorized people. Hence, up to date the main challenge in digital audio steganography is to obtain robust high capacity steganographic systems. 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*

1. INTRODUCTION

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 2 describes parameters that need to be satisfied by audio steganography technique and various techniques used for audio steganography. Section 3 describes related work for Least Significant Bit (LSB) method. Proposed work and experimental results is presented in Section 4 and 5 respectively

2. 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].

3. RELATED WORK

In the past few years, several techniques for data hidden in audio sequences have been presented. All of the developed techniques take benefit of the perceptual properties of the human auditory system (HAS).Genetic Algorithm based approach[8] encrypt text message using RSA encryption algorithm. Then applying proposed LSB algorithm, embed message bits to the audio bit steam (16 bit sample) in higher LSB layer positions at random (increase the robustness) to get a collection of chromosomes. Then Genetic Algorithm operators are used to get the next generation chromosomes. It provides higher level of security but increases computational complexity.

For simplification variable low-bit encoding 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 because everyone notices the existence of secret data. There is some amount of distortion introduced because message bits are embedded in first LSB layer.

In multiple LSB based technique[10], it shifts the maximum limit from 4 LSBs to 7 LSBs of audio samples for data hiding. These method checks the MSBs of the samples of cover audio and depending upon the values of MSBs of corresponding samples, the number of LSBs for data hiding is decided. In this way, multiple and variable LSBs are used for embedding secret data. These proposed methods remarkably increase the capacity for data hiding as compared to the standard LSB method without causing any noticeable perceptual distortion to the host audio signal. It suffers from increased distortion due to multiple LSB bits are used for embedding.

In paper[4] authors devised a hash function that is represented as epos=h(x,y) where epos is a simple variable, x is a message bit(0 or 1)and y is a integer value varies from 0 to 7 in value. Value of epos generates 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. Distortion due to data is embedded at higher LSB layer and additional queue is required to store the hash value.

Dynamic technique of substitution based audio steganography[7], parity of audio sample is obtained and XOR operation performed between parity position bit is and message bit. This result is stored at that parity bit position that introduce large amount of distortion that is noticeable to human ear.

Dual randomness LSB based technique proposed in paper[6] that embed message bits based on MSB of audio sample. To increase security level used cryptography technique at first level and then ciphertext is embedded within an audio sample using proposed method. All samples of audio are not used for embedding so it reduces capacity of system.
There is need of model that provides higher capacity along with transparency of audio will maintained.

4. PROPOSED SYSTEM

In proposed 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 using faster and powerful AES (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.

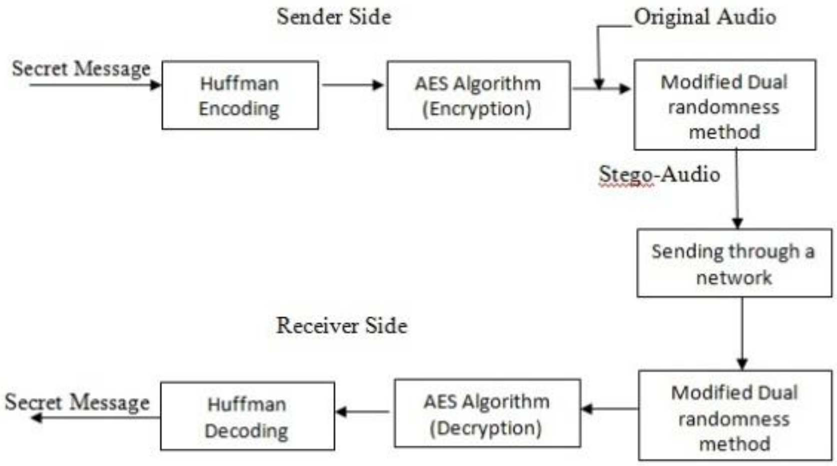

Sender Side
Original Audio
Secret Message
Huffman Encoding
AES Algorithm (Encryption)
Modified Dual randomness method
Stego-Audio
Sending through a network
Receiver Side
Secret Message
Huffman Decoding
AES Algorithm (Decryption)
Modified Dual randomness method

Fig-1. Proposed System

4.1 Huffman Coding

Character encoding is used to map characters to bits and bits to characters in the reverse operation. On the transmitter side, the secret message is in the form of characters. These characters are converted to bits before they are embedded in the cover audio. Usually a standard character encoder like the ASCII (American Standard Code for Information Interchange) encoders is used. But ASCII coder leaves a system which is more vulnerable to steganalysis than a custom defined encoder. Custom character encoders are not only less vulnerable to steganalysis but it also help in achieving compression, resulting in increased capacity.[15]

4.2 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+1
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 if first 3 MSB of i =111 then
Next sample i+8
Secret message bit 2nd and 1st LSBs
End
```

4.3 Modification Procedure

This procedure describes how the modification of original amplitude value done after the replacing 4th or 3rd LSBs of amplitude of audio signal with the bit of the character.
Adjustment Algorithm has three cases: a_i bit can be 4th LSB or 3rd LSB based on modifies dual randomness LSB method.

1. The 4th or 3rd LSB of sample amplitude is modified from 0 to 1 then perform,
Case 1: If a_{i-1}=1 and a_{i+1}=1 then,
Set all the bits (a_{i-1}, a_{i-2}, …, a_0) to the right of the a_i (i.e. towards LSB) to 0.
Case 2: If a_{i-1}=1 and a_{i+1}=0
Set all the bits (a_{i-1}, a_{i-2}, …, a_0) to the right of the bit a_i (i.e. towards LSB) to 0.
Case 3: If a_{i-1}=0 and a_{i+1}=1
Set all the bits (a_{i-1}, a_{i-2}, …, a_0) to the right of the bit (a_i)(i.e. towards LSB) to 1 and set bit (ai+1)to the 0.
Case 4: If a_{i-1}=0 and a_{i+1}=0
Set all the bits (a_{i-1}, a_{i-2}, …, a_0) to the right of the bit (a_i)(i.e. towards LSB) to 1 and then set all the bits to the left of the bit (a_i) (i.e. towards the MSB) with value 0 to 1 until a 1 is encountered. If a 1 is encountered, set it to 0 and stop the process.

2. The 4th or 3rd LSB of sample amplitude is modified from 1 to 0 then perform,
Case 1: If a_{i-1}=0 and a_{i+1}=0 then,
Set all the bits (a_{i-1}, a_{i-2}, …, a_0) to the right of the ai (i.e. towards LSB) to 1
Case 2: If a_{i-1}=0 and a_{i+1}=1
Set all the bits (a_{i-1}, a_{i-2}, …, a_0) to the right of the bit ai (i.e. towards LSB) to 1
Case 3: If a_{i-1}=1and a_{i+1}=0
Set all the bits (a_{i-1}, a_{i-2}, …, a_0) to the right of the bit (ai)(i.e. towards LSB) to 0 and set bit (ai+1)to the 1.
Case 4: If a_{i-1}=1 and a_{i+1}=1
Set all the bits (a_{i-1}, a_{i-2}, …, a_0) to the right of the bit (ai)(i.e. towards LSB) to 0 and then set all the bits to the left of the bit (a_i) (i.e. towards the MSB) with value 1 to 0 until a 0 is encountered. If 1 is encountered, set it to 1 and stop the process.

3. The 4th or 3rd LSB remain the same as original i.e. we place 1 in place of 1 or 0 in place of 0.
No change at all that means if the bit which we want to place at the 4th or 3rd LSB position of the amplitude is same with the 4th or 3rd LSB of the original amplitude then the original amplitude value become unchanged i.e. 1 is replaced with 1 or 0 is replaced with 0.

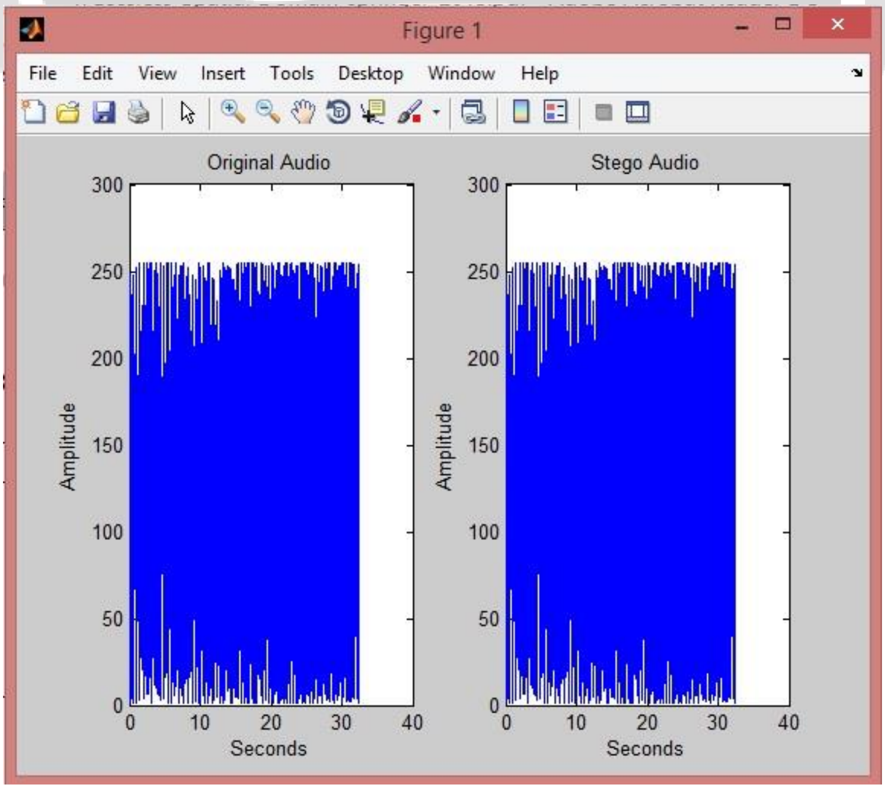
5. ALGORITHM

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 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 using modified dual randomness method and modify other bits of audio sample using modification procedure in order to maintain transparency.
Step 9: Convert the binary audio samples into same audio format, such as the input audio file.

6. 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 original audio signal is: Fig 2a – Clock_mantle.wav and Stego audio signal is: Fig 2b- Stego.wav. Fig 2 shows histogram results of both original and stego audio signals.



(a) (b)

Fig 2- Histogram results of original and Stego audio signals

Experimental Parameters:

Different size of audio are tested under this proposed system and table given below shows experimental results among PSNR and MSE parameters.

Table 1. Metric values of Audio signals in LASSD

Source Audio	MSE(Proposed Method)	PSNR(Proposed Mehod)
Clock_mantle	2.0415	64.1778
1.wav	2.0678	65.8907
Rec1.wav	2.3890	62.6523

7. CONCLUSIONS

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. This is achieved by embedding multiple bits in selected sample randomly and appropriate modification will be performed to reduce the distortion and increases robustness.

9. 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