Audio Steganography Using Modified LSB Method

Jithu Vimal[1], Ann Mary Alex[2]
[1] *PG Scholar, Dept.of Electronics and Communication Engineering, Mar Baselios College of Engg & Technology, Trivandrum, India.*
[2] *Assistant Professor, Dept. of Electronics and Communication Engineering, Mar Baselios College of Engg & Technology, Trivandrum, India.*
Email: jithulmc@gmail.com[1] , amyl.alex@gmail.com[2]

Abstract-: In the current internet scenario, secure data transmission is limited due to its attack made on data communication. So more robust methods are required to ensure secure data transmission. One solution to the above problem is Steganography. Audio steganography is concerned with hiding information in a cover (host) audio signal in an imperceptible way. Hidden information is retrieved from the cover audio using a key similar to the one that was employed during the hiding phase. Least Significant Bit (LSB) modification technique is the most simple and efficient technique used for audio steganography. But conventional LSB technique have poor interface, difficult to understand and valid only for certain audio formats with restricted message size. The objective is to design an audio steganography scheme which is used to hide data in an audio file in such a way that the data hiding point or sample point is randomly selected so that with every new embedding process the position of sample point changes and thereby increasing the confidentiality of the secret message.

Index Terms- Steganography; Audio Steganography; LSB technique

1. INTRODUCTION

In today's fast growing demand of internet applications secure data transmission is very important. Techniques such as cryptography are being used on a large scale for transmitting information secretly. Steganography is a new approach of providing secure data transmission. The term steganography is derived from two greek words, "stegano" means "secret" and "graphy" means "writing". So steganography literally means secret writing. Steganography is the art and science of writing hidden messages in such a way that only the sender and intended recipient suspects the existence of the message.

Audio Steganography hides the secret message in an audio signal called cover audio. Once the secret message is embedded in the cover audio, the resulting message is called stego message and stego message is transmitted to the receiver side.

For any audio steganographic technique to be implementable it needs to satisfy three conditions [1]:

Capacity means the amount of secret information that can be embedded within the host message

Transparency evaluates how well a secret message is embedded in the cover audio

Robustness measures the ability of secret message to withstand against attacks

Section 2 describes the related work for Least Significant Bit (LSB) method. An audio steganographic system is briefed in section 3. Section 4 presents the system architecture. Experimental Results and conclusions are presented in section 5 and 6 respectively.

2. RELATED WORK

Audio steganography is an active research area these days.

Different techniques have been used to achieve the same goals. One of the earliest technique is LSB modification [2].

In LSB method consecutive LSB's in each sample of cover audio is replaced with secret message bit. LSB method is very easy to implement but have low robustness. However, conventionally single bit is being used, but changing more than one bit in a sample has no differentiable change in the properties of the host message [3]. This increases the capacity of the technique but might also increase the amount of noise in the stego message [4].

In [5], an audio steganographic system that provides improved security is proposed. 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.

In [6] the problems faced by substitution technique and solution to the problems are discussed. The main problem is low robustness against attacks. In conventional LSB method secret message is embedded in the least significant bit. This method is more vulnerable to attack. So by embedding message in bits other than LSB more security can be achieved. More robustness can be achieved if message is embedded into deeper bits. But the problem is that as one move into the MSBs the host audio signal gets

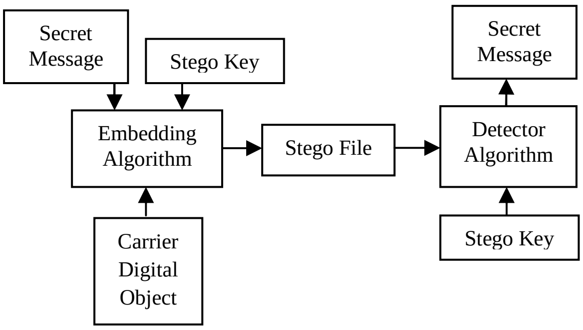

Fig 1. Steganographic System

altered. This problem can be solved by an intelligent algorithm which embeds the message bits in the MSB and alter other bits to decrease the error.

3. BLOCK DIAGRAM

The basic block diagram of a steganographic system is shown in Fig 1. The secret message to be transmitted is hidden inside a cover file. Cover file could be images, videos or audio. A stego key is also used to provide security. Using a suitable embedding algorithm secret message is embedded into the carrier object. The resultant file is called stego file and this stego file is transmitted to the receiver side. At the receiver side stego file is decoded using the stego key to extract the secret message. In the case of an audio steganographic system cover file is an audio file.

4. SYSTEM ARCHITECTURE

The system architecture consists of two different layers to fight against steganalysis; character encoding and modified LSB method. As shown in Fig 2, the message transmitted by Bob will pass through character encoding and modified LSB method layers before it is transmitted over the network. On the receiver side, the same operations are performed but in reverse order. However, the capacity of a steganographic technique is also important; the system architecture focuses more on security of secret messages which are related to transparency and robustness parameters of the steganographic technique

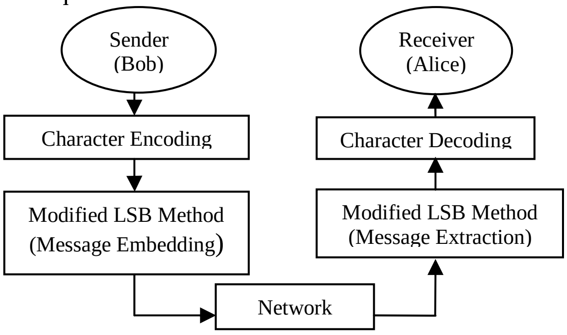
Sender (Bob)
Character Encoding
Modified LSB Method (Message Embedding)
Network
Receiver (Alice)
Character Decoding
Modified LSB Method (Message Extraction)

Fig 2. System Architecture

4.1. *Character encoding*

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. A possible custom character encoding is Huffman coding. A Huffman character encoder is proposed by Dr. David A. Huffman in 1952. Here the Code word lengths are no longer fixed like ASCII; Code word lengths vary and will be shorter for the more frequently used characters. Huffman coding is a lossless coding scheme with an efficient compression ratio. A codeword is assigned to all possible characters that can occur in the secret message [7].

4.2. *Modified LSB method*

The conventional LSB method is quite vulnerable to steganalysis. It embeds the secret message bits in fixed LSBs and any intruder who detects bit modification pattern can easily retrieve the secret message. In an 8 bits sample of a cover audio, changing the first, second or third LSB of any sample of the audio doesn't result in a detectable change, but the fourth LSB change becomes detectable Therefore, one or multiple bits from three LSBs can be used to embed a secret message.

Modified LSB Method proceeds in two steps: bit selection and sample selection. Since any of the three LSBs can be used to hide the secret message bit, every sample used different LSB to hide the secret message bit. LSB selection is done by making use of first two MSBs of the same sample. Table 1 shows the bit selection mapping.

Table 1. Bit Selection Mapping

1st MSB	2nd MSB	Secret Message Bit
0	0	1st LSB
0	1	1st LSB
1	0	2nd LSB
1	1	3rd LSB

Sample selection is done to provide more randomness by randomly selecting the samples. Every samples of the cover audio will not contain the secret message bit. Randomness is controlled by selecting the first three MSBs of the selected sample. Table 2 shows the sample selection mapping. Let the first secret message bit is embedded in sample i, then the sample containing the next secret message bit depends on first three MSBs of sample i [8].

Table 2. Sample Selection Mapping

1st MSB	2nd MSB	3rd MSB	Sample containing next secret message bit
0	0	0	i+8
0	0	1	i+7
0	1	0	i+6
0	1	1	i+5
1	0	0	i+4
1	0	1	i+3
1	1	0	i+2
1	1	1	i+1

5. RESULTS AND DISCUSSION

The objective is to design an audio steganographic system that provides more security by introducing randomness. Here randomness is achieved in two phases: one by random bit selection and another by random sample selection. The text message to be transmitted is embedded in an audio file and that stego audio file is transmitted to the receiver. While embedding text message in an audio file, the structure of input audio file must be preserved. If the audio structure has changed then the unintended recipient can detect the existence of communication. Fig 4 and Fig 5 shows the audio before steganography and after steganography respectively.

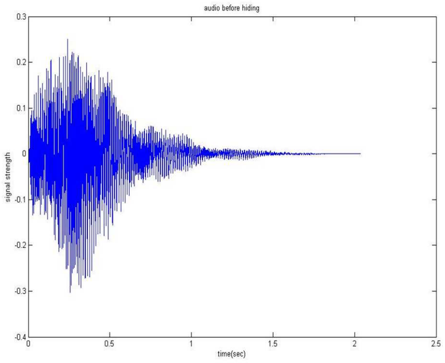

Fig 4. Audio before Steganography

Size of audio file=175 KB
Length=2 seconds
Secret Message is ‘india is my country’
Size of secret message=19*8=152 bytes

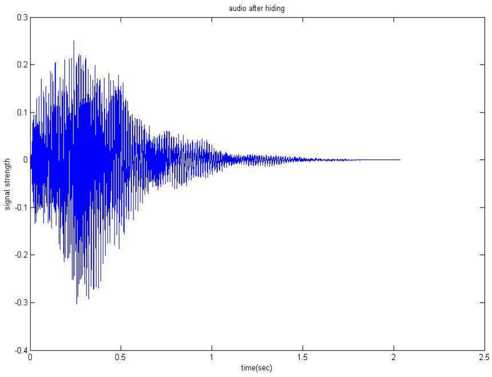

Fig 5. Audio after Steganography

6. CONCLUSIONS

In this paper an approach to increase the confidentiality of secret message is proposed. As compared to conventional LSB method the proposed method embeds the data in variable LSBs depending on the MSBs of cover audio samples. Also there is an increase in capacity due to the use of Huffman coding. Inorder to provide more capacity multiple bits of the selected samples can be used to hide the secret message. This can be solved in future work

ACKNOWLEDGEMENTS

We would like to thank the almighty for giving us the strength to work on this subject and coming up with this paper. We are grateful to our families for supporting us and praying for us. We would like to express our gratitude towards the professors of Mar Baselios College of Engineering and Technology for their valuable guidance. We are also thankful to all those who directly or indirectly helped us in making this paper a reality.

REFERENCES

[1] S.S. Divya, M. Ram Mohan Reddy, “Hiding text in audio using multiple LSB steganography and provide security using cryptography”, International journal of Scientific and Technology Research,vol. 1, issue 6, july 2012 .

[2] Walter Bender, Daniel Gruhl, Norishige Morimoto, Anthony Lu, “Techniques for Data Hiding”, IBM Systems Journal, vol. 35, pages: 313-316.

[3] Nedeljko cvejic, Tapio Seppanen, “Increasing the capacity of LSB-based audio steganography”, 2002 IEEE Workshop on Multimedia Signal Processing, pages: 336-338.

[4] Kaliappan Gopalan, Qidong Shi, “Audio Steganography Using Bit Modification- A Tradeoff on Perceptability and Data Robustness for Large Payload Audio Embedding”, 19th

International Conference on Computer Communications and Networks, pages: 1-6.

[5] Lovey Rana, Saikat Banerjee, “Dual Layer Randomization in Audio Steganography Using Random Byte Position Encoding” , International Journal of Engineering and Innovative Technology, Volume 2, Issue 8, February 2013

[6] Mazdak Zamani *et.al* , “A Secure Audio Steganography Approach”, International Conference for Internet Technology and Secured Transactions 2009.

[7] Muhammad Asad, “Text Steganography Using Huffman Coding”, International Conference on Intelligent and Information Technology 2010, Volume: 1, Pages: 445 - 447.

[8] Muhammad Asad, Junaid Gilani ,Adnan Khalid, “ An enhanced least Significant bit modification technique for audio steganography”, 2011 International conference on Computer Networks and Information Technology, pp. 143-147