International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 4, April - 2013

LSB Technique And Its Variations Used In Audio Steganography: A Survey

Jyoti Bah l[1], Dr. R. Ramakishore [2]

ABSTRACT

Steganography is an art of hiding information in such a manner so that no one other than the intended recipient knows the existence of the hidden information as message. It is an approach to secret communication where no one can suspect even the existence of the message. There's a cover object which is transmitted, hidden message (image, audio, video, text etc.) is embedded into it. The cover object after embedding of secret message is now named as stego object. The transmission is possible in spite of the various attacks. Audio Steganography is one kind of steganography in which hidden message is embedded into the audio file.

The basic idea of this paper is to present LSB (Least Significant Bit) technique of audio steganography and its variations, so as to achieve high security, high data rate and robustness. The methods are briefly explained followed by comparative study. The survey provides information about the existing methods, the methods are briefly described followed by the comparative and collective discussions, the paper gives scope of their improvement, helpful enough to explore new ideas for more efficient evaluation techniques.

KEYWORDS
Steganography, audio, LBS, Data Hiding

1. INTRODUCTION

In the current scenario, Internet holds a vast space in the communication field. Communication is easy, fast and effective but at the same time it is highly unsafe being suspectible to attacks. Security is one of the main concerns in case of hiding the exchange of data [2].

Eq. (1) provides description of steganographic process [1] as:

Cover_medium + hidden_data + stego_key = stego_medium …….. (1)

Here, cover_medium is the object (any file, audio, video, image, text etc.) in which we hide the information, followed by the encryption using stego_key. The resulting object is the stego_medium or stego file.

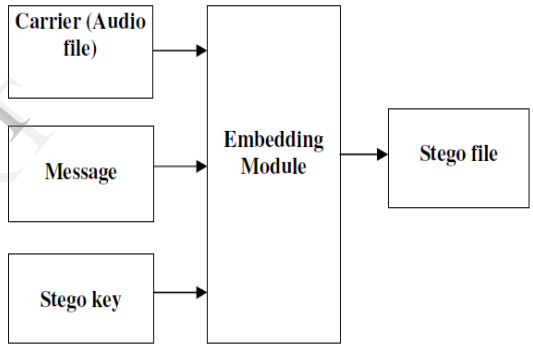

Fig 1.1: Audio Steganographic Model [7]

Every steganography technique has to satisfy two basic requirements. First one is transparency ie. Cover object (object not containing any additional data) and stego object (object containing secret message) must be perceptually indiscernible. The second constraint is high data rate of the embedded information. Steganography maintains this discipline by not only hiding the information but also keeping the existence of information a secret.

Steganographic algorithms are characterized by certain properties. Few of them are Transparency, Capacity and Robustness [8].

Transparency: Both cover object and stego object are indistinguishable.

Data Rate (Capacity): It refers to amount of information that a data hiding scheme can be successfully embedded without introducing perceptual distortion.

Robustness: It measures the ability of the embedded data due to signal intentional and unintentional attacks.

NEED FOR STEGANOGRAPHY

(i) Organizations and Individuals look for Steganography to avoid suspicion and provide secret privacy.

(ii) In today's world, with computer development e- communication is spreading at a vast pace and so is the demand of steganography to provide data hiding in terms of text, audio, video, images etc.

RELATED WORK

There have been various techniques for hiding information in audio in a manner such that it is easy to transmit audio, video as hidden messages. One of the most common approaches includes LSB (Least Significant Bit). In LSB coding, the cover is of 8 bytes.

LSB Coding:

The bit at units place is the LSB. Being the rightmost bit, it tells whether it is even or odd. The least significant bit in bytes of cover file is used to hide the secret message.

For example [7], to hide letter "a" (ASCII value 97: binary equivalent 01100001)

10010010
01010011
10011011
11010010
10001010
00000010
01110010
00101011

The decoding process recovers the message by reading eight LSB's 01100001of letter "a". If the bit to be replaced in cover byte is same as the LSB to be replaced with then, the bit doesn't change and this helps in minimizing quality degradation.

Fig 1.1 illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSB method [7]. Here the secret information is 'HEY' and the cover file is audio file. HEY is to be embedded inside the audio file. First the secret information 'HEY' and the audio file are converted into bit stream. The least significant column of the audio file is replaced by the bit stream of secret information 'HEY'. The resulting file after embedding secret information 'HEY' is called Stego-file.

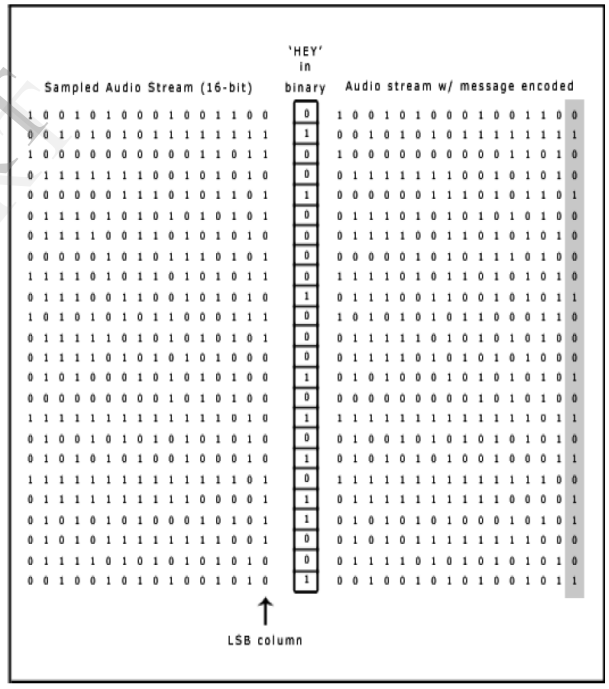

Fig. 1.1: LSB coding of text "HEY" in an audio file [7].

The computational complexity of LSB is low with high channel bit rate but it is less robust with low data rate.

To overcome these drawbacks there are few variations in LSB technique.

2. VARIATIONS IN LSB TECHNIQUE

2.1 Parity

Jayaram P [9] suggested the following method in which LSB's of the cover audio is not changed directly instead it is decided whether to change LSB or not on the basis of the cover samples.

If the message bit is 0, then LSB of the sample is either changed/unaffected such that the parity of the sample after embedding message bit is even. Similarly, If the message bit is 1, then LSB of the sample is either changed/unaffected such that the parity of the sample after embedding message bit is odd [9].

2.2 XORing of LSB's

The another method suggested by Jayaram P [9] is based upon XOR method. In this method, XOR operation is performed on the LSB and the bit next to LSB.

If the message bit is 0, then LSB bit is changed/ unaffected such that XORing of LSB and bit next to LSB is 0. Similarly, If the message bit is 1, then LSB bit is changed/unaffected such that XORing of LSB and bit next to LSB is 1.

LSB	Bit next to LSB	XOR	Action if message bit is 0	Action if message bit is 1
0	0	0	No Change	Flip LSB
0	1	1	Flip LSB	No Change
1	0	1	Flip LSB	No Change
1	1	0	No Change	Flip LSB

Table 1: Procedure for finding LSB on the basis of XORing method [9].

The advantage of this method is that it is easy to implement, lesser complexity and computationally inexpensive.

2.3 Embedding at 4th and 5th LSB layers

Using LSB directly introduces distortion to the cover audio at the time of embedding. To make steganography more secure, embedding at the 4th and 5th bit LSB of the original audio file with same data and different data reduces distortion of the host audio. The above written concept was proposed by Padmashree G [10].

Algorithm: Embedding of text file inside cover audio file at sender side [10]:

Step1: Select the audio file for embedding the secret message.

Step2: Play the audio file so that it sounds clear to the end user.

Step3: Select the text file containing the secret message.

Step4: Encrypt the text file contents.

Step5: Compare the two files, text file and audio file size. If text file size > audio file contents Error message is displayed. Else Embed the secret message in the audio file in the 4th and 5th LSB bit of every sample.

Step6: Display of message to user of the new audio file created after embedding secret message.

Algorithm for extracting the embedded text from audio file at receiver [10]:

Step 1: Select the new audio file for extracting the secret message.

Step 2: Extract the secret message from the audio file from the 4th and 5th LSB bit of every sample.

Step3: If secret message is present in the cover audio file Then Display message to end user after extracting message. Else Display that no hidden data is present in the text.

Step4: Decrypt the secret message.

Step5: Display message to end user after decrypting the message.

2.4 GENETIC ALGORITHM

Bankar Priyanka [11] proposed a solution which provides security and robustness by performing RSA encryption on secret message to convert plain text into cipher text. After embedding the message into audio file, Genetic Algorithm based LSB algorithm is applied. Finally, public key, private key and LSB layer value is applied to the stego file.

RSA Encryption is done first to read the file and to store every cipher character in ciphertext file (T').

The Algorithm works in two phases [11]. The first phase encrypts the data file before embedding and in the second phase security is provided. The encryption is done using any asymmetric public key algorithm. These bits are then inserted randomly at higher LSB layers of the cover audio. The algorithm performs crossover and mutation over bits.

For recovering of message the cipher text is extracted from stego file using public and private key, and then by using RSA decryption algorithm plain text is recovered.

3. PERFORMANCE EVALUATION BETWEEN PARITY CONSIDERATION AND USING LSB DIRECTLY

The data travels from sender's end to the receiver's end. During this communication the secret message can be lost or might get corrupted. The purpose is to receive the message without noise and distortion. Therefore, preservation of the originality and the original dimensions of the message without any noise is the key element. This objective is achieved with the correct and effective algorithm. There are various algorithms to perform the task but we have to evaluate whether the algorithm preserves the originality. For Evaluation an image is taken as an input, LSB technique with its parity variation is applied and on extracting the embedded message is found to be free of noise.

Figure 3.1[9] illustrates the performance of the LSB technique with parity consideration.

Fig 3.1 (a): Original Secret Message

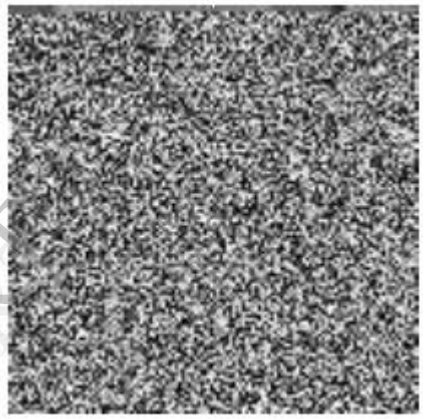

Fig 3.1 (b): Retrieved secret message image using LSB directly which includes noise.

Fig 3.1 (c): Retrieved secret message from cover audio using Parity.

CONCLUSION

In this paper we have seen the importance of Steganography in today's world. Audio Steganography is the field of embedding secret message inside audio file. LSB technique when combined with various other methods like encryption and decryption using cryptography provides one of the effective and highly secured communications.

1. LSB method when used directly introduces distortion in the audio cover file.
2. The parity method suggests that it is an efficient method with high SNR but it has high data rate.
3. The XORing method shows that using more uwe can increase the capacity of the cover audio by using more than just the single LSB layer for data embedding but the disadvantage is that it can be used only for single audio format .wav.
4. The method of embedding text in 4^{th} and 5^{th} layers with same and different data along with encryption and decryption of the secret message using public key cryptographic algorithm is an efficient method with lesser noise distortion and high SNR and PSNR ratio.
5. LSB when combined with GA supports various file formats like .aiff, .wav, .AU. Message length is increased by this method upto 1000 characters. Although, the computational complexity of this method is high.

FUTURE SCOPE

The results show that even with the variations made to directly usage of LSB, furthermore improvement can be done to get highly secured retrieval of data, with more robustness, higher data rate, full recovery of cover audio and which can work on various audio formats.

REFERENCES

[1] Gary c Kessler,"Steganography: Hiding Data within Data", September 2001.

[2] C. Parthasarathy and Dr. S.K. Srivatsa,"Increased Robustness of LSB Audio Steganography by reduced distortion of LSB coding.

[3] Dr. H.B. Kekre and A.A. Archana,"Information Hiding using LSB technique with increased capacity", International Journal of Cryptography and Security, Vol.1, No. 2, October 2008

[4] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

[5] Audio Steganography: A Survey on Recent Approaches, Masond Nosrati, Ronak Karimi, Mehdi Harii.

[6] Audio Steganography using LSB, Bankar Priyanka R, Katariya Vrushrabh R, Patil Komal K, Shashikant M. Pingle.

[7] Information Hiding using Audio Steganography – A Survey, Jayaram P, Ranganatha HR, Anupama H S

[8] Hiding Text in Audio using Multiple LSB Steganography and provide Security using Cryptography, S.S. Divya, M. Ram Mohan Reddy, July 2012.

[9] Information Hiding in Audio Signals, H.B. Kekre, Archana Athawale, Swarnalata Rao, Uttara Athawale.

[10] Audio Steganography and Cryptography: Using LSB Algorithm at 4^{th} and 5^{th} LSB Layers.

[11] Audio Steganography using LSB, Bankar Priyanka R. Katariya Vrushabh R. Patil Komal K. Shashikant M. Pingle.

[12] Audio Steganography using GA, 2010, Krishna Bhowal, Anindya Jyoti Pal, Geetam S. Tomar.

[13] A Genetic Algorithm Based Approach for Audio Steganography, Zamani M., Manaf A. A., Ahmad R.B., Zeki A.M., Abdullah S.

[14] MP3STEGO: Hiding text in MP3 files, The Sans Institute InfoSec Reading Room.

[15] Dr.H.B.Kekre and A.A.Archana, "Information hiding using LSB technique with increased capacity",

International Journal of Cryptography and Security, vol. 1, No.2, October 2008.

[16] N. Cvejic, T. Seppanen, "Increasing Robustness of LSB Audio Steganography using a novel embedding method", in Proc. IEEE Int. Conf Info. tech.: Coding and Computing, Vol. 2, pp.533-537, April 2004.

[17] K. Geetha and P.Vanitha Muthu, "Implementation of ETAS (Embedding Text in Audio Signal) Model to Ensure Secrecy" (IJCSE) International Journal on Computer Science and Engineering, Vol. 02, No. 04, 2010, 1308-1313.

[18] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, "A Tutorial Review on Steganography".

[19] Ajay.B.Gadicha1, "Audio Wave Steganography", and International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-1, Issue-5, and November 2011.

[20] Cambridge,UK, May30-June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.1-7 Benderr, D. Gruhl, N. Morimoto and A.Lu, "Techniques for Data Hiding", IBM System‟s Journal, Volume 35, Issue 3 and 4, 1996, p.p., 313-336.

[21] Lee.Y.K. And Chen L.H. "High Capacity Image Steganographic Model", IEEE proceedings vision, Image And Signal Processing, 2000, 288-294.

[22] Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe. "The Real-Time Steganography Based on Audio-to-Audio Data Bit Stream",Technical report of IEICE, ISEC, vol.106 pp.15-22, September 2006.

[23] Nedeljko Cvejic, Tapio Seppben "Increasing the capacity of LSB-based audio steganography " FIN-90014 University of Oulu, Finland ,2002.

[24] Bandyopadhay, S. K.; Datta, B.; Dutta, K., "Information Hiding in Higher LSB Layer in an Audio Image", International Journal of Advanced Research in Computer Science, Vol. 2, No. 3, 2011.

[25] Bandyopadhyay S. K.; Datta B.; Chakrabarty D.; Majumdar A.; Bhowmick S.; Ghosh N., "Hide Text within an Audio Clip", Journal of Current Computer Science and Technology, Vol. 1, Issue 6, 2011, pp. 305-315.