International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 1, Issue 2, July – August 2012 ISSN 2278-6856

Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique

Prof. Samir Kumar Bandyopadhyay1 and Barnali Gupta Banik2

[1]Professor, Dept. of Computer Science & Engineering, University of Calcutta,
92 A.P.C. Road, Kolkata – 700009, India

[2]Asst. Prof., Dept. of Computer Science & Engineering, St. Thomas' College of Engineering & Technology,
4 D.H. Road, Khidderpore, Kolkata – 700023, India

Abstract: ***Steganography is a very well-known method of information security through information hiding. Here two different steganographic methods have been used instead of using one steganographic method. This has been done with a layering approach. This method is named as multi-level steganography. Multi-Level Steganography has advantage of difficult decoding and sending two secret message through a single cover object.***

Keywords: Information security, Information hiding, Steganography, Multi-level-steganography Model, Decoy object

1. INTRODUCTION

Steganography can be applied to different objects like text, picture, image, audio or video. This objects called cover object or carrier object of the steganographic method. The secret message can also be of types like text, picture, image, audio or video. These objects are called message object. After application of steganographic method the produced output file is called stego-object. These cover object, message object and stego object are very well known to the people who are working on Steganography. Dr. Al Najjar first introduced [1] another type of object which is called intermediate object or decoy object. This decoy object is output of first level steganographic method and input of second level steganographic method. Decoy object actually nullifies the requirement of two different cover objects for sending two different secret messages.

2. LITERATURE SURVEY

2.1 Least Significant Bit (LSB) Coding

One of the earliest techniques studied in the information hiding of digital audio (as well as other media types) is Least Significant Bit modification coding technique. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message [2].

Advantage: It is the simplest way to embed information in a digital audio file. It allows large amount of data to be concealed within an audio file, use of only one LSB of the host audio sample gives a capacity equivalent to the sampling rate which could vary from 8 kbps to 44.1 kbps (all samples used) [3]. This method is more widely used as modifications to LSBs usually not create audible changes to the sounds.

Disadvantage: It has considerably low robustness against attacks.

2.2 Parity Encoding

Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit.

If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region [5].

Advantage: The sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive manner.

Disadvantage: This method like LSB coding is not robust in nature.

3. PROPOSED METHOD

3.1 Multilevel Steganography

Here two secret messages rather than one can be transmitted with a single cover file. Layering approach gives opportunity to do so. In this paper two layered approach has been presented. At the first level, cover file (C) can be embedded with the first secret message S1. Assuming the stego file as C1 which is cover file for next level where secret message can be denoted as S2. Now the final stego file created as C12. So C12 holds both S1 and S2.

Two levels of steganography can be identified as layer 1 and layer 2. At layer 1 LSB modification technique and at layer 2 parity encoding technique has been used.

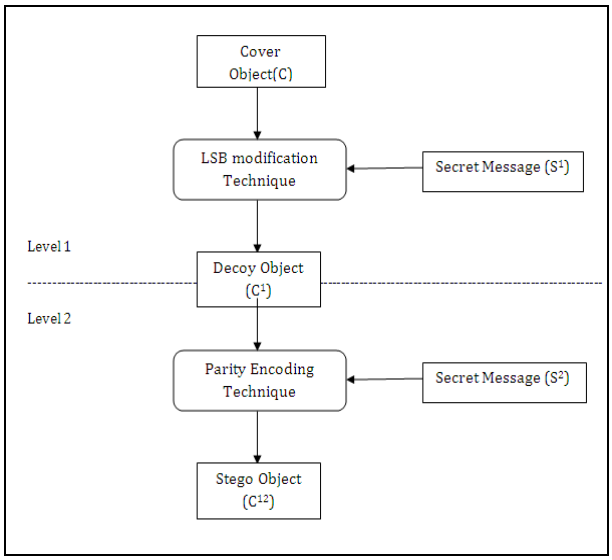


Figure 1 Flow-chart for proposed method

3.2 LSB Modification

3.2.1 Method

The LSB modification technique has been implemented with the following algorithm:

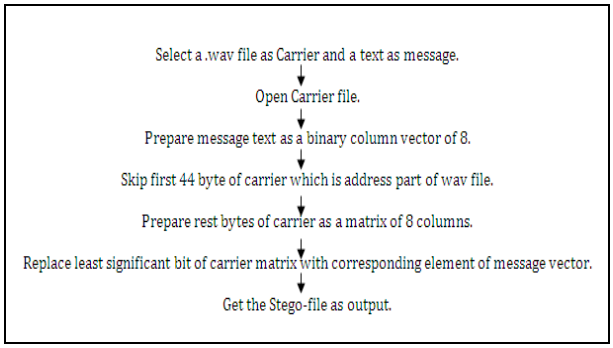
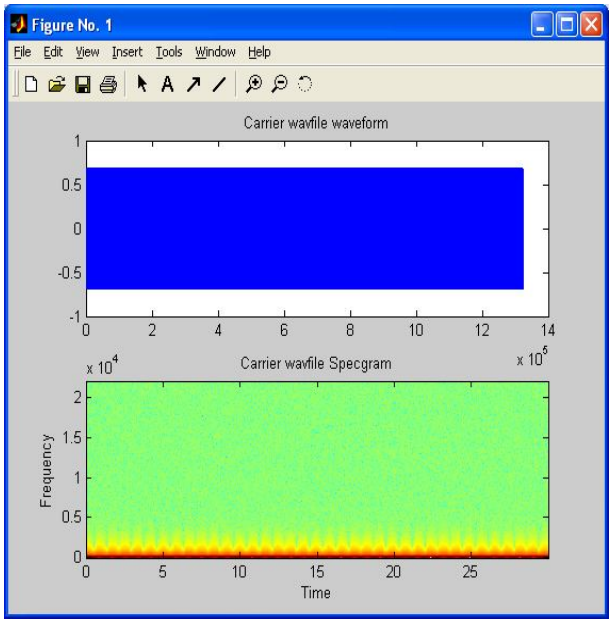


Figure 2 Flow-chart of LSB modification Technique

3.2.2 Result



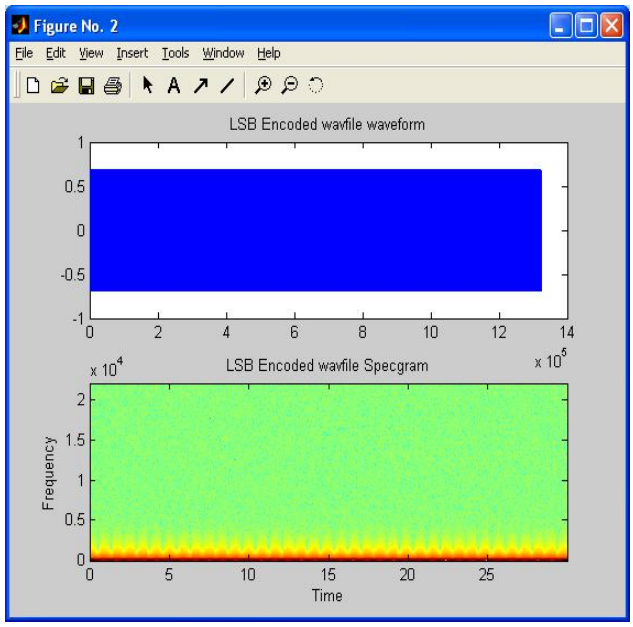


Figure 3 Result of LSB modification technique

It is observed that stego-file hasn't been audibly modified. Also the graphical representation also shows that there is reasonable no change between input carrier file and output stego file.

3.3 Parity Encoding

3.3.1 Method

The parity encoding has been implemented by breaking the data part of the wav file into number of regions. Each region includes same number elements of secret message text. Then parity flag of each region calculated. If it does not match with the message bit then we change the last bit of that region with the message bit.

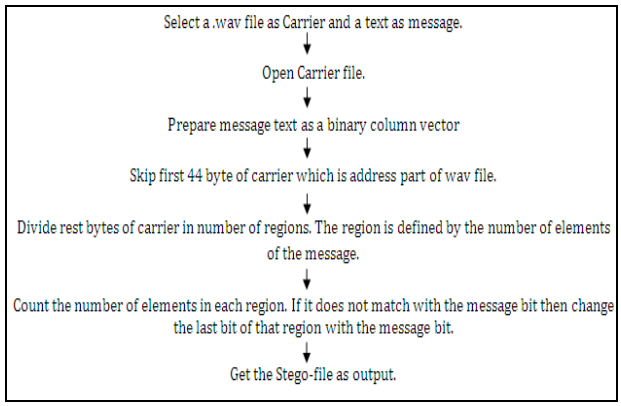


Figure 4 Flow-chart of Parity Encoding Technique

3.3.2 Result

Stego object hasn't been audibly modified. Also after decoding, secret message object can be retrieved.

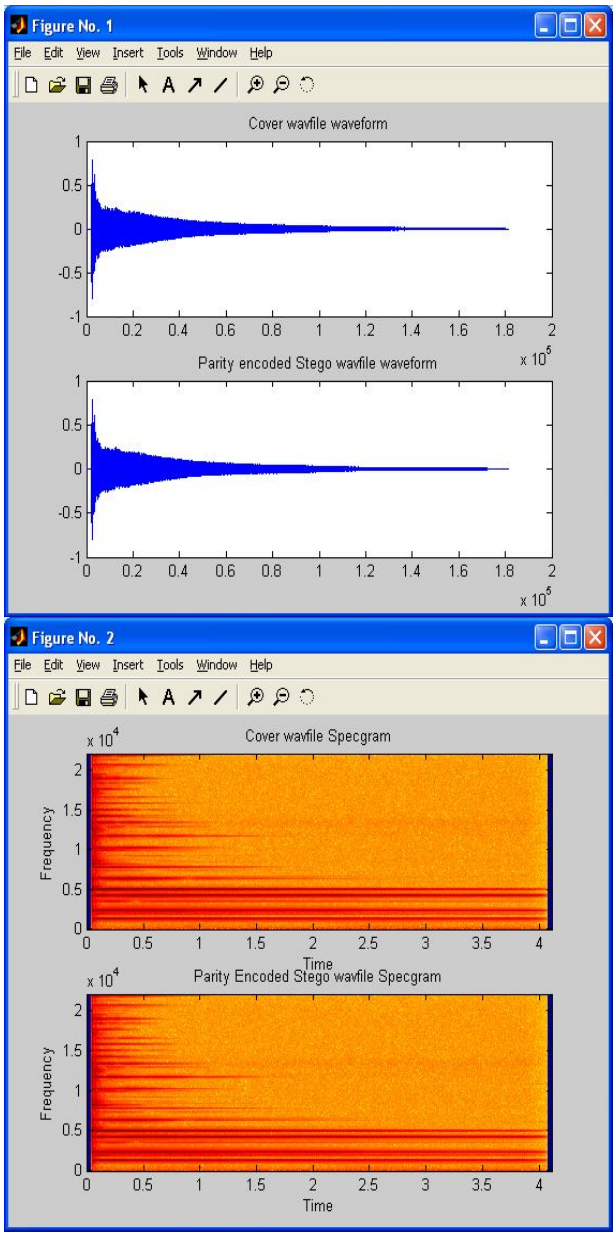


Figure 5 Result of Parity Encoding Technique

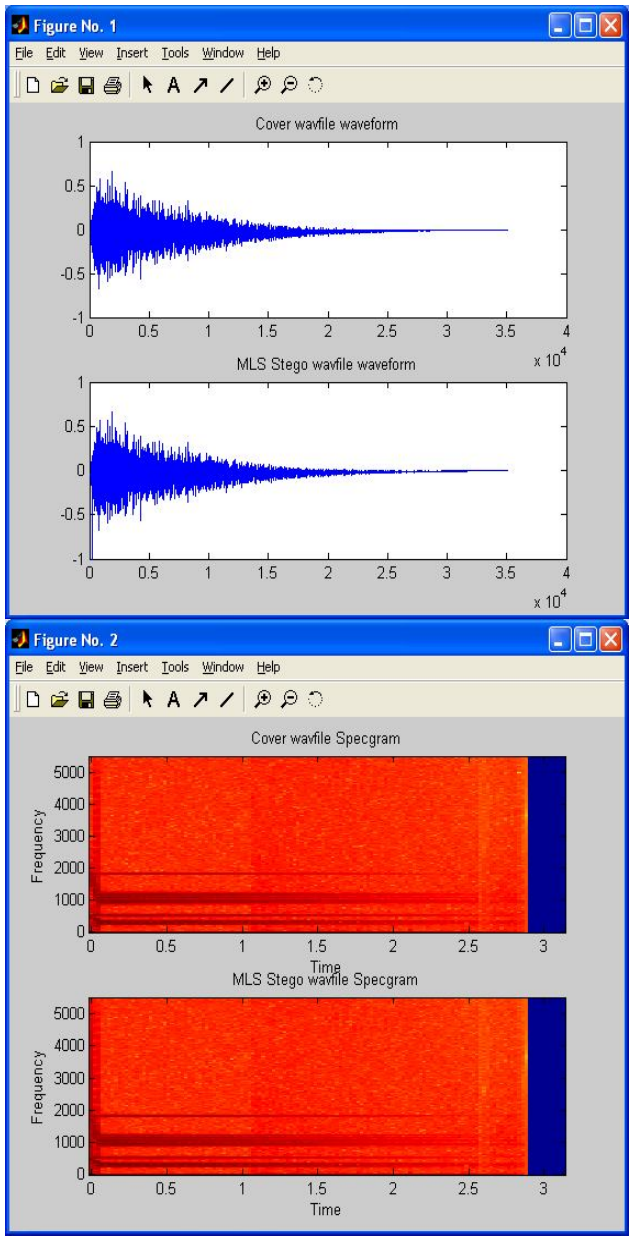


Figure 6 Result of Proposed MLS Technique

3.4 Blend of LSB modification and Parity Encoding in Multi-Level Steganography (MLS)

3.4.1 Method

At level 1 first message object hided under cover object using LSB modification technique as discussed earlier. The output of this level is an intermediate object which is called decoy object. This decoy object is input for next level. In level 2 second secret message hided under decoy object using parity encoding technique.

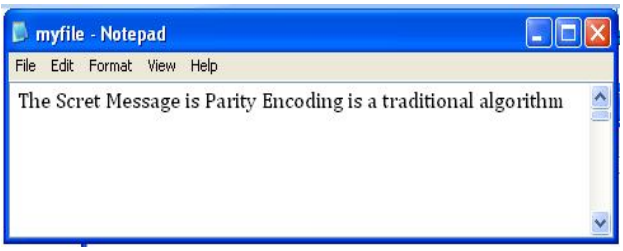
3.4.2 Result

After using MLS algorithm the audibility of the cover object hasn't been modified and secret objects are retrieved.

3.5 Decoding Result

When stego object decoded means passes through the decoding algorithm of phase encoding method the secret message of second level is retrieved.

When decoy object passes through the decoding algorithm of LSB modification method the secret message of first level is retrieved.



4. CONCLUSION

In this paper a new method of audio steganography presented where two secret messages can be hidden. Two traditional method of steganography blended in a level based approach to reach the goal. The output stego object is very difficult to decode which makes this method successful in the world of audio steganography.

REFERENCES

[1] Dr. Atef Jawad Al-Najjar1, Computer Engineering Department, King Fahd University of Petroleum & Minerals, Saudi Arabia, "*The Decoy: Multi-Level Digital Multimedia Steganography Model*" 12th WSEAS International Conference on Communications, Heraklion, Greece, July 23-25, 2008.

[2] "*audio steg: methods*", Internet publication on http://www.snotmonkey.com/work/school/405/methods.html

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

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

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

[6] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal, "*Data Hiding Through Multi Level Steganography and SSCE*", Journal of Global Research in Computer Science, Volume 2, No. 2, February 2011

[7] Jithesh K, Dr. A V Senthil Kumar, "*Multi Layer Information Hiding -A Blend of Steganography and Visual Cryptography*", Journal of Theoretical and Applied Information Technology, 2005 - 2010

AUTHORS

Prof. Samir Kumar Bandyopadhyay, B.E., M.Tech., Ph.D (Computer Science & Engineering), C.Engg., D.Engg., FIE, FIETE, Sr. Member IEEE, currently Professor of Computer Science & Engineering, University of Calcutta, Kolkata, India. He has 25 years of Teaching & Research experience and over 300 research papers publication in International & Indian Journals and 5 leading text books of Computer Science & Engineering. His research interests include Bio-Medical Engineering, Mobile Computing, Pattern Recognition, Software Engineering, Network Security etc.

Barnali Gupta Banik, B.Tech, M.Tech is currently working as Asst. Professor, Computer Science & Engineering Dept., St. Thomas' College of Engineering & Technology, Kolkata, India. She has around 5 years of Teaching experience & 2 years of IT experience working for MNC in India & UK. She is at present pursuing Research work in Network Security under the guidance of Prof. Samir Kumar Bandyopadhyay.