ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2012

LSB Modification and Phase Encoding Technique of Audio Steganography Revisited

Prof. Samir Kumar, BandyopadhyayBarnali, Gupta Banik

Department of Computer Science and Engineering, University of Calcutta, Kolkata India.
Department of Computer Science, St' Thomas College of Engineering & Technology, Kolkata India.

ABSTRACT— ***Information security is becoming very important part of our life now-a-days. Information hiding is the fundamental of information security. Information hiding can be achieved by steganography as well. LSB modification and phase encoding technique are very primitive in steganography. Here these two primitive techniques are revisited to get an idea of how steganography in audio file works.***

Keywords— **Steganography, Least Significant Bit, Phase Encoding**

I. Introduction

Information hiding is a part of information Security. Steganography is a technique of information hiding that focuses on hiding the existence of secret messages. The aim of steganographic methods is to hide the existence of the communication and therefore to keep any third-party unaware of the presence of the Steganographic exchange.

In practice there are three types of steganographic protocol used. They are Pure Steganography, Secret Key Steganography and Public Key Steganography.

Pure Steganography is defined as a steganographic system that does not require the exchange of a cipher such as a stego-key. There is two input, carrier object and message object. The steganographic algorithm is used to embed message object onto carrier object. The main criteria for this embedding is no third party observer can see, listen or suspect about the message. It should be lie in secret. Different type of object can be used as carrier and message object. It can be Image, Text, audio and video.

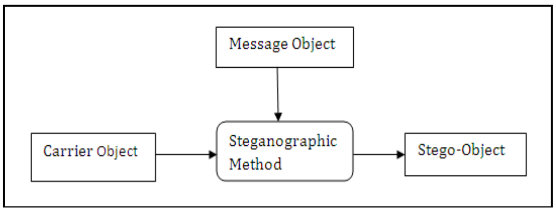


Figure 1: General Steganography Block Diagram

Audio Steganography

Embedding secret messages into digital sound is known as audio Steganography. It is usually a more difficult process than embedding messages in other media. Audio Steganography methods can embed messages in WAV, AU, and even MP3 sound files.

The properties of the human auditory system (HAS) are exploited in the process of audio Steganography. Auditory perception is based on the critical band analysis in the inner ear where a frequency-to-location transformation takes place along the basilar membrane. The power spectra of the received sounds are not represented on a linear frequency scale but on limited frequency bands called critical bands. [3]

Digital Audio

Digital audio is discrete rather than continuous signal as found in analog audio. A discrete signal is created by sampling a continuous analog signal at a specified rate. For example, the standard sampling rate for CD digital audio is about 44 kHz.

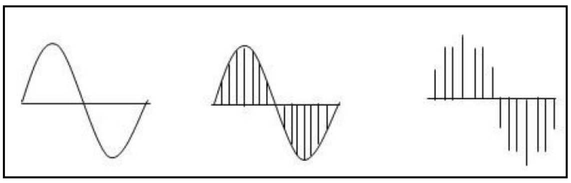


Figure 2: Continuous analog sound wave is sampled to produce digital signal

Digital audio is stored in a computer as a sequence of 0's and 1's. With the right tools, it is possible to change the individual bits that make up a digital audio file. Such precise

ISSN : 2278 – 1021

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2012

control allows changes to be made to the binary sequence that are not discernible to the human ear.

In the digital domain, PCM (Pulse Code Modulation) is the most straightforward mechanism to store audio. The analog audio is sampled in accordance with the Nyquest theorem and the individual samples are stored sequentially in binary format. The wave file is the most common format for storing PCM data and the WAVE file format is a subset of Microsoft's RIFF specification for the storage of multimedia files. That's why .wav files have been used here for below mentioned experiments.

II. LITERATURE SURVEY

This section reviews the related background literature and describes the concept of steganography in audio file. Information hiding can be achieved either exploiting loopholes of Human Visual System (HVS) or Human Auditory System (HAS). Steganography of audio signals is more challenging than Steganography of images due to wider dynamic range of the HAS in comparison with human visual system (HVS). The HAS perceives sounds over a range of power greater than 109 to 1 and a range of frequencies greater than 103 to 1. Two properties of the HAS used in steganographic algorithms are frequency masking and temporal masking. Frequency (simultaneous) masking is a frequency domain trend where a low level signal can be made inaudible (masked) by a simultaneously appearing stronger signal (the masker).

To embed data secretly onto digital audio file there are few techniques introduced earlier. The lists of methods are:

- LSB Coding
- Phase Coding
- Parity Coding
- Spread Spectrum

In LSB coding technique least significant bit is modified to embed data. In phase encoding scheme the phase of carrier file is replaced with reference phase which represents hidden data. In parity coding signals are divided into regions, then parity bit of each region calculated and matched with secret message bit. Depending on parity matching result encoding is done. In spread spectrum method secret information is spread over the audio signal's frequency spectrum as much as possible.

III. PROPOSED WORK

A. *LSB MODIFICATION TECHNIQUE*

1) *METHOD*

Here one of the traditional methods of Steganography which is based on least significant bit modification has been implemented. The flowchart of the algorithm is given as follows:

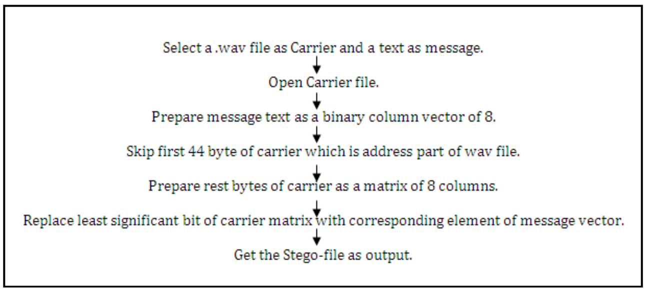


Figure 3: Flowchart of LSB modification Technique for Audio Steganography

After executing the program the procedure can showed with the help of original data as follows:

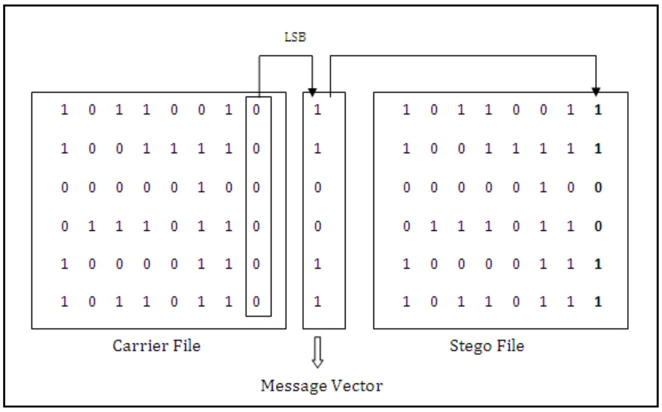
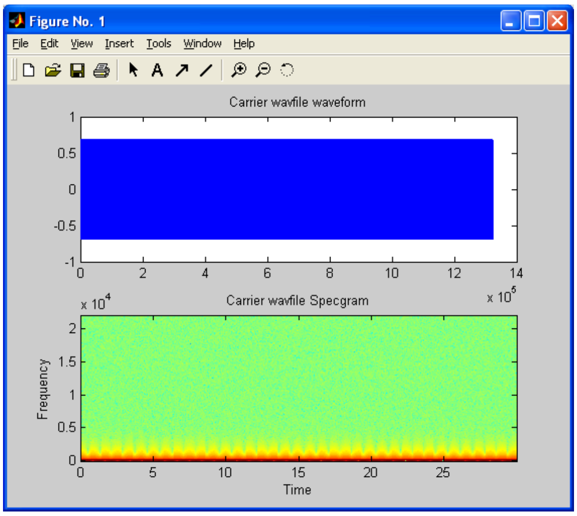
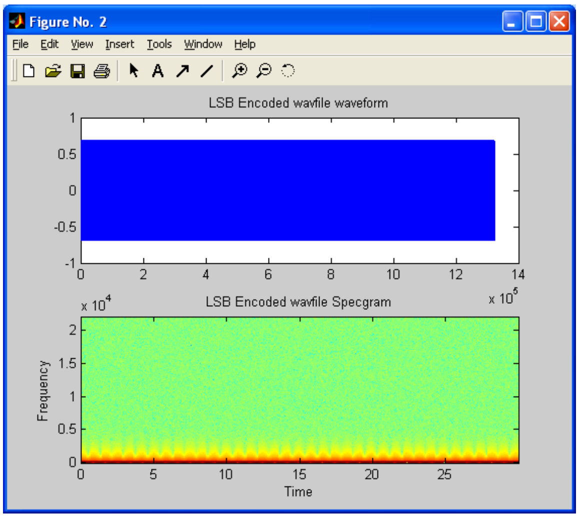


Figure 4:LSB modification procedure for Audio Steganography

2) *RESULT*

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





B. *PHASE ENCODING TECHNIQUE*

1) METHOD

The basic idea is to split the original audio stream or cover file(C) into blocks and embed the whole message data sequence into the phase spectrum of the first block. One drawback of the phase coding method is a considerably low payload because only the first block is used for secret message (M) embedding. In addition, the M is not distributed over C – that means it is localized data and thus can be removed easily by the cropping attack. [1]

Phase coding is explained in the following procedure:

- The original sound signal (C) is segmented to extract the header. The rest portion to is broken up into smaller segments whose lengths equal the size of the message to be encoded.
- A Discrete Fourier Transform (DFT) is applied to each segment to create a matrix of the phases.
- The secret message is inserted in the phase vector of the first signal segment as follows:

$$\text{New Phase} = \begin{cases} \text{Old Phase} + \pi/2 & \text{if message bit} = 0 \\ \text{Old Phase} - \pi/2 & \text{if message bit} = 1 \end{cases}$$

- A new phase matrix is created using the new phase of the first segment and the original phase matrix.
- Using the new phase matrix the sound signal is reconstructed by applying the inverse DFT and then concatenating the sound segments with original header.

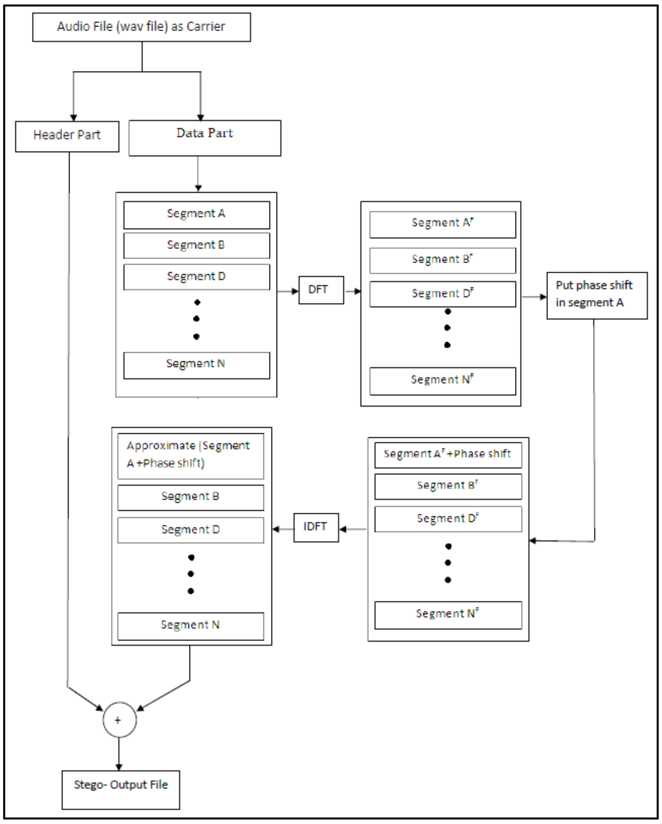


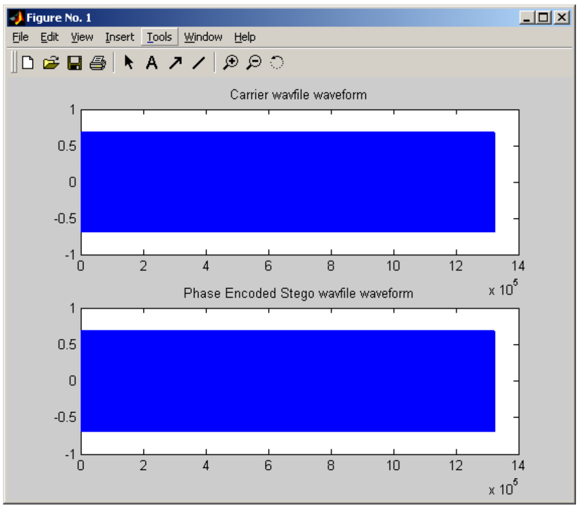
Figure 5: Flow-chart for audio steganographic technique using phase encoding

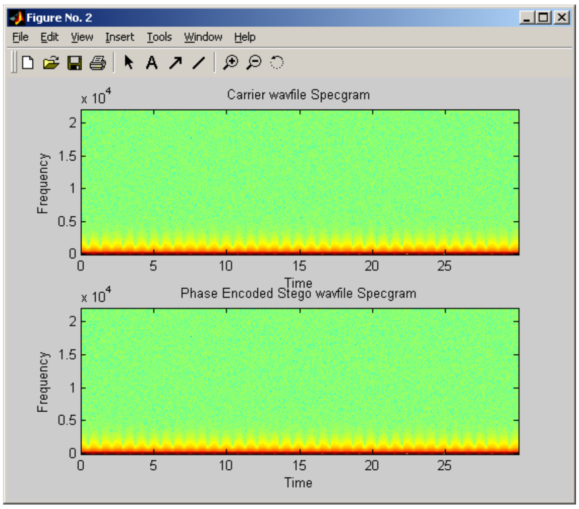
ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 4, June 2012

2) RESULT

The output stego-file is correct and audible. There is no such discrepancy found compared to the input carrier file. So it can be shown with the help of graphical result:





IV. CONCLUSION

An effective audio steganographic scheme should possess the following three characteristics: Inaudibility of distortion (Perceptual Transparency), Data Rate (Capacity) and Robustness. These characteristics (requirements) are called the magic triangle for data hiding [9].

This method of LSB modification of Steganography is the least secure. This method's security lies on the presumption that no other parties are aware of this secret message. This method is easy to implement but is very susceptible to data loss due to channel noise and re-sampling.

Disadvantages associated with phase coding are a low data transmission rate due to the fact that the secret message is encoded in the first signal segment only and to extract the secret message from the sound file, the receiver must know the segment length. As a result, this method can be used when only a small amount of data needs to be concealed. Otherwise this can be proved as a good method for audio Steganography.

REFERENCES

[1] Bret Dunbar, SANS Institute InfoSec Reading Room "*A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment*".

[2] Alex Toumazis, "*Steganography*".

[3] Cvejic, Nedeljko, Department of Electrical and Information Engineering "*Algorithms for audio watermarking and Steganography*"Information Processing Laboratory, University of Oulu, Finland 2004.

[4] PoulamiDutta, Debnath Bhattacharyya, Tai-hoon Kim "*Data Hiding in Audio Signal: A Review*", International Journal of Database Theory and Application Vol. 2, No. 2, June 2009.

[5] Prof. Samir Kumar Bandyopadhyay, SarthakParui *"A Method for Public Key Method of Steganography"*, International Journal of Computer Applications (0975 – 8887) Volume 6– No.3, September 2010.

[6] Vivek Jain, Lokesh Kumar, Madhur Mohan Sharma, MohdSadiq, KshitizRastogi, "*Public-Key Steganography Based On Modified Lsb Method*" Journal of Global Research in Computer Science ,Volume 3, No. 4, April 2012.

[7] Soumyendu Das, Subhendu Das, BijoyBandyopadhyay, SugataSanyal, "*Steganography and Steganalysis: Different Approaches*"

[8] Jayaram P, Ranganatha H R, Anupama H S,Department of Computer Science and Engineering, R V College of Engineering,Bangalore, INDIA," *Information Hiding Using Audio Steganography – A Survey*" The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.

[9] H.B.Kekre, ArchanaAthawale, SwarnalataRao, UttaraAthawale, "*Information Hiding in Audio Signals*" International Journal of Computer Applications (0975 – 8887) Volume 7– No.9, October 2010.

[10] Xiaoxiao Dong, Mark F. Bocko, ZeljkoIgnjatovic, University of Rochester, Rochester, NY, 14627 USA, "*Data Hiding Via Phase Manipulation of Audio Signals*"