Volume 4, Issue 1, January 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Multi-Level Steganographic Algorithm for Audio Steganography using LSB, Parity Coding and Phase Coding Technique

Kamalpreet Kaur
Student
M.tech, Department of CSE
RBIEBT, Kharar(Pb)-India

DeepankarVerma
Assistant Professor
M.tech, Department of CSE
RBIEBT, Kharar(Pb)-India

Abstract*— Internet world is characterized by many users among which are crackers and thieves. Hence, the need for a secured system to safely exchange confidential information among users across the web is required. Of such tool is steganography that simply hides the user information under other kind of information such as audio so that no one suspects that a sensitive data is being transferred. Its purpose is to hide the presence of communication. Here three 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. It uses at least two steganographic methods in which one method serves as a carrier for the second one. Multi-Level Steganography has advantage of difficult decoding and sending two or more secret message through a single cover object. This paper defines a method for audio steganography using LSB coding, parity coding and phase coding technique in multi-level steganography. In this thesis the review of three layered approach for audio multi-level steganography has been presented. Here three secret messages rather than one can be transmitted with a single cover file. In this paper, three permutations of audio steganography methods are compared. The result of the stego audios is compared by PSNR graph. Each permutation has three levels. Three levels of audio steganography can be identified as layer 1, layer 2 and layer 3. This method has provided an effective way to achieve higher security, increased undetectability and the maintained consistency in the clarity of digital audio signal.

Keywords* — Information security, Information hiding, Steganography, Audio steganography, Multi-level steganography, Stego object, Decoy object.

I. INTRODUCTION

A. Steganography

Steganography is an art and a science of communicating in a way, which hides the existence of the communication. It is also called as "covered writing", because it uses a "cover" of a message for sending any important secret message. Steganography serves as a means for private, secure and sometimes malicious communication. Steganography is the art to hide the very presence of communication by embedding the secret message into the innocuous-looking cover media objects. Steganography is a powerful tool which increases security in data transferring and archiving. [5] 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. Dr. Al Najjar first introduced 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 [1].

B. Audio Steganography

Audio steganography is the technique of hiding information inside an audio signal. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio steganography software can embed messages in WAV, AU, and even MP3 sound files. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images [7]. As data is embedded in the signal, it gets modified. This modification should be made imperceptible to the human ear. Image can also be taken as a medium but audio steganography is more challenging because of the characteristics of Human Auditory System (HAS) like large power, dynamic range of hearing and large range of audible frequency [10].

C. Multi-Level Steganography

Multi-Level Steganography is a new concept of information hiding in telecommunication networks that uses features of an existing steganographic method (the upper level method) to create a new one (the lower-level method). Multi-Level Steganography (MLS) was originally proposed by Al-Najjar for picture steganography. MLS is based on combining two or more steganographic methods in such a way that one method (the upper-level) is a carrier for the other method (the lower-level) [2].

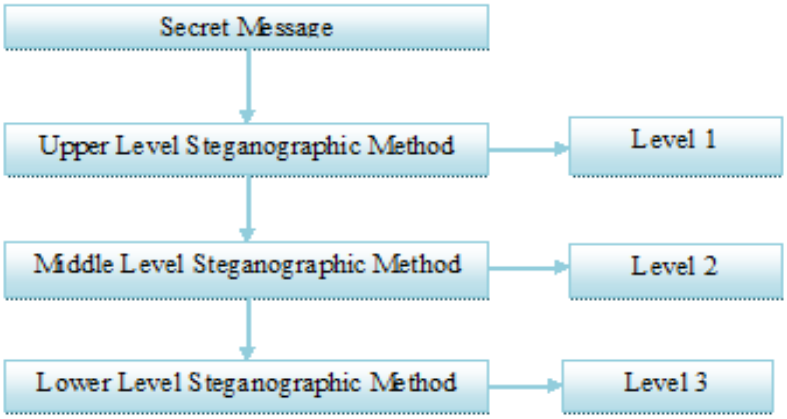

Fig. 1: Overview of Proposed Multi-level Steganography System

D. Least Significant Bit (LSB)

LSB hiding is a simple and fast method for embedding information in an audio signal. It consists of embedding each bit from the message in the least significant bit of the cover audio in a specific way. LSB hiding schemes provide a very high channel capacity for transmitting many kinds of data and is easy to implement and to combine with other hiding techniques. The length of the secret message to be encoded should be smaller than the total numbers of samples in a sound file [9]. The LSB technique takes advantage of the HAS which cannot hear the slight variation of audio frequencies at the high frequency side of the audible spectrum. The LSB technique allows high embedding rate without degrading the quality of the audio file. Furthermore, it is relatively effective and easy to implement [8].

E. Parity Coding

In parity coding method, sample region's parity bit is used for data embedding. In this case signal breaks down into separate region of samples instead of individual samples. If the secret bit to be encoded does not match with the sample region's parity bit then process flips the LSB of one of the samples in the region. Therefore the sender has more of a choice in encoding the secret bit [9].

F. Phase Coding

Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. It works by substituting the phase of an initial audio segment with a reference phase that represents the data. The phase of subsequent segments is then adjusted in order to preserve the relative phase between segments [4].

II. RELATED WORK

Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique (Prof. Samir Kumar Bandyopadhyay and Barnali Gupta Banik): 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 [1].

Multi-Level Steganography: Improving Hidden Communication in Networks (Wojciech Frączek, Wojciech Mazurczyk, Krzyszt of Szczypiorski): The paper presents Multi-Level Steganography (MLS), which defines a new concept for hidden communication in telecommunication networks. In MLS, at least two steganographic methods are utilized simultaneously, in such a way that one method (called the upper-level) serves as a carrier for the second one (called the lower-level). Such a relationship between two (or more) information hiding solutions has several potential benefits. The most important is that the lower-level method steganographic bandwidth can be utilized to make the steganogram unreadable even after the detection of the upper-level method: e.g., it can carry a cryptographic key that deciphers the steganogram carried by the upper-level one. It can also be used to provide the steganogram with integrity. Another important benefit is that the lower-layer method may be used as a signaling channel in which to exchange information that affects the way that the upper-level method functions, thus possibly making the steganographic communication harder to detect[2].

The Decoy: Multi-Level Digital Multimedia Steganography **Model (**Atef jawad Al-najjar): Define four types of objects: message-object, intermediate-object, cover-object, and stego-object. All objects are represented by a finite set of elements, where each element is in turn represented by a finite sequence of bits. The bits make the primitive components of the representation. A multimedia (MM) object can be in one of several classes: text, picture, image, audio, or video. MM objects are used for human-human, human-machine, or machine-machine communication. Hence, MM objects have storage and transmission requirements. For example, an audio object can be represented in several formats, e.g., wav and MP3. Text objects can be represented using an image, ASCII or Unicode, among other representations. MM objects can be published or hidden. The focus of this paper is twofold to develop an abstract multi-level model; and to use a published object to conceal (hide) a secret object using the proposed model. An example of hiding a text message-object,

represented by a black and white (B&W) image object, into a gray-image (intermediate-object, or decoy) that is then hidden in a color image object in RGB-color format, is given [3].

An Integrated Synchronized Protocol for Secure Information Transmission derived from Multilevel Steganography and Dynamic Cryptography (Navneet Singh Sikarwar): In this paper a protocol is elucidated, it is based on multilevel steganography and dynamic cryptography in the secure information transmission, because the growing possibilities of modern communications require the special means of confidential and intellectual property protection against unauthorized access and use. Especially these problems are actually for computer networks, which make possible to exchange the large amount of digital information (text, audio, video, and image). The use of multilevel steganography provides more strength compare to simple steganography technique [6].

Data hiding technique: Audio steganography using LSB technique (Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar): In this era of emerging technologies, electronic communication has become an integral and significant part of everyone's life because it is simpler, faster and more secure. The objective of this paper is to come up with a technique hiding the presence of secret message. Steganography is the art of secret communication. Its purpose is to hide the presence of communication, as opposed to cryptography, which aims to make communication unintelligible to those who don't possess the right keys. Audio steganography is concerned with hiding information in a cover (host) audio signal in an imperceptible way. Hidden information from the stego, or data-embedded audio signal, is retrieved 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. Proposed technique has been tested successfully on a .wav file at a sampling frequency of 3000 samples/second with each sample containing 8 bits [5].

Audio Steganography: A Survey on Recent Approaches (Masoud Nosrati Ronak Karimi Mehdi Hariri): In this study, we will have a survey on audio steganography recent researches. Due to it, some basic concepts of audio steganography and HAS including Least Significant Bit (LSB) Coding, Parity Coding, Phase Coding, Spread Spectrum (SS) and Echo data hiding are covered. In follow, a brief introduction and abstract of 7 recent methods for audio steganography is presented [4].

III. PROPOSED METHOD

Here three secret messages rather than one can be transmitted with a single cover file. Layering approach gives opportunity to do so. In this paper three layered approach has been presented. At the first level, cover file (C) can be embedded with the first secret message S1. Assuming the decoy file as C1 which is cover file for next middle level where secret message can be denoted as S2. Assuming the decoy file as C12 which is cover file for next lower level where secret message can be denoted as S3. Now the final stego file created as C123. So C123 holds three secret messages S1, S2 and S3. In this paper, three permutations of audio steganography methods are compared. The result of the stego audios is compared by PSNR graph. Each permutation has three levels. Three levels of multi-level audio steganography can be identified as layer 1, layer 2 and layer 3.

To achieve the set objectives, our proposal will focus on developing a better technique for audio multi-level steganography that will maintain the higher security, undetectability and clarity of digital audio signal. We will propose the technique using LSB, parity coding and phase coding technique in multi-level steganography and implement it in MATLAB. The proposed work will be based on mainly three steps:

Step1: In permutation one:

- In level 1, an audio file will be selected whose audio samples are selected, using LSB technique and will be used to conceal the secret data. In this level first secret message hided under cover object using LSB technique.
- In level 2, the output of the level 1 is the input for level 2. In this level second secret message hided under decoy object using parity coding technique.
- In level 3, the output of the level 2 is the input for level 3. In this level third secret message hided under decoy object using phase coding technique. Output of this level is called stego object.

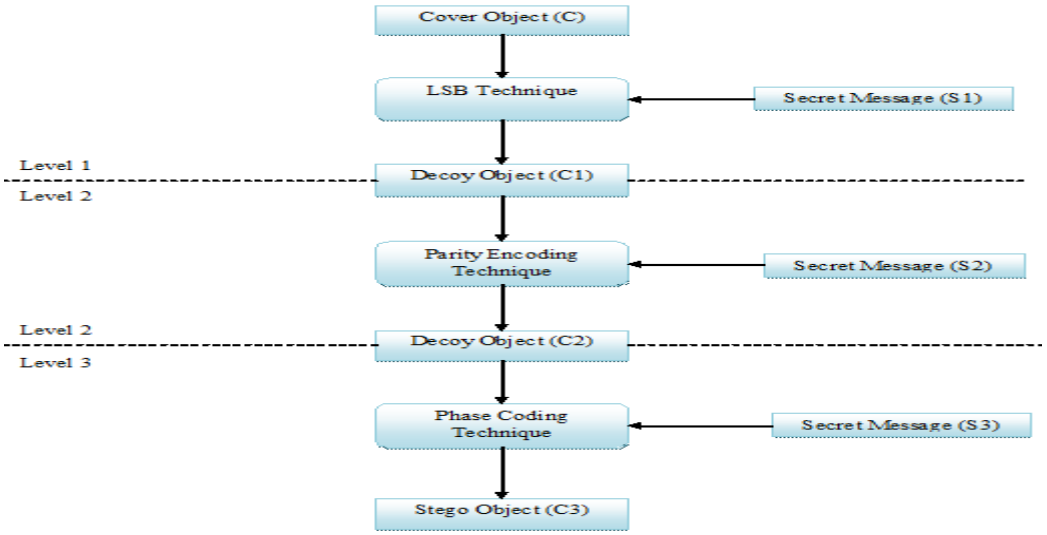

Fig. 2: Permutation 1

Step 2: In permutation 2:

- In level 1, first secret message hided under cover object using parity coding technique.
- In the level 2, the output of the level 1 is the input for level 2. In this level second secret message hided under decoy object using LSB technique.
- In the level 3, the output of the level 2 is the input for level 3. In this level third secret message hided under decoy object using phase coding technique. Output of this level is called stego object.

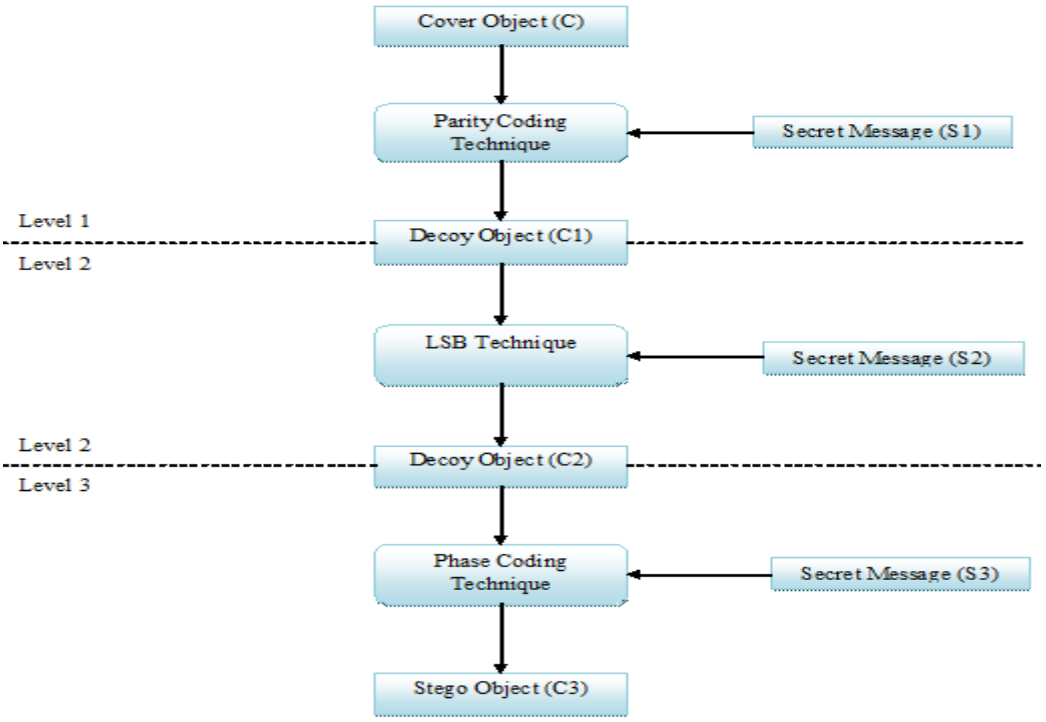

Fig. 3: Permutation 2

Step 3: In permutation 3:

- In level 1, an audio file will be selected whose audio samples are selected, using LSB technique and will be used to conceal the secret data. In this level first secret message hided under cover object using LSB technique.
- In the level 2, the output of the level 1 is the input for level 2. In this level second secret message hided under decoy object using phase coding technique.
- In the level 3, the output of the level 2 is the input for level 3. In this level third secret message hided under decoy object using parity coding technique. Output of this level is called stego object.
- After performing three permutations of audio steganography they are compared by PSNR graph.

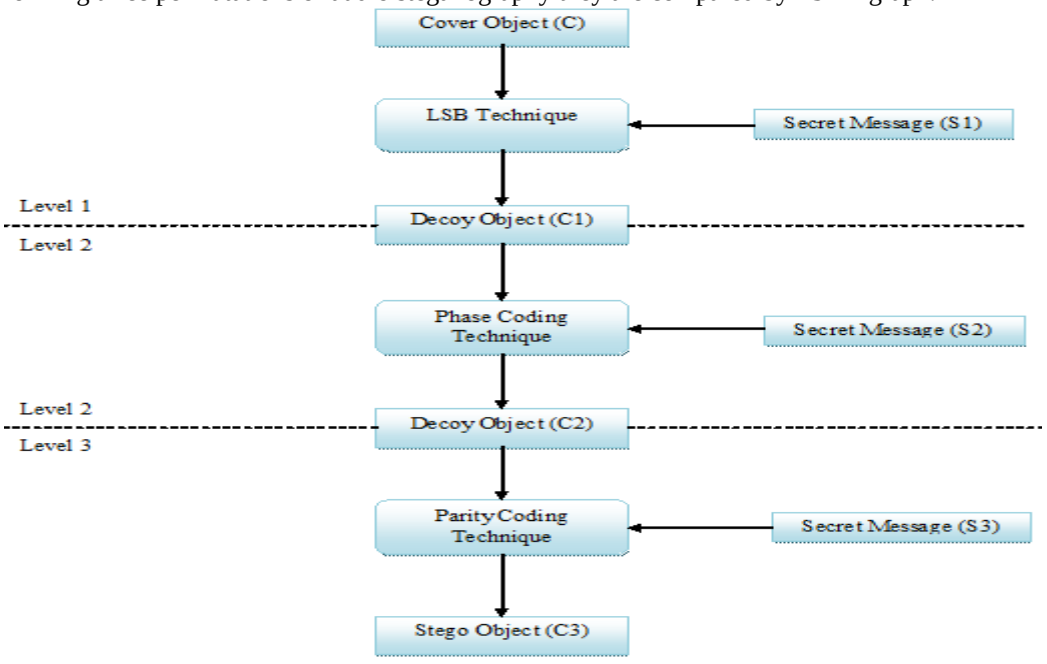

Fig. 4: Permutation 3

IV. RESULTS

We have implemented the multi-level audio steganography method on MATLAB. We can test the performance of the proposed method by comparing both the original audio with embedded audio, and see whether any changes is visible in embedded audio and result of the stego audio is compared by PSNR graph.

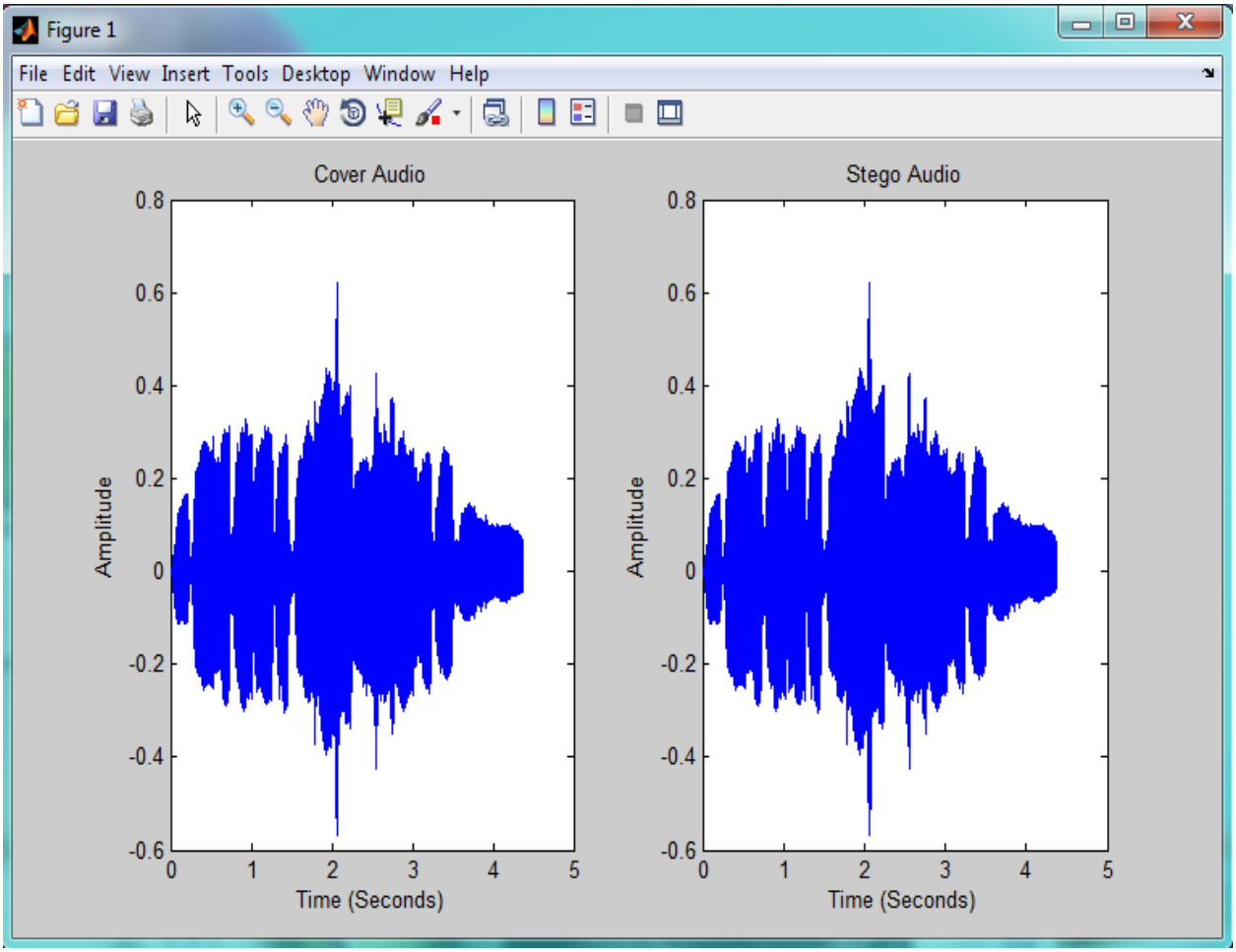

Fig. 5: Before & After Steganography Audio File

As you see in Figure 5 there are no visible changes when compared to cover audio with stego audio. There are mainly two aspects that should be taken into account when discussing the results of the audio steganography. They are higher security, undetectability of secret message. This method satisfies both security aspects and undetectability. This method hides three secret messages through three different algorithms which are very difficult to detect the original message which may be present in any level of proposed method. So undetectability of original message is achieved. The security level has increased through the encoding of the secret messages through three levels. When goes from sender to receiver he can't find out whether there is any message in the audio. Because there are no visible distortion exists in the audio. Second, when we compare the original audio graph with the embedded one there is no visible difference in both graphs. Third, if any third person finds that there is some message in audio and tries to extract it then he can't extracts it because there are three levels in this method and we can hide the secret message in any one level.

Mean Squared Error (MSE): It is defined as the square of error between cover audio signal & stego audio signal. The distortion in the audio signal can be measured using MSE. It is calculated as follows.

$$MSE = \frac{\sum [f(i,j) - F(i,j)]^2}{N^2}$$

where f(i,j) represent cover audio signal and F(i,j) represent stego audio signal.

Peak Signal-to-Noise Ratio (PSNR): It is the measure of quality of audio signal by comparing cover audio with stego audio. PSNR in decibels (dB) is computed by using:

$$PSNR = 20 \log_{10} \left(\frac{255}{RMSE} \right)$$

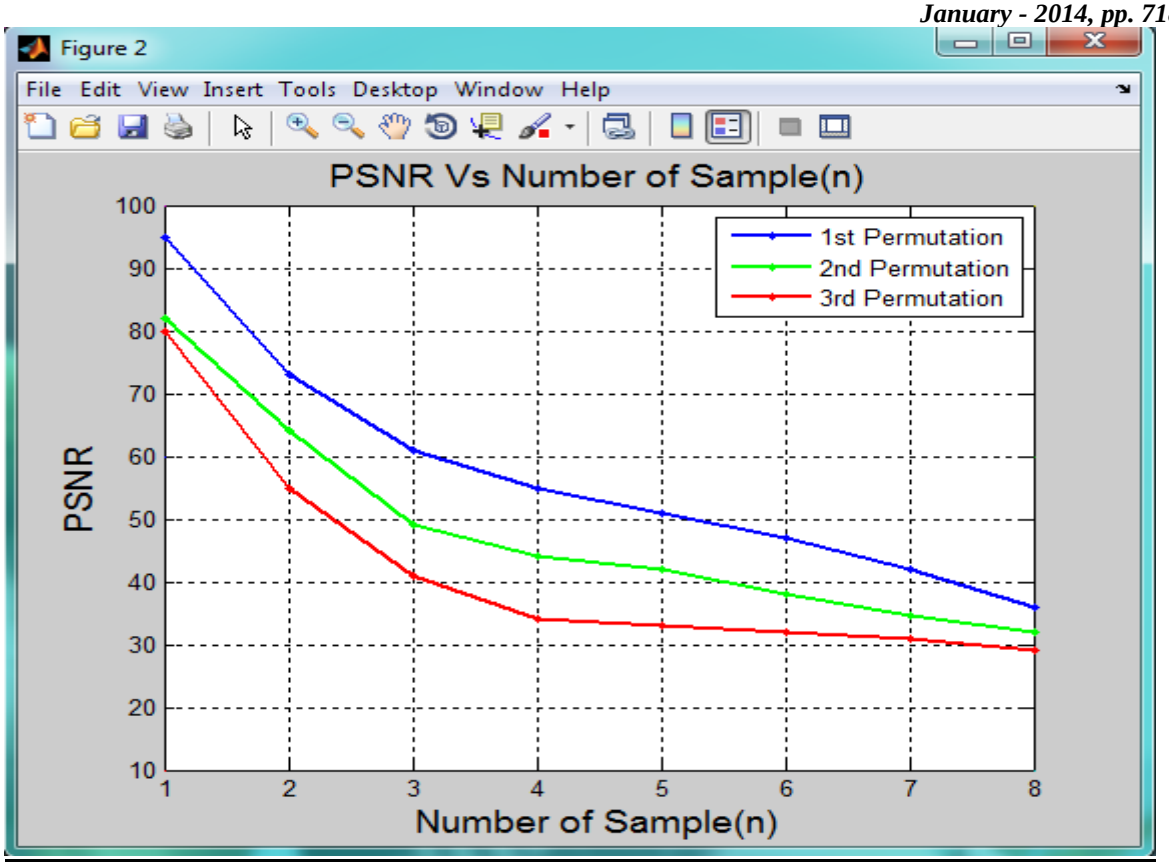

Fig. 6: PSNR Graph

V. CONCLUSIONS

This paper proposed an audio steganography technique for hiding text data into digital audio files based on three different techniques to select the carrier audio samples into which bits of the secret data are to be hidden. In this paper three secret messages can be hidden. Three 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] Prof. Samir Kumar Bandyopadhyay and Barnali Gupta Banik: *"Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique",* Volume 1, Issue 2, July – August 2012.

[2] Wojciech Fraczek, Wojciech Mazurczyk, Krzysztof Szczypiorski: *"Multi-Level Steganography: Improving Hidden Communication in Networks",* Cornell University Library, Jan 2011, http://arxiv.org/ftp/arxiv/papers/1101/1101.4789.pdf

[3] Al-Najjar AJ: *"The Decoy: Multi-Level Digital Multimedia Steganography Model",* In Proc. Of 12th WSEAS International Conference on COMMUNICATIONS, Heraklion, Greece, July 23-25, 2008.

[4] Masoud Nosrati, Ronak Karimi, Mehdi Hariri: *"Audio Steganography: A Survey on Recent Approaches"*, World Applied Programming, Vol (2), No (3), March 2012.

[5] Ashwini Mane, Gajanan Galshetwar, Amutha Jeyakumar*:"Data hiding technique: Audio steganography using LSB technique",* Vol. 2, Issue 3, May-Jun 2012, pp.1123-1125

[6] Navneet Singh Sikarwar*:"An Integrated Synchronized Protocol for Secure Information Transmission derived from Multilevel Steganography and Dynamic Cryptography",* Volume 3, Issue 4, April 2012.

[7] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das: *"A Tutorial Review on Steganography",* IC3–2008.

[8] Youssef Bassil*: "A Two Intermediates Audio Steganography Technique",* VOL. 3, NO.11 Nov, 2012.

[9] Pooja P. Balgurgi, Prof. Sonal K. Jagtap, *"Intelligent Processing: An Approach of AudioSteganography"*, 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India.

[10] B. Santhi, G. Radhika and S. Ruthra Reka: *"Information Security using Audio Steganography -A Survey"*, Research Journal of Applied Sciences, Engineering and Technology 4(14): July 15, 2012.

