Journal of Al-Qadisiyah for computer science and mathematics
Vol.5 No.2 year 2013

Page89-98

A New Audio Steganography Technique For Hiding Text Message

Zena A. Alwan
College of Elec. & Electronic Techniques Organization
Foundation of Technical Education
Bagdad,Iraq
Email: zena782004@Yahoo.com

Recived : 12 /6 /2013 Revised: 2 /7 / 2013 Accepted: 18 /11 / 2013

Abstract:
The world is tend now a lot of development in communication field specially in internet , therefore it is very important to find security methods for files that is send from one place to another.One of these security approaches is steganography which have characteristic of transfer massages within transmission media (files) without notice from any obtrusive. This paper provide anew suggested method for hiding text in audio file (wav file), first the text file will be read to extract the massage which is hidden, for more security this massage will be encrypted (or coded) before hiding it inside sound media (in time domain) . This algorithm was applied on more than one example and good results were obtained without missing the text massage or notice any noise in the cover file.

Keywords: Audio steganography, Text hiding, (LSB) technique.

1. INTRODUCTION

By development of computer and the expansion of its use in different areas of life and work, the issue of security of information has gained special significance. One of the concerns in the area of Information security is the concept of hidden exchange of information [1]. Steganography is a sub-discipline of Information hiding that focuses on concealing the existence of messages [2]. The term hiding refers to the process of making the information imperceptible or keeping the existence of the information secret. Steganography is a word derived from the ancient Greek words steganos, which means covered and graphia, which in turn means writing [3]. The Eq. (1) provides a very generic description of the pieces of the steganographic process [4]:

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

In this context, the cover_medium is the file in which we will hide the hidden_data, which may also be encrypted using the stego_key. The resultant file is the stego_medium. Any steganography technique has to satisfy two basic requirements.

The first requirement is perceptual transparency, i.e. 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 data [5]. Unlike cryptography, which simply conceals the content or meaning of the message, Steganography conceals the very existence of a message [6].

Modern advances in computer, communication and signal processing have enabled the discovery of sophisticated techniques of steganography. These advances have broadened steganography's use to include various types of medium and various forms of information. The developed techniques allow text, audio, video, graphics, or codes to be concealed in electronic documents containing text, graphics, images and even in electronic audio or video files. Steganography has numerous applications like digital rights management, access control, covert communication, annotation etc [7].

2. STEGANOGRAPHY

Steganography is a process of hiding a secret message into an image or hiding a secret image into a cover image. There are two basic methods implemented in steganography: Least significant bit (LSB) Spatial Domain Technique and Transform-based (DCT) - Frequency Domain Technique. LSB steganography is a one of the simplest methods. Data hidden in images using this method is highly sensitive to image alteration & vulnerable to attack. DCT steganography is potentially more resistant to loss from image manipulation and increases the difficulty to a potential attacker. In this paper, we mainly deal with only LSB steganography method [8].

The steganography application hides different types of data within a cover file. The resulting stego also contains hidden information, although it is virtually identical to the cover file. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them, although there are programs available that can do what is called Steganalysis (Detecting use of Steganography) [9].

The components of steganographic system are:

Emb: The message to be embedded.

Cover: The data in which emb will be embedded.

Stego: A modified version of cover that contains the embedded message emb.

Key: Additional secret data that is needed for the embedding and extracting processes and must be known to both, the sender and the recipient.

fE: A steganographic function that has cover, emb and key as parameters and produces stego as output.

F_E-1: A steganographic function that has stego and key as parameters and produces emb as output. F_E-1 is the inverse function of $F_E$in the sense that the result of the extracting process F_E-1 is identical to the input E of the embedding process F_E.

The embedding process F_E embeds the secret message E in the cover data C. The exact position (S) where E will be embedded is dependence on the key K. The result of the embedding function is slightly modified version of C: the stego data C'. After the recipient has received C' he starts the extracting process F_E-1 with the stego data C' and the key K as parameters. If the key that is supplied by the recipient is the same as the key used by the sender to embed the secret message and if the stego data the recipient uses as input is the same data the sender has produces (i.e., it has not been modified by an adversary), then the extracting function will produce the original secret message E [9].

3. AUDIO STEGANOGRAPHIC METHODS

The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information.
Basically, the model for steganography is shown in Fig. 1. Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file.

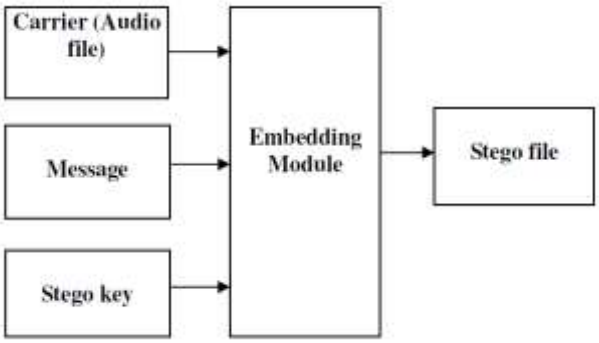

Fig.1: Basic Audio Steganographic Model

Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file.
There have been many techniques for hiding information or messages in audio in such a manner that the alterations made to the audio file are perceptually indiscemible. Common approaches include [7, 12]:
Least Significant Bit (LSB) Coding
Echo Data Hiding
Parity Coding
Phase Encoding
Spread Spectrum

LSB CODING

A very popular methodology is the LSB (Least Significant Bit) algorithm, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data. That's usually an effective technique in cases where the LSB substitution doesn't cause significant quality degradation, such as in 24-bit bitmaps.
In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position.

1	0	0	1	0	1	0	1

Fig. 2: Binary representation of decimal 149

The binary representation of decimal 149, with the LSB highlighted. The MSB in an 8-bit binary number represents a value of 128 decimal. The LSB represents a value of 1. For example, to hide the letter "a" (ASCII code 97, which is 01100001) inside eight bytes of a cover, you can set the LSB of each byte like this:

10010010
01010011
10011011
11010010
10001010
00000010
01110010
00101011

The application decoding the cover reads the eight Least Significant Bits of those bytes to recreate the hidden byte—that is 0110001—the letter "a." As you may realize, using this technique let you hide a byte every eight bytes of the cover. Note that there's a fifty percent chance that the bit you're replacing is the same as its replacement, in other words, half the time, the bit doesn't change, which helps to minimize quality degradation.

Fig 3 illustrates how the message 'HEY' is encoded in a 16-bit CD quality sample using the LSBmethod. 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 [6].

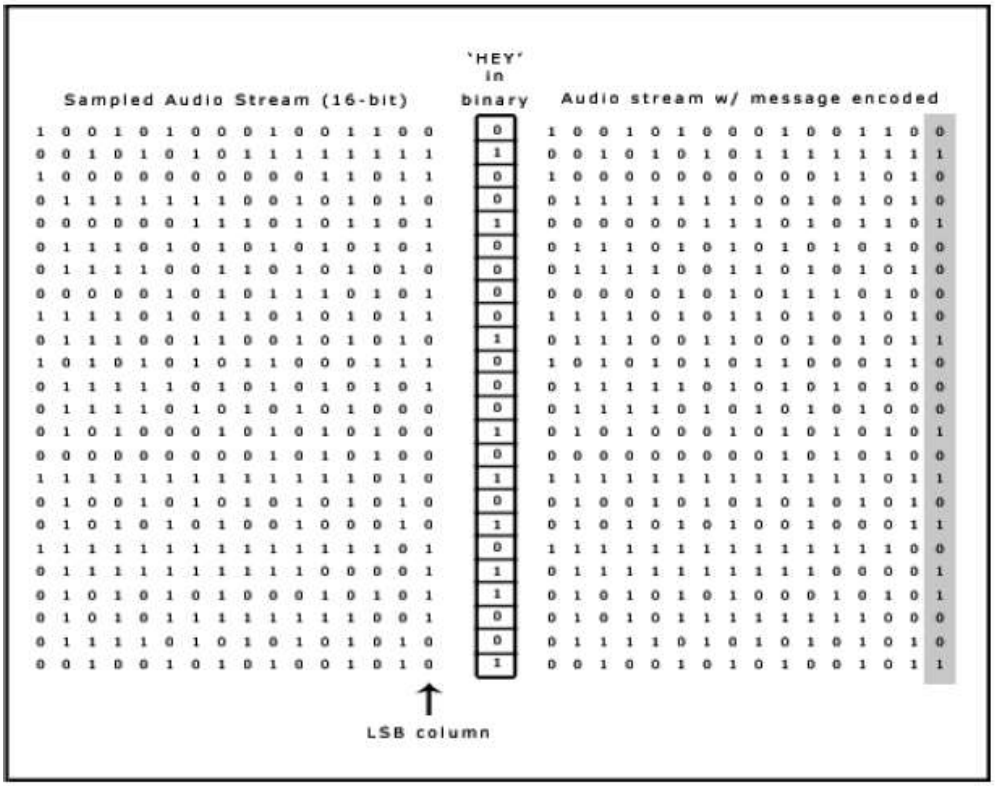

Fig. 3 LSB coding example

3.2 ECHO HIDING

Echo hiding technique embeds secret information in a sound file by introducing an echo into the discrete signal. Echo hiding has advantages of providing a high data transmission rate and superior robustness when compared to other methods. Only one bit of secret information could be encoded if only one echo was produced from the original signal. Hence, before the encoding process begins the original signal is broken down into blocks. Once the encoding process is done, the blocks are concatenated back together to create the final signal [5, 20]. Echo Hiding is shown in Fig.4.

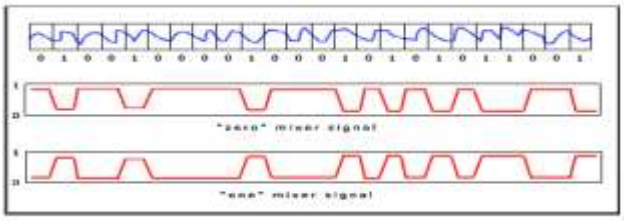

Fig4. Echo hiding

Above we are discussing the disadvantages of the previous procedure and how those are different with present method. The main disadvantages associated with the use of existing methods like echo hiding, spread spectrum and parity coding are, human ear is very sensitive to noise and it can often detect even the slightest bit of noise introduced into a sound file and another problem is robustness.Among different information hiding techniques proposed to embed secret information within audio file, Least Significant Bit (LSB) coding method is the simplest way to embed secret information in a digital audio file by replacing the least significant bit of audio file with a binary message. Hence LSB method allows large amount of secret information to be encoded in an audio file.

4. PROPOSED METHODS

This method uses LSB coding technique for data hiding in audio. However, instead of directly replacing LSBs of digitized samples with the message bits, first we cipher the text message and then hide them in audio file, the cipher method we used private method to increase more secrete to message text ,this private key only the sender and received know them,the following pseudo code show the proposed method of ciphering:

4.1 Hide Algorithm:

This algorithm consist of two stages, these stages contribute to each other to obtain a secure algorithm. The first one is the enciphering stageand the second is embedding stage. Hiding algorithm is based on hoping style. The proposed algorithm details can be described in the following steps:

A. Cipher a Text Message:

Pseudo Code for Cipher a Text Message in Audio File
Read text message and covert it to binary according to its ASCII code. Split text stream into couple char. It mean (16 bit). Convert the four end bit of each char. In the same couple with the other four end bit of the second char. Do this conversion to all couple of text stream.

The cutting process of couple charactors to the text stream shown inFig.5, this proces will make broken of message is very diffeculte.These methods provide an additional level of security.

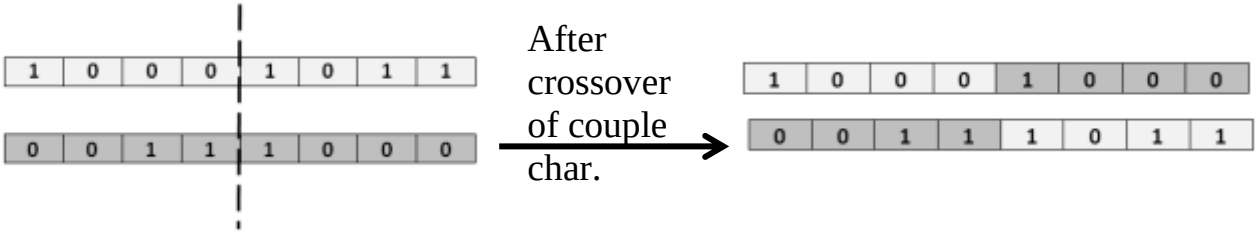

Fig. 5 The Process Cut of Couple Charactors

B. Embed a Text Message:

After cipher text message wasperformed, the XOR operation applied on 7bit LSB and the message bit then the result of XOR operation and to be embedded, the LSB of the sample is modified or kept unchanged. The method described below performs XOR operation on first 2 LSBs to increase the level of encryption.The primary merit of the XOR operation is that it is simple to implement, and it is computationally inexpensive. The steps for data embedding and data retrieval are explained below in Fig.6:

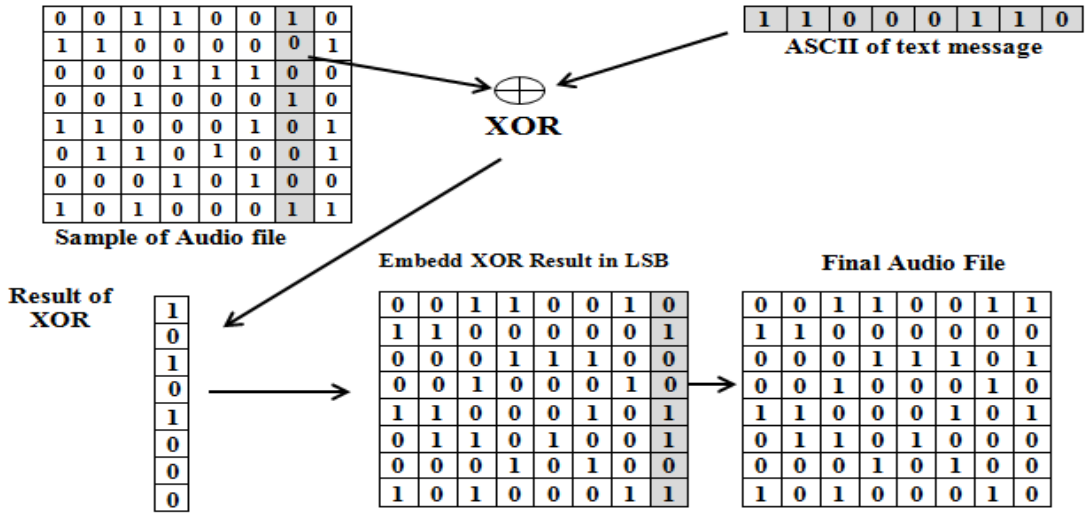

Fig.6EmbedsMethod of Text message Data in Audio File

Pseudo Code for Hide a Text Message in Audio File

1. Get text message from Interface.
2. Read Size of Text message.
if ((Row*Column*8) > count)
'Message too big'
else
Convert message to binary.
Reshape the message binary in a column vector.
 	
End
3. Processing is done as follows:
Take XORing tothe message bit and 7 LSB bit and the result but in 8 LSB bit of audio samples .
Do this step to all text message.
4. Every message bit is embedded into the LSBs of the cover
5. The modified cover audio samples are then written to the file

4.2 Recover Text Message from Audio File:

Pseudo Code for Recover Text Message from Audio File
Read audio file. Take 7LSB bit and 8LSB bit from the audio file. 2. Processing is done as follows: Take XORing tothe 7 LSB bit and the 8 LSB bit of audio samples . Do this step to all audiosample. take the result of XORing and Exchange between every 16bit (i.e.2chr) To rebuilt the right text message that be hide. then written to the file

5. RESULTS AND DISCUSSIONS

In this section, a number of experiments which are used to investigate the effectiveness of our proposed method will be performed. The algorithm is programmed in MATLAB 2010a using different music clips and speech samples. Clips were with varying sampling frequencies, mono audio files, represented by 16 bits per sample. Duration of the clips ranged from 2 to 8 seconds. The secret messages used for embedding text.
The performance of the proposed methods is analyzed in terms of MSE (Mean Squared Error), PSNR (Peak Signal-to-Noise Ratio) and SNR (Signal-to- Noise Ratio). Subjective quality evaluation of these methods has also been carried out by performing listening tests

involving ten persons. From the results of subjective tests, no difference has been found in the perceptual quality of the original audio files and their corresponding stego audio files.

Table 1 Results of XOR method

Cover	MSE	PSNR	SNR
Guitar	1.49e-06	154.57	34.30
Triangle	8.88e-07	156.84	32.99
Speech	8.05e-07	157.27	26.91

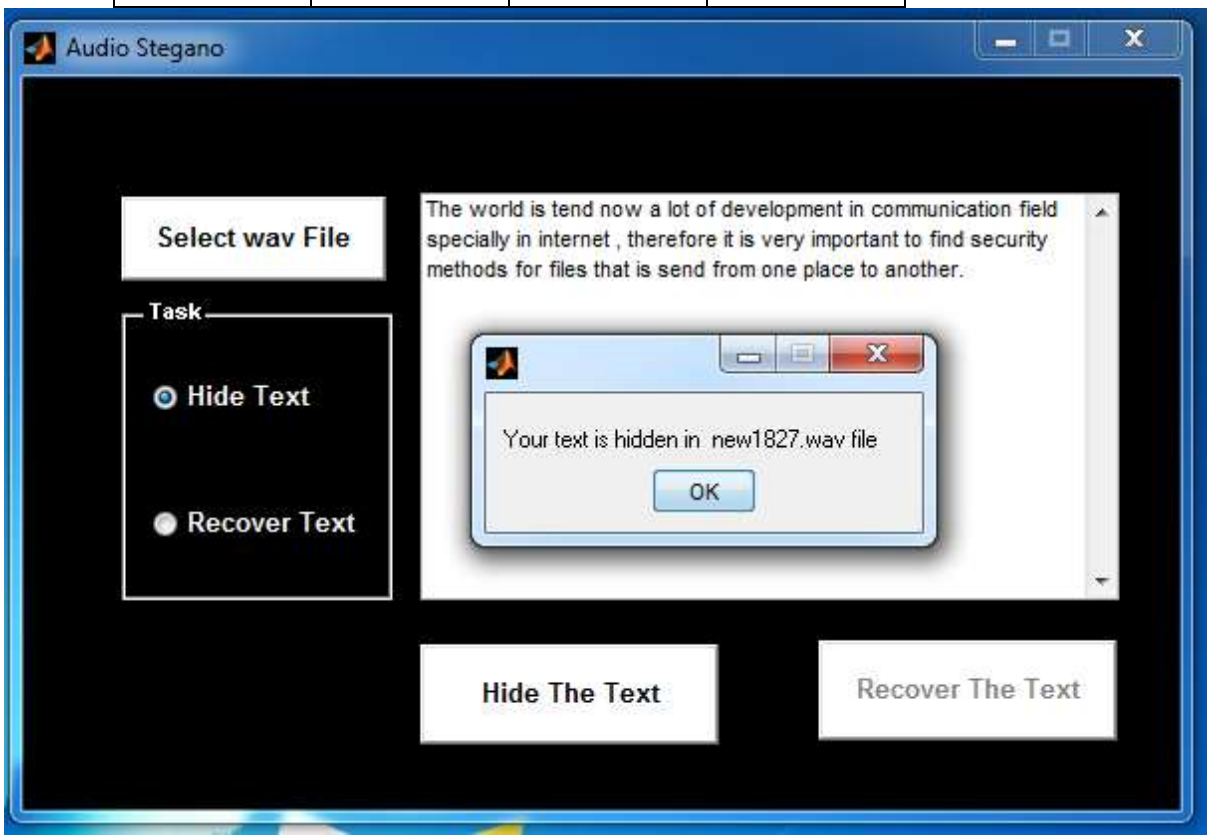

Fig.7 Interface For Hiding Text Message inAudio File

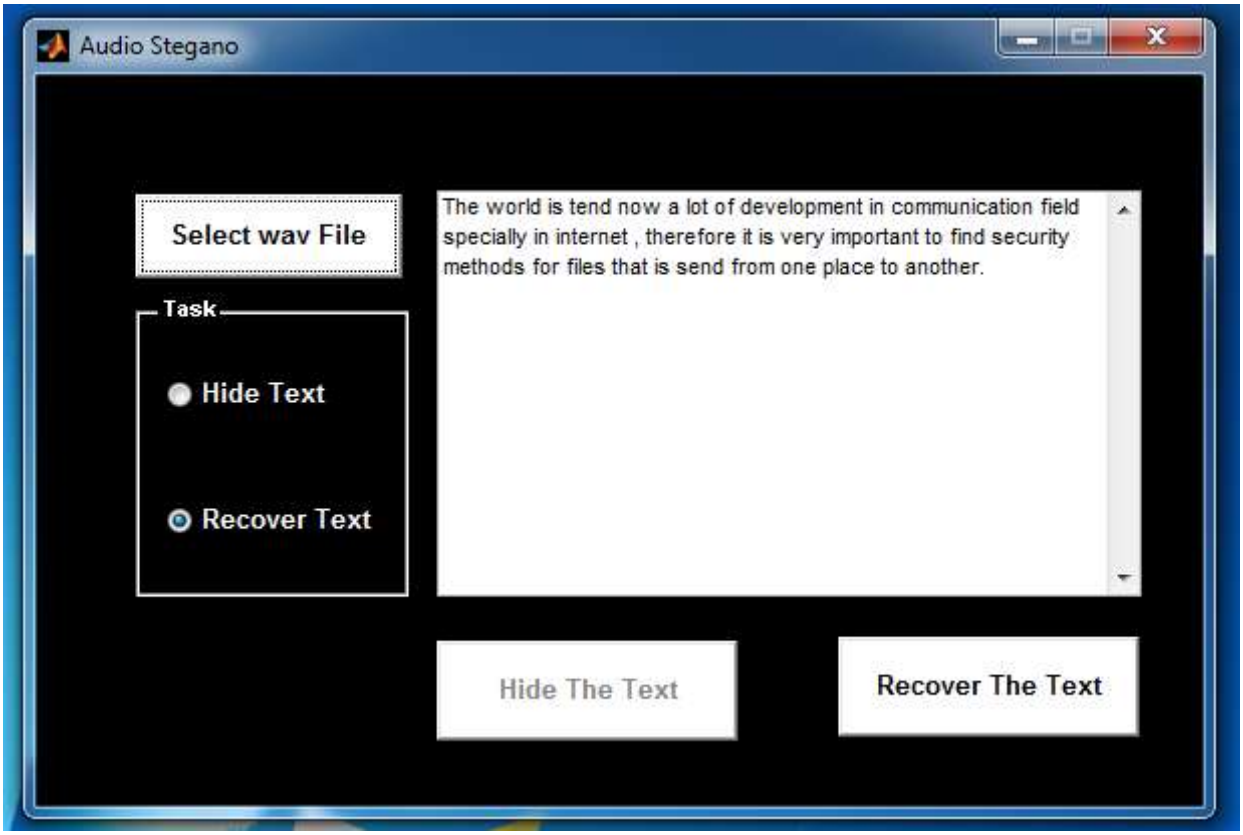

Fig.8 Interface For Recover Text Message from Audio File

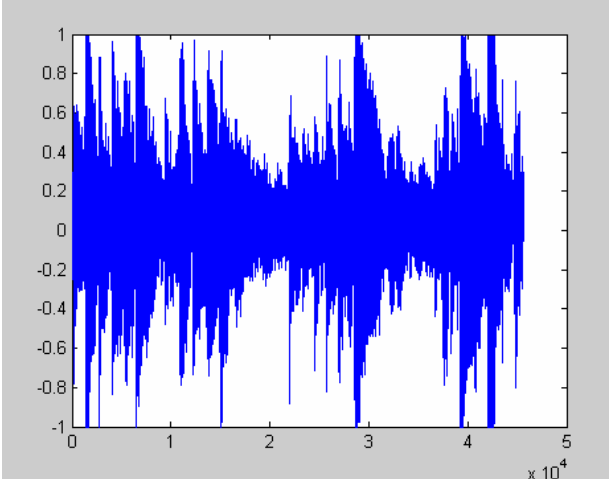

Fig 9-a Show the Signal Before Embeds Data

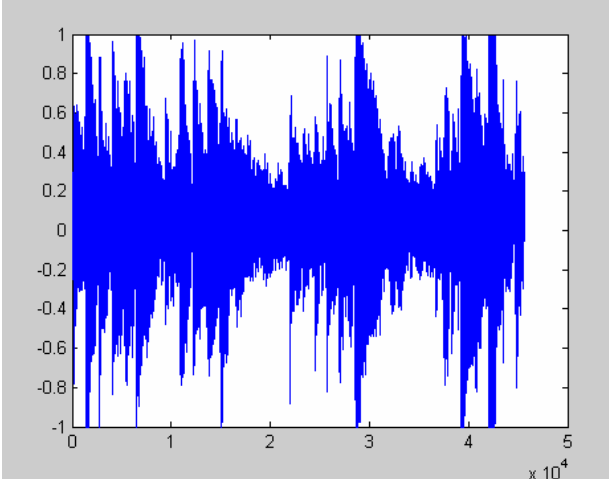

Fig 9-b Show The Signal After Embeds Data

6. CONCLUSION

The paper proposes two methods using LSB coding along with encryption to hide a text message in digital audio files. In the first method, the information is dividing the couple char. into two parts and then exchanges them. In the second method, binary result is hidden by performing XOR operation on7bit LSBs. In both these methods, swap couple char. and indirect LSB extraction will only result in noise. Thus, by using encryption along

with steganography, these methods provide an additional level of security. From experimental results, it is seen that the proposed methods are effective. From listening tests, no difference is found between the original audio signal and the stego audio signal. The hidden information is recovered without any error. This approach increases the capacity of the cover audio by as much as 8 times and also provides robust encryption. This will give great security and the embedded message cannot be extracted without the knowledge of the embedding process.

7. REFERENCES:

[1] Shahreza S.S. and Shalmani M.T.M., "Adaptive wavelet domain audio steganography with high capacity and low error rate", in *Proc. IEEE International Conference on Acoustics,Speech and Signal Processing*, pp: 1729 – 1732, 2008.

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

[3] NedeljkoCvejic , " Algorithms for audio watermarking and steganography", *http://herkules.oulu.fi/isbn9514273842/isbn9514273842.pdf*,

[4] Gary C. Kessler, "Steganography: Hiding Data Within Data", http://www.garykessler.net/library/steganography.html, September 2001.

[5] C. Parthasarathy and Dr. S.K.Srivatsa, "Increased Robustness OfLsb Audio Steganography By Reduced Distortion Lsb Coding" 2005. *www.jatit.org/volumes/research-papers/Vol7No1/9Vol7No1.pdf*,

[6] 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.

[7] Athawale , A.,etal. ,(2010),"Information Hiding in Audio Signals", *International Journal of Computer Applications (0975 – 8887), Volume 7– No.9,IVSL*.

[8] Bhavana.S and K.L.Sudha,(2012)"TEXT STEGANOGRAPHY USING LSB INSERTION METHOD ALONG WITH CHAOS THEORY", arXiv , IVSL.

[9] Jayaram. P, etal. H.S., (2011), "Information Hiding Using Audio Steganography – A Survey", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, IVSL.