ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Audio Steganography using Parity Method at higher LSB layer as a variant of LSB Technique

Jyoti Bahl[1], Dr. R. Ramakishore[2]

Assistant Professor, Dept. of Comp Sc, Poornima University, Jaipur, India

Associate Professor, USICT, GGSIPU, Delhi, India

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 a variant of LSB (Least Significant Bit) technique of audio steganography. In this variant parity method is used for encryption of text and text hiding is implemented at higher LSB layer to achieve high security, high data rate and robustness. The method is briefly explained followed by comparative study. The paper provides information about the existing method, the modified method and the collective discussions. It also describes GUI application to hide data containing text in an audio file such that audio does not lose its original parameters and provides high security by making data hiding undetectable.

KEYWORDS: Steganography, audio, LSB, Data Hiding, Parity

I. Introduction

Steganography is a type of cryptography in which the secret message is hidden. While cryptography is preoccupied with the protection of the contents of a message or information, Steganography concentrates on concealing the very existence of such messages from detection.
The term Steganography is adapted from the Greek word steganographia, meaning "covered writing" and is taken in its modern form to mean the hiding of information inside other information. Naturally these techniques date back throughout history, the main applications being in couriering information during times of war.
Steganography is mainly oriented around the undetectable transmission of one form of information within another. In order for a data hiding technique to be successful it must adhere to two rules:

A. The embedded data must be undetectable within its carrier medium (the audio or image file used). The carrier should display no properties that flag it as suspicious, whether it is to the human visual/auditory system or in increased file size for the carrier file.

B. The embedded data must maintain its integrity within the carrier and should be easily removable when received. Audio Steganography is one kind of steganography in which hidden message is embedded into the audio file.

Various Techniques used for Audio Steganography are:
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.

Parity coding is one of the robust audio steganographic techniques. Instead of breaking a signal into individual samples, this method breaks a signal into separate samples and embeds each bit of the secret message from a parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process inverts the LSB of one of the samples in the region.

Phase coding technique works by replacing the phase of an initial audio segment with a reference phase that represents the secret information. The remaining segments phase is adjusted in order to preserve the relative phase between segments.

Spread spectrum (SS) method attempts to spread secret information across the frequency spectrum of the audio signal. Spread Spectrum method spreads the secret information over the frequency spectrum of the sound file using a code which is independent of the actual signal [2]. As a result, the final signal occupies a bandwidth which is more than what is actually required for transmission.

The main disadvantages associated with the use of existing methods like 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. Phase coding has main disadvantage of low data transmission rate because of the fact that the secret message is encoded only in the first signal segment. Hence this method is used only when a small amount of data needs to be transferred.

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.
In this technique, LSB of binary equivalent of each sample of digitized audio file is replaced with a binary equivalent secret message [3]. A program has been developed which can read the audio file bit by bit and stores them in a different file [3].

II. RELATED WORK

Numerous researches based on audio steganography have been used for performing data hiding. Out of which LSB is one of the most efficient technique. To accomplish effective transmission LSB has gained enormous popularity in recent years. A brief review of some recent significant researches is presented here.
Divya [4], analyzed that compared to standard LSB coding method, embedding data in multiple and variable LSBs depending on the MSBs of the cover audio samples is an efficient approach. There is a remarkable increase in capacity of cover audio for hiding additional data and without affecting the perceptual transparency of the Text and provide the keys concept for secure data. The main advantage of this proposed method is they are simple in logic and the hidden information is recovered without any error.
Xuping Huang [5], proposed synchronized audio to audio technique in which secret speech data is recorded and embedded into audio data when it is playing, as synchronously as trusted receiver extracted secret speech from stego with shared secret key.
Hosai Matsouka [6], proposed the sub-band phase shifting as a method of processing the original audio signal so that the data signal can be easily retrieved at the receiver. It is considered that the pre-processing methods where the original audio signal is processed before embedding is effective.

Ahmad Delforouzi [7], For lossless data hiding, Adaptive Digital Audio Steganography scheme employs integer transform and has high transparency, full recovery and demonstrates correctness of the analytical formula.

III. PROPOSED ALGORITHM

A. *Design Considerations:*

Parity Method

- Even Parity: No. of one's is even.
- Odd Parity: No. of one's is odd.
- Audio cover is splitted into samples of 16 bits.
- Parity of samples is checked, and LSB of sample is modified.

SNR [18] (Signal to Noise Ratio)

$$\mathrm{SNR_{dB}} = 10\log_{10}\left(\frac{A_{\mathrm{signal}}}{A_{\mathrm{noise}}}\right)^2 = 20\log_{10}\left(\frac{A_{\mathrm{signal}}}{A_{\mathrm{noise}}}\right).$$

B. *Description of the Proposed Algorithm:*

The modified algorithm is composed of two variants of LSB. The replacement of LSB is done at higher LSB layer i.e. 6th layer. The parity of samples of cover audio is checked along with secret message bit and accordingly LSB of sample is modified/ unchanged.

Advantages of Proposed Algorithm

1. LSB at higher layer makes it undetectable and unsuspicious.
2. Increased capacity since data is hidden at 6th layer.
3. Parity method provides efficiency to algorithm since it reduces distortion due to noise.

Difficult to detect hidden text.

IV. PSEUDO CODE

1. Read audio file.
2. Read the secret message.
3. Make 16 bit samples of cover audio.
4. Choose LSB to be a higher order bit.
5. Embed the secret message into LSB's of samples.
6. Check the parity of each sample.
7. If parity of sample is even and message to be embedded was 0, no change in LSB.
8. If parity of sample is even and message to be embedded was 1, change LSB to 0.
9. If parity of sample is odd and message to be embedded was 0, change LSB to 1.
10. If parity of sample is odd and message to be embedded was 1, no change in LSB.
11. Transmit the modified audio.
12. At the receiving end, the parity of samples is checked.
13. If parity is odd, message bit is 1.
14. If parity is even, message bit is 0.
15. A vector of received message bits is made and secret message is decoded from these bits.

Graphical User Interface
The designed GUI is user friendly. It helps to perform steganography and Desteganography. Its features are:

1. Read the Audio file.
2. Type the text
3. Hide the text in audio file.

4. Retrieve the text from stego audio
5. Display the retrieved text.

V. RESULTS

The following snapshots describe step by step application of the algorithm.

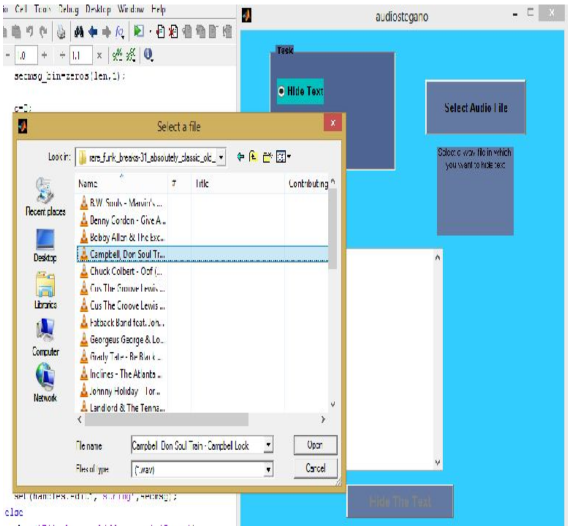
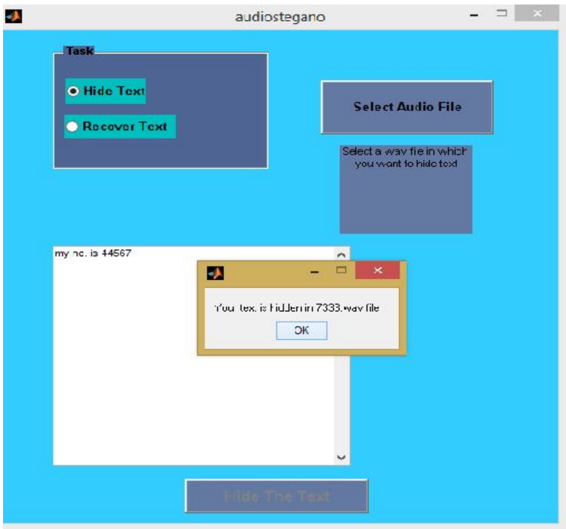


Fig.1 Audio Selection for audio cover



my no. is 44567

You text is hidden in 7333.wav file

Fig. 2. Hidden text in an audio file – Steganography

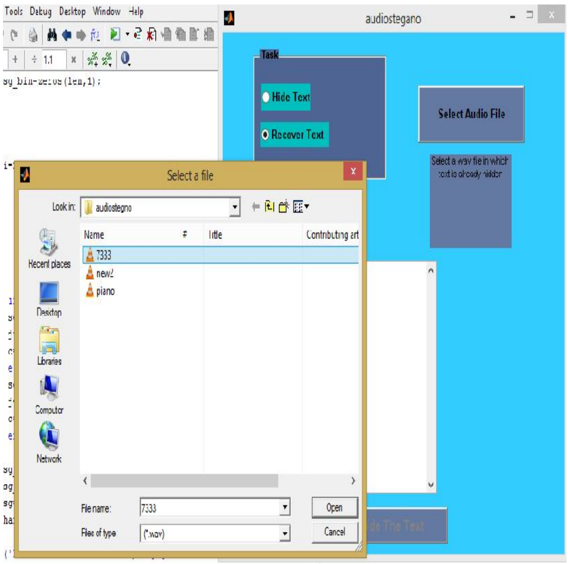
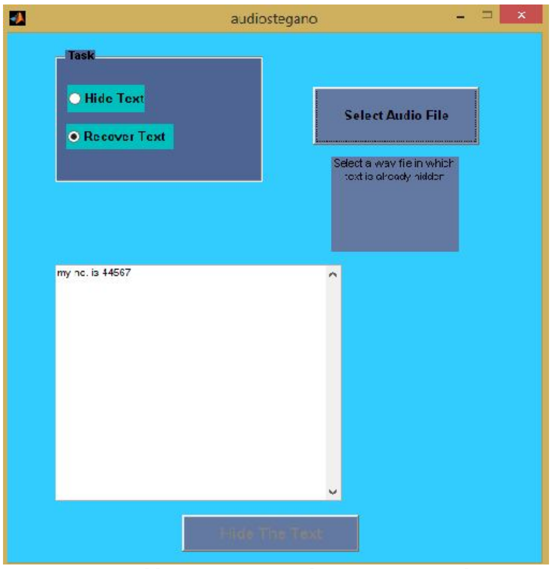


Fig. 3. Selection of audio file to recover text



my no. is 44567

Fig 4. Hidden Text recovered - DeSteganography

Fig 1 describes the snapshot for selection of audio among various available audio files. After selection of audio as the stego cover, the typed text is embedded inside the cover. An audio is generated randomly with text hidden in it as shown by Fig 2. Fig 4 shows that to recover text the same randomly generated audio file is selected and the hidden text appears on the text box as shown in Fig 4.

The following table shows the comparative study of two methods. First being the modified method defined under proposed method section of this paper and second method is the conventional lsb algorithm in which data hiding is done directly in the last bit of the cover audio samples. The comparison has been done by taking same audio signals and the text messages in both the methods. The text could be alphanumeric or any other character.

S.No	**Audio Sample**	**Hidden Text**	**SNR (Signal to Noise Ratio)**	
			Modified Algorithm	Existing Algorithm
1.	new2	Text1	**5.7305e -009**	**1.9864e -009**
2.	piano	Hello to all	**4.2746e -006**	**- 2.5292e -009**
3.	440 sine (audio with noise)	Numeric Text, 6789	**1.7319e -006**	**2.3247e -009**
4.	Campbe ll, Don Soul Train	Alphanum eric Text,my no. is 44567	**4.7281e -008**	**- 3.0347e -010**

Table 1: SNR Comparison

The result shows high SNR in case of modified algorithm proving it to be an efficient approach for implementing audio steganography.

VI. CONCLUSION AND FUTURE WORK

- The modified algorithm provides an efficient method for audio steganography with low complexity, more robustness.
- High SNR as compared to the existing algorithm where hidden message is directly embedded and directly extracted from the LSB of cover audio.
- Easy to use implementation.
- More security such that the secret message is recovered without an error.
- More secured as it is difficult to detect the message.
- High robustness, as in LSB method bits are embedded in LSB, but in the algorithm bits are embedded in higher layer that too modified according to parity.

The paper has possibility of improvements with respect to different type of data hiding like hiding of image into audio, hiding of audio inside audio. This paper is based on work upon .wav files whereas this can be extended to other audio formats like .mp3, .au etc. Audio Processing can be used to reduce noise for more improved PSNR with data hiding.

REFERENCES

1. PeiK. Gopalan, "Audio steganography using bit modification", Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Vol. 2, pp. 421-424, April 2009.
2. Mengyu Qiao, Andrew H. Sung , Qingzhong Liu "Feature Mining and Intelligent computing for MP3 Steganalysis" International Joint Conference on Bioinformatics, Systems Biology and Intelligent Computing 2009.
3. C. C. Chang, T. S. Chen and H. S. Hsia, "An Effective Image Stenographic Scheme Based on Wavelet Transform and Pattern- Based Modification", IEEE Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing, 2003.

4. Hiding Text in Audio using Multiple LSB Steganography and provide Security using Cryptography, S.S. Divya, M. Ram Mohan Reddy, July 2012.
5. Design and implementation of synchronized audio to audio steganography scheme , Xuping Huang
6. Spread Spectrum Audio Steganography using Sub-band Phase Shifting, Hosei Matsuoka .
7. Adaptive Digital Audio Steganography Based on Integer Wavelet Transform, Ahmad Delforouzi, Mohammad Pooyan.
8. "Face Recognition Using IPCA-ICA Algorithm", Issam Dagher and Rabih Nachar.
9. Gary c Kessler,"Steganography: Hiding Data within Data", September 2001.
10. C. Parthasarathy and Dr. S.K. Srivatsa,"Increased Robustness of LSB Audio Steganography by reduced distortion of LSB coding.
11. 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
12. S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.

BIOGRAPHY

Jyoti Bahl has worked as an Assistant Professor in Computer Science Department of Poornima University, Jaipur as well as in MCA college (BCIIT) of Guru Gobind Singh Indraprastha University, Delhi. She received Master of Technology (IT) in 2013 from USIT, GGSIPU and Master of Computer Application (MCA) degree in 2009 from BCIIT, GGSIPU, Delhi, India. Her research interests are Image Processing, Signal Processing, Pattern Matching, Algorithms etc.