Volume 4, Issue 7, July 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

3 Level Dwt Audio Steganography

Mahesh S Patel
PG Students, Department
Of Electronics & Communication,
PCST, Bhopal, India

Hemant Kumar Soni
Assistant.Professor, Department
of Electronics & Communication,
PCST, Bhopal, India

Sameena Zafar
HOD, Department
of Electronics & Communication,
PCST, Bhopal, India

Abstract:-Data transmission over the communication media will not secure in recent scenario. Different type of secure data transmission technique will developed in past few years. One of the most useful and efficient data hiding techniques is watermarking. Many works done in this data hiding technique related to image watermarking techniques. This paper focused on the data (Image or text) hiding using audio which is known as audio steganography.

Keywords: Audio steganography, DWT, LSB modified steganography, 3 Level DWT,Data Hiding

I. INTRODUCTION

Before the invention of steganography and cryptography, it was challenging to transfer secure information and, thus, to achieve secure communication environment [1]. Some of the techniques employed in early days are writing with an invisible ink, drawing a standard painting with some small modifications, combining two images to create a new image, shaving the head of the messenger in the form of a message, tattooing the message on the scalp and so on. Normally an application is developed by a person or a small group of people and used by many. Hackers are the people who tend to change the original application by modifying it or use the same application to make profits without giving credit to the owner. It is obvious that hackers are more in number compared to those who create. Hence, protecting an application should have the significant priority. Protection techniques have to be efficient, robust and unique to restrict malicious users. The development of technology has increased the scope of steganography and at the same time decreased its efficiency since the medium is relatively insecure. This lead to the development of the new but related technology called "Watermarking". Some of the applications include ownership protection, proof for authentication, air traffic monitoring, medical applications etc. [1] [2] [3]. Steganography for audio signal has greater importance because the music industry is one of the leading businesses in the world. Data (image or text) are embedding on the audio and that embedded audio will send to the destination. Least Significant Bit (LSB) of the host audio signal will replaced with the secret test or data image. The conversion from time domain to frequency and vice-versa will do during embedding and extraction process utilize discrete wavelet transform (DWT).

This paper contains four sections. Section I will give an introduction about the audio steganography and its background. Section II will focus on the related work done in audio steganography. Section III will discuss the methodology used in audio steganography. Section IV gives result of audio steganography.

II. LITERATURE REVIEW

An audio steganography technique could be grouped into two assemblies dependent upon the area of operation. Steganography is implementing using audio as host and image or text as watermark data or secret data. Least significant bit (LSB) is used for watermarking process on the audio. Few work done by researchers [4,5] on this technique, which is one of the common techniques employed in signal processing applications. It is based on the substitution of the LSB of the carrier signal with the bit pattern from the stego noise [4]. The robustness depends on the number of bits that are being replaced in the host signal [4, 5]. This type of technique is commonly used because, each frame is represented as an integer hence it will be easy to replace the bits. The audio signal has real values as samples, if converted to an integer will degrade the quality of the signal to a great extent. The operation of the 2-bit LSB coding is shown in Figure 2.1.

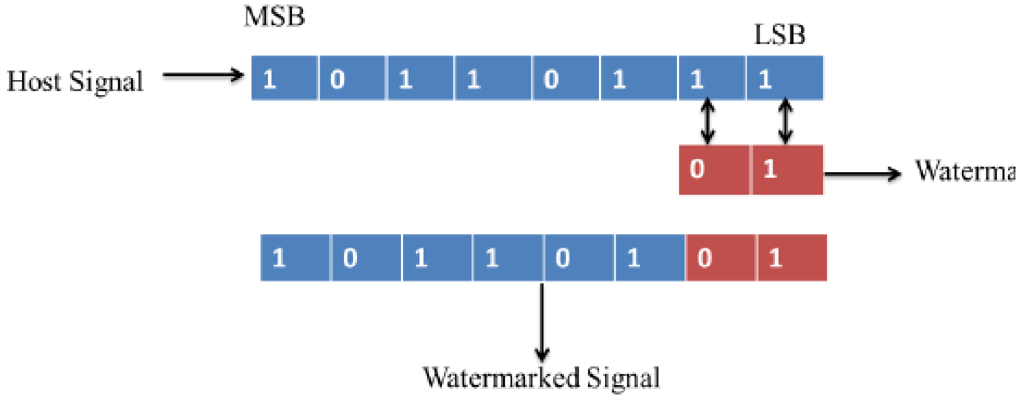


Figure 2.1: 2-Bit LSB modification

III. AUDIO STEGANOGRAPHY TECHNIQUES

(1) LSB: LSB [9], [10] is one of the earliest and simplest methods for hiding information in audio signals. It is the commonly used technique for audio steganography. In LSB encoding, the least significant bits of the cover media/original audio is altered to include the secret message.

(2) Parity coding:Parity coding technique [7], [8] operates on a group of samples instead of individual samples. Here individual samples are grouped and parity of each group is calculated. For inserting message bit one by one, check the parity bit of a group of samples

(3) Echo hiding: In echo hiding [11] method data is embedded in the echo part of the host audio signal. The echo is a resonance added to the host signal and hence the problem with the additive noise is avoided here. While using echo hiding three parameters are to be considered: they are initial amplitude, offset (delay), and decay rate, so that echo is not audible. The main disadvantage of this method is lenient detection and low detection ratio.

(4) Wavelet domain: [12] is suitable for frequency analysis because of its multi-resolution properties that provides access to both most significant parts and details of spectrum. Wavelet domain techniques works with wavelet coefficients. Upon applying the inverse transform, the stegano signal can be reconstructed.

Summary of Audio Stegnography Techniques:

Method	**Strength**	**Weakness**
LSB	Simple	Easy to Extract
Parity Coding	More Robust than LSB	Easy to Extract
Echo Hiding	Avoids Problem with additive noise	Low Capacity
Wavelet Domain	High Hiding Capacity & Transparency	Lossy Data retrieval

(5) Proposed Technique

In this paper discrete wavelet transform (DWT) is used for steganography. Majority of the signals in practice are represented in time domain. Time-amplitude representation is obtained by plotting the time domain signal. However, the analysis of the signal in time domain cannot give complete information of the signal since it cannot provide the different frequencies available in the signal. Frequency domain provides the details of the frequency components in the signal [6], which are importance in some applications. The frequency spectrum of a signal is basically the frequency components (spectral components) of that signal.

Time domain representation can provides details of the signal strength at certain time. Whereas, the frequency domain provides the frequencies present in the signal. Thus, frequency domain does not provide any information about the time scales where the signal has a certain frequency and vice-versa. Wavelet domain provides the time-frequency relationship of the signal; allowing to find the sensitive parts for embedding additional information into the signal [5, 6]. For analysis and finding the dc-components and elementary frequency components discrete cosine transformations are used. Inserting additional information throughout the signal will render the quality of signal due to the inclusion of more noise (additional information). Thus, choosing the signal with particular energy levels will increase the quality of the signal.
The steganography technique is divided into two blocks embedding and extraction. Embedding block is used to add the additional information into the host signal; whereas, extraction block is used to extract the stego information embedded in the audio signal. The stego information embedded is a binary image of dimension.
Audio steganography process is shown in figure 3.1..

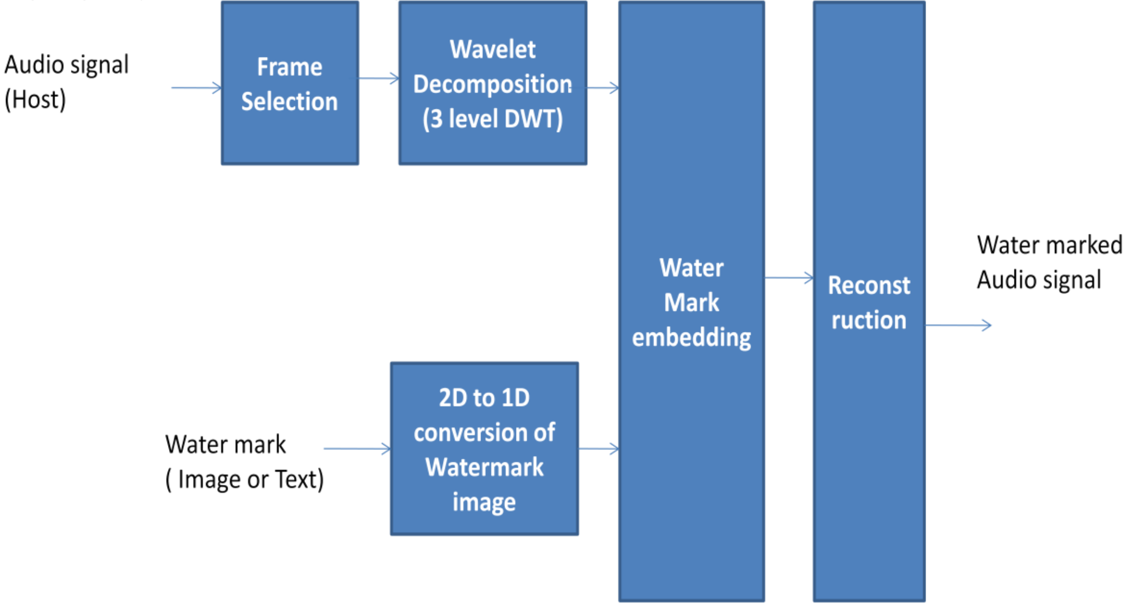
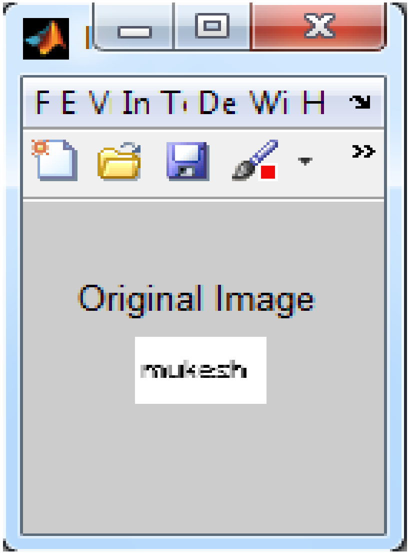

Audio signal
(Host)
Frame Selection
Wavelet Decomposition (3 level DWT)
Water Mark embedding
Reconst ruction
Water marked Audio signal
Water mark
(Image or Text)
2D to 1D conversion of Watermark image

Figure 3.1: Audio steganography embedding

IV. EXPERIMENTAL RESULTS

Experiment is carried out through MATLAB. Original image which is watermark image is shown in figure 4.1 as below. This watermark image is embedded in the audio which is show in figure 4.2.



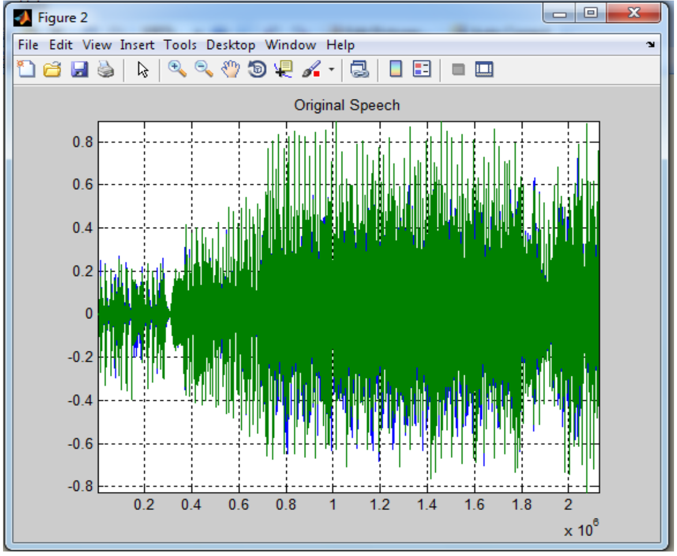
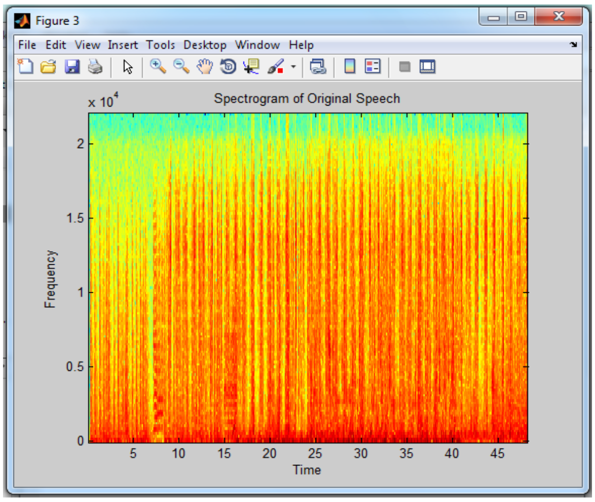


Figure 4.1: Watermark Image

Figure 4.2: Original Audio Speech

Figure 4.3 is the spectrogram of the original speech which represents the frequency component with respect to time. After this conversion into frequency text image will embedded on it and steganography audio speech is shown in the figure 4.4. The stenographic audio speech spectrograph is also shown in figure 4.6.



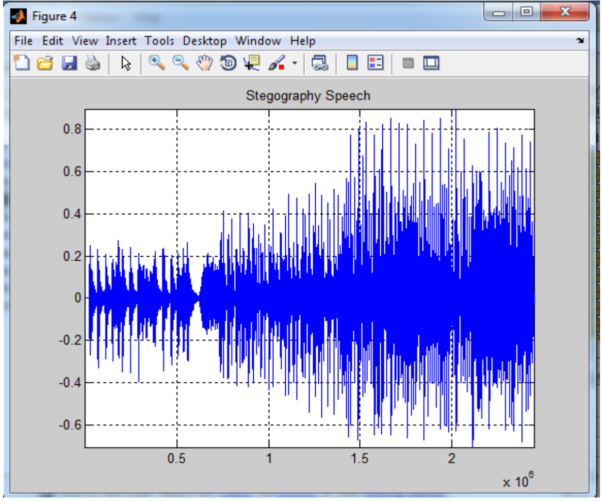


Figure 4.3: Spectrogram of Audio Speech

Figure 4.4: Steganography Audio Speech

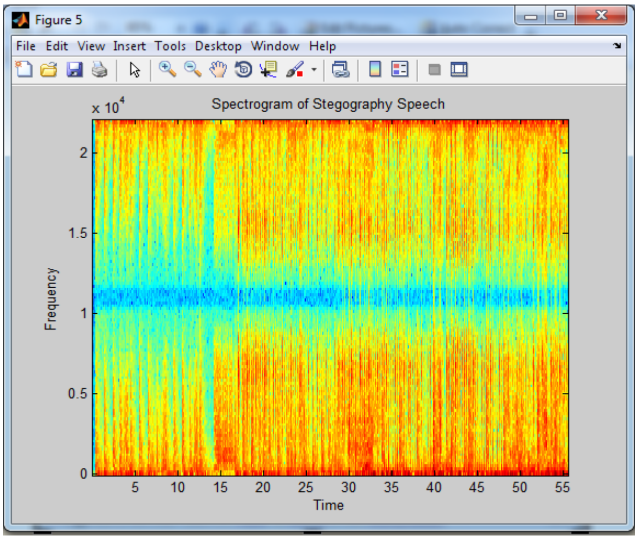
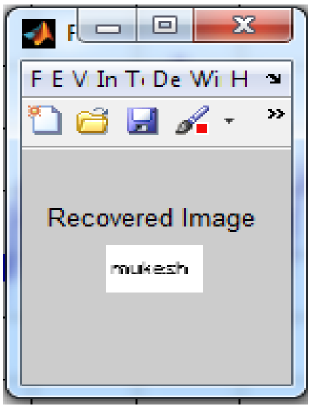


Figure 4.5: Spectrogram of Steganography Audio Speech

Now for reconstruction of the original text image from the steganography audio speech, extraction process is carried out and recovered image is shown in figure 4.6.



Recovered Image

mukesh

Figure 4.5 Recovered Image from Steganography Audio

V. CONCLUSION

Basic concept of Audio steganography was discussed in this paper with its past work done by the different researches and their techniques used for audio steganography. Time domain to frequency domain conversion with the help of DWT is used instead of Bit modification of the host audio with the LSB of the watermark image/text. Results are accurate an image also extracted exactly. From summary of Audio stegnography it can be seen by using DWT techniques PSNR value will be high as compare to othe techniques and MSE will be low compare to other method.

REFERENCES

[1] N.F. Johnson, S. Jajodia, and Z. Duric, Information hiding: Steganography and watermarking attacks and countermeasures, Kluwer academic Publishers, 2000.

[2] X. Wang, and H. Zhao, “A Blind Audio Watermarking Robust Against Synchronization Attacks,” CIS 2005, Part II, LNAI 3802, pp. 617-622, 2005.

[3] S. Katzenbeisser, and F.A.P. Petitcolas, Information hiding techniques for steganography and digital watermarking, Artech House Publishers, 2000. C. V. Hari, J. Joseph, S. Gopi, V. P. Felix, and J. Amudha, “Mid-point Hough transform: A fast line detection method,” in Proceedings of IEEE INDICON 2009, pp. 237–240, 2009.

[4] Mazdak Zamani, Azizah Bt Abdul Manaf, Rabiah Bt Ahmad, Farhang Jaryani, “A secure audio steganography approach”, International Conference for Internet Technology and Secured Transactions, Page(s): 1 – 6, 2009.

[5] Kaliappan Gopalan., “Audio steganography using bit modification”, 2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, Page(s): II - 421-4 vol.2.

[6] Ankit Chadha, Neha Satam, Rakshak Sood, and Dattatray Bade, “An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution”, International Journal of Computer Applications (0975 – 8887) Volume 77– No.13, September 2013.

[7] P. Jayaram, H. Ranganatha, and H. Anupama, “Information hiding using audio steganography-a survey”, International Journal of Multimedia and its Applications, 2011.

[8] H. Kekre, A. Athawale, S. Rao, and U. Athawale, “Information hiding in audio signals”, International Journal of Computer Applications, IJCA, vol. 7,no. 9, pp. 14-19, 2010.

[9] M. Asad, J. Gilani, and A. Khalid, ”An enhanced least significant bit modification technique for audio steganography”, 2011 International Conference on Computer Networks and Information Technology (ICCNIT), IEEE, 2011.

[10] 10 K. Bhowal, A. Pal, G. Tomar, and P. Sarkar, “Audio steganography using GA”, 2010 International Conference on Computational Intelligence and Communication Networks (CICN), IEEE, 2010.

[11] F. Djebbar, B. Ayad, H. Hassmam, and K. Abed-Meraim, “A view on latest audio steganography techniques”, 2011 International Conference on Innovations in Information Technology (IIT), IEEE, 2011.

[12] S. Shahreza and M. Shalmani, “High capacity error free wavelet domain speech steganography", IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2008