International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 1 Issue 3 June 2014

Three Level Audio Steganography

Sawaliya K. Patidar
Bhanpura, India
Sawaliyakumar84@yahoo.co.in

Abstract: - *Information transmission over the communication media will not secure in recent state of affairs. Completely different kind of secure information transmission technique will developed in past few years. One in all the foremost useful and economical information concealment techniques is watermarking. Many works drained this information concealment technique related to image watermarking techniques. This paper targeted on the information (Image or text) concealment exploitation audio that's understood as audio steganography.*

Keywords: - *Audio steganography, DWT, LSB modified steganography, 3 Level DWT*

1. INTRODUCTION

Before the invention of steganography and cryptography, it absolutely was difficult to transfer secure information and, thus, to attain secure communication setting [1]. a number of the techniques utilized in period are writing with an invisible ink, drawing a regular painting with some small modifications, combining 2 pictures to form a replacement image, shaving the pinnacle of the traveler within the kind of a message, tattooing the message on the scalp so on. Usually an application is developed by someone or a small cluster of individuals and utilized by several. Hackers are those that tend to vary the initial application by modifying it or use an equivalent application to form profits while not giving credit to the owner. It's obvious that hackers are additional in variety compared to those that produce. Hence, protective an application ought to have the many priority. Protection techniques need to be economical, strong and distinctive to limit malicious users. The event of technology has inflated the scope of steganography and at an equivalent time shriveled its potency since the medium is comparatively insecure. This cause the event of the new however connected technology referred to as "Watermarking". a number of the applications embrace possession protection, proof for authentication, traffic observation, medical applications etc. [1] [2] [3]. Steganography for audio signal has greater importance as a result of the music business is one in every of the leading businesses within the world. Information (image or text) are embedding on the audio which embedded audio can send to the destination. Least vital Bit (LSB) of the host audio signal can replaced with the key test or information image. The conversion from time domain to frequency and vice-versa can do throughout embedding and extraction method utilize discrete wavelet transform (DWT).

This paper contains four sections. Section I will provide an introduction regarding the audio steganography and its background. Section II can specialize in the related work wiped out audio steganography. Section III will discuss the methodology utilized in audio steganography. Section IV provides results of audio steganography.

2. LITERATURE REVIEW

An audio steganography technique might be classified into 2 assemblies dependent upon the area of operation. Steganography is implementing victimisation audio as host and image or text as watermark information or secret information. Least significant bit (LSB) is employed for watermarking method on the audio. Few work done by researchers [4,5] on this method, that is one in every of the common techniques utilized in signal process applications. It's supported the substitution of the LSB of the carrier signal with the bit pattern from the steganography noise [4]. The strength depends on the quantity of bits that are being replaced within the host signal [4, 5]. This kind of technique is usually used as a result of, every frame is diagrammatic as an integer therefore it'll be simple to switch the bits. The audio signal has real values as samples, if born-again to an integer can degrade the standard of the signal to a good extent. The operation of the two-bit LSB committal to writing is shown in Figure 1.

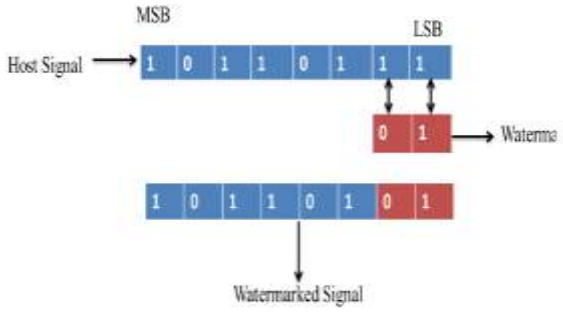

Fig. 1: 2-Bit LSB modification

3. AUDIO STEGANOGRAPHY TECHNIQUES

3.1 LSB

LSB [9], [10] is one in every of the earliest and simplest strategies for concealing information in audio signals. It's the normally used technique for audio steganography. In LSB encoding, the smallest amount important bits of the

cover media/original audio is altered to incorporate the key message.

3.2 Parity coding

Parity coding technique [7], [8] operates on a bunch of samples rather than individual samples. Here individual samples are classified and parity of every cluster is calculated. For inserting message bit one by one, check the check bit of a bunch of samples

3.3 Echo hiding

In echo hiding [11] methodology information is embedded within the echo a part of the host audio signal. The echo could be a resonance supplementary to the host signal and thus the matter with the additive noise is avoided here. Whereas mistreatment echo hiding 3 parameters are to be considered: they're initial amplitude, offset (delay), and decay rate, in order that echo isn't audible. The most disadvantage of this methodology is lenient detection and low detection quantitative relation.

3.4 wavelet domain

[12] Is appropriate for frequency analysis due to its multi-resolution properties that has access to each most important elements and details of spectrum. Wavelet domain techniques works with wavelet coefficients. Upon applying the inverse transform, the steganography signal will 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

4. PROPOSED TECHNIQUE

In this paper discrete wavelet transform (DWT) is employed for steganography. Majority of the signals in observe are portrayed in time domain. Time-amplitude illustration is obtained by plotting the time domain signal. However, the analysis of the signal in time domain cannot provide complete information of the signal since it cannot give the various frequencies on the market within the signal. Frequency domain provides the main points of the frequency elements within the signal [6] that are importance in some applications. The frequency spectrum of a signal is largely the frequency elements (spectral components) of that signal.

Time domain illustration will provides details of the signal strength at bound time. Whereas, the frequency domain provides the frequencies gift within the signal. Thus, frequency domain doesn't give any information regarding the time scales wherever the signal contains a sure frequency and vice-versa. Wavelet domain provides the time-frequency relationship of the signal; permitting to seek out the sensitive elements for embedding extra information into the signal [5, 6]. For analysis and finding the dc-components and elementary frequency elements separate cosine transformations are used. Inserting extra information throughout the signal can render the standard of signal because of the inclusion of a lot of noise (additional information). Thus, selecting the signal with specific energy levels can increase the standard of the signal.

The steganography technique is split into 2 blocks embedding and extraction. Embedding block is employed to add the extra information into the host signal; whereas, extraction block is employed to extract the steganography information embedded within the audio signal. The steganography information embedded could be a binary image of dimension.

Audio steganography method is shown in figure two.

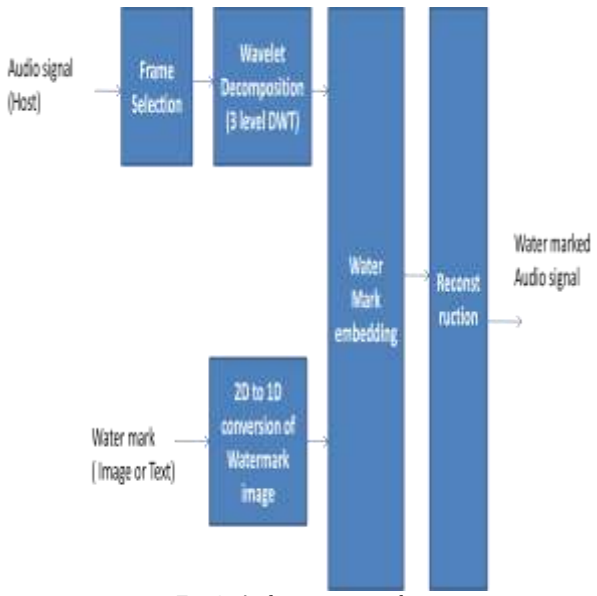

Fig. 2: Audio steganography

5. EXPERIMENTAL RESULTS

Experiment is meted out through MATLAB. Original image that is watermark image is shown in figure three as below. This watermark image is embedded within the audio that is show in figure four.

Fig. 3: Watermark Image

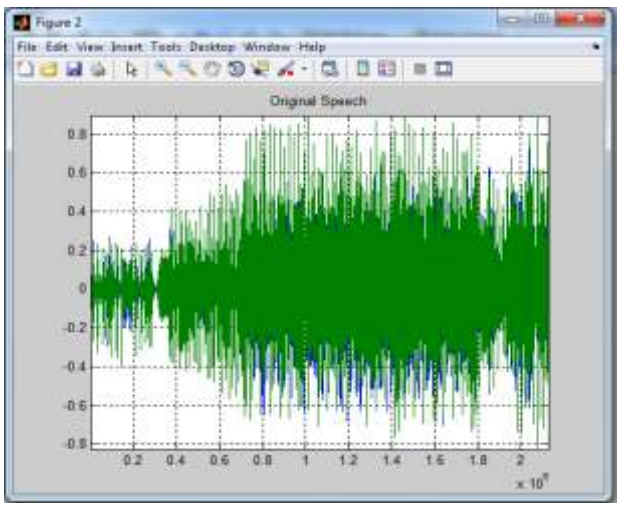

Fig. 4: Original Audio Speech

Figure five is that the photograph of the first speech that represents the frequency element with relevance time. When this conversion into frequency text image can embed thereon and steganography audio speech is shown within the figure six. The stenographic audio speech spectrograph is additionally shown in figure seven.

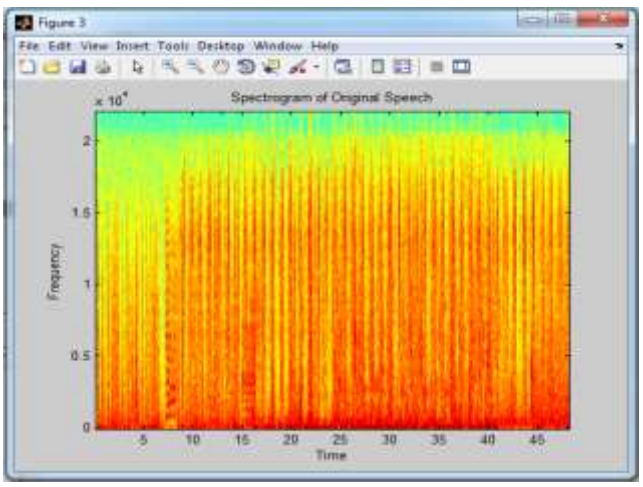

Fig. 5: Spectrogram of Audio Speech

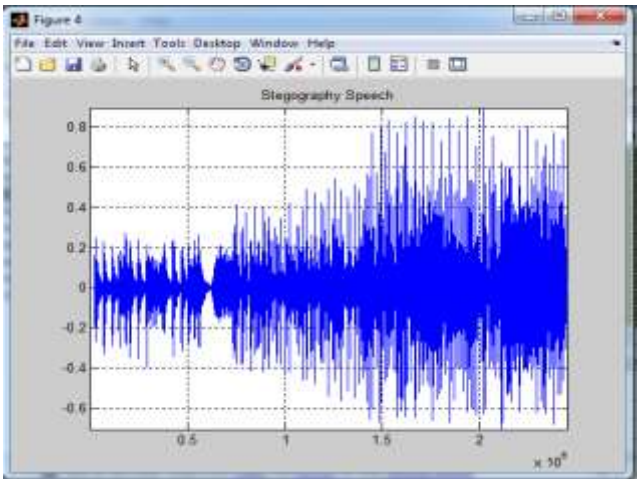

Fig. 6: Steganography Audio Speech

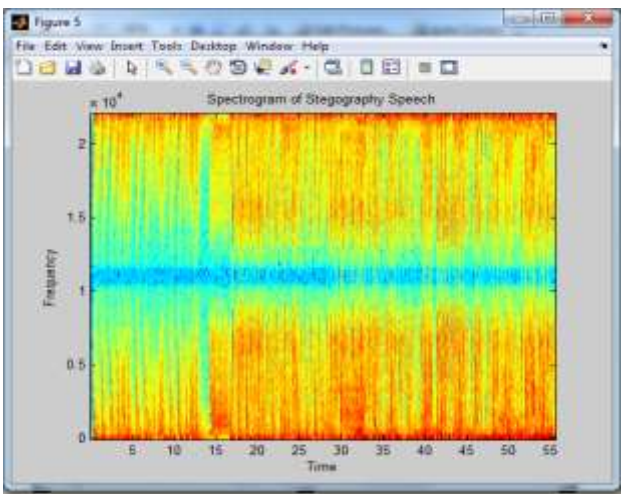

Fig. 7: Spectrogram of Steganography Audio Speech

Now for reconstruction of the first text image from the steganography audio speech, extraction method is disbursed and recovered image is shown in figure eight.

Fig. 8: Recovered Image from Steganography Audio

6. CONCLUSION

Basic conception of Audio steganography was mentioned during this paper with its past work done by the various

researches and their techniques used for audio steganography. Time domain to frequency domain conversion with the assistance of DWT is employed rather than Bit modification of the host audio with the LSB of the watermark image/text. Results are correct a picture conjointly extracted specifically. From outline of Audio stegnography it will be seen by mistreatment DWT techniques PSNR worth are high as compare to other techniques and MSE are low compare to different methodology.

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]. 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