International Journal of advancement in electronics and computer engineering (IJAECE)
Volume 5, Issue 5, Sep.2016, pp.980-982, ISSN 2278 -1412

Dwt and Lsb Based Audio Steganography- A Review

Punita Parnami[1], Manish Trivedi[2]
[1]*Mtech. Scholar, Department of ECE RKDFIST, punitaparnami@gmail.com, India;*
[2,] *Associate Prof., Department of ECE RKDFIST,trivedi.work@gmail.com, India;*

Abstract *– Steganography may be a technique for hiding data in a host signal. The host signal may be a still image, speech or video and therefore the message signal that's hidden within the host signal can be a text, image or an audio signal. For data hiding in acoustic, discrete cosine transform (DCT) and discrete wavelet transform (DWT) both are used. Perfect audio Steganography technique aim at embedding data in an imperceptible, robust and secure way and so extracting it by authorized people. Hence, up to this point the main challenge in digital audio steganography is to get robust high capacity steganography systems. Leaning towards designing a system that ensures high capacity or robustness and security of embedded data has LED to great diversity within the existing steganography techniques. In this paper, we tend to present a existing position of art literature in digital audio steganography technique. In this paper a completely unique methodology for digital audio steganography someplace encrypted concealed data is embedded by adaptively modifying wavelet packet coefficients of host audio signal. Steganography is an information hiding technique where secret message is embedded into unsuspecting cover signal. Measuring of fine steganography algorithmic rule includes security, capacity, robustness and imperceptibility.*

Keywords*: Audio steganography*, DWT, PSNR, LSB.

I. Introduction

Steganography is the idea of hiding the existence of secret info by concealing it into another medium like image or audio. It originates from the Greek word steganos (covered) and graptos (writing). Steganography is completely different from cryptography, which is the science of hiding the meaning of information. Steganography and watermarking techniques embed info in a digital media in a transparent manner. Steganography may be a technique for covert info, but digital watermarking may not hide the existence of the message from 3rd persons.

Steganography is usually employed in covert communication in military application and government communication application. Often it needs relatively high payloads in comparison to watermarking. The major needs that should be glad for good steganography algorithms include perceptual transparency, payload or capacity and robustness. High capacity is considered as a very important aspect for steganography when compared to watermarking. For watermarking, robustness must be a main aspect. Improvement for one among the mentioned requirements will tend to degrade the other performances as they're contradictory consistent with the magic triangle. Steganography has evolved into a digital strategy of hiding a get into some type of muItimedia, such as an image, an acoustic file (like a .wav or mp3) or maybe a video file [1]. Stenographic systems are often divided into 2 classes. In which one is very existence of the message is kept secret and different non-steganography Systems. The main goal of steganography is to communicate securely in an exceedingly completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. That’s not to information even exists. Steganography is of 3 types Audio, Image and Video.Through image steganography is that the additional illustrious of the 2, audio steganography is nowadays more secure due to the fact that the hackers don't suspect the presence of a hidden message in an audio file.

Main goal of steganography is to communicate securely in a entirely imperceptible way and to avoid drawing suspicion to the transmission of a hidden data. It’s not only prevents others from knowing the hidden data, simply it also prevents others from thinking that the data even exists. Although a steganography technique causes somebody to suspect there's secret info in a carrier medium, then the method has failed. The ways that embeds data in sound files use the properties of the Human auditory system (HAS).

II. Literature Review

Neha Gupta et. al. [1] “Dwt and Lsb Based Audio Steganography” In this the main aim is to come up with a method to hide the information in audio file in such the way there aren't any perceivable changes within the audio file after the message insertion. Also, if the message that's to hidden was also encrypted then the level of security could be hidden was furthermore encrypted then the level of security would be further elevate to a extra reasonable level. The someone whom got the message would only have the encrypted type of the message with no approach of decrypting it so the hidden messages were to be discovered. Planned scheme has been discussed in this article for implant image in hidien aural file. Emphasis is on proposed scheme from simple LSB based mostly data hiding in acoustic, and their robustness in expression of steganolysis. Proposed methodology is better by using the concept of DWT (Discrete wavelet Transform) along with LSB system. By means of taking the higher frequency from DWT and using in LSB (Least significant Bit) we get the PSNR values.

Mansour Sheikhan et. al.[2] “Improvement of Embedding Capacity and Quality of DWT-Based Audio Steganography Systems”, in this paper within which information hiding is performed in a hybrid format. In this way, the host signal has been segregated into several subbands through DWT. The energy of given subbands are compared with human being's hearing threshold and therefore the subbands have been classified into 3 types: subbands with energy state advanced than around equal to lesser than the hearing threshold, respectively. Information hiding has been performed in LSBs of DWT coefficients and for subbands with lower energy level than hearing threshold, direct message replacement in DWT subbands has been applied. Since only those subbands have been utilised for steganography which have lower/equal energy as compared to the hearing threshold.

Ankit Chadha et. al. [3] “An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution”, in this the main advantage of the method could be a very high watermark channel capacity; the use of only 1 LSB of the host audio sample provides capacity of 44.1 kbps. The obvious disadvantage is the extremely low robustness of the method, because of proven fact that random changes of the LSBs destroy the coded watermark. In addition, it's most unlikely that embedded watermark would survive digital to analogue and subsequent analogue to digital exchange. Since no computationally demanding transformation of the host signal within the basic version of this technique has to be done, this algorithmic rule includes a very small algorithmic delay. This permits the exploit on this LSB in instantaneous use. This algorithm rule is a good basis for steganographic applications for audio signals and a base for steganalysis.

Fatiha Djebbar et. al. [4] “A view on latest audio steganography techniques”, in this paper to ensure digital information security, various techniques has been given in recent researchers work. Audio steganography, in particular, addresses problems related to the need to secure and care for the reliability of data hidden in tone of voice communications, even when the latter passes through insecure channels. This paper presents a review of the current state of art literature in digital audio steganography techniques and approaches. Paper existing some of the main interesting audio steganography method. In the paper discussed their potentials and limitations in ensuring secure communication. In paper point of view, a comparison and an analysis for the reviewed techniques has been also given. The advantage on using one technique over another one depends strongly on the form of the function and its necessity like hiding capacity or the type of attacks that may encounter the transmitted signal.

Haider Ismael Shahadi et. al. [5] “High Capacity and Inaudibility Audio Steganography Scheme”, in this a high capacity and high stego-signal quality audio steganography scheme based on DWPT and bits block corresponding. The DWPT, bits block corresponding, and adaptive implant in LSB of canopy samples depend upon their strength are enabled the algorithmic program to realize very high embedding capacity for various data type which will reach up to forty two take pleasure in the input audio file size with lest of fifty decibel SNR for the output stego signal.

Mazdak Zamani et. al. [6] “Efficient Embedding for Audio Steganography”, in this paper Steganography may be a type of security technique through obscurity; the science and art of hiding the existence of a communicational message among sender and intentional recipient. Steganography has been used to hide secret messages in various kinds of files, including digital images, audio and video. The 3 most significant parameters for audio steganography are imperceptibility (indicated as PSNR), pay-load (bit rate or capacity), and robustness. Any technique that tries to enhance the payload or robustness should preserve imperceptibility. The noise which is introduced because of bit modification would limit payload. This paper presents 3 analyses on embedding efficiency in audio steganography that's supported experimental results.

III. Method

The creation of digital records in their kind of design has attracted a particular curiosity as of researchers to make sure their safety. System like encryption and watermarking are already utilize during this regard. Though, the necessity for new procedure and new algorithms to counter constantly-changing malicious makes an effort to the integrity of digital information has been converted into a necessity in today's digital time. Steganography, that literary means that "covered writing" has drawn additional consideration within the last few years. Its main goal is to hide the particular fact that a communication is taking place between two elements. The sender implant secret data of any sort using a key in a digital cover file to provide a stego file, in such the way that an observer cannot detect the existence of the hidden data. At the other end, the receiver processes the received stego-file to extract the hidden data. An example of audio steganography is depicted in Fig. one where the cover file being employed can be a digital audio signal. A lucid application may well be a cowlt communication exploitation innocuous cover audio signal, such as phone or video talk's conversations. various features influence the standard of audio steganographic methods. The importance and therefore the impact of every feature depend upon the applying and therefore the transmission atmosphere. The most important properties include robustness to noise and to signal manipulation, safety and hiding ability of embedded information. Robustness requirement is tightly related to the application and is the most difficult to satisfy during a steganographic system. Additionally, there is a trade-off between robustness and hiding-capacity. Generally, they hardly coexist inside the same steganographic system.

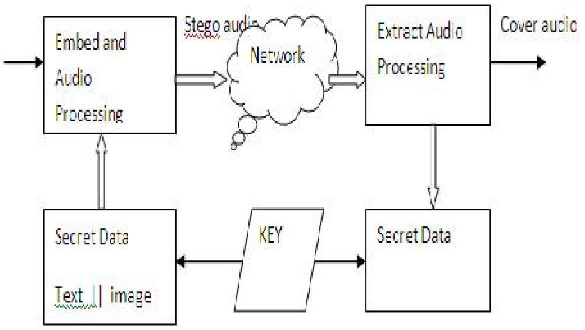

Fig. 1: Blocks diagram for audio steganography.

IV. Conclusion

The main aim is to come up with a technique to hide the data in audio file in such a way there are no perceivable changes in the audio file after the message insertion. Ensure digital information security, various techniques have been presented in recent researchers work. Audio steganography, in particular, addresses issues related to the need to secure and preserve the integrity of information hidden in voice communications, even when the latter passes through insecure channels. This paper presents a review of the current state of art literature in digital audio steganography techniques and approaches.

References

[1] Neha Gupta, Ms. Nidhi Sharma, "Dwt and Lsb Based Audio Steganography" 2014 International Conference on Reliability, Optimization and Information Technology - ICROIT 2014, India, Feb 6-8 2014

[2] Mansour Sheikhan, Kazem Asadollahi and Reza Shahnazi "Improvement of Embedding Capacity and Quality of DWT-Based Audio Steganography Systems" World Applied Sciences Journal 13 (3): 507-516, 2011 ISSN 1818-4952

[3] Ankit Chadha, Neha Satam, Rakshak Sood, 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

[4] Fatiha Djebbar, Beghdad Ayady, Habib Hamamzand Karim Abed-Meraimx "A view on latest audio steganography techniques" 2011 International Conference on Innovations in Information Technology

[5] Haider Ismael Shahadi, Razali Jidin "High Capacity and Inaudibility Audio Steganography Scheme" 978-1-4577-2155-7/11/$26.00 2011 IEEE

[6] M. M Amin, M. Salleh, S. Ibrahim, M.R.K atmin, and M.Z.I.Shamsuddin "Information Hiding using Stegangraphy" 4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, 2003.

[7] N F. Johnson. Steganography tools. Available from: http://www.jjtc.com/Security/stegtools.htm 2005.

[8] R.Anderson, F.Petitcolas: On the limits of the steganography, IEEE Journal Selected Areas in Communications, VOL .16, NO.4, MAY 1998.

[9] M. Wu, B.Liu. "Multimedia Data Hiding", Springer- Verlag New York, 2003

[10] N.F.Johnson Z.Duricands.jajodia "Information Hiding Steganography and Water marking –Attacks and Countermeasures", Kluwer Academic Publishers, 2001