International Journal of Advanced Trends in Computer Applications
www.ijatca.com

A REVIEW ON WAVELET TRANSFORM BASED STEGANOGRAPHY TECHNIQUE TO HIDE AUDIO SIGNALS

[1]**Deepak Sharma**
Assistant Professor (CSE)
B.B.P.U.C.C. Balachaur
ddbbpucc@gmail.com

Abstract: *Data security is one of the most significant aspects to be deliberated when some specific secret data has to be interconnected amongst two different parties. Steganography and cryptography are the two methods utilized for this reason. In cryptography, they scrambles the secret data, however it discloses the actuality of the specific data. In steganography, it hides the authentic existence of the specific data so that anybody else other than the sender as well as the recipient couldn't identify the actual transmission. In steganography, the top-secret data which has to be interconnected is concealed in some other form of carrier in such a manner so that the secret data is imperceptible. In this review paper, we discussed about steganography, specifically audio steganography and wavelet transformation of audio signal which is utilized to hide audio signal in image in the transform domain. Our main objective is to discover a technique which is robust and it can withstand the attacks.*

Keywords: *Audio Steganography, Wavelet Transform, Audio signal, Image.*

I. INTRODUCTION

With the enlargement in utilization of internet, communication of data has turn out to be quiet easy. In contrast with the data communication in analog form, digital communication offers us several aids for instance enhanced/superior quality, high speed, compression of data etc. However, digital data communication has some shortcomings also, such as the fear of information theft throughout the transmission. The security of the specific data is one of the significant necessities in the arena of information transmission, whether it is the transmission of information/data in military-applications or transmission of pictures on internet that desires to be safer than before. Steganography, also offers security towards the specific data to be transferred. It is the skill of hiding undisclosed message in a specific cover message. Cover message could be of image, audio, video, or text. Steganography technique could be matched with the cryptography technique; which is an additional method for data security.

II. STEGANOGRAPHY

Steganography is a type of greek-word which came from 'stegnos' plus 'graphie' which means secure dinscription/writing. This technique is quiteancient which actually taking place in 440B.C. In steganography, it doesn't modify the specific structure of some particular secret message, but then hides this one inside a specific cover picture so secret message could not be perceived. A cipher text in some specific message, for example, it might possibly stimulate doubton any part of the receiver despite the fact that an "imperceptible" message is generated with some steganography techniques will not. In some other words, it also precludes an unintended receiver from doubting that the information actually be present. In addition to that, the security of the conventional-steganography framework depends upon confidentiality of the data encoding framework. When the encoding framework is acknowledged, the steganography system is conquered [1,2].

The subsequent tfacts could be attributed towards the regeneration of steganography:

i. Government-ban on digital-cryptography. Several companies and individuals who seek out secrecy appearance towards steganography as an imperative complementary since merging both of the cryptography as well as steganography could assist in evadingmistrust and safe guard confidentiality/secrecy.

ii. The enlarged requirement to safeguard intellectual rights of property by owners of digital content, utilizing competent watermarking.

iii. The style towards the electronic-communications as well as humans longing to hide messages from many probing eyes. With some speedy encroachment in technology, steganography software is becoming very effective in hiding data in text, image, audio, or video files [3,4].

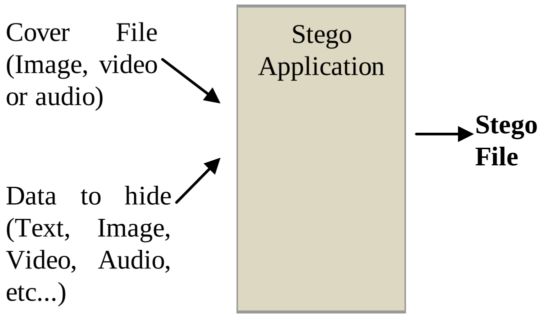
Cover File (Image, video or audio)
Data to hide (Text, Image, Video, Audio, etc...)
Stego Application
Stego File

Figure 1: Steganography Application Scenario

The application of steganography conceals dissimilar categories of data inside a specific cover file. The resultantstegolike wiseen compasses concealed data, even though it is practically indistinguishable to the specific cover file. What Steganography technique does fundamentally is to exploit perception of any human; human intellects are not skilled to seek out for data files which have data hidden inside of them, even though there are several types of programs accessible which could possibly do whatever is entitledas Steganalysis (Discovering Steganographyuse.)

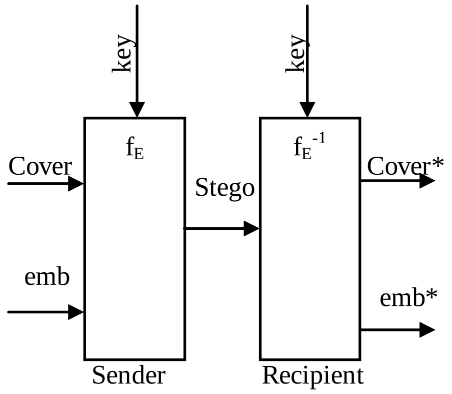

Figure 2: The block diagram of a secure steganography framework. I/p messages could possibly be video, images, texts, or audio.

The constituents of steganography framework are given below:

Emb: Embedded message.

Cover: The specific data in which emb message will be implanted.

Stego: Anamended form of cover which also encompasses the emb i.e. embedded message.

Key: Another top-secret data which is required for the implanting as well as extracting procedures and it must be acknowledged to both of them, the sender as well as the receiver.

f_E: A steganography function which has cover, emb along with key as constraints and also generates stegofile as O/p file.

F_E^{-1}: It is inverse function of f_E such that the outcome of the abstracting procedure f_E^{-1} is indistinguishable to the I/p i.e. E of the embedding procedure f_E.

The embedding procedure f_E implants the top-secret message E in the specific cover data i.e. C. The precise location (S) wherever E would be implanted is reliance upon the specific key K. The outcome of the embedding function is marginally altered form of C: the stego data file C'. Afterwards the receiver has acknowledged C' receiver initiates the extracting procedure f_E^{-1} with the stego data file C' as well as the key K such as parameters. In some specific condition the key which is delivered through the receiver is similar as the specific key utilized through the sender to implant the secret type message and in some condition, the stego information the receiver utilizes as I/p is the equivalent data which sender has generated, at that point the extracting function will generate the unique secret message i.e. E.

III. OVERVIEW OF AUDIO STEGANOGRAPHY

Steganography means, factually, enclosed text/letters. This is the science and a specific type of art of concealing some confidential data in a file cover in such a way that simply sender as well as recipient could only discover the presence of the secret data [5]. A secret data is encrypted in a way such that the presence of the data is hidden.

The key goal of steganography technique is to interconnect safely in an absolutely untraceable way [2] as well as to evade drawing doubt towards the hidden information transmission [6]. This one is not just precludes others from knowing hidden data, but then again it also inhibits others from thinking in which the data even occurs. If in some condition, a steganography technique causes somebody to get suspicious that there is a some kind of secret data in a specific carrier medium, then this technique has been unsuccessful [7, 8].

The elementary model of Audio steganography comprises of Message, Audio file (Carrier), along with Password. Carrier is also acknowledged as a cover-type file that also hides the secret data.

Fundamentally, the prototypical model for steganography technique is presented in Figure given below. Message is the specific information in which the sender desires to keep on it private. Message possibly could be just image, plain text, audio or any other sort of file. Password is acknowledged as a stego-key that also make sure that only the receiver who identifies the equivalent decoding key would possibly be capable to take out the important parts of the message from a specific cover-file. This specific cover-file along with the undisclosed data is acknowledged as stegofile.

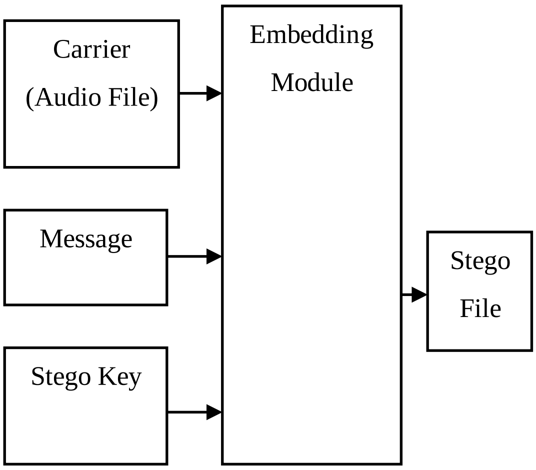

Figure 3: Basic Audio Steganography Model

3.1 Audio Steganography Applications

Audio information hiding could be utilized any-time an individual need to conceal information. There are several explanations to conceal information but then again most significant is to avoid unapproved peoples from becoming alert of the presence of a specific message. In the commercial world, Audio information hiding could be utilized to conceal atop-secret biochemical plans or procedure for a novel development [9].
Audio information hiding could also be utilized in the non-business area to conceal data which somebody desires to preserve privately. Terrorists could also utilize Audio information hiding to preserve their undisclosed communications as well as to manage several attacks. Information hiding in audio along with video, is of concern for the safeguard of digital media copyrighted, and towards the government for security of information systems as well as for concealed communications [10, 11]. It could also be utilized in several forensic applications for implanting hidden information into several types of audio files for the confirmation of the words spoken as well as other sounds, and in business of music for observing of the specific songs over the broadcast radio.

IV. WAVELET TRANSFORMATION OF AUDIO SIGNAL

The wavelet transform has grown pervasively approval in compression of image as well as signal processing. It is the breaking down a specific signal into scaled along with shifted versions of the unique wavelet [12]. A wavelet is a type of waveform of efficiently restricted duration which has average value of zero. And for signals; the identity of the specific signal is specified through the component of low-frequency. The content of high-frequency only communicates nuance or savior. In an individual's voice, if components of high frequency are extracted, the voice which sounds different, but still it could be understood easily. If components of low frequency are extracted, the signal sounds will gabble. On implementing wavelet transformations on specific audio signal, detail and approximation audio components could be attained easily.
The approximations are components of low-frequency of the specific signal in addition to that detail are components of high-frequency signal. The first-level detail-coefficients have a lesser amount of importance in contrast with the detail-coefficients of subsequent levels and the coefficients of approximation due to their low-energy-level. Below figure also displays the disintegration of audio signal on WT.

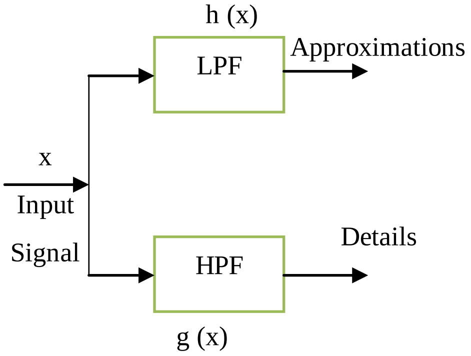

Figure 4: One stage signal decomposition.

We can approximate a discrete signal in k^2 (X)^1 by

$$f[b] = \frac{1}{\sqrt{N}} \sum_j Q_\phi[h_0, j]\, \phi_{h_0,j}[b] + \frac{1}{\sqrt{N}} \sum_{h=h_0}^{\infty} \sum_j Q_\psi[h,j] \psi_{h,j}[b] \quad (1)$$

Here, $f[b], \phi_{h_0,j}[b]$ and $\psi_{h,k}[b]$ are discrete functions which are defined in [0, N-1], to-tally N points. For the reason that the sets $\{\phi_{h_0,j}[b]\}_{j\in x}$and $\{\psi_{h,j}[b]\}_{(h,j)\in x^2, h\geq j_0}$are orthogonal to each other. We can simply take the inner product to obtain the wavelet coefficients:

$$Q_\phi[h_0,j] = \frac{1}{\sqrt{N}}\sum_b f[b]\,\phi_{h_0,j}[b] \qquad (2)$$

$$Q_\psi[h_0,j] = \frac{1}{\sqrt{N}}\sum_b f[b]\,\psi_{h,j}[b] \quad h\geq h_0 \qquad (3)$$

(2) are called approximation coefficients while (3) are called detailed coefficients.

V. PREVIOUS WORK DONE

In latest years, numerous researchers have focused on evolving procedures for concealing information into an audio signal.

Jisna Antony et al [13] talk over about different audio steganography methods which are accessible in different type of domains. Lots of research work is completed in all kind of domains.

Baritha and Venkataramani [14] recommend a novel dictionary dependent various text compression method. Dictionary dependent compression bits are concealed into the Least Significant Bit of audio signals. In this top-secret text is concealed utilizing a specific identifier. An identifier together with length as well as width is secreted inside a specific audio. Identifier also specifies whether there is a top-secret text concealed or not. This paper is instigated in the temporal domain.

Ahmad Delforouzi and Mohammad Pooyan [15] suggests a procedure that implants secret information in the temporal domain. In this technique, initially implanting/embedding threshold in the specific time domain is assessed. At that time, this specific threshold is utilized for camouflage the information in the specific time domain. Disadvantage of the audio steganography in temporal domain is even though it is quite easy to conceal information; it shortages security and also has less concealing capacity as compared to concealing in specific wavelet domain.

Dora and Juan [16] offers a new structure of information concealing that takes benefit of the disguising possessions of the Human Auditory System in order to conceal a secret type signal(speech) into a host type signal(speech). In implanting procedure, the wavelet coefficients of the top-secret signal are organized as well as implanted in the coefficients of wavelet of the specific host signal. And their actual locations are utilized as key. Delay is inserted in each cycle to achieve synchronization. This approach consumes more time; retrieved secret signal is not same as the original because there is error in reconstruction of host signal. Also as there is need to store the positions of frames in stego signal, it reduces the hiding capacity of the host signal.

Yongfeng Huang et al [17], proposed an algorithm which performs data embedding while pitch period prediction is conducted. Embedding the secret data is done during low bit-rate speech encoding. Drawback of this technique is that stego audio has been detected in steganalysis.

CONCLUSIONS

Steganography is a specific type of art of concealing some confidential data in a file cover in such a way that simply sender as well as recipient could only discover the presence of the secret data. In this review paper, we have talked about steganography specifically about audio steganography and its application along with wavelet transformation of audio signal i.e. about one stage signal decomposition along with this we have discussed about some previous research work done in the same field. Here, our main goal is to create a steganography technique by using wavelet transformation for hiding audio signal in a specific image.

REFERENCES

[1] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz, S. Pogreb, “Techniques for data hiding”, IBMSystems Journal, Volume 39 , Issue 3-4, July 2000, pp. 547 – 568.

[2] NedeljkoCvejic, TapioSeppben “Increasing the capacity of LSB-based audio steganography ” FIN-90014 University of Oulu, Finland ,2002.

[3] R.A. Santosa and P. Bao, “Audio-to-image wavelet transform based audio steganography,” Proc. Of 47th Int. Symposium ELMAR, June 2005, pp. 209- 212.

[4] Xuping Huang, Ryota Kawashima, NorihisaSegawa, Yoshihiko Abe International Conference onIntelligent “Information Hiding and Multimedia Signal Processing” © 2008 IEEE.

[5] Robert Krenn, “Steganography and steganalysis”, An Article, January 2004.

[6] SajadShirali-Shahreza M.T. Manzuri-Shalmani “High capacity error free wavelet domain speechsteganography” ICASSP 2008

[7] Neil F.Johnson, Z.Duric and S.Jajodia. “Information Hiding Steganography and Watermarking-Attacksand Countermeasures”,Kluwer Academic Publishers, 2001

[8] Min Wu, Bede Liu. “Multimedia Data Hiding”, Springer- Verlag New York, 2003.

[9] S. Shirali-Shahreza, M. T. Manzuri-Shalmani, "Adaptive Wavelet Domain Audio Steganography with High Capacity and Low Error Rate", IEEE International Conference on Information and Emerging Technologies, 2007, 06-07 July 2007 pp 1-5.

[10] Yincheng Qi, Jianwen Fu, and Jinsha Yuan, “Wavelet domain audio steganalysis based on statisticalmoments of histogram”, Journal of System Simulation, Vol 20, No. 7, pp. 1912-1914, April 2008.

[11] MengyuQiao, Andrew H. Sung ,Qingzhong Liu “Feature Mining and Intelligent Computing for MP3Steganalysis” International Joint Conference on Bioinformatics, Systems Biology and Intelligent Computing 2009.

[12] Michael Weeks, ”Digital Signal Processing Using MATLAB and Wavelets”, Pearson publications,ISBN – 81-297-0272-X.

[13] Jisna Antony and Sobin C,” Audio Steganography in Wavelet Domain – A Survey”, InternationalJournal of Computer Applications, Volume 52, No.13, 2012, pp. 33-37

[14] M.Baritha Begum and Y.Venkataramani, ”LSB Based Audio Steganography Based on TextCompression”, International Conference on Communication Technology and System Design, 2011,pp. 703-710

[15] Ahmad Delforouzi and Mohammad Pooyan, “Adaptive and Efficient Audio Data Hiding Method inTemporal Domain”, IEEE ICICS, 2009.

[16] Dora M. Ballesteros L and Juan M. Moreno A,” Real-time, speech-in-speech hiding scheme based onleast significant bit substitution and adaptive key”, Computers and Electrical Engineering Vol 39,Elsevier, 2013,pp. 1192-1203

[17] Yongfeng Huang, Chenghao Liu and Shanyu Tang,” Steganography Integration into a Low-Bit RateSpeech Codec”, IEEE transactions on information forensics and security, vol. 7, no. 6, 2012