An Extensive Review on Audio Steganography

Uma Shankar Anant
Student, M.Tech, Department Of Computer Science and Engineering, Swami Vivekanand College of Science & Technology, Bhopal, India

Keshav Tiwari
Assistant Professor Department Of Computer Science and Engineering, Swami Vivekanand College of Science & Technology, Bhopal, India

Pinkeshwar Mishra
Head Of Department, Computer Science and Engineering, Swami Vivekanand College of Science & Technology, Bhopal, India

Abstract-Digital steganography has been proposed as a new, alternative method to enforce intellectual property rights and protect digital media from tampering. Digital steganography is defined as imperceptible, robust and secure communication of data related to the host signal, which includes embedding into and extraction from the host signal. The main challenge in digital audio steganography and steganography is that if the perceptual transparency parameter is fixed, the design of a watermark system cannot obtain high robustness and a high watermark data rate at the same time. An approach that combined theoretical consideration and experimental validation, including digital signal processing, psychoacoustic modeling and communications theory, is used in developing algorithms for audio steganography and steganography. Broadband Internet connections and near error-free transmission of data facilitate people to distribute large multimedia files and make identical digital copies of them. In this review paper we have studied the audio steganography methodology in order to enhance the strength of the existing system model.

Keywords:- LSB, PSNR, Audio steganography.

I. INTRODUCTION

The rapid development of the Internet and the digital information revolution caused significant changes in the global society, ranging from the influence on the world economy to the way people nowadays communicate. Broadband communication networks and multimedia data available in a digital format (images, audio, video) opened many challenges and opportunities for innovation. Versatile and simple-to-use software and decreasing prices of digital devices (e.g. digital photo cameras, camcorders, portable CD and mp3 players, DVD players, CD and DVD recorders, laptops, PDAs) have made it possible for consumers from all over the world to create, edit and exchange multimedia data. Broadband Internet connections and almost an errorless transmission of data facilitate people to distribute large multimedia files and make identical digital copies of them. Digital media files do not suffer from any quality loss due to multiple copying processes, such as analogue audio and VHS tapes. Furthermore, recording medium and distribution networks for analogue multimedia are more expensive. These first-view advantages of digital media over the analogue ones transform to disadvantages with respect to the intellectual rights management because a possibility for unlimited copying without a loss of fidelity cause a considerable financial loss for copyright holders [1, 2, 3]. The ease of content modification and a perfect reproduction in digital domain have promoted the protection of intellectual ownership and the prevention of the unauthorized tampering of multimedia data to become an important technological and research issue [4]. A fair use of multimedia data combined with a fast delivery of multimedia to users having different devices with a fixed quality of service is becoming a challenging and important topic. Traditional methods for copyright protection of multimedia data are no longer sufficient. Hardware-based copy protection systems have already been easily circumvented for analogue media. Hacking of digital media systems is even easier due to the availability of general multimedia processing platforms, e.g. a personal computer. Simple protection mechanisms that were based on the information embedded into header bits of the digital file are useless because header information can easily be removed by a simple change of data format, which does not affect the fidelity of media. Encryption of digital multimedia prevents access to the multimedia content to an individual without a proper decryption key. Therefore, content providers get paid for the delivery of perceivable multimedia, and each client that has paid the royalties must be able to decrypt a received file properly. Once the multimedia has been decrypted, it can be repeatedly copied and distributed without any obstacles.

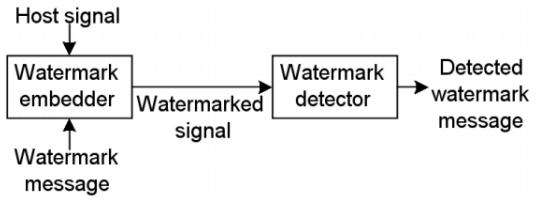

Fig. 1. A block diagram of the encoder.

Modern software and broadband Internet provide the tools to perform it quickly and without much effort and deep technical knowledge. One of the more recent examples is the hack of the Content Scrambling System for DVDs [5, 6]. It is clear that existing security protocols for electronic commerce

serve to secure only the communication channel between the content provider and the user and are useless if commodity in transactions is digitally represented. Digital steganography has been proposed as a new, alternative method to enforce the intellectual property rights and protect digital media from tampering. It involves a process of embedding into a host signal a perceptually transparent digital signature, carrying a message about the host signal in order to "mark" its ownership. The digital signature is called the digital watermark. The digital watermark contains data that can be used in various applications, including digital rights management, broadcast monitoring and tamper proofing. Although perceptually transparent, the existence of the watermark is indicated when watermarked media is passed through an appropriate watermark detector. Figure 1.1 gives an overview of the general steganography system [2]. A watermark, which usually consists of a binary data sequence, is inserted into the host signal in the watermark embedder. Thus, a watermark embedder has two inputs; one is the watermark message (usually accompanied by a secret key) and the other is the host signal (e.g. image, video clip, audio sequence etc.). The output of the watermark embedder is the watermarked signal, which cannot be perceptually discriminated from the host signal. The watermarked signal is then usually recorded or broadcasted and later presented to the watermark detector. The detector determines whether the watermark is present in the tested multimedia signal, and if so, what message is encoded in it. The research area of steganography is closely related to the fields of information hiding [7, 8] and steganography [9, 10]. The three fields have a considerable overlap and many common technical solutions. However, there are some fundamental philosophical differences that influence the requirements and therefore the design of a particular technical solution. Information hiding (or data hiding) is a more general area, encompassing a wider range of problems than the steganography [2]. The term hiding refers to the process of making the information imperceptible or keeping the existence of the information secret. Steganography is a word derived from the ancient Greek words steganos [2], which means covered and 19 graphia, which in turn means writing. It is an art of concealed communication. Steganography systems as systems in which the hidden message is related to the host signal and non-steganography systems in which the message is unrelated to the host signal. On the other hand, systems for embedding messages into host signals can be divided into steganographic systems, in which the existence of the message is kept secret, and non-steganographic systems, in which the presence of the embedded message does not have to be secret.

II. HISTORY

The first steganographic technique was developed in ancient Greece around 440 B.C. The Greek ruler Histaeus employed an early version of steganography. He shaved the head of a slave and then tattooed the message on the slaves scalp, waited for the hair to grow to cover the secret message. Once the secret message is covered he sent the slave on his way to deliver the message. The recipient shaves the slave's head to read the message. Steganographic techniques have been used for ages and they date back to ancient Greece. The aim of steganographic communication back then and now, in modern applications, is the same: to hide secret data (a steganogram) in an innocently looking cover and send it to the proper recipient who is aware of the information hiding procedure. In an ideal situation the existence of hidden communication cannot be detected by third parties.

What distinguishes historical steganographic methods from the modern ones is, in fact, only the form of the cover (carrier) for secret data. Historical methods relied on physical steganography – the employed media were: human skin, game, etc.. Further advances in hiding communication based on the use of more complex covers, e.g. with the aid of ordinary objects, whose orientation was assigned meaning. This is how semagrams were introduced. The popularisation of the written word and the increasing literacy among people had brought about methods which utilised text as carrier. The World Wars had accelerated the development of steganography by introducing a new carrier – the electromagnetic waves. Presently, the most popular carriers include digital images, audio and video files and communication protocols. The latter may apply to network protocols as well as any other communication protocol (e.g. cryptographic).

The way that people communicate evolved over ages and so did steganographic methods. At the same time, the general principles remained unchanged.

III. LITERATURE REVIEW

This chapter reviews the appropriate background literature and describes the concept of information hiding in audio sequences. Scientific publications included into the literature survey have been chosen in order to build a sufficient background that would help out in solving the research subproblems problems.

1. Gupta, N. and Sharma N. [1] presented Steganography is a fascinating and effective method of hiding data that has been used throughout history. Methods that can be employed to uncover such devious tactics, but the first step are awareness that such methods even exist. There are many good reasons as well to use this type of data hiding, including watermarking or a more secure central storage method for such things as passwords, or key processes. Regardless, the technology is easy to use and difficult to detect. Researchers and scientists have made a lot of research work to solve this problem and to find an effective method for image hiding .The proposed system aims to provide improved robustness, security by using the concept of DWT (Discrete Wavelet Transform) and LSB (Least Significant Bit) proposed a new method of Audio Steganography. The emphasize will be on the proposed scheme of image hiding in audio and its comparison with simple Least Significant Bit insertion method for data hiding in audio.

2. Bugar, G., Banoci and V., Broda [2] investigated the science of hiding secret information in another unsuspicious data. usually, a steganographic secret message could be a widely useful multimedia: as a picture, an audio file, a video file or a message in clear text - the covertext. The most recent steganography techniques tend to hide a secret message in digital images. Authors proposed and analyzed experimentally a blind steganography method based on specific attributes of two dimensional discrete wavelet transform set by Haar mother wavelet. The blind steganography methods do not require an original image in the process of extraction what helps to keep a secret communication undetected to third party user or steganalysis tools. The secret message is encoded by Huffman code in order to achieve a better imperceptibility result. Moreover, this modification also increases the security of the hidden communication.

3. Geethavani, B., Prasad, E.V. and Roopa, R. [3] described that Steganography is an information hiding technique where secret message is embedded into unsuspicious cover signal. In this paper, a novel approach of integrating the features of cryptography and audio Steganography is presented. The information to be transmitted is encrypted by using modified blowfish algorithm and resultant cipher text is embedded into a cover audio file using discrete wavelet transform (DWT). The resultant stego audio is transmitted to the receiver and the reverse process is done in order to get back the original plain text. The proposed method presents a steganographic scheme along with the cryptographic scheme which enhances the security of the algorithm.

4. Khademi, Mahdi and Tinati, M.A [4] analyzed the important methods for encryption of secret messages in secure purposes. Although several methods have been proposed, most of them have poor performance in encrypting the secret messages especially in presence of environmental noises, so that enemy can easily detect the secret message in the transmitted information. In this paper a new method for audio steganography is proposed. Researchers propose an algorithm to encrypt the secret message by transforming it to LPC coefficients and noise term and then substituting it in safe places in discrete wavelet transform (DWT) as a cover message frames in the transmitted data. Moreover, authors apply their method to some audio files from TIMIT database. Simulations results show good performance of their proposed system and large security and capacity of steganography toward previous methods especially in presence of environmental noises.

5. Zhang Kexin [5] researched for audio information hiding has attracted more attentions recently. Spread spectrum (SS) technique has developed rapidly in this area due to the advantages of good robustness and immunity to noise attack. Accordingly steganalysis of the SS hiding effectively verify the presence of the secrete message in an important issue. In this paper authors present two algorithms for steganalysis SS hiding. Both the two methods based on machine learning theory and discrete wavelet transform (DWT). In the algorithm I, they introduce Gaussian mixture model (GMM) and generalize Gaussian distribution (GGD) to character the probability distribution of wavelet sub-band. Then the absolute probability distribution function (PDF) moment is extracted as feature vectors. In the algorithm II, authors propose distance metric between GMM and GGD of wavelet sub-band to distinguish cover and stego audio. Four distances (Kullback-Leibler Distance, Bhattacharyya Distance, Earth Mover's Distance, L2 Distance) are calculated as feature vectors. The support vector machine (SVM) classifier is utilized for classification. The experiment results of both two proposed algorithms may obtain better detecting performance. Its simplicity and extensibility indicate further application in other audio steganalysis.

6. Cairong Li, Wei Zeng, Haojun Ai and Ruimin Hu [6] proposed the Audio steganalysis has attracted more attentions recently. DSSS steganalysis is one of the most challenging research fields. In this paper, a novel algorithm to detect DSSS steganography in audio signal is proposed. Firstly, it takes DWT transform of special segment of audio and takes the detail sub-band coefficients, and then uses GMM to model the coefficients. Secondly, in order to monitor the effect of DSSS hiding, authors calculate the

GMM PDF (possibility density function) as to measure the difference. Thirdly, considering the two variables composed of wavelet coefficients and GMM PDF, the multivariate skewness and kurtosis were taken as features. Lastly, the SVM classifier is utilized for classification. All of the 800 various audios are trained and tested in author's experimental work. With various embedding parameters for training and testing audios, the proposed algorithm can achieve a good classification, and the correct rate of detecting is up to 80%.

7. Wang Junjie, Mo Qian and Mei Dongxia; Yao Jun, [7] proposed the method of information hiding, a novel algorithm for security speech communication is designed in this paper, and the synchronization code can be used to search the embedded location. Firstly, the DWT is performed on each segment of the original carrier audio; Secondly, the embedding bits are constructed by the synchronization code and secret audio ,and the secret bits are formed by chaotic encrypting; Thirdly, the secret bits are embedded into the low frequency point of Discrete Wavelet Transform (DWT) by quantization; Lastly,the IDWT are performed on each segment and the setgo audio are constructed.The original carrier audio is not required in the secret audio recovery. Experimental results show that the stego audio has transparent feature, and the quality of the recovered audio is satisfying. The algorithm is strongly robust to many attacks, such as resampling, cropping and so on.

8. Johnson N and Jajodia S [8] proposed the goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, then this goal is defeated. Discovering and rendering useless such covert messages is a new art form known as steganalysis. In this paper, we provide an overview of some characteristics in information hiding methods that direct the steganalyst to the existence of a hidden message and identify where to look for hidden information.

9. Hartung, F. and Kutter, M. [12] describe the Multimedia watermarking technology has evolved very quickly during the last few years. A digital watermark is information that is imperceptibly and robustly embedded in the host data such that it cannot be removed. A watermark typically contains information about the origin, status, or recipient of the host data. In this tutorial paper, the requirements and applicationsfor watermarking are reviewed. Applications include copyright protection, data monitoring, and data tracking. The basic concepts of watermarking systems are outlined and illustrated with proposed watermarking methods for images, video, audio, text documents,
and other media. Robustness and security aspects are discussed in detail. Finally, a few remarks are made about the state of the art and possible future developments in watermarking technology.

10. Warkar, R. ; More, P. ; Waghole, D. [15] The article covers a brief summary of modern approaches for embedding additional data in audio signals. It could have many causes - for the purposes of access control or identification related to particular type of audio. This top-secret information is not "visible" for a user. The leading determination for watermarking by audio is to defend beside probable extortions in the audio records and for copyright harm or illegal altering; reality for such information can be unsure by audio watermarking. Steganography and cryptography are two techniques these techniques are related in the manner that they together are used to safeguard private facts. There is lack in characteristic of original image we recommend a generalized form of Reversible Contrast Mapping (RCM) is an in complex integer transform that applies to pairs of pixels. For image watermarking Contrast mapping is invertible procedure, because least significant bits (LSBs) of the transformed pixels are forfeit. The data space occupied by the LSBs is expedient for information hiding. The embedded information bit-rates of reversible watermarking structure are highest bit-rates till date. The system does not need further records compression, and, in terms of mathematical complexity, it is having lowest complexity. Also robustness against cropping can be guaranteed.

IV. RESEARCH PROBLEM

The fundamental process in each steganography system can be modeled as a form of communication where a message is transmitted from watermark embedder to the watermark receiver [2]. The process of steganography is viewed as a transmission channel through which the watermark message is being sent, with the host signal being a part of that channel. In Figure 2, a general mapping of a steganography system into a communications model is studied. After the watermark is embedded, the watermarked work is usually distorted after watermark attacks.

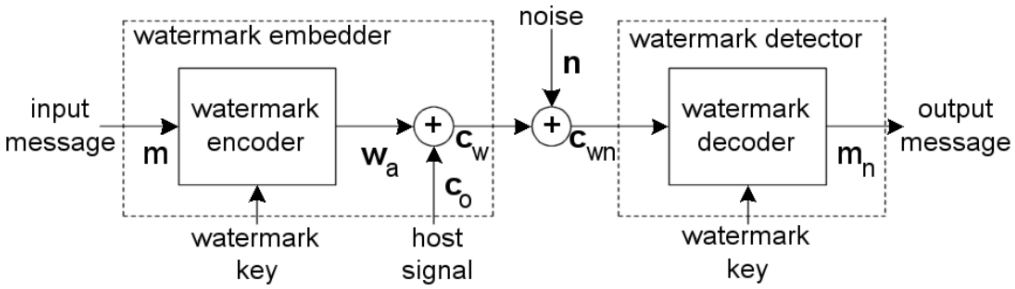

Fig. 2. A steganography system and an equivalent communications model.

V. FREQUENCY MASKING

Frequency masking is a frequency domain phenomenon where a low level signal, e.g. a pure tone, can be made inaudible by a simultaneously appearing stronger signal (the masker), e.g. a narrow band noise, if the masker and maskee are close enough to each other in frequency. A masking threshold can be derived below which any signal will not be audible. The masking threshold depends on the masker and on the characteristics of the masker and maskee (narrowband noise or pure tone). For example, with the masking threshold for the sound pressure level (SPL) equal to 60 dB, the masker in Figure 2.1 at around 1 kHz, the SPL of the maskee can be surprisingly high - it will be masked as long as its SPL is below the masking threshold. The slope of the masking threshold is steeper toward lower frequencies; in other words, higher frequencies tend to be more easily masked than lower frequencies. It should be pointed out that the distance between masking level and masking threshold is smaller in noise-masks- tone experiments than in tone-masks-noise experiments due to HAS's sensitivity toward additive noise. Noise and low-level signal components are masked inside and outside the particular critical band if their SPL is below the masking threshold. Noise contributions can be coding noise, inserted watermark sequence, aliasing distortions, etc. Without a masker, a signal is inaudible if its SPL is below the threshold in quiet, which depends on frequency and covers a dynamic range of more than 70 dB as depicted in the lower curve of Figure 2. The qualitative sketch of Figure 3 gives more details about the masking threshold. The distance between the level of the masker (given as a tone in Figure 3) and the masking threshold is called signal-to-mask ratio (SMR).

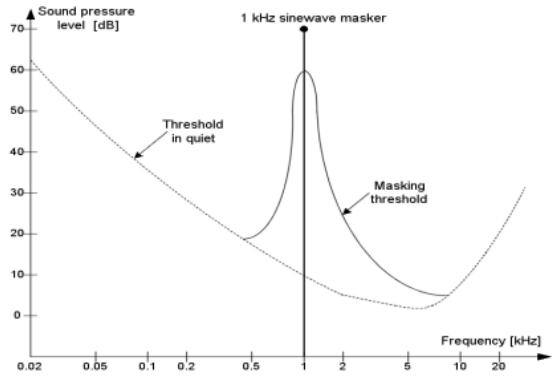

Fig. 3

Frequency masking in the human auditory system (HAS), reference sound pressure level is $p_0 = 2 \cdot 10^{-5}\, Pa$.

Its maximumvalue is at the left border of the critical band. Within a critical band, noise caused by watermark embedding will be audible as long as signal-to-noise ratio (SNR) for the critical band is higher than its SMR. Let SNR(m) be the signal-to-noise ratio resulting from watermark insertion in the critical band m; the perceivable distortion in a given subband is then measured by the noise to mask ratio:

NMR(m)=SMR-SNR(m)

The noise-to-mask ratio NMR(m) expresses the difference between the watermark noise in a given critical band and the level where a distortion may just become audible; its value in dB should be negative.

VI. PROPOSED METHODOLOGY

In this review paper, a multidisciplinary approach LSB would be applied for solving the security problems. The signal processing methods may used for steganography embedding and extracting processes, derivation of perceptual thresholds, transforms of signals to different signal.

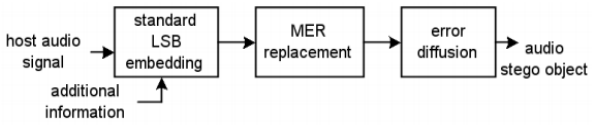

Fig. Block-diagram of the proposed methodology.

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.
Steps to hide secret information using LSB are:

a. Covert the audio file into bit stream.
b. Convert each character in the secret information into bit stream.
c. Replace the LSB bit of audio file with the LSB bit of character in the secret information.

This proposed method provides greater security and it is an efficient method for hiding the secret information from hackers and sent to the destination in a safe and undetectable manner. This proposed system also ensures that the size of the file is not changed even after encoding and it is also suitable for any type of audio file format.

VII. APPLICATION AREAS

Digital steganography is considered as an imperceptible, robust and secure communication of data related to the host signal, which includes embedding into and extraction from the host signal. The basic goal is that embedded watermark information follows the watermarked multimedia and endures unintentional modifications and intentional removal attempts. The principal design challenge is to embed watermark so that it is reliably detected in a watermark detector. The relative importance of the mentioned properties significantly depends on the application for which the algorithm is designed. For copy protection applications, the watermark must be recoverable even when the watermarked signal undergoes a considerable level of distortion, while for tamper assessment applications, the watermark must effectively characterize the modification that took place. In this section, several application areas for digital steganography will be presented and advantages of digital steganography over standard technologies examined. Ownership Protection In the ownership protection applications, a watermark containing ownership information is embedded to the multimedia host signal. The watermark, known only to the copyright holder, is expected to be very robust and secure (i.e., to survive common signal processing modifications and intentional attacks), enabling the owner to demonstrate the presence of this watermark in case of dispute to demonstrate his ownership. Watermark detection must have a very small false alarm probability. On the other hand, ownership protection applications require a small embedding capacity of the system, because the number of bits that can be embedded and extracted with a small probability of error does not have to be large. Proof of ownership It is even more demanding to use watermarks not only in the identification of the copyright ownership, but as an actual proof of ownership. The problem arises when adversary uses editing software to replace the original copyright notice with his own one and then claims to own the copyright himself. In the case of early watermark systems, the problem was that the watermark detector was readily available to adversaries. As elaborated in [2], anybody that can detect a watermark can probably remove it as well. Therefore, because an adversary can easily obtain a detector, he can remove owner's watermark and replace it with his own. To achieve the level of the security necessary for proof the of ownership, it is indispensable to restrict the availability of the detector. When an adversary does not have the detector, the removal of a watermark can be made extremely difficult. However, even if owner's watermark cannot be removed, an adversary might try to undermine the owner. As described in [2], an adversary, using his own steganography system, might be able to make it appear as if his watermark data was present in the owner's original host signal. This problem can be solved using a slight alteration of the problem statement.

VIII. CONCLUSION

Communication principles and models are used for channel noise modeling, different ways of signalling the watermark (e.g. a direct sequence spread spectrum method, frequency hopping method), derivation of optimized detection method (e.g. matched filtering) and evaluation of overall detection performance of the algorithm (bit error rate, normalized correlation value at detection). The basic information theory principles are used for the calculation of the perceptual entropy of an audio sequence, channel capacity limits of a watermark channel and during design of an optimal channel coding method. The research methods also include algorithm simulations with real data (music sequences) and subjective listening tests.

ACKNOWLEDGEMENT

I would like to thank the almighty for giving me the strength to work on this subject and coming up with this literature review paper. I am grateful to my family for supporting me and praying for me. I would like to express my gratitude towards the professors of Swami Vivekanand Collage of Science and Technology for their valuable guidance.

REFERENCES

[1] Gupta, N.; Sharma, N., *"Dwt and Lsb based Audio Steganography"*, Process of IEEE Optimization, Reliabilty, and Information Technology (ICROIT), 2014 International Conference on , vol., no., pp.428,431, 6-8 Feb. 2014.

[2] Bugár, G.; Bánoci, V.; Broda, M.; Levický, D.; Dupák, D., *"Data hiding in still images based on blind algorithm of steganography"* Radioelektronika (RADIOELEKTRONIKA), In proc. 24th IEEE International Conference , vol., no., pp.1,4, 15-16 April 2014.

[3] Geethavani, B.; Prasad, E.V.; Roopa, R., *"A new approach for secure data transfer in audio signals using DWT"* In Proc. IEEE Advanced Computing Technologies (ICACT), 15th International Conference on , vol., no., pp.1,6, 21-22 Sept. 2013.

[4] Khademi, Mahdi; Tinati, M.A., *"Audio steganography by using of linear predictive coding analysis in the safe places of discrete wavelet transform domain"* In Proc. IEEE Electrical Engineering (ICEE), 19th Iranian Conference on , vol., no., pp.1-5, 17-19 May 2011.

[5] Zhang Kexin, *"Audio steganalysis of spread spectrum hiding based on statistical moment"* In Proc. IEEE Signal Processing Systems (ICSPS), 2nd International Conference on , vol.3, no., pp.V3-381,V3-384, 5-7 July 2010.

[6] Cairong Li; Wei Zeng; Haojun Ai; Ruimin Hu, *"Steganalysis of Spread Spectrum Hiding Based on DWT and GMM"* In Proc. IEEE Networks Security, Wireless Communications and Trusted Computing, NSWCTC '09. International Conference on , vol.1, no., pp.240,243, 25-26 April 2009.

[7] Wang Junjie; Mo Qian; Mei Dongxia; Yao Jun, *"Research for Synchronic Audio Information Hiding Approach Based on DWT Domain"* In Proc. IEEE E-Business and Information System Security. EBISS '09. International Conference on , vol., no., pp.1,5, 23-24 May 2009.

[8] Johnson N & Jajodia S, Steganalysis: *the investigation of hidden information*. In: Proc. IEEE Information Technology Conference, Syracuse, NY, p 113–116, 3 Sept. 1998.

[9] Katzenbeisser S & Petitcolas F, *Information Hiding Techniques for Steganography and Digital Steganography*. Artech House, Norwood, MA. 1999.

[10] Bender W, Gruhl D & Morimoto N, Anthony lu, *"Techniques for data hiding"*. IBM Systems Journal 35(3): p 313–336,1996.

[11] Cox I & Miller M, *Electronic steganography: the first 50 years.* In: Proc. IEEE Workshop on Multimedia Signal Processing, Cannes, France, p 225–230, 2001.

[12] Hartung F & Kutter M, *Multimedia watermarking techniques.* Proceedings of the IEEE 87(7), p 1709–1107. 1999.

[13] Tanwar, R. ; Bisla, M., *Audio steganography* In Proc. IEEE International Conference on Optimization, Reliabilty, and Information Technology (ICROIT), P. 322 – 325, 6-8 Feb. 2014.

[14] Binny, A. ; Koilakuntla, M., *Hiding Secret Information Using LSB Based AudioSteganography*. In Proc. IEEE International Conference on Soft Computing and Machine Intelligence (ISCMI), P. 56 – 59, 26-27 Sept. 2014.

[15] Warkar, R. ; More, P. ; *Waghole, D., Digital audio watermarking and image watermarking for information security*. In proc. IEEE International Conference on , pp. 1-5, 8-10 Jan. 2015.