International Journal For Technological Research In Engineering
Volume 1, Issue 9, May-2014 *ISSN (Online): 2347 - 4718*

A REVIEW ON DIFFERENT METHODS OF WATERMARKING FOR COPYRIGHT PROTECTION

Apeksha G. Dengre[1] (M.E. Scholar), Dr. S. R. Gupta[2] (Assistant Professor)
Computer Science and Engineering,
PRMIT and R, Badnera, Maharashtra, India.

Abstract: Digital watermarking is an important role for protecting digital contents from unauthorized copying. This paper proposes a new audio watermarking method based on Discrete Cosine Transformation (DCT) for copyright protection. In our proposed watermarking method, the original audio is transformed into DCT domain. The absolute values of DCT coefficients are divided into an arbitrary number of segments and the energy of each segment is calculated. Watermarks are then embedded into the selected peaks of the highest energy segment. Watermarks are extracted by performing the inverse operation of watermarking embedding process. Simulation results indicate that our proposed watermarking method is highly robust against various kinds of attacks such as noise addition, cropping, re-sampling, re-quantization, MP3 compression, and echo. Genetic algorithm for principled approach to resolve the remained problems of substitution technique of audio watermarking. Using the proposed genetic algorithm, message bits are embedded into multiple, vague and higher LSB layers, resulting in increased robustness. . The basic idea of this paper is to present methods that hide information in cover audio using Least Significant Bit (LSB) coding method along with encryption so as to increase the security. The robustness specially would be increased against those intentional attacks which try to reveal the hidden message and also some unintentional attacks like noise addition as well. It is mainly required for increasing security in transferring and archiving of audio files

Keywords: Copyright protection, Digital Watermarking, Discrete Cosine Transform (DCT), Sound Contents, audio signal. Data hiding, substitution techniques, audio watermarking, artificial intelligence, genetic algorithm.

I. INTRODUCTION

The rapid development of digital information revolution cased significant changes in the global society, ranging from the influence on the world economy to the way people nowadays communicate: [1]. Digitizing of multimedia data has enabled reliable, faster and efficient storage, transfer and processing of digital data. It also leads to the consequence of illegal production and redistribution of digital media. Digital watermarking is identified as a partial solution to related problems which allow content creator to embed hidden data such as author or copyright information into the multimedia data [2]. In cryptographic techniques significant information is encrypted so that only the key holder has access to that information. Once the information is decrypted the security is lost. Information hiding is unlike cryptography, message is embedded into digital media, which can be distributed and used normally. Information hiding doesn't limit the use of digital data. Within past few years several algorithms for embedding and extraction of watermark in audio sequence have been published [3-7]. Almost all audio watermarking algorithms work by exploiting the perceptual property of Human Auditory System (HAS). The simplest visualization of the requirements of information hiding in digital audio is possible via a magic triangle [3]. Inaudibility, robustness to attacks and the watermark data rate are in the corners of the magic triangle. In order to satisfy the requirements of magic triangle, watermarks are seen embedded in Fourier domain [4], time domain [5], sub-band domain [6]. wavelet domain [7]. and by echo hiding . Audio watermarking should meet the following requirements : (a) Imperceptibility: the digital watermark should not affect the quality of original audio signal after it is watermarked; (b) Robustness: the embedded watermark data should not be removed or eliminated by unauthorized distributors using common signal processing operations and attacks; (c)Capacity: capacity refers to the numbers of bits that can be embedded into the audio signal within a unit of time; (d) Security: security implies that the watermark can only be detectable by the authorized person. All these requirements are often contradictory with each other. However, it should satisfy the important properties such as imperceptibility and robustness.

II. WATERMARKING APPLICATIONS

Obviously, the most significant applications of data hiding are covert communication. Several application areas for digital watermarking are introduced below.

A. 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.

B. 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 were that the watermark detector was readily available to adversaries 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 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 [15], an adversary, using his own watermarking 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. Instead of adirect proof of ownership by embedding e.g. "Dave owns this image" watermark signature in the host image, algorithm will instead try to prove that the adversary's image is derived from the original watermarked image. A Novel Approach for Audio Watermarking 104 Such an algorithm provides indirect evidence that it is more probable that the real owner owns the disputed image, because he is the one who has the version from which the other two were created.

C. Authentication and Tampering Detection:

In the content authentication applications, a set of secondary data is embedded in the host multimedia signal and is later used to determine whether the host signal was tampered. The robustness against removing the watermark or making it undetectable is not a concern as there is no such motivation from attacker's point of view. However, forging a valid authentication watermark in an unauthorized or tampered host signal must be prevented. In practical applications it is also desirable to locate (in time or spatial dimension) and to discriminate the unintentional modifications (e.g. distortions incurred due to moderate MPEG compression [12]) from content tampering itself. In general, the watermark embedding capacity has to be high to satisfy the need for more additional data than in ownership protection applications. The detection must be performed without the original host signal because either the original is unavailable or its integrity has yet to be established. This kind of watermark detection is usually called a blind detection.

D. Fingerprinting:

Additional data embedded by watermark in the fingerprinting applications are used to trace the originator or recipients of a particular copy of multimedia file. For example, watermarks carrying different serial or identity (ID) numbers are embedded in different copies of music CDs or DVDs before distributing them to a large number of recipients. The algorithms implemented in fingerprinting applications must show high robustness against intentional attacks and signal processing modifications such as lossy compression or filtering. Fingerprinting also requires good anti-collusion properties of the algorithms, i.e. it is not possible to embed more than one ID number to the host multimedia file, and otherwise the detector is not able to distinguish which copy is present. The embedding capacity required by fingerprinting applications is in the range of the capacity needed in copyright protection applications, with a few bits per second.

E. Broadcast monitoring:

A variety of applications for audio watermarking are in the field of broadcasting. Watermarking is an obvious alternative method of coding identification information for an active broadcast monitoring. It has the advantage of being embedded within the multimedia host signal itself rather than exploiting a particular segment of the broadcast signal. Thus, it is compatible with the already installed base of broadcast equipment, including digital and analogue communication channels. The primary drawback is that embedding process is more complex than a simple placing data into file headers. There is also a concern, especially on the part of content creators, that the watermark would introduce distortions and degrade the visual or audio quality of multimedia. A number of broadcast monitoring watermark-based applications are already available on commercial basis. These include program type identification, advertising research, broadcast coverage research etc. Users are able to receive a detailed proof of the performance information that allows them to:

• Verify that the correct program and its associated promos aired as contracted;
• Track barter advertising within programming;
• Automatically track multimedia within programs using automated software online.

III. ALGORITHMS

Watermarking algorithms were primarily developed for digital images and video sequences; interest and research in audio watermarking started slightly later. In the past few years, several algorithms for the embedding and extraction of watermarks in audio sequences have been presented. All of the developed algorithms take advantage of the perceptual properties of the human auditory system (HAS) in order to add a watermark into a host signal in a perceptually transparent manner. A broad range of embedding techniques goes from simple least significant bit (LSB) scheme to the various spread spectrum methods. The overview given in this section presents the best known general audio watermarking algorithms, with an emphasis on the algorithms that were used as a basis for published work (LSB algorithm, spread spectrum, improved spread spectrum, etc.).

A. Least Significant Bit (LSB) Coding

One of the earliest techniques studied in the information hiding of digital audio (as well as other media types) is LSB coding. In this technique LSB of binary sequence of each

sample of digitized audio file is replaced with binary equivalent of secret message. For example if we want to hide the letter „A" (binary equivalent1000001) into a digitized audio file where each sample is represented with 16 bits, then LSB of 7 consecutive samples (each of 16 bit size) is replaced with each bit of binary equivalent of the letter. Advantages: It is the simplest way to embed information in a digital audio file. It allows large amount of data to be concealed within an audio file, use of only one LSB of the host audio sample gives a capacity equivalent to the sampling rate which could vary from 8 kbps to 44.1 kbps (all samples used). This method is more widely used as modifications to LSBs usually not create audible changes to the sounds. Disadvantage: It has considerably low robustness against attacks.

B. Parity Coding

Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region.
Advantage: The sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive manner. Disadvantage: This method like LSB coding is not robust in nature.
Phase Coding: Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. It "works by substituting the phase of an initial audio segment with a reference phase that represents the data. The phase of subsequent segments is then adjusted in order to preserve the relative phase between segments".
Disadvantage: It is a complex method and has low data transmission rate.
Spread Spectrum (SS): It attempts to spread out the encoded data across the available frequencies as much as possible. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. However, unlike LSB coding, the SS method spreads the secret message over the sound files frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission. Advantage: It offers moderate data transmission rate while maintaining a high level of robustness.
Disadvantage: It can introduce noise into a sound file.

C. Echo data hiding:

Text can be embedded in audio data by introducing an echo to the original signal. The data is then hidden by varying three parameters of the echo: initial amplitude, decay rate, and offset. If only one echo is produced from the original signal, then only one bit of information could be encoded. Digital watermarking life-cycle phases: The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

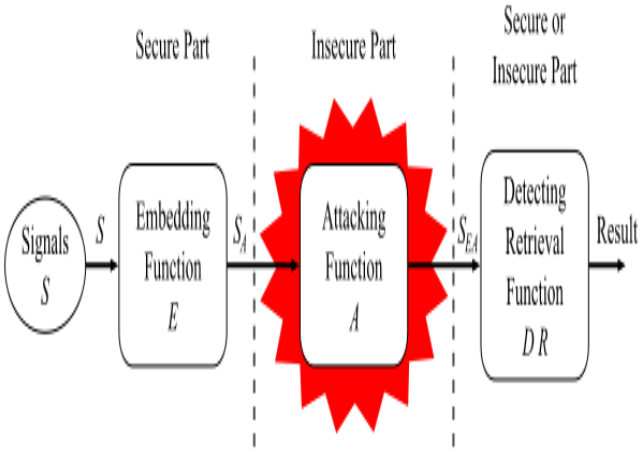

Fig. 1: Process of Watermarking

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise.
Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal.

IV. METHOD OF WATERMARKING USING DCT METHOD

In this section, we give an overview of our basic watermarking method which consists of watermark embedding process and watermark detection process. In this implementation, a watermark consists of a sequence of real numbers X= {x1, x2, x3,..., xn}. We create a watermark where each value of xi is chosen independently according to N (0,1) where N(μ, _2) denotes a normal distribution with mean μ and variance .

A. Watermark Embedding Process

The proposed watermark embedding process is shown in Figure 1. The embedding process is implemented in the following seven steps:

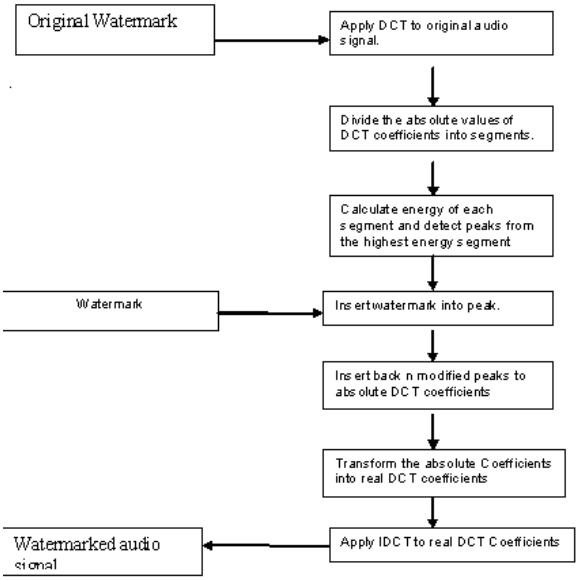

Fig. 2: Watermark embedding process

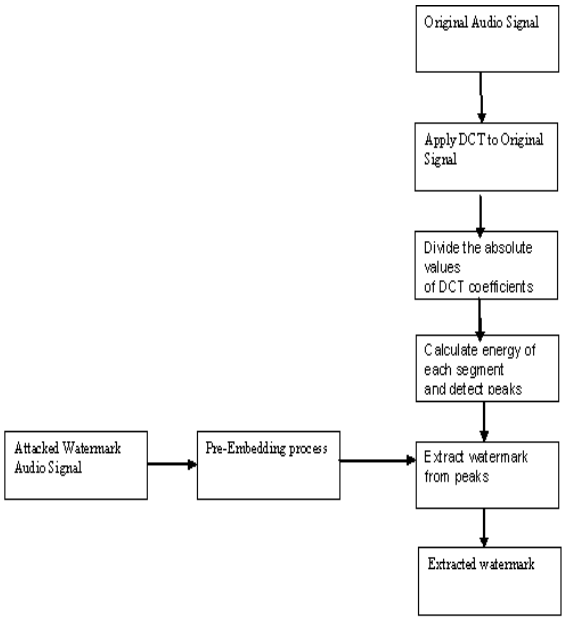

Fig. 3: Watermark detection process

Step 1: The original audio signal is transformed into DCT domain to calculate the DCT coefficients.
Step 2: Absolute values of the DCT coefficients are divided into an arbitrary number of segments.
Step 3: Energy of each segment is then calculated. Mathematically, the energy is calculated using the mathematical equation.
Step 4: Find the most prominent peaks from the highest energy segment using a peak detection algorithm.
Step 5: The watermark is then embedded into the selected N peaks of the highest energy segment, where N is the length of watermark. This ensures that the watermark is located at the most significant perceptual components. When we insert the watermark X into V to obtain V', we specify a scaling parameter _, which determines the extent to which X alters V.
Step 6: Insert back the modified peak into the highest energy segment of absolute DCT coefficients and transform these absolute coefficients to real DCT coefficients.
Step 7: Apply an inverse Discrete Cosine Transformation (IDCT) to the real DCT coefficients to Obtaining the watermark audio signal.

B. Watermark Detection Process

The detection process is implemented in the following three steps:
Step 1: The attacked watermarked audio signal is transformed into DCT domain.
Step 2: Extract the highest prominent peaks from the absolute DCT coefficients which are located at the same position in the embedding process above.
Step 3: The watermark sequence * * * * * 1 2 3 , , ,..., n X = x x x x is then extracted by performing the inverse operation .

METHOD OF WATERMARKING using Genetic Algorithm Approach
As Figure shows, there are four main steps in this algorithm that are explained below.
Alteration:
At the first step, message bits substitute with the target bits of samples. Target bits are those bits which place at the layer that we want to alter. This is done by a simple substitution that does not need adjustability of result be measured.
Modification:
In fact this step is the most important and essential part of algorithm. All results and achievements that we expect are depending on this step. Efficient and intelligent algorithms are useful here. In this stage algorithm tries to decrease the amount of error and improve the transparency. For doing this stage, two different algorithms will be used. One of them that is more simple likes to ordinary techniques, but in aspect of perspicacity will be more efficient to modify the bits of samples better. Since transparency is simply the difference between original sample and modified sample, with a more intelligent algorithm, I will try to modify and adjust more bits and samples than some previous algorithms. If we can decrease the difference of them, transparency will be improved. There are two example of adjusting for expected intelligent algorithm below. Sample bits are: 00101111 = 47 Target layer is 5, and message bit is 1.
Without adjusting: 00111111 = 63 (difference is 16) after adjusting: 00110000 = 48 (difference will be 1 for 1 bit embedding) Sample bits are: 00100111 = 39. Target layers are 4&5, and message bits are 11 without adjusting: 00111111 = 63 (difference is 24) after adjusting: 00011111 = 31 (difference will be 8 for 2 bits embedding) another one is a Genetic Algorithm which the sample is like a chromosome and each bit of sample is like a gene. First generation or first parents consist of original sample and altered sampled.

Fitness may be determined by a function which calculates the error. It is clear, the most transparent sample pattern should be measured fittest. It must be considered that in crossover and mutation the place of target bit should not be changed.

Verification: In fact this stage is quality controller. What the algorithm could do has been done, and now the outcome must be verified. If the difference between original sample and new sample is acceptable and reasonable, the new sample will be accepted; otherwise it will be rejected and original sample will be used in reconstructing the new audio file instead of that.

Reconstruction: The last step is new audio file (stego file) creation. This is done sample by sample. There are two states at the input of this step. Either modified sample is input or the original sample that is the same with host audio file. It is why we can claim the algorithm does not alter all samples or predictable samples. That means whether which sample will be used and modified is depending on the status of samples (Environment) and the decision of intelligent algorithm.

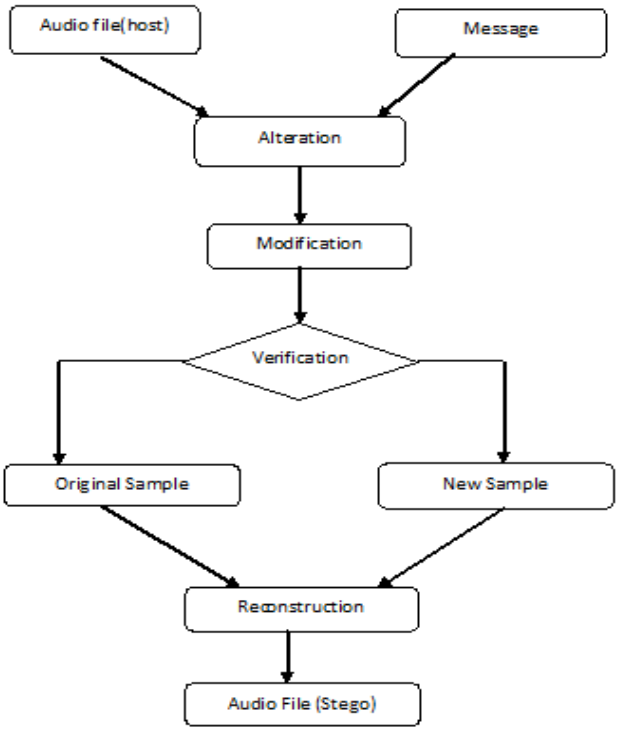

Fig. 4: Approach Diagram

V. SPATIAL-DOMAIN TECHNOLOGIES

Spatial-domain technologies refer to those embedding watermarks by directly changing pixel values of host images. Some common spatial-domain algorithms include Least Significant Bit (LSB) Modification, Patchwork, Texture Block Coding, etc. The most serious drawback of spatial-domain technologies is limited robustness. It is difficult for spatial-domain watermarks to survive under attacks such as lossy compression and low-pass filtering. Also the information can be embedded in spatial domain is very limited. In recent years they are becoming generally abandoned. We introduce the most famous spatial-domain technology, LSB Modification, to keep the discussion complete. The LSB is the most straight-forward method of watermark embedding. Given the extraordinarily high channel capacity of using the entire cover for transmission in this method, a smaller object may be embedded multiple times. Even if most of these are lost due to attacks, a single surviving watermark would be considered a success. LSB substitution however despite its simplicity brings a host of drawbacks. Although it may survive transformations such as cropping, any addition of noise or lossy compression is likely to defeat the watermark. An even better attack would be to simply set the LSB bits of each pixel to one, which fully defeating the watermark with negligible impact on the cover object. Furthermore, once the algorithm is discovered, the embedded watermark could be easily modified by an intermediate party. The algorithm however would still be vulnerable to replacing the LSB's with a constant. Even in locations that were not used for watermarking bits, the impact of the substitution on the cover image would be negligible. LSB modification proves to be a simple and fairly powerful tool for stenography, however lacks the basic robustness that watermarking applications require.

VI. FREQUENCY-DOMAIN TECHNOLOGIES

Compared to spatial-domain watermark, watermark in frequency domain is more robust and compatible to popular image compression standards. Thus frequency-domain watermarking obtains much more attention. To embed a watermark, a frequency transformation is applied to the host data. Then, modifications are made to the transform coefficients. Possible frequency image transformations include the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and others. The first efficient watermarking scheme was introduced by Koch et al. In their method, the image is first divided into square blocks of size 8x8 for DCT computation. A pair of mid-frequency coefficients is chosen for modification from 12 predetermined pairs. After dividing the image into blocks of size 8x8, certain blocks are selected based on a Gaussian network classifier decision. The middle range frequency DCT coefficients are then modified, using either a linear DCT constraint or a circular DCT detection region. A DCT domain watermarking technique based on the frequency masking of DCT blocks was introduced by Swanson. Cox developed the first frequency-domain watermarking scheme. After that a lot of watermarking algorithms in frequency domain have been proposed. Most frequency-domain algorithms make use of the spread spectrum communication technique. By using a bandwidth larger than required to transmit the signal, we can keep the SNR at each frequency band small enough, even the total power transmitted is very large. When information on several bands is lost, the transmitted signal can still being recovered by the rest ones.

The spread spectrum watermarking schemes are the use of spread spectrum communication in digital watermarking. Similar to that in communication, spread spectrum watermarking schemes embed watermarks in the whole host

image. The watermark is distributed among the whole frequency band. To destroy the watermark, one has to add noise with sufficiently large amplitude, which will heavily degrade the quality of watermarked image and be considered as an unsuccessful attack.

VII. CONCLUSION

In this paper, we have presented different watermarking methods for copyright protection of audio data. In most watermark hiding techniques, the watermark is hidden in the audio either in the spatial or frequency domain. The audio will suffer a certain degree of distortions for the embedment. This technique indicate that watermarking method shows strong robustness and data will secure or protected from unauthorized accessing users or against several kinds of attacks such as noise addition, cropping, re-sampling, re-quantization, MP3 compression, and echo attack. The process of the algorithm, including watermark embedding, and watermark detection, is described in detail. Thus watermarking method can be a suitable for audio copyright protection. Results from the experimental testing on the several different attacks showed that the recovered watermarks are visually clear, robust and imperceptible.

REFERENCES

[1] W. N. Lie and L. C. Chang, "Robust and High-Quality Time-Domain Audio Watermarking Based on Low-Frequency Amplitude Modification," IEEE Transaction on Multimedia, vol. 8, no. 1, pp. 46-59,February, 2006.

[2] P. Bassia, I. Pitas and N. Nikolaidis "Robust Audio Watermarking in the Time domain," IEEE Transaction on Multimedia, vol. 3, no. 2, pp. 232-241, June, 2001.

[3] L. Xie, J. Zhang and H. He, "Robust Audio Watermarking Scheme Based on Nonuniform Discrete Fourier Transform," in Proceedings of IEEE International Conference on Engineering of Intelligent System, pp. 1-5, 2006.

[4] G. Zeng and Z. Qiu, "Audio Watermarking in DCT: Embedding Strategy and Algorithm," in Proceedings of 9th International Conference on Signal Processing (ICSP'09), pp. 2193-2196, 2008.

[5] J. Huang, Y. Wang, and Y. Q. Shi, "A Blind Audio Watermarking Algorithm with Self- Synchronization," in Proceedings of IEEE International Symposium on Circuits and Systems, (ISCAS'02), vol. 3, pp. 627–630, 2002.

[6] "Algorithms for Audio Watermarking and SteganoGraphy", NEDELJKO, CVEJIC Department of Elec T r i cal and Information Engineering, Information Processing Laboratory, University of OULU 2004.

[7] L. T. Bruton, J. D. Gordy, Performance Evaluation of Digital Audio Watermarking Algorithms, Proceedings of the 43rd IEEE Midwest Symposium, Michigan, Volume 1, pp.456-459, 8-11 August 2000.

[8] M. D. Swanson, B. Zju, A. H. Tewfik, Robust audio watermarking using perceptual masking, Signal processing, vol.66,pp.337-355,1998.

[9] P. Bassia, I. Pitas, Robust audio watermarking in time domain, IEEE Trans. On Multimedia, vol.3, No.2, pp.232-241, June 2001.

[10] W. Bender, D. Grul, N. Morimoto, A. Lu, Techniques for data hiding, IBM System Journal,vol.35, pp.313-336,1996.

[11] Cvejic N. and Seppänen T. "Increasing the capacity of LSB based audio steganography", Proc. 5th IEEE International Workshop on Multimedia Signal Processing, St. Thomas, VI, December 2002, pp. 336-338.

[12] Fridrich, Jessica and others. "Steganalysis of LSB Encoding in Color Images." Proceedings of the IEEE International Conference on Multimedia and Expo. 1279– 1282. New York: IEEE Press, 2000.

[13] Lee, Y. K. and Chen L. H. "High Capacity Image Steganographic Model". IEEE Proceedings Vision, Image and Signal Processing, pp. 288-294, 2000.

[14] Martín Alvaro, Sapiro Guillermo and Seroussi Gadiel, "Is Image Steganography Natural?" IEEE Transactions On Image Processing, Vol. 14, No. 12, December, 2005.

[15] Pal S.K., Saxena P. K. and Mutto S.K. "The Future of Audio Steganography". Pacific Rim Workshop on Digital Steganography, Japan, 2002.

[16] Westfeld A. and Pitzmann A. "Attacks on Steganographic Systems". Lecture Notes in Computer Science, vol. 1768, Springer-Verlag, Berlin, pp. 61-75, 2000.

[17] Huang Cheh Huang, Chi-Ming Chu and Jeng-Shyang Pan, "The optimized copyright protection system with genetic watermarking", 2009, pp. 333-343, 2009.

[18] Shahreza S.S. and Shalmani M.T.M., "Adaptive wavelet domain audio steganography with high capacity and low error rate", in Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, pp: 1729 – 1732, 2008.

[19] "Audio steg: overview", Internet publication on www.snotmonkey.com,http://www.snotmonkey.com/work/school/405/overview.html.

[20] Gary C. Kessler, "Steganography: Hiding Data Within Data",http://www.garykessler.net/library/steganography.html, September 2001.

[21] C. Parthasarathy and Dr. S. K. Srivatsa, "Increased Robustness of Lsb Audio Steganography By Reduced Distortion Lsb Coding" 2005. www.jatit.org/volumes-/research papers/Vol7No1/9Vol7No1.pdf.

[22] Dr. H. B. Kekre and A. A. Archana, "Information hiding using LSB technique with increased capacity", International Journal of Cryptography and Security, vol. 1, No.2, October 2008.

