ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

Vol. 2, Issue 5, May 2013

FREQUENCY DOMAIN BASED DATA HIDING TECHNIQUE FOR AUDIO SIGNAL

Yatin Baluja[1], Shray Mishra[2], Trilok Singh Saini[3] , M.V. Patil[4]

Research Student, Dept. of Electronics, Bharati Vidyapeeth College of Engineering, Pune, Maharashtra, India[1]

Research Student, Dept. of Electronics, Bharati Vidyapeeth College of Engineering, Pune, Maharashtra, India[2]

Research Student, Dept. of Electronics, Bharati Vidyapeeth College of Engineering, Pune, Maharashtra, India[3]

Assistant Professor, Dept. of Electronics, Bharati Vidyapeeth College of Engineering, Pune, Maharashtra, India[4]

Abstract: Audio watermarking has been proved as a possible solution to avoid illegal usage of audio files. It embeds copyright information into audio files as a proof of their ownership. This paper deals with the design a system which is capable of hiding digital data inside an audio signal . Digital data which is to be embedded can be binary sequence, text or image. The proposed method can embed the watermark data in approximation coefficients of discrete wavelet transform. Experimental results for different audio signals show that this watermarking technique is robust against the common signal processing attacks such as resampling, Requantization, Low pass filtering, Volume scaling & Noise addition.

Keywords: Watermarking, Cover object, Covert data, Stego-object, Embed, Extraction.

I. INTRODUCTION

Watermarking [1] is an art of sending hidden data or secret messages over a public channel so that a third party cannot detect the presence of the secret messages. The goal of watermarking is different from classical encryption, which seeks to conceal the content of secret messages; watermarking is about hiding the very existence of the secret messages. Modern watermarking is generally understood to deal with electronic media rather than physical objects. There have been numerous proposals for protocols to hide data in channels containing pictures, video, audio and even typeset text. This makes sense for a number of reasons. First of all, because the size of the information is generally quite small compared to the size of the data in which it must be hidden (the cover text), electronic media is much easier to manipulate in order to hide data and extract messages. Secondly, extraction itself can be automated when the data is electronic, since computers can efficiently manipulate the data and execute the algorithms necessary to retrieve the messages. Electronic data also often includes redundant, unnecessary and unnoticed data spaces which can be manipulated in order to hide messages.

The main goal of this paper was to find a way so that an audio file can be used as a host media to hide textual message without affecting the file structure and content of the audio file.

A watermarking system, in general, is expected to meet three key requirements, namely, imperceptibility of embedding accurate recovery of embedded information, and large payload. In a pure watermarking framework, the technique for embedding the message is unknown to anyone other than the sender and the receiver. An effective watermarking scheme should posses the following desired characteristics:

Secrecy: A person should not be able to extract the cover data from the host medium without the knowledge of the proper secret key used in the extracting procedure.

Imperceptibility: The medium after being embedded with the covert data should be indiscernible from the original medium. One should not become suspicious of the existence of the covert data within the medium.

High capacity: The maximum length of the covert message that can be embedded should be as long as possible

Resistance: The covert data should be able to survive when the host medium has been manipulated, for example by some lossy compression scheme

Accurate extraction: The extraction of the covert data from the medium should be accurate and reliable.

The rest of the paper is organized as follows: Section two gives the literature review of digital watermarking techniques for audio .Implementation of the proposed work is described in section III. Experimental results are shown in section IV followed by the conclusion in the last section.

II. LITERATURE REVIEW

Ali Al-Haj & Ahmad Mohammad [1] an effective, robust, and an inaudible audio watermarking algorithm have been proposed. The effectiveness of the algorithm has been brought by virtue of applying a cascade of two powerful mathematical transforms; the discrete wavelets transform (DWT). The watermark bits are not embedded directly on the wavelet coefficients, but rather on the elements of singular values of the DWT sub-bands of the audio frames. By virtue of cascading the two transforms, inaudibility and different levels of robustness are achieved.

DR. A DAMODARAM & **R SRIDEVI [2]** is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safer manner. Though it is well modulated software it has been limited to certain restrictions. The quality of sound depends on the size of the audio which the user selects and length of the message. Though it shows bit level deviations in the frequency chart, as a whole the change in the audio cannot be determined.

Hyoung Joong Kim [3] surveys the audio watermarking schemes. State-of-the-art of the current watermarking schemes and their implementation techniques are briefly summarized. They are classified into five categories: quantization scheme, spread-spectrum scheme, two set scheme, replica scheme, and self- marking scheme. Quantization scheme is not so robust against attacks, but easy to implement. Spread spectrum scheme requires psycho-acoustic adaptation for inaudible noise embedding. This adaptation is rather time- consuming. Of course, most of the audio watermarking schemes need psycho acoustic modelling for inaudibility.

Driss Guerchi, Siwar Rekik & Habib Hamam [4] performance of audio watermarking compression system using discrete wavelet transform (DWT) is studied. Audio steganography coding is the technology of transforming stego-speech into efficiently encoded version that can be decoded in the receiver side to produce a close representation of the initial signal (non compressed). Experimental results prove the efficiency of the used compression technique since the compressed stego-speech are perceptually intelligible and indistinguishable from the equivalent initial signal, while being able to recover the initial stego-speech with slight degradation in the quality.

Youssef Bassil [5] proposes a novel randomized watermarking algorithm for hiding digital data into uncompressed audio files using two carrier intermediates to deliver the secret data. The first intermediate is a carrier audio file holding the secret data inside the LSBs of its audio samples which are selected randomly. The second intermediate is a grammatically correct English paragraph made up of several English sentences pointing to the location of the random carrier audio samples, that is, the location of the secret data in the carrier audio file.

J. D. Gordy and L. T. Bruton [6] is to present an algorithm- independent set of criteria for quantitatively comparing the performance of digital watermarking algorithms. This framework is then used to evaluate a selection of five audio watermarking algorithms from the literature. The paper is organized as follows. We present our evaluation criteria, and we provide experimental data and an analysis of the evaluated algorithms.

M. Nutzinger [7] is a novel combination of various basic signal processing operations for the generic prevention of watermarking communications in audio cover media. While many of the existing approaches, dealing with watermarking prevention, perform some kind of steganalysis, our approach is different. As mentioned above, no evidence for the existence of embedded data is searched.

III. IMPLEMENTATION TECHNIQUES

A. *DISCRETE WAVELET TRANSFORM*:

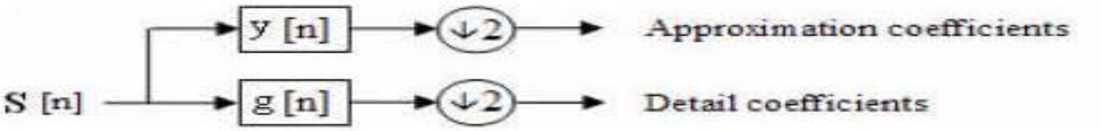

Fig.1 Discrete Wavelet Transform

The discrete wavelet transform (DWT) is a discipline capable of giving time-frequency representation of signal. Starting from the original audio signal S, DWT produces two sets of coefficients: the approximation coefficients y (low frequencies) and the detail coefficients g (high frequencies) as seen in Fig.1. Depending on the application and also the duration of signal, the low frequencies part might be further decomposed into two parts of high and low frequencies. In the DWT, each level is calculated by passing only the previous approximation coefficients through low and high pass filters.

B. *DISCRETE COSINE TRANSFORM*:

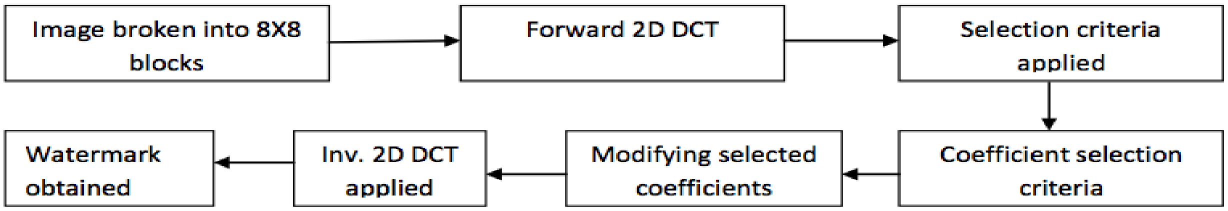
Image broken into 8X8 blocks
Forward 2D DCT
Selection criteria applied
Coefficient selection criteria
Modifying selected coefficients
Inv. 2D DCT applied
Watermark obtained

Fig.2 Discrete Cosine Transform

Discrete cosine transform (DCT): It is a process which converts a sequence of data points in the spatial domain to a sum of sine and cosine waveforms with different amplitudes in the frequency domain as can be observed from Fig.2 . The DCT is a linear transform, which maps an n-dimensional vector to set of n coefficients. A linear combination of n known basis vectors weighted with the n coefficients will result in the original vector. The known basis vectors of transforms from this class are “sinusoidal“, which means that they can be represented by sinus shaped waves or, in other words, they are strongly localized in the frequency spectrum [2].

C. *DIFFERENCE*:

- In Image compression:-DCT divides an image into 8-by-8 or 16-by-16 blocks while DWT represents image on different resolution levels.
- The compression standard JPEG2000, accepted quite recently, is based on DWT and it commonly provides considerably better quality of decoded images than JPEG.
- Multi-resolution analysis is available in DWT while in DCT it is not possible.

IV.BLOCK DIAGRAM OF AUDIO WATERMARKING

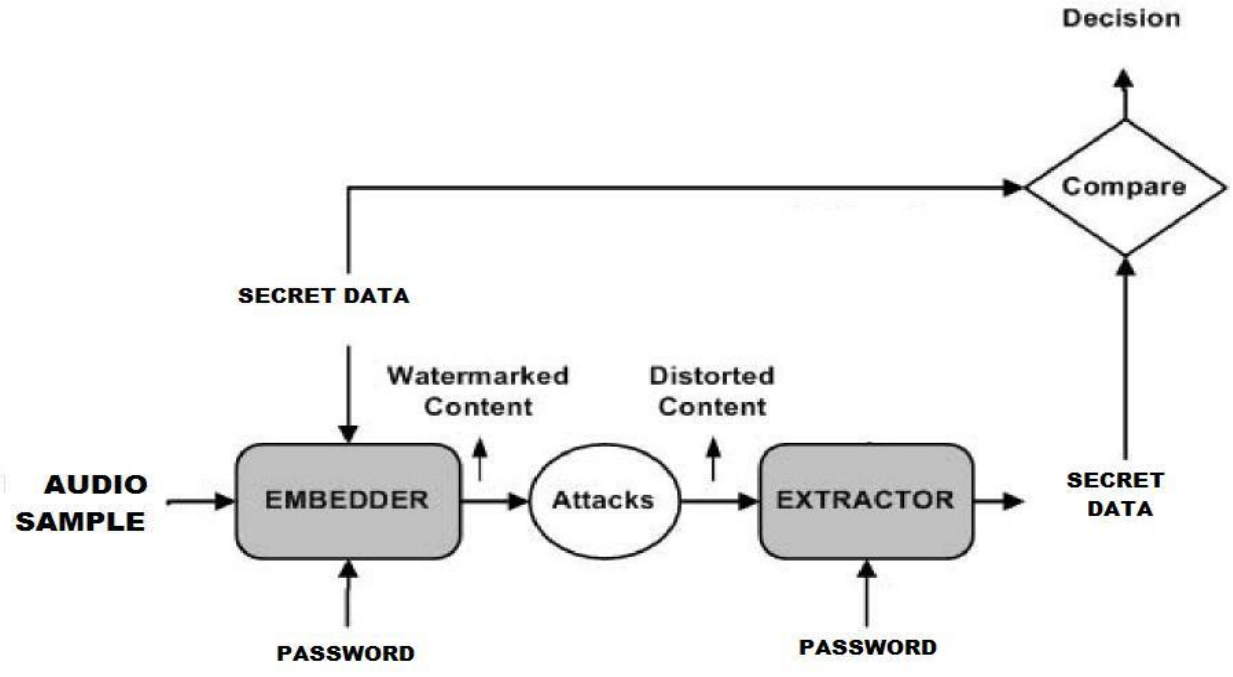

Fig.3 An overview of watermarking process

A typical watermarking system is shown in Fig.3 which includes watermark embedder and watermark extractor. The inputs to the watermark embedder are secret data, audio sample and password. The purpose of this password is to enhance the security of watermarking system. The output of the watermarking embedder is the watermarked content. The inputs to the watermark extractor are the watermarked content, the password (same as used at the time of embedding) and depending on the method, the original cover content or the watermark.

A watermark detector involves two step process:The first step is watermark extraction that applies one or more pre-process to extract a vector called as extracted watermark. Then the second step is to determine whether the extracted watermark is same as original watermark or not. This process usually involves the comparing of the extracted watermark with the original also called reference watermark and result could be some kind of measurement indicating how likely the original watermark is present in the content [10].

V. EVALUATION CRITERIA

A. MSE:

Mean Squared Error is essentially a signal fidelity measure. The goal of a signal fidelity measure is to compare two signals by providing a quantitative score that describes the degree of similarity/fidelity or, conversely, the level of error/distortion between them. Usually, it is assumed that one of the signals is a pristine original, while the other is distorted or contaminated by errors. The MSE between the signals is given by the following formula:

$$\mathbf{MSE = 1/_{N}\sum i|x(i)- e(i)|^{2}}$$

Here x and e are the encrypted watermarked audio signals respectively and N is the number of samples in the audio signal.

B. BER:

Bit error rate refers to the amount of watermark data that may be reliably embedded within a host signal per unit of time or space, such as bits per second or bits per pixel. A higher bit rate may be desirable in some applications in order to embed more copyright information. In this study, reliability was measured as the bit error rate (BER) of extracted watermark data. The BER (in percent) is given by the expression:

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(\frac{-u^2}{2} \right) du$$

where x is a function of the block size.

C. PERCEPTUAL QUALITY:

Perceptual quality refers to the imperceptibility of embedded watermark data within the host signal. In most applications, it is important that the watermark is undetectable to a listener or viewer. This ensures that the quality of the host signal is not perceivably distorted, and does not indicate the presence or location of a watermark. In this study, the signal-to-noise ratio (SNR) of the watermarked signal versus the host signal was used as a quality measure:

$$SNR = 10 \cdot \log_{10} \left\{ \frac{\sum_{n=0}^{N-1} x^2(n)}{\sum_{n=0}^{N-1} [\tilde{x}(n) - x(n)]^2} \right\}$$

D. PSNR

Embedding this extra data must not degrade human perception about the object. Namely, the watermark should be “invisible” in a watermarked image or “inaudible” in watermarked digital music. Evaluation of imperceptibility is usually based on an objective measure of quality, called peak signal to noise ratio (PSNR), or a subjective test with specified procedures [6]. The PSNR values can be obtained using following formula-

PSNR = 20log10 (65535/√MSE)

VI. RESULT

Table1: Performance analysis of watermarked audio under different attacks

SERIAL NO.	TYPES OF ATTACKS	MSE	SNR	PSNR	BER
1.	NO ATTACK	2.94533e-006	26.6935	55.3087	0
2.	VOLUME SCALING	2.94602e-006	26.6555	55.3076	0
3.	ADDITIVE NOISE	3.04204e-006	26.4523	55.1684	10
4.	LOW PASS FILTER	0.00165588	26.764	27.8097	100
5.	REQUANTIZATION	2.94533e-006	26.6935	55.3087	0
6.	RESAMPLING	0.00167371	26.4987	27.7632	100

Experimental results prove that the quality of stego-audio is not affected drastically, when various attacks are carried out on stego-audio. The compressed stego-audio are perceptually intelligible and indistinguishable from the equivalent initial signal, while being able to recover the initial stego-speech with slight degradation in the quality [6],[7],[9].

VII. CONCLUSION

Data hiding in audio signal is a concept which is experiencing continuous progress. Frequency Domain based data hiding is the best method to carry out watermarking because it has more robustness compared to spatial domain based data hiding technique. Moreover, frequency based method is suitable where less payload is required and even the size of the audio signal is not varied when watermark is encoded in audio signal. Hence, we can conclude that data hiding using frequency domain is ideal when watermarking using audio signal has to be performed.

REFERENCES

[1] Al-Haj, A., Mohammad, A., Digital Audio Watermarking Based on the Discrete Wavelets Transform and Singular Value Decomposition, European Journal of Scientific Research , Vol.39 No.1, pp.6-21,2010

[2] Sridevi ,R., Damodaram, Dr.A., Narasimham, Dr.S., Efficient Method Of Audio Steganography By Modified Lsb Algorithm And Strong Encryption Key With Enhanced Security, Journal of Theoretical and Applied Information Technology,2009 .

[3] Kim,H.J, Audio Watermarking Techniques ,Department of Control and Instrumentation Engineering, Kangwon National University, Korea.

[4] Rekik, S ,Guerchi, D, Hamam, H ,Selouani,S.D., Audio Steganography Coding Using the Discrete Wavelet Transforms , International Journal of Computer Science and Security , Volume 6 , Issue 1, 2012

[5] Youssef ,B., A Two Intermediates Audio Watermarking Technique, Journal of Emerging Trends in Computing and Information Sciences, VOL. 3, NO.11, 2012

[6] Gordy , J. D, Bruton , L. T. , Performance Evaluation of Digital Audio Watermarking Algorithms, Department of Electrical and Computer Engineering University of Calgary,2500 University Drive N.W. Calgary, Alberta, Canada T2N 1N4.

[7] Nutzinger, M., Real-time Attacks on Audio Watermarking, Journal of Information Hiding and Multimedia Signal Processing c 2012 ISSN 2073-4212 Ubiquitous International Volume 3, Number 1, January 2012.

[8] Kahalkar, C., Digital Audio Watermarking for Copyright Protection, India, International Journal of Computer Science and Information Technologies, Vol. 3,pp. 4185-4188, 2012.

[9] Chadha, A., Gangundi, S., Goel, R. Dave, H., Roja, M.M ,Audio Watermarking with Error Correction, INDIA, International Journal of Advanced Computer Science and Applications, Vol. 2, No. 9, 2011.

[10] Abrar Ahmed Syed, Digital Watermarking, 1000614216, , The University of Texas , Arlington.