Analyzing Audio Watermarking algorithms

Amita[1], Parveen Khanchi[2]

[1]M.Tech Scholar, BIMT Gohana
[2]A.P., BIMT Gohana

Abstract: **Memories take important role in development of new technology because memory may fail during their operation with their expected life time. So memory is needed to keep on test mode and validates that whether it is error free or not. In the virtue of submicron effect redundant circuit must kept on chip to replace faulty part. That method is known as BIST. Module synthesizes the cut the faulty part. The chip tastes the circuit each time before they start up. The main purpose of this to have error free circuit, small area and low power. The paper concluded some test problems and its reliable solution.**

Key words: **Audio Watermarking**

I. INTRODUCTION

The concept of watermarking has evolved from paper watermarking to digital watermarking. This concept has a long history, which can be traced back to 1282 when paper watermarks first appeared in Italy [KP00]. The watermarks were made by adding thin wire patterns to the paper moulds during the manufacturing process. The paper would be slightly thinner where the wire patterns were added and hence more transparent. The exact reason and purpose of the introduction of this watermark are uncertain. They may have been used for practical functions such as identifying the mould on which sheets of papers were made, or as trademarks to identify the paper maker.

By the eighteenth century, watermarks on paper made in Europe and America had become more clearly utilitarian. They were used as trademarks to record the date the paper was manufactured, and to indicate the sizes of original sheets. It was also about this time that watermarks began to be used as anti-counterfeiting measures on money and other documents. The term watermark appears to have been coined near the end of the eighteenth century and may have been derived from the German term wassermarke.

In 1954, Emil Hembrooke of the Muzak Corporation filed a patent for "watermarking" musical works. An identification code was inserted in music by intermittently applying a narrow notch filter centred at 1 kHz. The absence of energy at this frequency indicated that the notch filter had been applied and the duration of the absence used to code either a dot or a dash. The identification signal used Morse code. The 1961 U.S. Patent describing this invention states:

"The present invention makes possible the positive identification of the origin of a musical presentation and thereby constitutes an effective means of preventing such piracy".

This system was used by Muzak until around 1984. It is interesting to note that there was speculation at the time that this invention was delivering subliminal advertising messages to its listeners.

It is difficult to exactly determine when the concept of digital watermarking was first proposed. For example, in 1979, Szepanski described a machine-detectable pattern that could be placed on documents for anti-counterfeiting purposes. Nine years later, Holt et al. described a method for embedding an identification code in an audio signal. However, it was Komatsu and Tominaga, in 1988, who appeared to have first used the term digital watermark. It was not until the mid 1990‟s that interest in digital watermarking began to soar, and this interest has continued until the present day.

II. WATERMARKING ALGORITHM

In this section, the definition and characteristics of a watermarking algorithm will be illustrated.

Watermarking definition

Digital watermarking is the process by which a discrete data stream called a watermark is embedded within a digital content. It is a special form of steganography, which is concerned with developing methods of writing hidden messages in such a way that no one, apart from the intended recipient, knows of the existence of the message. Generally, the process of watermarking can be divided into two parts: embedding and detection, the embedding process is depicted in Figure 1.1.

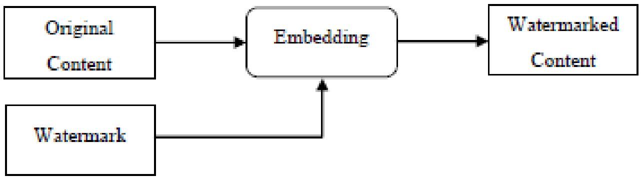

Figure 1.1 The flowchart of the embedding process

As seen from Figure 1.1, the process of watermark embedding is very straightforward, that is, the watermark is generated and then is embedded into the original content by some means. A variety of embedding algorithms have been developed which rely on the manipulation of some properties of the original content.

The detection process, as depicted in Figure 1.2, illustrates the embedded watermark information being recovered only by the use of the key.

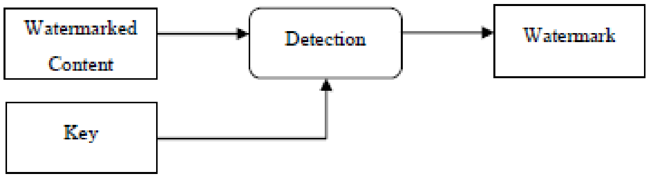

Figure 1.2 One type of detection processes

A more complex detection process, as depicted in Figure 1.3, illustrates the detection of the presence of watermark information, which requires not only the key, but also the original watermark and/or the original content. Compared with the detection process described in Figure 1.2, this needs extra storage capability for the original watermark information or original host information. However, the advantage of using the detection process described in Figure 1.3 is that the detection performance can be greatly improved when the original host or original watermark bit sequence is available.

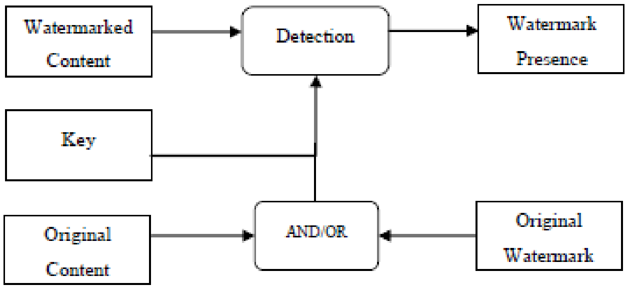

Figure 1.3 The other type of detection processes

Watermarking characteristics

A watermarking algorithm has the following characteristics [NC06, Cve07]:

1. Imperceptibility: in general, the embedded watermark should not affect the human perception of the content. Namely, the watermark should be "invisible" in an image/video or "inaudible" in audio. However, in some special application scenarios, the watermark should be obtrusive to serve as a statement of ownership. Therefore, watermarking algorithms can be classified as „perceptible" where the embedded watermark can be perceived and „imperceptible" where the embedded watermark cannot be perceived.

2. Robustness: any manipulation of the watermarked content is defined as an attack. The embedded watermark should be robust against attacks. That is, the watermark recovery accuracy should not be decreased significantly after the watermarked content is attacked. Attacks on watermarks can be accidental or intentional. Accidental attacks are the result of standard signal processing that the signal might undergo, such as Analogue to Digital (A/D) conversion, Digital to Analogue (D/A) conversion and lossy compression. Intentional attacks refer to those that deliberately distort or remove the embedded watermarks. As far as audio is concerned, the main attacks, both intentional and accidental, can be divided into the following groups:

I. Filtering: such as highpass filtering, lowpass filtering and equalization. An equalizer only increases or decreases specified spectral regions.

II. Lossy compression: such as MP3 or Advance Audio Coding (AAC), which are used to reduce the amount of audio data.

III. Noise: such as noise adding or removal.

IV. Conversion: such as A/D, D/A or conversion of the sampling frequency (for example, from 32 kHz to 48 kHz).

V. Time stretch: increasing or decreasing the duration of an audio signal without changing its pitch.

VI. Pitch shift: change the pitch without changing the speed of the audio.

The task of designing a robust watermarking algorithm, which is able to withstand all or even a subset of possible attacks, appears to be quite difficult. Each algorithm currently proposed has its own weakness against certain types of attack. However, not every attack is possible with particular applications. Thus, identifying potential attacks that are associated with a specified application is essential. The most powerful attacks are those that can remove or distort the watermark information without severely degrading the content quality. With these attacks, the watermark information cannot be recovered but the audio can be used normally. Watermarking algorithms can be classified as „robust", „fragile" and „semi-fragile" according to their robustness against attacks.

3. Capacity: the watermarking algorithm should be capable of embedding a large amount of watermark information into the digital content.

4. Blindness: in general, the watermarking algorithm should be blind, that is, the embedded watermark can be detected without requiring access to the original content or original watermark. However, some watermarking algorithms can only detect the presence of the original watermark. Therefore, watermarking algorithms can be classified as „blind" and „informed" in terms of how much information is required at the detection stage. The „blind" watermarking algorithm only

requires a „key‟ to detect the watermark. While the „informed‟ watermarking algorithm needs the original watermark or the original content to detect the presence of the watermark information.

5. Computational efficiency: the efficiency of the watermarking algorithm will determine if it can be applied in time-critical applications.

6. Security: Kerchhoff‟s Principle states that a cryptosystem should be secure even if everything about the system, except the key, is publicly known. This principle was reformulated by Claude Shannon as "the enemy knows the system", which is embraced by cryptographers worldwide. As far as watermarking systems are concerned, the algorithm might be published or made public. However, an unauthorized user, who may even know the exact watermarking algorithm, should not be able to detect the embedded watermark unless the secret keys are disclosed.

7. Adjustability: The algorithm should be tuneable to various degrees of robustness, imperceptibility and capacity to facilitate diverse applications.

Watermarking trade-off

The imperceptibility, robustness and capacity are the three most important characteristics of a watermarking algorithm. However, there is a trade-off between these three characteristics. This trade-off can be represented as shown in Figure 1.4.

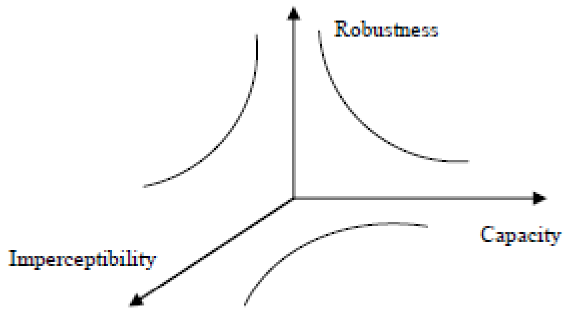

Figure 1.4 Trade-off presents in watermarking system

As seen from Figure 1.4, imperceptibility, robustness and capacity are conflicting characteristics of a watermarking system. For example, a specific application may determine what the capacity is needed. After it is determined, there exists a trade-off between imperceptibility and robustness. If one then wants to make the watermark more robust against attacks, a larger modification of the signal‟s properties to embed the watermark will be necessary. However, this will worsen the imperceptibility. Another scenario may be that with a predefined requirement for the imperceptibility, there will exist a trade-off between the capacity and robustness. For instance, the fewer the message bits that are embedded, the more redundant the watermark can be. Therefore, the watermarking will have a better error correction capability against attacks, that is, it is more robust.

III. EXISTING WORKS

[1]. In this paper, need for audio watermarking along with its important properties is explained. The paper also brings to view works done by various on digital audio watermarking. This paper surveyed those papers and presented some of the important techniques used for digital audio watermarking. 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 psychoacoustic modeling for inaudibility. Another disadvantage of spread-spectrum scheme is its difficulty of synchronization. On the other hand, replica method is effective for synchronization. However, echo hiding is vulnerable to attack. Amplitude modulation technique requires large channel capacity. Also it introduces large amount of noise which is audible. The impact of this noise is a direct function of the content of the host signal. In case of dither watermarking, it provides better sampling of a signal when converting it into digital signal as distortion in the signal are almost eliminated but noise is increased to very large extent. Self-marking method can be used especially for synchronization or for robust watermarking, for example, against time-scale modification attack. Such five seminal works have improved watermarking schemes remarkably. However, more sophisticated technologies are required. As every technique is different from another one, comparison among them cannot be done.

[2]. A semi-blind, imperceptible, and robust digital audio watermarking algorithm is developed in this paper. The proposed algorithm is based on cascading two well-known transforms: the discrete wavelet transform and the singular value decomposition. The two transforms provide different, but complementary, levels of robustness against watermarking attacks. The uniqueness of the proposed algorithm is twofold: the distributed formation of the wavelet coefficient matrix and the selection of the off-diagonal positions of the singular value matrix for embedding watermark bits. Imperceptibility, robustness, and high data payload of the proposed algorithm are demonstrated using different musical clips.

[3]. This paper proposed efficient audio watermarking embedding and extracting techniques, which mainly use Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD), in which a new matrix formation of details sub-bands is proposed. Additionally, massive experimental work

was conducted to investigate the contributions of operating different watermark intensities and multiple levels of DWT to our proposed techniques. Two performance objectives are employed in this work which involve imperceptibility and robustness. To further boost the imperceptibility, we incorporate the code assignment method to our techniques that do outperform what are closely connected in the literature.

[4]. This paper presents a digital audio watermarking scheme based on spread spectrum technique to embed the watermark. This method does not need the original audio carrier signal when extracting watermark using the blind extraction audio watermark. The experimental results demonstrate that the embedding technique is not only less audible but also more robust against the common signal processing attacks like low-pass filter, adding white Gaussian noise, shearing, and compression.

[5]. This paper presents a novel approach for blind audio watermarking. The proposed scheme utilizes the flexibility of discrete wavelet packet transformation (DWPT) to approximate the critical bands and adaptively determines suitable embedding strengths for carrying out quantization index modulation (QIM). The singular value decomposition (SVD) is employed to analyze the matrix formed by the DWPT coefficients and embed watermark bits by manipulating singular values subject to perceptual criteria. To achieve even better performance, two auxiliary enhancement measures are attached to the developed scheme. Performance evaluation and comparison are demonstrated with the presence of common digital signal processing attacks. Experimental results confirm that the combination of the DWPT, SVD, and adaptive QIM achieves imperceptible data hiding with satisfying robustness and payload capacity. Moreover, the inclusion of self-synchronization capability allows the developed watermarking system to withstand time-shifting and cropping attacks.

[6]. Paper proposed a new approach for optimization in digital audio watermarking using genetic algorithm. The watermarks are embedded into the low frequency coefficients in discrete multiwavelet transform domain. The embedding technique is based on quantization process which does not require the original audio signal in the watermark extraction. We have developed an optimization technique using the genetic algorithm to search for four optimal quantization steps in order to improve both quality of watermarked audio and robustness of the watermark. In addition, we analyze the performance of the proposed algorithm in terms of signal-to-noise ratio, normalized correlation, and bit error rate. The experimental results show that the proposed scheme can achieve a good robustness against most of the attacks which were included in this study.

[7]. In this paper, an innovative watermarking scheme for audio signal based on genetic algorithms (GA) is proposed. Designing an optimal audio watermarking system is an open difficult issue since its two basic performance measures, i.e., imperceptibility and robustness. So, an optimal audio watermarking scheme needs to optimally balance both imperceptibility and robustness. In order to realize such an optimal watermarking system, we propose an optimal audio watermarking scheme using genetic optimization with variablelength mechanism in this paper. The presented genetic optimization procedure can automatically determine optimal embedding parameters for each audio frame of an audio signal. Specially, employed variable-length mechanism can effectively search most suitable positions for watermark embedding, including suitable audio frames and their AC coefficients. By dint of the genetic optimization with variable-length mechanism, proposed audio watermarking scheme can not only guarantee good quality of watermarked audio signal but also effectively improve its robustness. Experimental results show that proposed watermarking scheme has good imperceptibility and high capability against common signal processing and some de synchronization attacks.

[8]. In the proposed framework, a multi-objective particle swarm optimization technique based on fitness sharing is applied to search optimal watermarking parameters and Pareto-optimal solutions are used to express the optimal parameters found. In addition, the proposed framework has the following advantages: (i) it can avoid the difficulty of determining optimal weighted factors in the existing single-objective watermarking schemes; (ii) Pareto-optimal solutions can offer the flexibility to select optimal parameters for satisfying different application demands

[9]. In this paper, survey has been performed of bio-inspired techniques for information hiding. The applications of bio-inspired optimization for information hiding or watermarking have emerged in early 2000’s. Due to the flexibility of algorithm designs, parameter selections, and performance metrics, the uses of bio-inspired optimization techniques provide effective solutions for information hiding. Relating schemes from different papers in literature are extensively surveyed and are briefly discussed. This survey aims at providing the background knowledge for further researches in this field.

[10]. In this paper, a watermark scheme with circulation, based on nonoverlapping discrete wavelet transform

(DWT) and singular value decomposition (SVD), is presented. First, the original host image and watermark image are divided into nonoverlapping blocks, respectively and to the former DWT and SVD is applied. Second, the scrambling watermark by Chebyshev chaotic map is embedded into the singular value matrix of original components with circulation. Extracting any consecutive four rows and columns from the blocked watermarked image can get complete watermark information. The quantity of embedded watermark information is large and the original image is not needed for watermark extracting. Both theoretical analysis and experimental results indicate that the proposed method can very effectively resist large degree of geometric attacks and compound attacks, and it is also strongly robust against common image processing attacks.

[11]. This paper proposed a novel blind audio watermarking algorithm, which combined Singular Value Decomposition(SVD) with Discrete Wavelet Transform(DWT). In our algorithm, We first partition the rearranged audio signal into blocks, then generate the vector by selecting the biggest singular values after performing SVD on these blocks. Finally we embed the watermark into the approximate components obtained from the DWT decomposition of the vector by means of quantization process. Experimental results showed that our algorithms good robustness against the common audio signals processing operations. Compared with earlier schemes based on SVD, the proposed scheme has satisfying imperceptibility and improved payload.

[12]. This paper proposed an audio watermarking and robust algorithm using DWT- SVD and ATS. The embedding intensity is searched by using an AI technique called the adaptive tabu search. Experimental result reveal that if we combined the concepts of existing algorithm, both the watermarked image quality and the Sim value use of the extracted watermarks after certain attacks was acceptable. Experiments have shown that the inaudibility and robustness performance goals can be achieved. When the audio Stirmark benchmark tool is used to evaluate the robustness performance against signal distortions, our algorithm performed better than the standard SNR.

[13]. This paper describes an audio watermarking method where a copyright information is imperceptibly added into the audio signal. The copyright information or watermark could be a binary logo or some unique binary pattern. In this paper we borrowed a cryptographic technique method known as secret sharing method. The secret sharing method along with discrete wavelet transform (DWT) and singular value decomposition (SVD) is used to embed and retrieve the watermark from the audio signal. The advantage using secret sharing in audio watermarking is that it will make the watermark robust to both cryptographic and compression attacks. The simulation results show that the new technique is robust against different attacks such as compression, noise, sampling rate conversion etc.

[14]. An efficient audio watermarking algorithm in the frequency domain by embedding the inaudible audio water mark is presented here. It is verified that the DWT-SVD technique is robust for most of the attacks rather than the DCT-SVD. By means of combining the two transforms DWT-DCT along with SVD, inaudibility and different levels of robustness can also be achieved.

[15]. In this paper, an efficient audio watermarking technique for copyright protection has been presented. The watermarking algorithm is based on DWT and SVD techniques. The scheme was subjected to a series of imperceptibility (audio fidelity) and robustness tests. The obtained test result showed improved performances. In order to attain higher hidden data density in the watermarked signal, more advanced techniques must be used such as spread spectrum, phase encoding, or echo hiding.

IV. EXISTING WORKS

The proposed scheme has high degree of robustness which is validated by recovering the watermark against print and scan attack which is among the strongest attacks. Even though scheme is blind in nature it gives result better than non-blind ones. Many of the existing DWT and SVD based approaches do not handle the issue of authentication and security. The proposed method covers this flaw by incorporating signature-based authentication mechanism. Thus the resultant method is both robust and secure.

REFERENCES

[1]. Komal V. Goenka, Pallavi K. Patil,” Overview of Audio Watermarking Techniques” International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 2, February 2012

[2]. Ali Al-Haj,” An imperceptible and robust audio watermarking algorithm” EURASIP Journal on Audio, Speech, and Music Processing 2014.

[3]. Darabkh, K.,”Imperceptible and Robust DWT-SVD-Based Digital Audio Watermarking Algorithm”, Journal of Software Engineering and Applications, 2014.

[4]. Yekta Said Can, Fatih Alagoz, Melih Evren Burus,” A Novel Spread Spectrum Digital Audio Watermarking Technique” Journal of Advances in Computer Networks, Vol. 2, No. 1, March 2014

[5]. Hwai-Tsu Hu, Hsien-Hsin Chou, Chu Yu and Ling-Yuan Hsu," Incorporation of perceptually adaptive QIM with singular value decomposition for blind audio watermarking" EURASIP Journal on Advances in Signal Processing 2014

[6]. Prayoth Kumsawat," A Genetic Algorithm Optimization Technique for Multiwavelet-Based Digital Audio Watermarking" EURASIP Journal on Advances in Signal Processing Volume 2010

[7]. Mehdi Sadeghzadeh, and Mahsa Taherbaghal,"A New Method for Watermarking using Genetic Algorithms" International Conference on Machine Learning, Electrical and Mechanical Engineering (ICMLEME'2014) Jan. 8-9, 2014 Dubai (UAE).

[8]. Hong Peng, Zulin Zhang, Jun Wang And Peng Shi," Audio Watermarking Framework Using Multi-Objective Particle Swarm Optimization" International Journal Of Innovative Computing, Information And Control ICIC International Control Volume **9**, Number **7**, July **2013**

[9]. Hsiang-Cheh Huang, Feng-Cheng Chang," Survey of Bio-inspired Computing for Information Hiding" Journal of Information Hiding and Multimedia Signal Processing, Volume 6, Number 3, May 2015

[10]. Hongqin Shi," DWT and SVD based Watermarking Scheme with Circulation" JOURNAL OF SOFTWARE, VOL. 9, NO. 3, MARCH 2014

[11]. Huan Zhao1,Fei Wang1, Zuo Chen1, Jun Liu," A Robust AudioWatermarking Algorithm Based on SVD-DWT", ELEKTRONIKA IR ELEKTROTECHNIKA, ISSN 1392-1215, VOL. 20, NO. 1, 2014.

[12]. Sartid Vongpraphip and Mahasak Ketcham," An Intelligence Audio Watermarking Based on DWT-SVD Using ATS", IEEE 2009

[13]. Krishna Rao Kakkirala and Srinivasa Rao Chalamala," Digital Audio Watermarking Using DWT-SVD and Secret Sharing", International Journal of Signal Processing Systems Vol. 1, No. 1 June 2013

[14]. N.V.Lalitha, G.Suresh, Dr.V.Sailaja," Improved Audio Watermarking Using DWT-SVD", International Journal of Scientific & Engineering Research Volume 2, Issue 6, June-2011

[15]. Jyotirmayee Mishra, M.V.Patil," An Effective Audio Watermarking using DWT-SVD", International Journal of Computer Applications (0975 – 8887) Volume 70– No.8, May 2013

[16]. AKSHYA KUMAR GUPTA, MEHUL S RAVAL," A robust and secure watermarking scheme based on singular values replacement", *Sa¯dhana¯* Vol. 37, Part 4, August 2012