

**Bachelor of Science in Computer Science and Engineering**

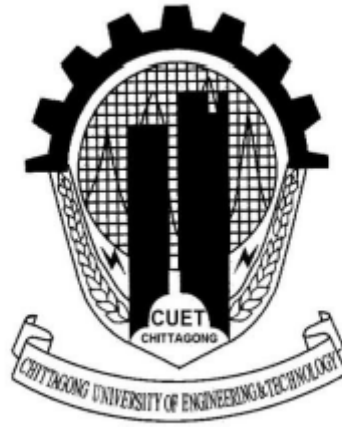
**A Zero-Watermarking Scheme Based on Discrete Hartley  
Transform for Audio Signal**

**Emtiaj Hasan  
ID: 1004050**

**March, 2016**

**Department of Computer Science & Engineering  
Chittagong University of Engineering & Technology  
Chittagong-4349, Bangladesh**

# **A Zero-Watermarking Scheme Based on Discrete Hartley Transform for Audio Signal**



This thesis is submitted in partial fulfillment of the requirement for the degree of Bachelor of Science in Computer Science & Engineering.

Emtiaj Hasan

ID: 1004050

Supervised by

Dr. Pranab Kumar Dhar

Assistant Professor

Department of Computer Science & Engineering (CSE)

Chittagong University of Engineering & Technology (CUET)

**Department of Computer Science & Engineering**

**Chittagong University of Engineering & Technology**

**Chittagong-4349, Bangladesh**

The thesis titled “**A Zero-Watermarking Scheme Based on Discrete Hartley Transform for Audio Signal**” submitted by Roll No. 1004050, Session 2013-2014 has been accepted as satisfactory in fulfillment of the requirement for the degree of Bachelor of Science in Computer Science & Engineering (CSE) as B.Sc. Engineering to be awarded by the Chittagong University of Engineering & Technology (CUET).

## Board of Examiners

1. \_\_\_\_\_

Chairman

Dr. Pranab Kumar Dhar

Assistant Professor

Department of Computer Science & Engineering (CSE)

Chittagong University of Engineering & Technology (CUET)

2. \_\_\_\_\_

Member

Professor Dr. Mohammed Moshiul Hoque

(Ex-officio)

Head

Department of Computer Science & Engineering (CSE)

Chittagong University of Engineering & Technology (CUET)

3. \_\_\_\_\_

Member

Md. Monjur-Ul-Hasan

(External)

Assistant Professor

Department of Computer Science & Engineering (CSE)

Chittagong University of Engineering & Technology (CUET)

# Statement of Originality

It is hereby declared that the contents of this thesis is original and any part of it has not been submitted elsewhere for the award of any degree or diploma.

---

**Signature of the Candidate**

**Date:**

## Acknowledgment

This thesis gives me an opportunity to thank all of the people who have helped me throughout my graduation life. First of all, I am grateful to my honorable project Supervisor Dr. Pranab Kumar Dhar, Assistant Professor, Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, for the guidance, inspiration and constructive suggestions which were helpful in the preparation of this project. I also convey special thanks and gratitude to Professor Dr. Mohammed Moshiul Hoque, honorable head of the Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, for his kind advice. I would also like to extend my gratitude to all of my teachers for their valuable guidance in every step of my learning stage. I would like to thank my friends for their cooperation that has helped in the successful completion of the project. Special thanks to the staffs of the department for their assistance. Last but not the least, I would like to thank my parents for supporting me throughout my entire life. Without their encouragement, it would not be possible to make this achievement.

# Abstract

Internet is the fastest medium of transferring data to any place in a world and a popular digital media is audio. Various cloud-based storage contains a huge database of digital audio. Moreover, for the cheaper price of different storage device e.g., flash drive, make it easier for people to share, distribution of audio files easily and sometimes illegally. For these reasons, the chances of copyright infringement are higher than ever and measures against piracy were never so demanded. In this view, an audio watermarking field is very important. Considering the growing demand for this field, this thesis proposes a new zero-watermarking scheme based on Discrete Hartley Transform (DHT) for audio signal. In this scheme, DHT is performed on audio and a binary pattern is generated so that it can be used for extraction of the watermark in later. The experimental results show that this algorithm can resist various attacks. In most of the cases, the correlation between the original watermark and the extracted watermark is more than 0.9 and also bit error rate is less than 12% which demonstrates that the proposed method is a suitable candidate for copyright protection. Furthermore, comparing with other existing schemes, it shows much better robustness against several attacks.

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Digital Watermarking . . . . .	1
1.1.1	General Concept of Watermarking . . . . .	2
1.1.2	Classification of Watermarking . . . . .	3
1.1.3	Properties of Watermark . . . . .	4
1.1.4	Application of Watermarking . . . . .	4
1.2	Motivation . . . . .	5
1.3	Prospect of the Proposed Watermarking Scheme . . . . .	6
1.4	Organization of the Thesis . . . . .	6
<b>2</b>	<b>Literature Review</b>	<b>7</b>
2.1	Audio Watermarking . . . . .	7
2.2	Audio Watermarking Techniques . . . . .	7
2.2.1	Time Domain Method . . . . .	7
2.2.2	Transform Domain Method . . . . .	8
2.2.3	Zero Watermarking Method . . . . .	9
<b>3</b>	<b>Proposed Audio Watermarking Scheme</b>	<b>11</b>
3.1	Background Information . . . . .	11
3.2	Proposed Method Based on Discrete Hartley Transform . . . . .	12
3.2.1	Watermark Embedding Process . . . . .	12
3.2.2	Attacks on the Host Audio . . . . .	14
3.2.3	Watermark Extraction Process . . . . .	15
<b>4</b>	<b>Implementation of the Project Work</b>	<b>17</b>
4.1	Audio Files Used for Simulation . . . . .	17
4.2	Image Used for Simulation . . . . .	17
4.3	Attacks Applied in Simulation . . . . .	17
4.4	Experimental Environment . . . . .	22
4.5	Normalized Coefficient . . . . .	22
4.6	Bit Error Rate . . . . .	23

4.7	False Positive Error . . . . .	23
4.8	False Negative Error . . . . .	23
<b>5</b>	<b>Simulation Result</b>	<b>25</b>
5.1	Imperceptibility Analysis . . . . .	25
5.2	Measuring the Robustness . . . . .	26
5.3	False Positive Error . . . . .	31
5.4	False Negative Error . . . . .	31
<b>6</b>	<b>Conclusion</b>	<b>33</b>
6.1	Summary . . . . .	33
6.2	Future Recommendation . . . . .	33
	<b>Bibliography</b>	<b>34</b>



# List of Figures

1.1	Basic structure of watermarking process . . . . .	2
3.1	Watermark embedding process of the proposed scheme . . . . .	13
3.2	Watermark extraction process of the proposed scheme . . . . .	16
4.1	The signal of original audio . . . . .	18
4.2	Watermark image with size 32X32 . . . . .	18
4.3	Original audio signal . . . . .	19
4.4	Audio signal after Gaussian noise adding . . . . .	19
4.5	Audio signal after re-sampling . . . . .	20
4.6	Audio signal after low-pass filtering . . . . .	20
4.7	Audio signal after re-quantization . . . . .	20
4.8	Audio signal after adding echo . . . . .	21
4.9	Audio signal after doing reverse . . . . .	21
4.10	Audio signal after compressed to mp3/32kbps format . . . . .	21
4.11	Audio signal after compressed to mp3/64kbps format . . . . .	22
4.12	Audio signal after compressed to mp3/128kbps format . . . . .	22
5.1	Imperceptibility of proposed watermarking scheme . . . . .	25
5.2	Graphical representation of NC comparison . . . . .	30
5.3	Graphical representation of BER comparison . . . . .	30
5.4	False positive probabilities under various watermarking bit . . . . .	31
5.5	False negative probabilities under various watermarking bit . . . . .	32

# List of Tables

3.1	Comparison of DFT and DHT . . . . .	12
5.1	The result of attacks for audio signal (a) . . . . .	27
5.2	The result of attacks for audio signal (b), (c), and (d) . . . . .	28
5.3	Comparison of NC among proposed and other algorithm . . . . .	29
5.4	Comparison of BER among proposed and other algorithm . . . . .	29

# Chapter 1

## Introduction

### 1.1 Digital Watermarking

This is the era of internet and people from every corner of the world are connected via this. The proliferation of internet gives the opportunities of easy access, sharing, distribution, storage of digital content such as images, video, audio, text. Since data exposed on the Internet is easily accessible to anyone, such media contents are facing serious challenges like piracy, illegal redistribution, forgery, etc. Digital watermarking technology is an effective solution to meet such challenges.

Embedding some kind of information into data for tamper detection, authentication, traitor tracing, etc is known as watermarking. The embedded data is called watermark. In visible digital watermarking, the information is visible in the picture, text or video. In invisible digital watermarking, information is added as digital data to audio, text, picture or video.

Digital watermarking is a procedure of hiding some information into digital multimedia content, possibly in an imperceptible way without degrading the quality of the content. Furthermore, the watermark must be either robust or fragile, depending on the application. A watermark is called fragile if detection fails with even minor modification. It is useful in tempering detection. A watermark is called robust if detection is accurate under any modification. It is used in copyright control application.

Recently, many efforts have been devoted to the problem of copyright protection by plenty of research communities. This is because that multimedia data has become a widely used carrier of information and the rapid growth of internet has made the copyright and integrity of digital media information more and more

crucial issues. To protect digital data against illegal use and tampering, digital watermarking has been proposed to accomplish copyright protection or content integrity authentication.

### 1.1.1 General Concept of Watermarking

The information to be embedded in a signal is called digital watermark, and 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 extraction.

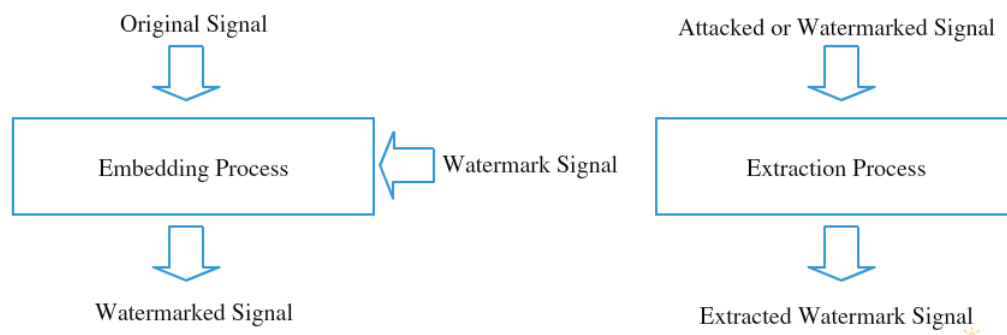


Figure 1.1: Basic structure of watermarking process

In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal.

Then the watermarked signal is transmitted or stored, usually transmitted to another person. If this person or the medium through which it is transmitted, makes a modification then this is called attack. Some attack may perform on host signal for practical reason, e.g., to consume storage, image or audio or video may be compressed. But the term “attack” may arise in perspective of sharing data, where man in the middle attempt to remove the digital watermark through modification.

Extraction (also called detection) is an algorithm which is applied to the attacked or watermarked signal to attempt to extract to 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, 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.

### 1.1.2 Classification of Watermarking

There are many watermarking techniques in terms of their application areas and purposes. And they have different insertion and extraction techniques.

Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows:

- Text Watermarking
- Image Watermarking
- Audio Watermarking
- Video Watermarking

According to human perception watermarking can be categorized as follows:

- Visible Watermarking, where watermark can be sensed by the human without extraction. For example, logos that are used in papers and videos.
- Invisible Watermarking, where watermark can be detected by only applying proper extraction algorithm.

Watermarking can also be divided into two categories according to the watermark extraction procedures requirement:

- Blind Watermarking, which do not require host signal to extract the watermark.
- Non-blind Watermarking, it needs the original signal to extract the watermark.

All watermarking techniques are not equally robust against attacks or manipulations. Based on the level of robustness, watermarks are classified into three categories:

- Robust Watermarking, it can recover watermark after applying severe attacks.
- Fragile Watermarking, it fails even on light attacks.
- Semi-fragile Watermarking, it is better than fragile but not than robust.

Based on the key used in embedding and extraction, watermarking techniques can be categorized into two classes:

- **Symmetric Watermarking**, here the embedding key and the detection key are same.
- **Asymmetric Watermarking**, this technique uses different embedding and detection key. This type of work is clearly more secured than the symmetric type but it also implies higher complexity.

### 1.1.3 Properties of Watermark

For a digital watermark to be effective and practical, it should exhibit the following properties:

- **Imperceptibility**: A digital watermark is called imperceptible if the original signal and the marked signal are perceptually indistinguishable. It is inaudible to human auditory system. It remains hidden in content and can be detected only by authorized agencies. And a digital watermark is called perceptible if its presence in the marked signal is noticeable.
- **Security**: The watermarking procedure should rely on secret keys, not the algorithm's secrecy, to ensure security, so that pirates cannot detect or remove watermark. If the key that is used during watermarking is lost or the key is public, the watermark can be read and also be removed.
- **Robustness**: It is not possible for a watermarking scheme to be robust against all possible signal processing operations. Practically no perfect method is proposed so far that can withstand against all kinds of attacks. But a robust watermark should be able to withstand the basic operation.

### 1.1.4 Application of Watermarking

- **Copyright Protection**: A person should embed watermark into host signal to protect against illegal distribution. Suppose, person A creates an image and embeds watermark into it. He sends it to person B for some reason. If person B tries to sell it to others without the permission of person A, then person A can extract his watermark and prove his ownership.
- **Source Tracking**: Different recipients get differently watermarked content so that no one can distribute to other. For example, watermark is embedded into each movie's DVD. If the movie is then leaked to the internet, the movie

producers could identify which recipient of the movie was the source of the leak.

- **Broadcast Monitoring:** Advertising agencies want to ensure their commercials are properly aired, as they want this commercial to be displayed at the exact time they wanted to. In this thing, watermark is applied. Information that can identify the individual video, embedded to video using watermarking, making broadcasting easier.
- **Fingerprinting:** The main purpose of fingerprinting is to protect customers. If someone got a legal copy of a product but redistributed illegally, fingerprinting can prevent this. This can be achieved by tracing the whole transaction by embedding unique robust watermark for each recipient. Thus, the owner can identify who redistributed this product by extracting the watermark from the illegal copy.
- **Indexing:** Comments and markers or key information related to the data are inserted as watermark. This watermark information is used by a search engine for retrieving the required data quickly and without any ambiguity.
- **Meta-data Tagging:** Watermarks convey object specific information to user of the object. For example, it is used to attach patient identification data to medical images.

## 1.2 Motivation

In recent years, the increasing amount of applications using digital multimedia technologies has emphasized the need to protect digital multimedia data from piracy. Authentication and information hiding, copyright protection, content identification, proof of ownership has also become important issue. Hence watermarking is becoming more and more important. Therefore, digital watermarking technique has received a great deal of attention recently in the literature and among the research community, but currently, most of the digital watermarking schemes mainly focus on image and video copyright protection. Digital audio watermarking technology provides a special challenge because the human auditory system is extremely more sensitive than the human visual system. Furthermore, audio signal contains one-dimensional data, thus it is difficult to hide additional information without compromising the quality of the audio signal. That is why audio watermarking is chosen for thesis work. To propose a watermarking method

that will be robust and imperceptible to be a strong contestant of currently available audio watermarking methods for copyright protection of audio content is the motivation.

### **1.3 Prospect of the Proposed Watermarking Scheme**

- To develop a watermarking scheme based on Discrete Hartley Transform.
- To develop a blind audio watermarking algorithm.
- To develop an imperceptible and robust audio watermarking algorithm.

### **1.4 Organization of the Thesis**

This thesis is divided into six chapters. This chapter briefly discussed a general watermarking scheme and its properties and application areas. In addition, the motivation and objectives of this thesis are presented. The remaining of this thesis is organized as follows:

In chapter 2, description about the previous research that have been done on audio watermarking is included. Chapter 3 presents the methodology of the proposed watermarking scheme, including watermarking embedding process and watermarking extraction process. Chapter 4 contains the detail description of the implementation procedures of the proposed watermarking scheme. Chapter 5 includes the simulation results and the performance evaluation of the proposed system in terms of robustness, imperceptibility and other properties. Chapter 6 concludes the thesis with mentioning the goal achieved by this research work.



# Chapter 2

## Literature Review

### 2.1 Audio Watermarking

Since the internet rapidly grows, networks carry large amounts of multimedia data. But the blessings of internet help unethical or bad people to reproduce unauthorized copies and illegally distribute these copies without the consent of the owner. To prevent this, the audio watermarking field is very important. By definition, audio watermarking is the technique of embedding of owner copyright identification into the host audio.

### 2.2 Audio Watermarking Techniques

A significant number of audio watermarking techniques have been reported in recent years in order to create robust and imperceptible audio watermarks. Audio watermarking techniques that proposed so far can be divided into various groups, such as, time domain, transform domain, zero-watermarking technique.

#### 2.2.1 Time Domain Method

Time domain based methods embed watermark information into the time domain. These methods are simple and easy to implement and most of them can retrieve watermark without referencing the original audio. The main disadvantage of time domain based schemes is its immunity to manipulations. Two main methods belonging to this category are least significant bit (LSB) based method and echo hiding based method.

The simplest time domain based watermarking is least significant bit [1] method which simply uses the least significant bits of the host audio signal to embed watermark data. A moderately robust time domain based spread spectrum

technique was proposed by Bassia [2]. Foote [3] proposed a non-blind watermarking scheme using time based modulation. Lie [4] proposed another time domain based watermarking scheme where they used differential average of absolute amplitude relations within each group of samples to represent one bit information. To preserve the time domain waveform envelope they employed low frequency amplitude modification to scale amplitudes in a group manner in selected sections of samples. Lemma [5] proposed modified audio signal keying (MASK) to modify the short time envelope of the audio signal in an imperceptible approach.

Echo hiding based watermarking techniques embed the watermark by introducing an echo. However, echo hiding can effectively embed watermarks in imperceptible way [6], [7] but in such schemes watermark can be easily detected by anyone.

### 2.2.2 Transform Domain Method

In transform domain watermarking techniques, an audio is processed by means of a specific transform. Transform domain based watermarking techniques have been proven to be much more effective with regard to accomplishing the imperceptibility and robustness requirements of digital watermarking algorithms. The frequency domains such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT) are more specifically to be dealing with audio watermarking system.

The DFT is a well known and powerful computational tool for performing frequency analysis of discrete time signals. Fast Fourier Transform (FFT) is an efficient algorithm for calculating DFT. It takes a discrete signal in the time domain and transforms the signal into the discrete frequency domain.

A novel time domain synchronization technique [8] was proposed together with a new blind watermarking scheme which works in the DFT domain. Fallahpour [9] proposed a novel high-capacity audio watermarking system to embed data and extract them in a bit-exact manner by changing some of the magnitudes of the DFT spectrum. Another computationally less complex DFT domain based audio watermarking scheme using quantization was proposed [10]. In addition those, various number of audio watermarking methods utilizing DFT have been proposed. Most methods embed watermark information into the magnitude of the DFT components.

The main idea behind the watermarking methods based on DWT is to segment the original audio signal into many frames first and then embed watermark bits

into the low or high frequency DWT coefficients.

A blind audio watermarking in DWT domain was proposed by Meng [11]. To enhance the robustness Chen[12] embedded the watermark in the lowest frequency coefficients in DWT domain. Another method was also proposed by same author [13]. Pooyan [14] introduced an audio watermarking system which embeds watermarks in wavelet domain. The watermarks are embedded into the low frequency coefficients in discrete multiwavelet transform domain by Kumsawat [15] to achieve robust performance against common signal processing procedures and noise corruptions.

Zeng [16] described a blind watermarking system which embeds watermarks into DCT coefficients by utilizing quantization index modulation technique. In [17], authors proposed a method based on DCT for copyright protection. Guo [18] proposed DCT domain based audio signal watermarking. A watermark algorithm based on DCT and audio feature quantization was also proposed [19].

Yong [20] proposed an audio watermarking scheme based on the dyadic wavelet transform. The combination of various transformations are also used in audio watermarking, e.g., combination of DWT and DCT [21], combination of DWT and DCT with Singular Value Composition (SVD) [22], combination of Lifting Wavelet Transform and Singular Value Decomposition [23], have been proposed.

### **2.2.3 Zero Watermarking Method**

In the watermarking schemes previously mentioned, the insertion of watermark into the original signal inevitably introduces some perceptible quality degradation. Another problem is the inherent conflict between imperceptibility and robustness. Zero watermarking technique can solve these problems successfully.

Zero-watermarking does not modify the original signal but constructs zero watermarks from it. Instead of embedding watermark into the host signal, the zero-watermarking approach just constructs a pattern based on the essential characteristics of the host signal and uses them for watermark recovery.

A zero-watermark algorithm was applied by Wen Quan [24], [25] for the first time for image authentication. In recent, the audio zero-watermarking scheme has acquired the considerable progress. A zero-watermarking scheme has been proposed to analyze the security of audio signals [26] presented a method for mapping the approximate coefficients of the wavelet transform of an audio segment into a binary matrix. A zero-watermarking algorithm, based on the Discrete Wavelet

Transform (DWT), has been used to construct secret keys [27], [28]. By using the audio's statistical character, [27] consults the mean of the approximation coefficients of a one dimensional signal and constructs the watermark sequence with the zero-watermark scheme. Since most of the audio's energy is concentrated at the lower frequency coefficient sets and therefore embedding watermarks in these coefficient sets may degrade the audio significantly, therefore, in [28], to increase robustness, watermark is embedded in the low frequency coefficient sets. Xueying [29] proposed a robust audio zero-watermarking algorithm which extracts the low frequency components of original audio to construct zero-watermarking by using the wavelet packet analysis method. Discrete Wavelet Transform (DWT) and Discrete Cosine Transformation (DCT) have been combined to generate the watermarking sequences [30], [31]. The multiresolution characteristic of discrete wavelet transform (DWT), the energy compression characteristic of discrete cosine transform (DCT) and the steady sign of certain DWT-DCT coefficients are combined in these two schemes. However, the Gaussian noise suppression property of higher order cumulant are also combined with DWT-DCT in [31]. Cip-tasari [32] proposed a modified version of [31] by producing a secret key rather than three secret keys. An audio zero-watermarking algorithm [33] has been proposed which combined DCT with zernike moments. The reason of using zernike moment is the characteristic of non sensitivity to noise of zernike moment. Based on the correlation of Linear Prediction Cepstrum Coefficients (LPCC) with adaptive factors, a zero-watermarking audio scheme has been proposed [34]. By calculating the bi-level characteristic sequence of audio signal through the Modified Discrete Cosine Transform (MDCT), a zero-watermark of audio is proposed by [35]. Coupled with bi-level watermark image and the secret key this scheme shows robustness against various attacks. The concept of the zero-watermark based on LPCC with a weighting function was proposed to protect audio signals [36], [37]. Using the correlation of LPCC with weighted factor, those can retrieve the available embedded watermark back after various attacks. Zero-watermark based on energy was also proposed to protect audio signals [38]. This scheme calculates the energy of each frame after segmenting the audio. The characteristic of energy is utilized to retrieve the watermark after various attacks.

## Chapter 3

# Proposed Audio Watermarking Scheme

From the previous chapter, it can be seen that several audio watermarking schemes have been proposed. As there is no need to embed the watermark in the zero-watermarking method, it can remove the contradiction between robustness and imperceptibility. Though various zero-watermarking schemes exist for the audio signal, still there is a need to work on this method. The main problem is, for some signal processing manipulation i.e., compression, adding echo, re-sampling, etc, existing schemes do not perform satisfactory result. To overcome the limitation, here, this thesis proposes a new zero-watermarking scheme based on discrete Hartley transform.

### 3.1 Background Information

Discrete Fourier transform (DFT) plays a vital role in signal processing. Despite its tremendous application, the DFT has an unattractive feature, that, it transforms a real-valued sequence also into a complex-valued sequence. R. N. Bracewell [39] proposed an inherently real-valued transform called the Discrete Hartley transform (DHT). The new transform has the advantage that a real-valued signal always generates a real-valued transform signal. Also, unlike the DFT, the DHT is symmetric i.e., both the forward and inverse transforms are identical. Moreover, for computing real sequence, Fast Hartley Transform (FHT) is faster than Fast Fourier Transform (FFT) [40]. Table 3.1 gives the comparative analysis between DFT and DHT.

<b>DFT</b>	<b>DHT</b>
It has complex values in the transform equation.	It has only real values in the transform equation.
The forward and inverse transforms are non-identical.	The forward and inverse transforms are identical.
It needs to keep track of +i and -i terms.	No such requirement.
Computational complexity is higher due to imaginary terms.	Computational complexity is lower as compared to its counterpart.

Table 3.1: Comparison of DFT and DHT

Considering a sequence of  $N$  real numbers  $x_n$  for  $n = 0, 1, \dots, N - 1$ , the DHT of this sequence is defined by equation 3.1.

$$H_k = \sum_{n=0}^{N-1} x_n \left[ \cos\left(\frac{2\pi nk}{N}\right) + \sin\left(\frac{2\pi nk}{N}\right) \right] \quad (3.1)$$

$$k = 0, 1, \dots, N - 1$$

## 3.2 Proposed Method Based on Discrete Hartley Transform

The proposed scheme is divided into three parts. These are watermark embedding process, applying attack and watermark extraction process. Firstly, in embedding process, a key to extract watermark is generated by using the properties of audio. After that, different types of attacks are applied to the audio and then, watermark is extracted from the attacked audio.

Let  $A = \{a(i); i = 1, 2, \dots, L\}$  be the host audio signal and  $W = \{w(i, j); i = 1, 2, \dots, M_1, j = 1, 2, \dots, M_2\}$  be the binary-valued image watermark to be embedded.

### 3.2.1 Watermark Embedding Process

The watermark embedding procedure shown in Fig. 3.1 at page 13 can be described as follows:

Step 1: The discrete Hartley transform is applied to the audio  $A$ , and can get the coefficient  $C = \{c(i); i = 1, 2, \dots, C_A\}$ , which has  $C_A$  samples.

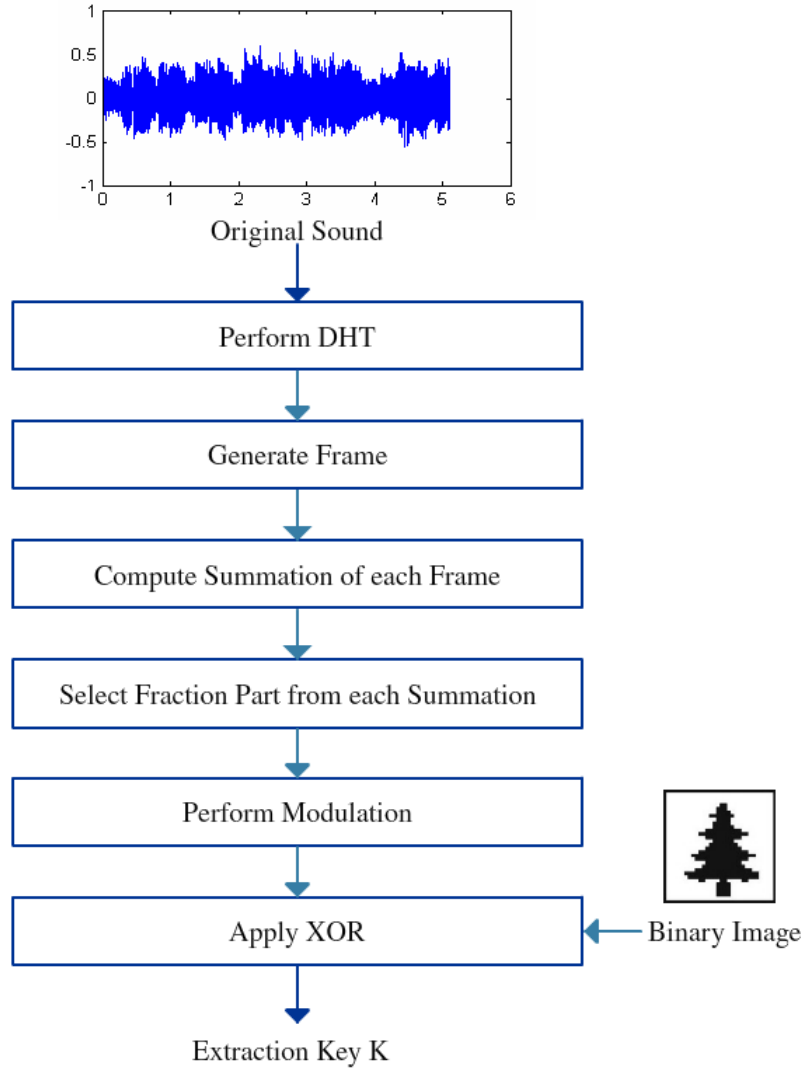


Figure 3.1: Watermark embedding process of the proposed scheme

Step 2:  $C$  is segmented into  $M$  frames, each frame includes  $Q$  samples.

Step 3: for  $i = 1 : M$

3.1) Compute  $s_i = \sum_{n=1}^Q |C_n|$ ; where  $|C_n|$  means absolute value of  $C_n$ .

3.2) Compute  $t_i = \text{convert}(s_i - \text{floor}(s_i))$ ; where  $\text{floor}(s_i)$ ; is a function which gives the largest integer less than or equal to  $s_i$ , in a word, a function which extract integer part from a real value, and  $\text{convert}()$ ; is a function which converts a fractional value into an integer value.

3.3) Compute  $x_i = \text{mod}(t_i^p, 2)$ ; where  $p$  is the  $t_i$  th prime.

Step 4: Convert  $x$  into  $M_1 X M_2$  matrix.

Step 5: Compute the watermarking extraction secret key  $k(i, j)$  by doing the exclusive or operation between  $w(i, j)$  and  $x(i, j)$ . Therefore,  $k(i, j) = w(i, j) \oplus x(i, j)$ .

Here, in step 3.2, the output value is the fractional part of the value found from previous step i.e., 3.1. Suppose after calculation of step 3.1, the summation value is 13.24. In that case, the output of step 3.2 is 24. And about step 3.3, here, considering previous example, as 24th prime is 89, the two parameter of modulus operation are  $24^{89}$  and 2 respectively.

### 3.2.2 Attacks on the Host Audio

In watermarking terminology, an “attack” is any process that may impair detection of the watermark or the information conveyed by the watermark. It can be classified as:

- Intentional attack, which is an attempt to weaken, remove or alter the watermark or original sound.
- Non-intentional attack, which can occur during audio processing and are not aimed at tempering. For example, lossy compression of audio such as, mp3 audio compression.

Different types of attack are described below:

1. **Additive Noise:** In audio, noise is generally any unpleasant sound and more technically, any unwanted sound that is unintentionally added to a sound. In digital recording sound, noise is often present. When doing digital recording, the conversion of a sound file from 16 bit to 8 bit adds a layer of noise. Noise may originate from Digital to Analog (DAC) and Analog to Digital (ADC) conversion or as a consequence of transmission error.
2. **Re-sampling:** Re-sampling or sample rate conversion is the process of changing the sampling rate of a discrete signal to obtain a new discrete representation of the underlying signal. Compact Disc Digital Audio and Digital Audio Tape systems use different sampling rates, 44.1 kHz and 48 kHz respectively. Sample rate conversion prevents changes in speed and pitch that would otherwise occur when transferring recorded material between such systems.
3. **Filtering:** A digital filter is a filter that operates on digital signals, such as sound. It is a computation which takes one sequence of numbers and



produces a new sequence of numbers. Being a frequency dependent amplifier, in its most basic form, an audio filter is designed to amplify, pass or attenuate (negative amplification) some frequency ranges. Common types include low-pass filters, which pass through frequencies below their cut-off frequencies, and progressively attenuates frequencies above the cut-off frequency.

4. **Quantization:** Quantization is the process of converting a continuous analog audio signal to a digital signal with discrete numerical values. In a compact disc, an analog recording is converted to a digital signal quantized with 16 bits of data per sample. During this process of conversion, quantization also achieves a tremendous deal of compression, because an analog sample is considered as having infinite resolution, thus requiring an infinite number of bits to represent, while a digital sample is of limited resolution and is represent using a limited number of bits.
5. **Echo:** In audio signal processing, an echo is a reflection of sound, arriving at the listener some time after the direct sound. Typical examples are the echo produced by the bottom of a well, by a building, or by the walls of an enclosed room and an empty room. To simulate the effect of echo, one or several delayed signals are added to the original signal. To be perceived as echo, the delay has to be of order 35 milliseconds or above.
6. **Compression:** Compression is an attack which reduces the size of the original audio for the purpose of reducing the storage. MPEG-1 or MPEG-2 audio layer III, more commonly referred to as mp3, is an audio coding format for digital audio which uses a form of lossy data compression.

### 3.2.3 Watermark Extraction Process

The watermark recovery procedure shown in Fig. 3.2 at page 16 can be carried out as follows:

Step 1: The discrete Hartley transformation is applied to the watermarked audio  $A^*$ , and can get the coefficient  $C^* = \{c^*(i); i = 1, 2, \dots, C_A^*\}$ , which has  $C_A^*$  samples.

Step 2:  $C^*$  is segmented into  $M$  frames, each frame includes  $Q$  samples.

Step 3: for  $i = 1 : M$

$$3.1) \text{ Compute } s_i^* = \sum_{n=1}^Q |C_n^*|$$

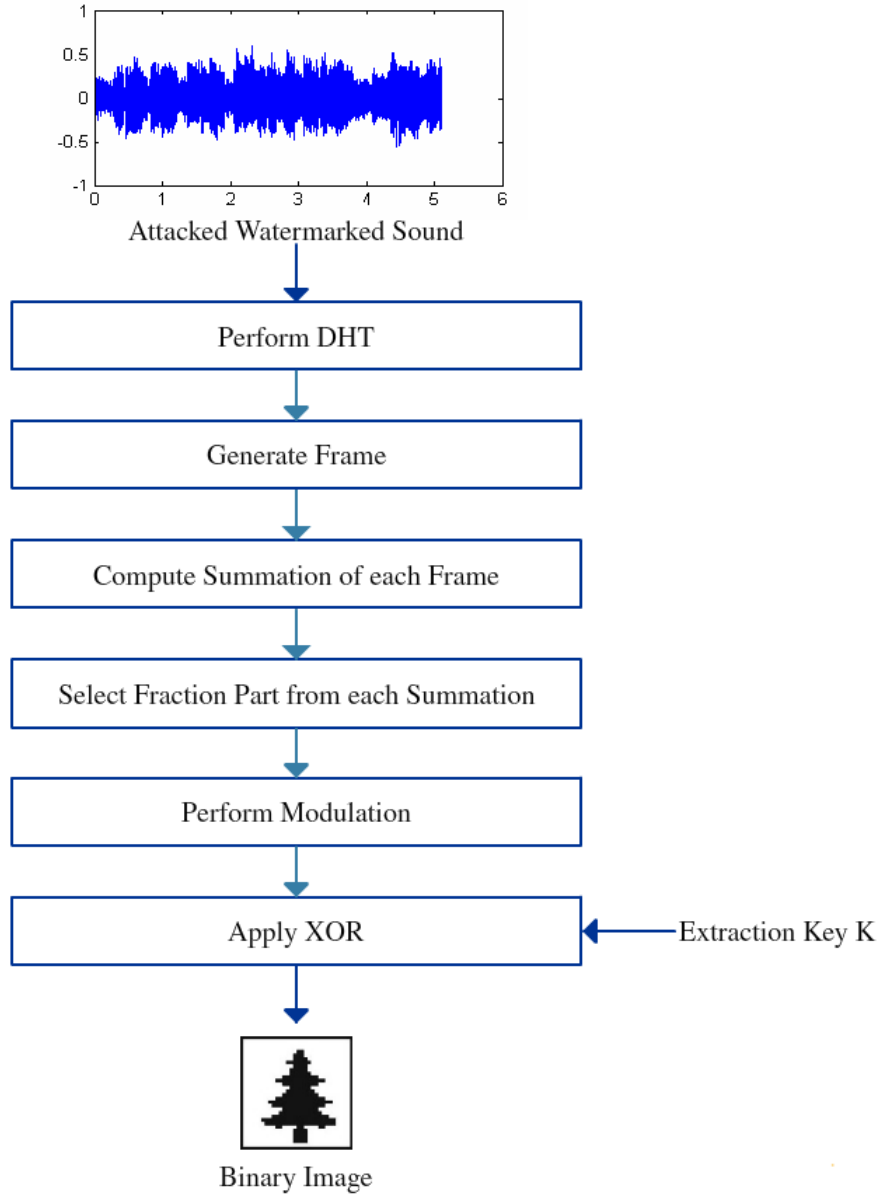


Figure 3.2: Watermark extraction process of the proposed scheme

3.2) Compute  $t_i^* = \text{convert}(s_i^* - \text{floor}(s_i^*));$

3.3) Compute  $x_i^* = \text{mod}(t_i^{*p}, 2);$  where  $p$  is the  $t_i^*$  th prime.

Step 4: Convert  $x^*$  into  $M_1 \times M_2$  size matrix.

Step 5: Compute the watermarking information  $W^*(i, j)$  by doing the exclusive or operation between  $k(i, j)$  and  $x^*(i, j)$ . Therefore,  $W^*(i, j) = k(i, j) \oplus x^*(i, j)$ .

# Chapter 4

## Implementation of the Project Work

### 4.1 Audio Files Used for Simulation

For evaluation the performance of the proposed watermarking method different types audio signals are used. The sound files are: (a) Citizen, Go Back to Sleep, (b) Beginning of the End, (c) Breathing on Another Planet, and (d) Thousand Yard Stare, included in the album *Rust* [41]. All audio files are 95 seconds long, sampled at 44.1 kHz with 16 bits per sample as shown in Fig. 4.1 at page 18 . Each audio file contains 4194304 samples. The frame length was fixed at 4096 samples.

### 4.2 Image Used for Simulation

In this experiment, a binary image with size 32X32 is used as the watermark shown in Fig. 4.2 at page 18. Image has taken from [42].

### 4.3 Attacks Applied in Simulation

In order to test the robustness of the proposed method, nine different types of attacks are as following:

1. Noise addition: 20 dB additive white Gaussian noise (AWGN) is added to the audio signal.
2. Re-sampling: The audio signal originally sampled at 44.1 kHz, is re-sampled at 22.050 kHz, and then restored by sampling again at 44.1 kHz.

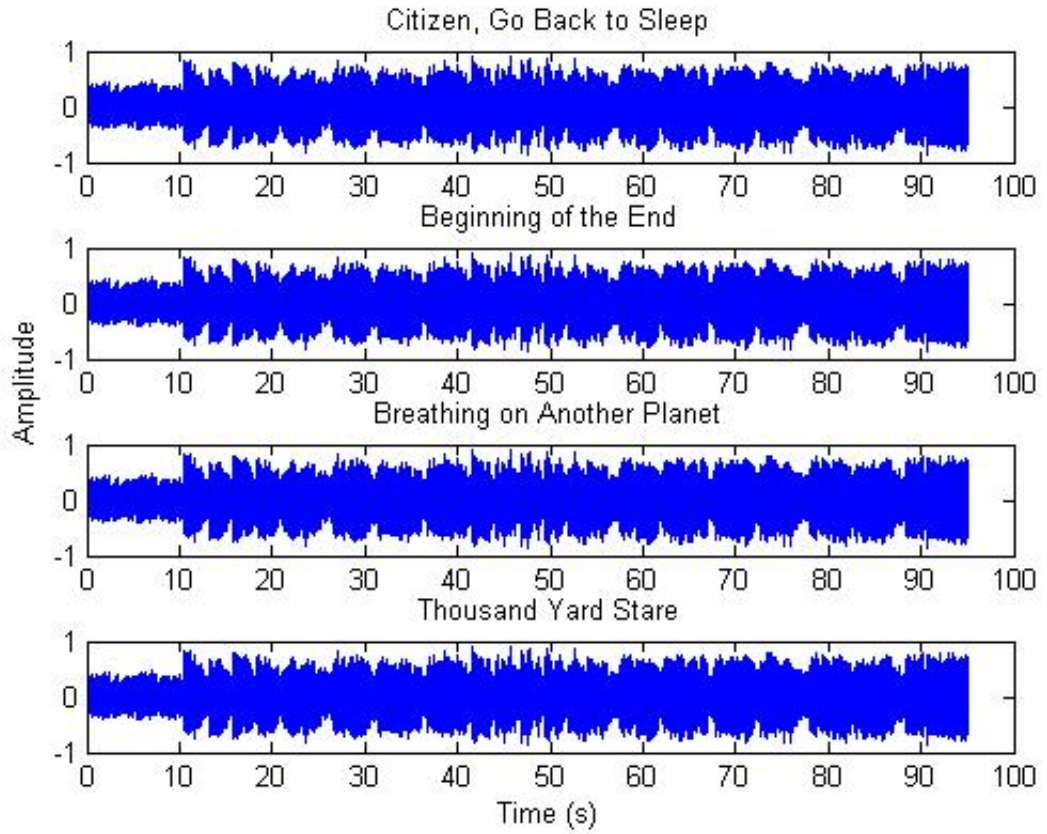


Figure 4.1: The signal of original audio

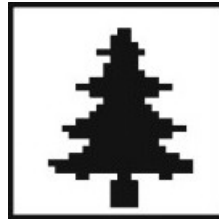


Figure 4.2: Watermark image with size 32X32

3. Low-pass filtering: Adopt a six order Butterworth filter with cut-off frequencies 11.025 kHz.
4. Re-quantization: The 16 bit audio signal is quantized down to 8 bits per sample and again re-quantized back to 16 bits per sample.
5. Echo: An echo signal with a delay of 0.5s is added to the audio signal.
6. Reverse: The audio is reversed to its original.
7. MP3 compression: MPEG-1 layer 3 compression is applied. The audio

signal is compressed at a bit rate of 32 kbps.

8. MP3 compression: MPEG-1 layer 3 compression is applied. The audio signal is compressed at a bit rate of 64 kbps.
9. MP3 compression: MPEG-1 layer 3 compression is applied. The audio signal is compressed at a bit rate of 128 kbps.

GoldWave [43] was used in this experiment for above mentioned attacks except the AWGN and the re-quantization. Those were implemented using MATLAB [44].

The original sound and attacked sound for sound file *Beginning of the End* are plotted in Fig. 4.3, Fig. 4.4, Fig. 4.5, Fig. 4.6, Fig. 4.7, Fig. 4.8, Fig. 4.9, Fig. 4.10, Fig. 4.11, Fig. 4.12 respectively.

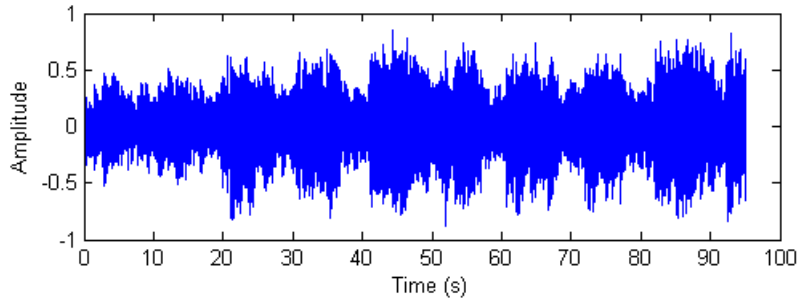


Figure 4.3: Original audio signal

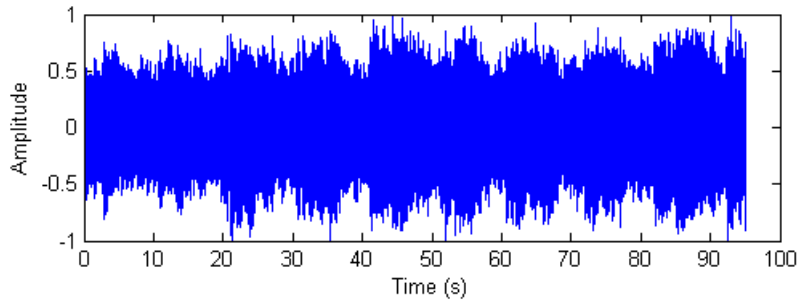


Figure 4.4: Audio signal after Gaussian noise adding

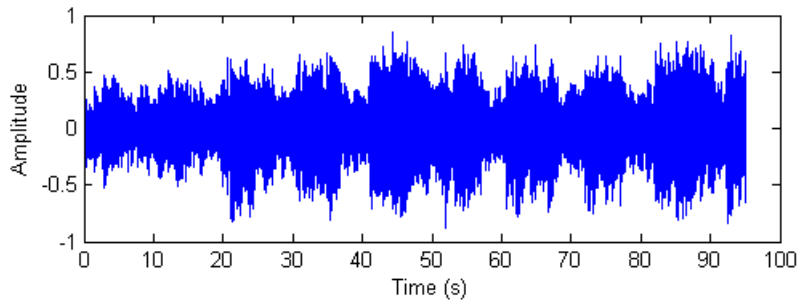


Figure 4.5: Audio signal after re-sampling

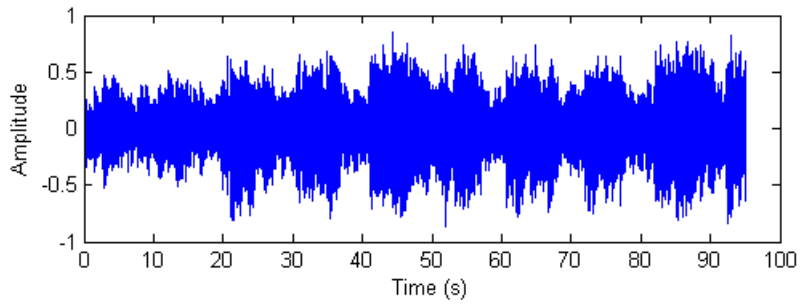


Figure 4.6: Audio signal after low-pass filtering

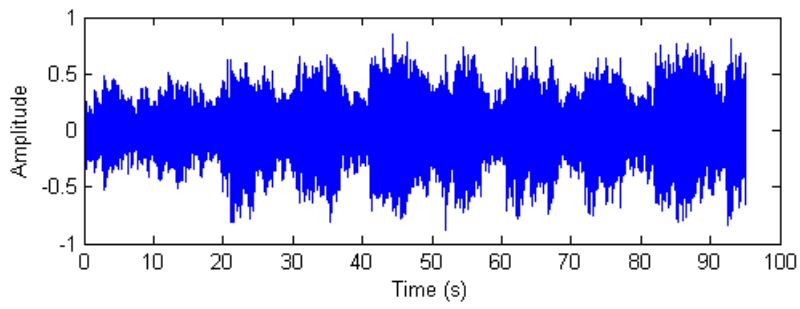


Figure 4.7: Audio signal after re-quantization

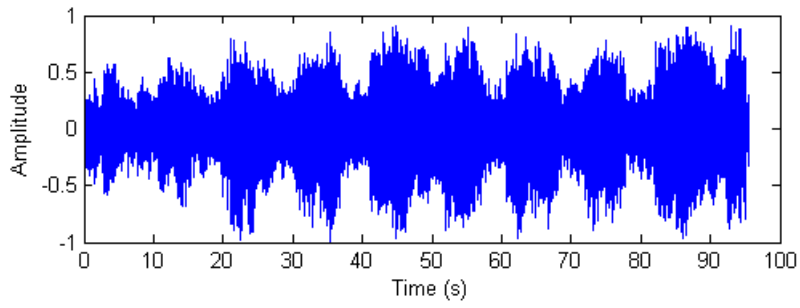


Figure 4.8: Audio signal after adding echo

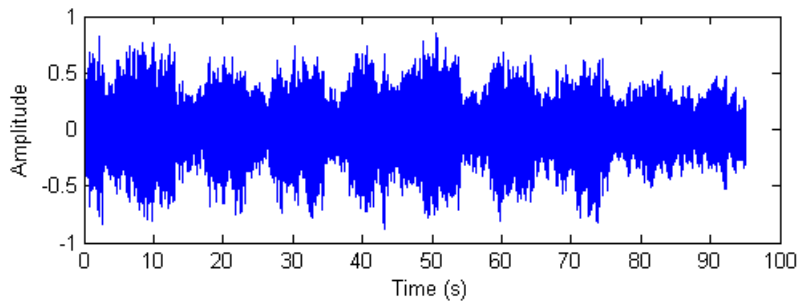


Figure 4.9: Audio signal after doing reverse

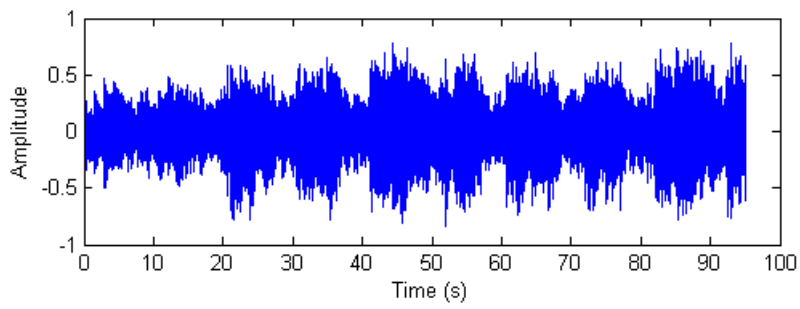


Figure 4.10: Audio signal after compressed to mp3/32kbps format

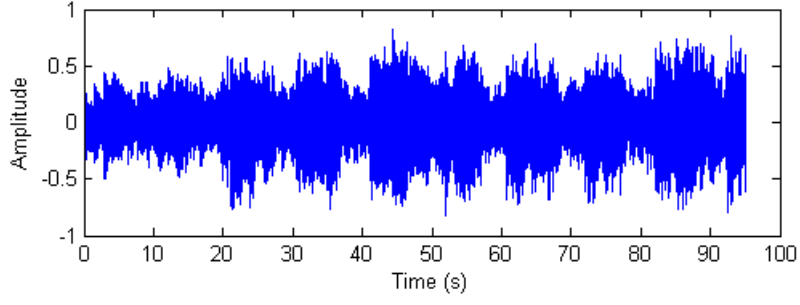


Figure 4.11: Audio signal after compressed to mp3/64kbps format

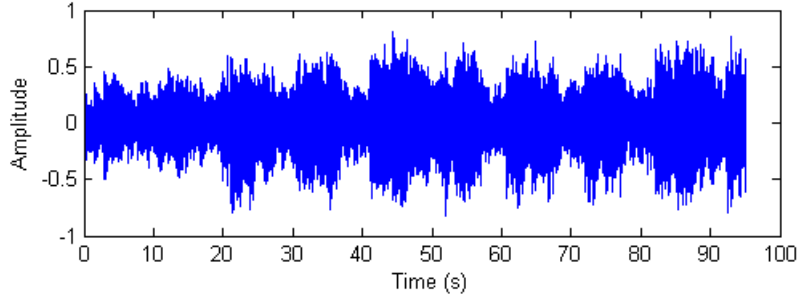


Figure 4.12: Audio signal after compressed to mp3/128kbps format

## 4.4 Experimental Environment

- **Processing Software:** MATLAB
- **Software for Applying Attack:** GoldWave

## 4.5 Normalized Coefficient

Normalized coefficient (NC) is used to evaluate the similarity between the original watermark and the extracted watermark. In order to evaluate the value of NC, the extracted watermark  $W^*$  is compared with the original watermark  $W$  and the NC is defined by equation 4.1.

$$NC(W, W^*) = \frac{\sum_{i=1}^{M_1} \sum_{j=1}^{M_2} W(i, j) W^*(i, j)}{\sqrt{\sum_{i=1}^{M_1} \sum_{j=1}^{M_2} W(i, j)^2} \sqrt{\sum_{i=1}^{M_1} \sum_{j=1}^{M_2} W^*(i, j)^2}} \quad (4.1)$$



where  $W(i, j)$  and  $W^*(i, j)$  are the original watermark and extracted watermark respectively.

## 4.6 Bit Error Rate

Bit error rate (BER) is used to evaluate the watermark detection accuracy after signal processing operations and a value of zero or very close to zero is required for good robustness. In order to evaluate the BER, the extracted watermark  $W^*$  is compared with the original watermark  $W$  and the BER is defined by equation 4.2.

$$BER(W, W^*) = \frac{\sum_{i=1}^{M_1} \sum_{j=1}^{M_2} |W(i, j) - W^*(i, j)|}{M_1 \times M_2} \times 100\% \quad (4.2)$$

where  $W(i, j)$  and  $W^*(i, j)$  are the original watermark and extracted watermark respectively, and  $M_1 \times M_2$  is the size of watermark image. In general, BER is expressed in terms of percentage.

## 4.7 False Positive Error

False positive error is the probability of declaring an non-watermarked audio as watermarked by decoder. The watermarking system is better with less false alarm probability. Let  $k$  be the total number of watermark bits, and  $t$  the number of matching bits. The false positive error probability  $P_{fp}$  can be calculated by equation 4.3.

$$P_{fp} = 2^{-k} \sum_{t=\lceil 0.8k \rceil}^k C(k, t) \quad (4.3)$$

where  $C(k, t)$  is the binomial coefficient.

## 4.8 False Negative Error

False negative error is the probability of declaring a watermarked audio as non-watermarked by decoder. The watermarking system is better with less false rejection probability. Let  $k$  be the total number of watermark bits, and  $t$  the number

of matching bits. The false negative error probability  $P_{fn}$  can be calculated by equation 4.4.

$$P_{fn} = \sum_{t=0}^{\lceil 0.8k \rceil - 1} [C(k, t)p^t(1-p)^{k-t}] \quad (4.4)$$

where  $C(k, t)$  is the binomial coefficient and  $p$  is the bit error probability of extracted watermark. Corresponding to different attack,  $p$  has different value. However, the approximate value of  $p$  may be obtained from bit error rate under determinate attack.

# Chapter 5

## Simulation Result

### 5.1 Imperceptibility Analysis

The watermarked audio is identical to original one because the watermark is, actually, embedded into the secret key, not into the audio. So without processing with various imperceptibility analysis methods, it is said to be an imperceptible scheme.

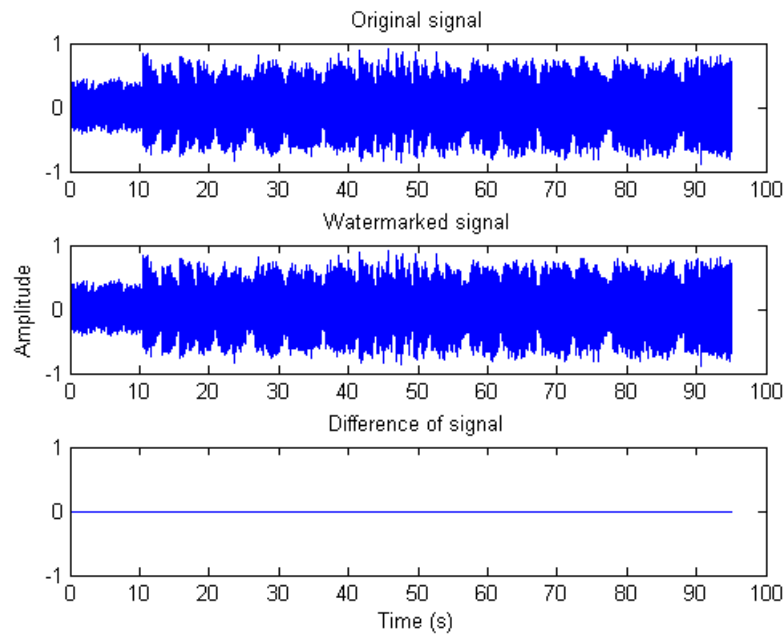


Figure 5.1: Imperceptibility of proposed watermarking scheme

Fig. 5.1 shows the imperceptibility of the proposed audio watermarking scheme. Here, it is observed that there is no difference between original audio and watermarked audio, which is the proof of its imperceptibility.

## 5.2 Measuring the Robustness

The robustness of a watermarking method is defined as the ability of watermark detector to extract the embedded watermark after common signal processing and attacks. Robustness is measured in terms of normalized coefficient and bit error rate as described earlier. In order to test the robustness of the proposed scheme, various types of attack are applied mentioned in chapter 4. In the following, the robustness of the proposed scheme against these types of attacks are demonstrate.

Tables 5.1 and 5.2 show the robustness result of audios (a) *Citizen, Go Back to Sleep*, (b) *Beginning of the End*, (c) *Breathing on Another Planet* and (d) *Thousand Yard Stare* respectively. In table 5.1, extracted watermark images are also shown. It is observed that extracted images almost look like the original image. It is seen that all NC values are ranges from 0.90 to 0.92. Also, all BER values are between 9% to 12%. By considering this performance, it can be said that this scheme has good robustness against various types of attack.










Attack	(a) Citizen, Go Back to Sleep		
	NC	BER	Extracted watermark
Noise addition	0.9206	10.06	
Re-sampling	0.9158	10.64	
Low-pass filtering	0.9145	10.84	
Re-quantization	0.9172	10.45	
Echo	0.9268	9.28	
Reverse	0.9199	10.16	
mp3 compression (32 kbps)	0.9225	9.77	
mp3 compression (64 kbps)	0.9279	9.18	
mp3 compression (128 kbps)	0.9271	9.28	

Table 5.1: The result of attacks for audio signal (a)

Tables 5.3 and 5.4 give the comparative results of proposed scheme with other watermarking schemes for audio *Citizen, Go Back to Sleep* in terms of NC and BER respectively.

Audio Signal	Attack	NC	BER
(b) Beginning of the End	Noise addition	0.9141	10.84
	Re-sampling	0.9172	10.45
	Low-pass filtering	0.9232	9.77
	Re-quantization	0.9262	9.38
	Echo	0.9108	11.33
	Reverse	0.9233	9.77
	mp3 compression (32 kbps)	0.9270	9.28
	mp3 compression (64 kbps)	0.9162	10.64
	mp3 compression (128 kbps)	0.9154	10.65
(c) Breathing on Another Planet	Noise addition	0.9264	9.57
	Re-sampling	0.9129	11.04
	Low-pass filtering	0.9135	10.94
	Re-quantization	0.9228	9.77
	Echo	0.9213	9.96
	Reverse	0.9170	10.45
	mp3 compression (32 kbps)	0.9194	10.16
	mp3 compression (64 kbps)	0.9156	10.64
	mp3 compression (128 kbps)	0.9108	11.23
(d) Thousand Yard Stare	Noise addition	0.9187	10.25
	Re-sampling	0.9194	10.26
	Low-pass filtering	0.9132	11.04
	Re-quantization	0.9214	9.96
	Echo	0.9162	10.64
	Reverse	0.9041	12.11
	mp3 compression (32 kbps)	0.9108	11.33
	mp3 compression (64 kbps)	0.9136	10.94
	mp3 compression (128 kbps)	0.9194	10.25

Table 5.2: The result of attacks for audio signal (b), (c), and (d)

Table 5.3 compares NC of the proposed algorithm and other algorithms for the audio *Citizen, Go Back to Sleep*. For attack 5 and 6 mentioned in chapter 4 i.e., adding echo and doing the reverse, the proposed scheme clearly shows the best result comparing with other schemes. For attacks of adding noise, low-pass filtering and three different types of mp3 compression, this scheme produces better NC values than [28] and [30]. Except attack 5 and 6, [38] clearly indicates that it is better than proposed scheme. But it should be noted that NC values

greater than 0.9 indicate its robustness against several attack.

Attack	NC			
	Proposed	[38]	[28]	[30]
	DHT	Frame energy	DWT	DWT+DCT
Noise addition	0.9206	0.9901	0.5870	0.6619
Re-sampling	0.9158	0.9950	0.9924	0.7847
Low-pass filtering	0.9145	0.9942	0.6272	0.5541
Re-quantization	0.9172	1.0000	0.9634	0.5454
Echo	0.9268	0.7559	0.5820	0.7867
Reverse	0.9199	0.4904	0.5737	0.6150
mp3 compression (32 kbps)	0.9225	0.9591	0.5774	0.4034
mp3 compression (64 kbps)	0.9279	0.9650	0.5673	0.4806
mp3 compression (128 kbps)	0.9271	0.9650	0.5524	0.7270

Table 5.3: Comparison of NC among proposed and other algorithm

Table 5.4 compares BER of the proposed algorithm and other algorithms for the audio *Citizen, Go Back to Sleep*. The proposed scheme clearly shows the best result comparing with other schemes for attacks of adding echo and doing reverse operation. For attacks of adding noise, low-pass filtering, and mp3 compression, this scheme produces better NC values than [28] and [30] but shows comparatively worse result than [38]. And table 5.4 shows that values of [38] clearly superior to the proposed scheme in term of BER except attack 5 and 6.

Attack	BER			
	Proposed	[38]	[28]	[30]
	DHT	Frame energy	DWT	DWT+DCT
Noise addition	10.06	1.17	47.85	37.50
Re-sampling	10.64	0.59	0.98	25.00
Low-pass filtering	10.84	0.68	43.65	50.00
Re-quantization	10.45	0.00	4.69	49.00
Echo	9.28	27.83	49.02	25.00
Reverse	10.16	56.64	48.63	43.75
mp3 compression (32 kbps)	9.77	4.79	49.51	62.50
mp3 compression (64 kbps)	9.18	4.10	49.71	56.25
mp3 compression (128 kbps)	9.28	4.10	52.25	31.25

Table 5.4: Comparison of BER among proposed and other algorithm

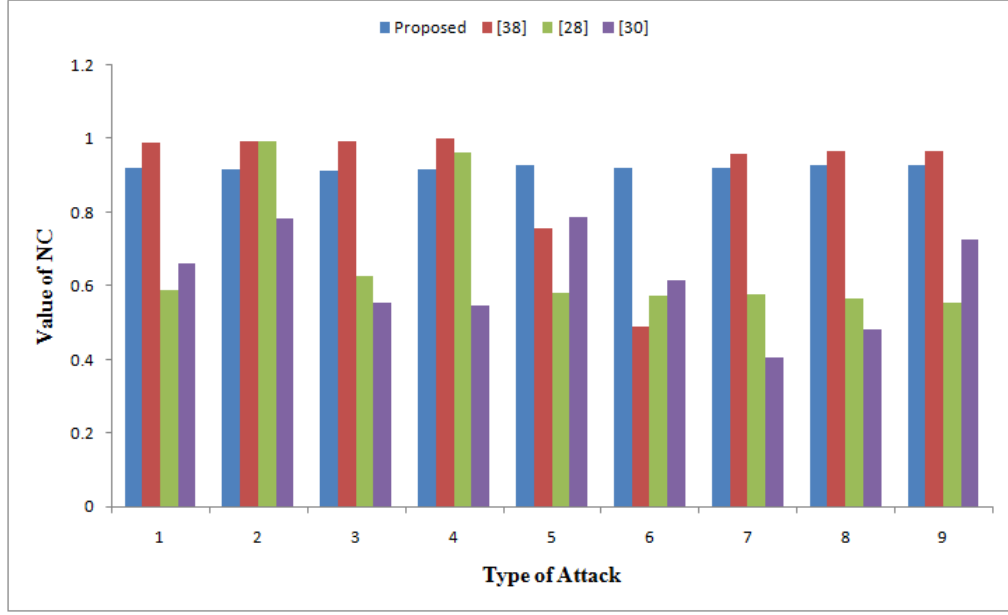


Figure 5.2: Graphical representation of NC comparison

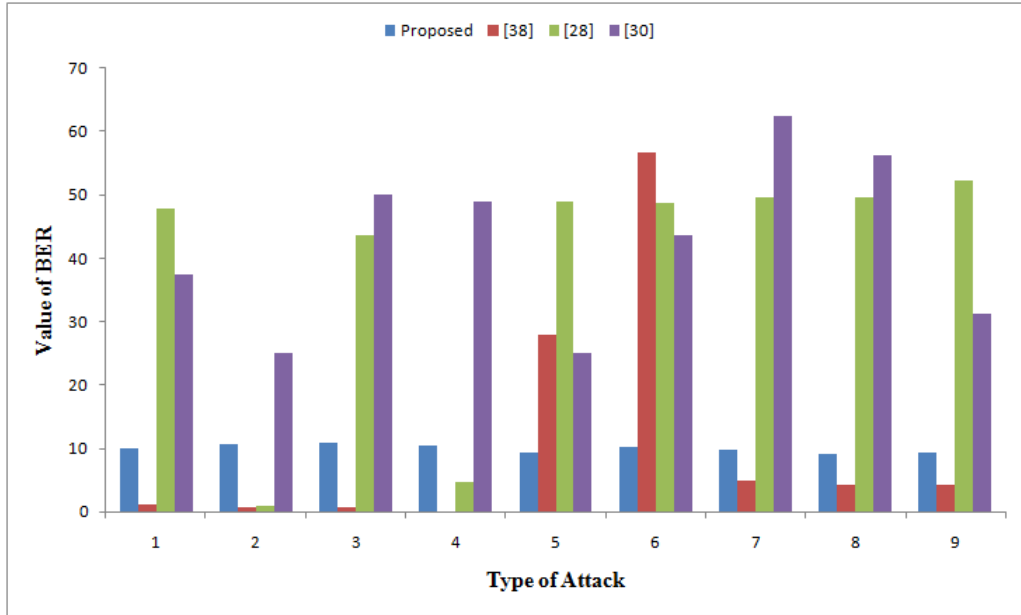


Figure 5.3: Graphical representation of BER comparison

Fig. 5.2 and Fig. 5.3 show the comparative graphical representation of proposed and other algorithms in terms of NC and BER for table 5.3 and 5.4 respectively.

Here, each attack is placed on the horizontal axis and value of NC and BER for each attack for different schemes is placed in the vertically against respective attack. From these two graphical charts, it can be easily observed which scheme



is better or worse against different attacks. For example, from Fig. 5.3, it can be seen that, for attack number 6, i.e., doing the reverse of audio, proposed scheme produces below 15% of BER, whereas other three schemes produce above 40% of BER, which indicates the out-performance of the proposed scheme.

Simulation results indicate that the proposed audio watermarking scheme provides better NC and BER as compared to [28], [30] and [38]. As in this method, there is no need to embeds watermark in the original audio, so it can be said imperceptible, actually the watermarked audio is identical to original one.

### 5.3 False Positive Error

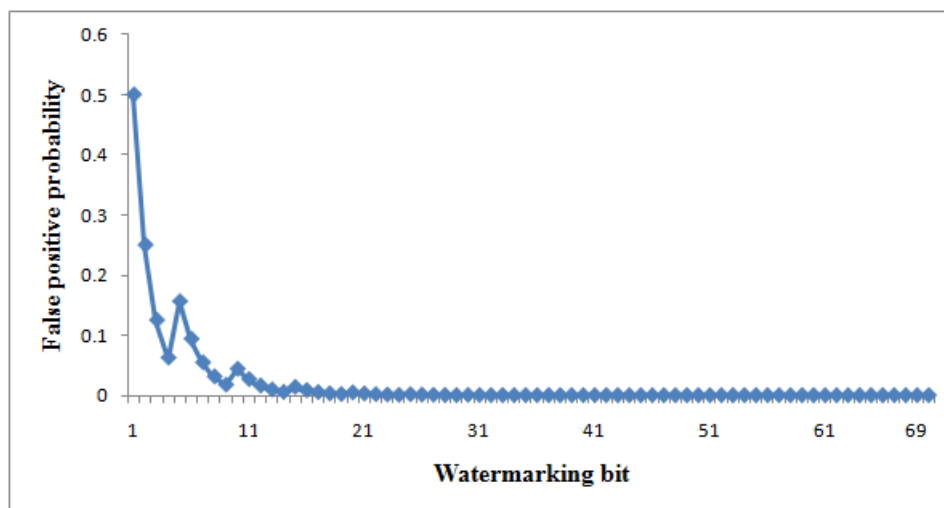


Figure 5.4: False positive probabilities under various watermarking bit

Fig. 5.4 gives the false positive probabilities when watermarking bit ( $q$ ) belongs to  $(0, 70]$ , and it tells us that the false positive probability trends to 0 when  $q$  is bigger than 14. In this proposed scheme,  $q = 1024$ , therefore, the false positive probability is approximately equal to 0.

### 5.4 False Negative Error

Fig. 5.5 gives the false negative probabilities when  $q$  belongs to  $(0, 70]$ , and it tells us that the false rejection probability trends to 0 when  $q$  is bigger than 10. In this proposed scheme,  $q = 1024$ , so, the false negative probability of the proposed

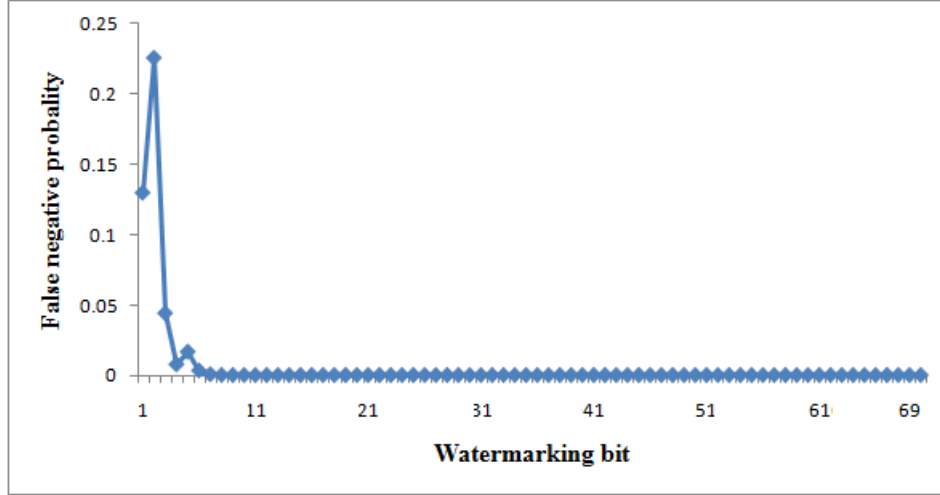


Figure 5.5: False negative probabilities under various watermarking bit

scheme is also approximately equal to 0. From tables 5.1, and 5.2, it is easily seen that the BERs are all less than 13%, so the value of  $p$  is assumed to be 0.87 in this proposed scheme and put this value in equation 4.4 given at page 24.

# Chapter 6

## Conclusion

### 6.1 Summary

The aim of this thesis was to develop an imperceptible and robust watermarking algorithm that would perform better than existing watermarking methods. For accomplishing this purpose, a new zero-watermarking scheme based on Discrete Hartley Transform has been proposed. Zero-watermarking which does not modify the original audio but constructs zero watermarks from it, is a useful technique for resolving the contradiction between robustness and imperceptibility. The experimental result shows that the proposed watermarking scheme is much better than other. The proposed method provides normalized coefficient (NC) values ranging from 0.90 to 0.92 and also provides bit error rate (BER) values ranging from 9% to 12%. Therefore, the proposed scheme provides better robustness against various attacks such as re-sampling, adding echo, compression, etc. Also, the proposed scheme is blind as extracting of the watermark does not require the original signal. Comparison of results with other schemes show that the proposed scheme can be a good competent in the field of audio watermarking.

### 6.2 Future Recommendation

Since zero-watermarking is a considerably new method and Discrete Hartley Transform (DHT) was not use in the field of audio watermarking, this work offers many opportunities for future work. The followings should consider for the upcoming newer in this field:

- Other properties of DHT can be considered for getting more robustness.
- Some modern attacks such as pitch-scale, channel fading, packet drop should be considered.

# Bibliography

- [1] Z. Xiaoming, Y. Zhaoyang, and L. Wenzhi, “Audio watermarking algorithm for public information transmission,” *Journal of Computer Applications*, vol. 29, no. 9, pp. 2323–2326, 2009.
- [2] P. Bassia, I. Pitas, and N. Nikolaidis, “Robust audio watermarking in the time domain,” *IEEE Transactions on Multimedia*, vol. 3, no. 2, pp. 232–241, 2001.
- [3] J. Foote and J. Adcock, “Time base modulation: A new approach to watermarking audio and images,” in *Proceedings of the International Conference on Multimedia and Expo*, vol. 1, 2003, pp. 221–224.
- [4] W. Lie and L. 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, 2006.
- [5] A. Lemma, J. Aprea, and W. Oomen, “A temporal domain audio watermarking technique,” *IEEE Transaction on Signal Processing*, vol. 51, no. 4, pp. 1088–1097, 2003.
- [6] H. Oh, J. Seok, J. Huang, and D. Youn, “New echo embedding technique for robust and imperceptible audio watermarking,” in *Proceedings of the International Conference on Acoustics, Speech, and Signal Processing*, vol. 3, 2001, pp. 1341–1344.
- [7] K. B. Seob, R. Nishimura, and Y. Suzuki, “Time-spread echo method for digital audio watermarking,” *IEEE Transaction on Multimedia*, vol. 7, no. 2, pp. 212–221, 2005.
- [8] D. Megias, J. S. Ruiz, and M. Fallahpour, “Efficient self-synchronised blind audio watermarking system based on time domain and FFT amplitude modification,” *Signal Process*, vol. 90, no. 12, pp. 3078–3092, 2010.

- [9] M. Fallahpour and D. Megias, "Audio watermarking based on fibonacci numbers," *IEEE/ACM Transaction on Audio, Speech, and Language Processing*, vol. 23, no. 8, pp. 1273–1282, 2015.
- [10] W. Tan, S. Yang, Y. Chen, and J. Zhou, "Research on DFT domain digital audio watermarking algorithm based on quantization," in *Proceedings of the International Workshop on Education Technology and Computer Science*, vol. 3, 2009, pp. 736–739.
- [11] M. Lihua, Y. Shuangyuan, and J. Qingshan, "A new algorithm for digital audio watermarking based on DWT," in *Proceedings of the WRI Global Congress on Intelligent Systems*, vol. 4, 2009, pp. 229–233.
- [12] S. T. Chen, G. D. Wu, and H. N. Huang, "Wavelet domain audio watermarking scheme using optimisation based quantisation," *IET Signal Processing*, vol. 4, no. 6, pp. 720–727, 2010.
- [13] S. T. Chen, H. N. Huang, C. J. Chen, T. K. Kun, and T. S. Yi, "Adaptive audio watermarking via the optimization point of view on the wavelet based entropy," *Digital Signal Processing*, vol. 23, no. 3, pp. 971–980, 2013.
- [14] M. Pooyan and A. Delforouzi, "Adaptive and robust audio watermarking in wavelet domain," in *Proceedings of the International Conference on International Information Hiding and Multimedia Signal Processing*, 2007, pp. 287–290.
- [15] P. Kumsawat, K. Attakitmongkol, and A. Srikaew, "Digital audio watermarking for copyright protection based on multiwavelet transform," in *Intelligence and Security Informatics*. Springer, 2008, pp. 155–164.
- [16] G. Zeng and Z. Qiu, "Audio watermarking in DCT: Embedding strategy and algorithm," in *Proceedings of the International Conference on Signal Processing*, 2008, pp. 2193–2196.
- [17] P. K. Dhar, M. I. Khan, and S. Ahmad, "A new DCT-based watermarking method for copyright protection of digital audio," *International Journal of Computer Science & Information Technology*, vol. 2, no. 5, pp. 91–101, 2010.
- [18] Q. Guo, Y. Zhao, P. Cheng, and F. Wang, "An audio digital watermarking algorithm against A/D and D/A conversions based on DCT domain," in *Proceedings of the International Conference on Consumer Electronics, Communications and Networks*, 2012, pp. 871–876.

- [19] W. Quan and J. Kim, "An audio watermarking algorithm using group quantization of DCT coefficients," in *Future Generation Information Technology*. Springer, 2012, pp. 159–166.
- [20] Y. Wang, S. Wu, and J. Huang, "Audio watermarking scheme robust against desynchronization based on the dyadic wavelet transform," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, no. 13, pp. 1–17, 2010.
- [21] Y. Ji and J. Kim, "A quantified audio watermarking algorithm based on DWT-DCT," in *Multimedia, Computer Graphics and Broadcasting*. Springer, 2011, pp. 339–344.
- [22] P. K. Dhar and T. Shimamura, "A DWT-DCT based audio watermarking method using singular value decomposition and quantization," *Journal of Signal Processing*, vol. 17, no. 3, pp. 69–79, 2013.
- [23] B. Lei, Y. Soon, F. Zhou, Z. Li, and H. Lei, "A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition," *Signal Processing*, vol. 92, no. 9, pp. 1985–2001, 2012.
- [24] T. Sun, W. Quan, and S. Wang, "Zero-watermark watermarking for image authentication," in *Proceedings of the International Conference Signal and Image Processing*, 2002, pp. 503–508.
- [25] Q. Wen, T. F. Sun, and S. X. Wang, "Concept and application of zero-watermark," *Acta Electronica Sinica*, vol. 31, no. 2, pp. 214–216, 2003.
- [26] X. Li and G. He, "A new audio zero-watermark algorithm for copyright protection based on audio segmentation and wavelet coefficients mapping," in *Proceedings of the International Conference on Digital Content, Multimedia Technology and its Applications*, 2011, pp. 22–26.
- [27] X. Zhong, X. Tang, and H. Yuc, "Zero-watermark scheme based on audio's statistical character," in *Proceedings of the International Symposium on Microwave, Antenna, Propagation, and EMC Technologies for Wireless Communications*, 2007, pp. 1227–1230.
- [28] Y. Yang, M. Lei, H. Liu, Y. Zhou, and Q. Luo, "A novel robust zero-watermarking scheme based on discrete wavelet transform," *Journal of Multimedia*, vol. 7, no. 4, pp. 303–308, 2012.
- [29] X. Zhang, W. Zhang, F. Li, and G. Liu, "A robust audio zero-watermarking algorithm based on wavelet packet analysis," in *Intelligent Data analysis and its Applications*. Springer, 2014, vol. 1, pp. 3–10.

- [30] H. L. Dai and D. He, "An efficient and robust zero-watermarking scheme for audio based on DWT and DCT," in *Asia Pacific Conference on Postgraduate Research in Microelectronics & Electronics*, 2009, pp. 233–236.
- [31] N. Chen and J. Zhu, "A robust zero-watermarking algorithm for audio," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, no. 103, pp. 1–7, 2008.
- [32] R. W. Ciptasari, F. A. Yulianto, A. Fajar, and K. Sakurai, "An efficient key generation method in audio zero-watermarking," in *Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2011, pp. 336–339.
- [33] Y. Xiong and R. Wang, "An audio zero-watermark algorithm combined DCT with zernike moments," in *Proceedings of the International Conference on Cyberworlds*, 2008, pp. 11–15.
- [34] Y. C. Lu, "Cepstral coefficients based zero-watermark scheme for digital audio," Master's thesis, Institute of Communication Engineering, Tatung University, Taipei, Taiwan, 2008.
- [35] M. L. Wang, H. X. Lin, and M. T. Lee, "Robust audio watermarking based on MDCT coefficients," in *Proceedings of the International Conference on Genetic and Evolutionary Computing*, 2012, pp. 372–375.
- [36] S. M. Tsai, "An efficient and robust zero-watermarking scheme for digital audio," in *Proceedings of the International Conference on Circuits and Systems*, 2013, pp. 51–54.
- [37] S. M. Tsai, "A robust zero-watermarking algorithm for audio based on LPCC," in *Proceedings of the International Conference on Orange Technologies*, 2013, pp. 63–66.
- [38] S. M. Tsai, "A robust zero-watermarking scheme for digital audio," *International Journal of Information and Electronics Engineering*, vol. 5, no. 2, pp. 117–121, 2015.
- [39] R. N. Bracewell, "The discrete hartley transform," *Journal of Optical Society of America*, vol. 73, no. 12, pp. 1832–1835, 1983.
- [40] G. E. J. Bold, "A comparison of the time involved in computing fast hartley and fast fourier transforms," *Proceedings of the IEEE*, vol. 73, no. 12, pp. 1863–1864, 1985.

- [41] [Online]. Available: <http://www.jamendo.com/en/album/7365>
- [42] V. Bhat, I. Sengupta, and A. Das, “An audio watermarking scheme using singular value decomposition and dither-modulation quantization,” *Multimedia Tools and Applications*, vol. 52, no. 2, pp. 369–383, 2011.
- [43] (Accessed on: Mar. 28, 2015). [Online]. Available: <https://www.goldwave.com/>
- [44] [Online]. Available: <https://www.mathworks.com/products/matlab/>