BINARY IMAGE WATERMARKING ON AUDIO SIGNAL USING WAVELET TRANSFORM

RAKAN SAADALLAH RASHID

DECEMBER 2014

BINARY IMAGE WATERMARKING ON AUDIO SIGNAL USING WAVELET TRANSFORM

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES OF
ÇANKAYA UNIVERSITY

BY
RAKAN SAADALLAH RASHID

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF
MATHEMATICS AND COMPUTER SCIENCE / INFORMATION TECHNOLOGY PROGRAM

DECEMBER 2014

Title of the Thesis : **Binary Image Watermarking on Audio Signal Using Wavelet Transform.**

Submitted by **Rakan Saadallah RASHID**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.

Prof. Dr. Taner ALTUNOK

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science

Prof. Dr. Billur KAYMAKÇALAN

Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Assist.Prof. Dr. Abdül Kadir Görür	Assist.Prof. Dr. Jafar R. Mohammed
Supervisor	Co-Supervisor

Examination Date: 23.12.2014

Examining Committee Members

Assoc. Prof. Dr. Ersin ELBAŞI	(Ipek Univ.)
Assist. Prof. Dr. Tolga PUSATLI	(Çankaya Univ.)
Assist. Prof. Dr. Abdül Kadir GÖRÜR	(Çankaya Univ.)

STATEMENT OF NON-PLAGIARISM PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : Rakan Saadallah, RASHID
Signature :
Date : 23.12.2014

ABSTRACT

BINARY IMAGE WATERMARKING ON AUDIO SIGNALS USING WAVELET TRANSFORM

RASHID, Rakan Saadallah
M.Sc., Department of Mathematics and Computer Science / Information Technology Program
Supervisor: Assist. Prof. Dr. Abdul Kadir GÖRÜR
Co-Supervisor: Assist. Prof. Dr. Jafar MOHAMMED
December 23, 43 pages

Digital watermarking approaches have recently become an important field of study in a number of practical applications. Generally, digital watermarking is the process of embedding particular information data into other signal data in such a way that the quality of the original information data is maintained. Watermarking can be performed on images, video, text, or audio to protect them from copyright violation. Among all of these types of watermarking, audio watermarking is difficult since the quality of such signals is highly affected by the watermark code. This thesis introduces some approaches that have features and may be applicable for audio watermarking.

Generally, the digital audio watermarking approaches may be performed in either the special domain or the transform domain. The approaches that are based on the transform domain are gaining more attention due to their robustness or resistance to attackers. The most commonly used transforms for achieving digital audio watermarking are discrete cosine transform (DCT), short-term Fourier transform (STFT), and digital wavelet transform (DWT). In this research work, the main attention is paid toward digital wavelet transforms such as Haar and Daubechies-4. In addition, this thesis investigates the process of embedding a binary image into various audio signals such as speech and music signals. The values of the pixels in the binary images are either 1 or 0. These pixels are inserted into samples of the speech signal in such a way that the quality of the speech signal is preserved.

One main reason to consider the audio watermarking approaches in the wavelet domain is that many modern multimedia standards such as JPEG2000 and MPEG-4 are based on the discrete wavelet transform. These common standards have brought new requirements such as low bit-rate transmission, coding, and many other advantages.

Finally, experimental results are presented to validate the performance of the proposed watermarking approach and to compare its performance with other related watermarking approaches. The results show that the performance, in terms of signal-to-noise ratio (SNR) and normalized correlation (NC), of the proposed watermarking approach outperforms other approaches based on DCT. In addition, the results show that the extraction process of the hidden code becomes complex when considering any signal processing operations such as MP3 compression and high pass filtering. The worst case is when using a high pass filter where the recovered binary image is not satisfactory.

Keywords: Watermarking, Wavelet Transform, Audio Signal, Binary Image.

ÖZ

DALGACIK DÖNÜŞÜMÜ KULLANARAK SES SİNYALİNDE İKİ BİLEŞENLİ GÖRÜNTÜ DAMGALAMA (FİLİGRAN BASMA)

RASHID, Rakan Saadallah
Yüksek Lisans, Matematik - Bilgisayar Anabilim Dalı / Bilgi Teknolojileri Bölümü
Tez Yöneticisi: Yrd. Doç. Dr. Abdül Kadir GÖRÜR
Eş Tez Yöneticisi: Yrd. Doç. Prof. Dr. Jafar MOHAMMED
Aralık 23, 43 sayfa

Sayısal Damgalama Yaklaşımları son zamanlarda birçok sayıdaki pratik uygulamaların daha da önemli bir çalışma alanı oldu. Sayısal damgalama genellikle başka bir sinyal verisi içine özel bilgi verisi gömme işlemidir. Böylece orijinal(ana) bilgi veri kalitesi korunur, sürdürülür. Damgalama; resimlerde, videolarda, metinlerde ya da işitsel/ses ile ilgili alanlarda telif hakkı ihlalini korumak için uygulanabilir. Bütün bu damgalama türleri arasında işitsel damgalama en zor olanıdır çünkü bu tür sinyallerin kalitesi filigran kodu tarafından yüksek derecede etkilenir. Bu tez bazı yaklaşımların iyi özelliklerini tanıtmak ve belki ses damgalaması/filigranı için uygulanabilir.

Sayısal ses damgalama yaklaşımları genellikle özel etki alanında/tanım kümesinde ve bu alanın dönüşümünde uygulanabilir. Tanım kümesi dönüşümü baz alınarak yapılan yaklaşımlar saldırganlara karşı dayanıklılık ya da dirençten dolayı daha fazla dikkat gerektirir.

Ayrık Kosinüs Dönüşümü (DCT), Kısa Dönemli Fourier Dönüşümü (STFT) ve Dijital Dalgacık Dönüşümü (DWT), sayısal ses damgalamasına erişmek için kullanılan en yaygın dönüşümlerdir. Bu araştırmada, dalgacık dönüşümüne (Haar(deniz sisi) ve Daubechies- 4) yarar sağlama esas ilgi/dikkattir. Ayrıca bu tezde çeşitli ses sinyalleri (konuşma ve müzik sinyalleri)içinde iki bileşenli görüntü gömme işlemi incelenir. İki bileşenli görüntünün piksel değeri bir ya da sıfırdır. Bu pikseller hız sinyalinin örnekleri/numuneleri içine yerleştirilir. Böylece, hız sinyalinin kalitesi korunur.

Dalgacık tanım kümesinde ses damgalama/filigran yaklaşımlarının değerlendirilmesinde/göz önünde bulundurulmasında ana nedenlerden biri de pek çok modern çoklu ortam standartlarıdır (JPEG2000 ve MPEG-4). Modern çoklu standartlar kesikli dalgacık dönüşümünde baz alınır. Bu yaygın standartlar küçük bit oran/ hız gönderimi, kodlama ve diğer avantajlar gibi yeni gereksinimler getirir.

Son olarak, geniş kapsamlı deney sonuçları, önerilen damgalama yaklaşımının verimliliğini geçerli kılmak ve onun performansını ilgili diğer damgalama yaklaşımlarıyla karşılaştırmak için gösterilir. Sonuçlar , sinyal gürültü oranına dayanarak(SNR) performansı ve standartlaştırılmış korelasyon (ilişki,oran) (NC) performansını, önerilen damgalama yaklaşımı daha iyi gösterir. Önerilen Damgalama yaklaşımı, DCT baz alınarak diğer yaklaşımlarla karşılaştırıldığında daha üstündür. Ayrıca sonuçlar, MP3 sıkıştırma ve yüksek geçiren süzgeç gibi herhangi sinyal işleme faaliyeti düşünüldüğü zaman, gizlenmiş/kapalı kodu özütleme işleminin daha karmaşık olduğunu gösterir. Yüksek geçiren süzgeç kurtarılmış iki bileşenli görüntüde kullanıldığı zaman yeterli değilse, bu en kötü durumdur.

Anahtar Kelimeler: Damgalama/Filigran Basma, Dalgacık Dönüşümü, Ses/İşitme Sinyali, İki Bileşenli Görüntü.

ACKNOWLEDGEMENTS

First of all, praise to GOD **"ALLAH"** on all the blessings, one of these blessings was the help in achieving this research to its end.

The author wishes to express his deepest gratitude and thanks to the supervisor **Assist. Prof. Dr. Abdül Kadir Görür** and **Assist. Prof. Dr. Jafar Ramadhan Mohammed** for their guidance, advice, criticism, encouragement and insights throughout the thesis.

Finally, my special thanks to my family for the endless help, patience and encouragement.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURES

FIGURES

LIST OF TABLES

TABLE

LIST OF ABBREVIATIONS

1D	One-Dimensional
AWGN	Additive White Gaussian Noise
CAZAC	Constant Amplitude Zero Autocorrelation
CCTV	Closed-Circuit Television
CDMA	Code Division Multiple Access
Db-4	Daubechies-4
DCT	Discrete Cosine Transform
DSP	Digital Signal Processing
DWT	Discrete Wavelet Transform
FFT	Fast Fourier Transform
GPS	Global Positioning System
HM	Haar Matrix
HPF	High Pass Filter
IHM	Inverse Haar Matrix
IP	Image Processing
JPEG	Joint Photographic Experts Group
LP	Linear Prediction
LPF	Low Pass Filter
LSFs	Line Spectral Frequencies
MRI	Magnetic Resonance Imaging
NC	Normalized Correlation
PC	Personal Computer
QIM	Quantization Index Modulation
SNR	Signal-To-Noise Ratio
SS	Spread Spectrum
STFT	Short-Term Fourier Transform

SVD	Singular Value Decomposition
WT	Wavelet Transform
LPC	Linear Predictive Coding

CHAPTER 1

INTRODUCTION

1.1 Overview

Nowadays, the amount of digital information is becoming huge and it can be easily distributed everywhere in the world by means of the Internet or computer networking. This digital information could be in any of the following forms: text, video, images, and audio (the form of digital information considered in this thesis is audio signals such as speech and music signals). These signals can be copied, duplicated, and/or digitally manipulated. To keep up with the transmission of digital information over the Internet, the reliability and originality of the transmitted information should be maintained. Thus, it is necessary that the available information should be protected and secured, especially important information and important applications such as biomedical and speech communication systems.

One method of coping with this problem is by embedding an invisible watermark code into the original information to mark the ownership of it. Generally, there are many methods of information protection, which can be divided into different categories such as cryptography, steganography, and watermarking [1]. In this thesis, the study mainly focused on watermarking, while steganography and cryptography are outside the scope of the thesis.

Generally, watermarking may be defined as the process of embedding information such as text, a binary image, audio, and so on into another signal such as an image, audio, and so on.

Recently, audio watermarking has become an interesting research topic. In order to protect audio media from informal duplication, the watermark code must be hidden with the original audio without affecting the quality of the original audio media. Moreover, only the owner has the ability to recover the watermark code.

Following this overview, the rest of this introductory chapter is organized as follows. Then, the problem statement and the objectives of the research work are presented in Sections 1.3 and 1.4 respectively. Finally, the organization of the overall thesis is presented in Section 1.5.

1.2 Problem Statement

The issue of copyright violation is a huge problem for copyright owners, especially when the data are in digital form and must be distributed over the World Wide Web (Internet). Digital watermarking techniques can be applied to different types of media such as pictures, audio, text, and movies to solve the problem of copyright violation.

1.3 Objectives of the Thesis

The objective of this research work is to focus on one of the most efficient techniques, which involves watermarking the binary image signal in the wavelet domain of the audio signal. The performance of this technique will be investigated through a number of computer simulation results. The following related issues will be particularly highlighted to show the effectiveness of the described watermarking approach:

- After the binary image watermark is embedded into the original audio signal, the distortion in the watermark audio signal should be kept at an acceptable level.

- In addition, the watermark image could have the ability to be recovered without using the original audio signal during the extraction process.
- The technique under study should be effective and unbreakable in many attack operations such as additive white Gaussian noise (AWGN), up and down sampling, low and high pass filters, and MP3 compression.

1.4 Organization of the Thesis

Following this introduction (**Chapter 1**), the remainder of this thesis is organized as follows:

Chapter 2: This chapter introduces the background and presents a literature review of watermarking in general. It also contains the related work and most commonly used approaches for audio watermarking. The importance of using transform-domains-based watermarking approaches over the special domain is also highlighted in this chapter. The basic principles of the transform domain such as wavelet transform are presented in this chapter.

Chapter 3: In this chapter, the structure and analysis of the proposed watermark approach are presented. It also contains all steps of embedding a binary image into an audio signal in the wavelet domain.

Chapter 4: This chapter presents the simulation results and the discussion of the proposed watermarking approach described in Chapter 3. These simulation results validate the performance of the proposed watermarking approach. This chapter also demonstrates its performance under various signal processing operations and in comparison to some exciting watermark approaches.

Chapter 5: The final chapter presents the conclusions of this research work and suggests or opens some new horizons which may be considered as future work.

1.5 Flowchart of the Planning Work

In order to carry out this research work, it is necessary to outline the essential requirements. The sequence and the details of these requirements are shown in Figure 1. As can be seen from this figure, it consists of three main steps: Data collection or recording, implementation of the proposed watermark approach and validation of its performance through a number of experimental results, and finally drawing of the main conclusions.

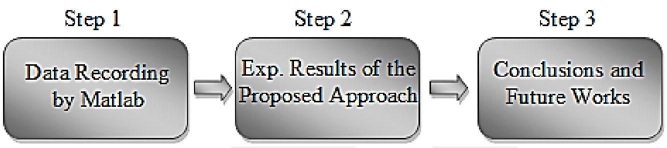

Figure 1: Flowchart of main steps to achieve the research work

The details of these steps are explained as follows:

Step 1: Data Collection

This step consists of recording some speech and music signals. It also consists of creating some specific binary images (watermark codes). These binary images with a certain number of pixels can be embedded into a speech signal for the purpose of watermarking. Matlab software can be used to record different speech signals (the sampling rate and the number of samples for each speech signal can be easily chosen by the specific Matlab commands). On the other hand, the binary image is created by means of computer programs where the number of pixels can be specifically chosen. In this research work, all the binary images are of the monochrome bitmap type and the dimensions of the required binary image are chosen to be equal to 45 × 45 pixels.

Step 2: Experimental Results

The computer simulation consists of a Matlab program that can be used for embedding the binary image into speech signals. This watermark algorithm is implemented in the wavelet domain of the speech signal. The types of wavelet transforms that are adopted in this research work are Haar transformation and Daubechies-4 transformation. The process of binary image watermarking on the speech signals is implemented by using Matlab software in conjunction with a wavelet toolbox. In this part, the performance of the watermark process will be analysed, where after the binary image watermark is embedded into the original speech signal, the watermark speech signal distortion should be kept inaudible. In addition, the watermark binary image could have the ability to be recovered without using the original speech signal during the extraction process. Furthermore, the results of the computer simulation of the watermarking process should be strong against many attackers (signal processing operations) such as low-pass filtering, AWGN, and MP3 compression.

Step 3: Concluding Remarks

In this step, general concluding remarks will be presented. Generally, it is necessary to divide the speech signal into frames with a certain number of samples. Then, we need to decompose every frame of the speech signal using Haar or Daubechies-4 wavelet transformation (the details of these two steps will be covered in Chapter 2 of this research work). The hidden binary data are retrieved by comparing the means of the corresponding detail coefficients computed before and after hiding. Sample results will be shown to illustrate the effectiveness of the described approach.

CHAPTER 2

BACKGROUND AND LITERATURE REVIEW

2.1 Watermarking Fundamentals

In 1990, the topic of digital watermarking became an important issue, especially when both the number of Internet users and the amount of data became huge. To protect these data it was necessary to insert an invisible watermark code.

After introducing the concept of watermarking, many scientists and researchers around the world started and still continue to develop many techniques to reach the goal of achieving a good and secure watermarking approach.

Generally, we may define digital watermarking as a process of inserting an invisible watermark code such as a binary image into the original data information. In the case of selecting the binary image as a watermark code, this code can be represented by a certain number of bits whose intensity values may be either one or zero (this is only true for the case of binary images).

Historically, the English word "watermark" is taken from the codes imprinted on organizational stationery. Apart from written watermarks, which are visible and readable, digital watermarks are intended to be highly invisible, or in the case of audio clips, inaudible. In addition, the bits representing the watermark code must be distributed throughout the signal in such a way that they cannot be identified and manipulated. The embedding technique must keep the original information unaffected and an extraction algorithm should detect the watermark code.

Following this introduction, the rest of this chapter is organized as follows. In Section 2.2, the related work (Literature Review) is introduced and discussed. In Section 2.3, basic information about the necessary requirements of digital watermarking methods is discussed. In Section 2.4, some applications of digital watermarking are mentioned, followed by a brief introduction to the types of watermarking approaches. In Section 2.5 some advantages of performing watermarking in the wavelet domain are highlighted. In Section 2.6, further details about wavelet transform are explained. Section 2.7 contains more detail about Haar transformation, and its results are explained in Section 2.8. Finally, more details about Daubechies-4 transformations are introduced in Section 2.9 and their results are explained in Section 2.10.

2.2 Literature Review

In the literature, there are several techniques in which a watermark code is embedded in an original audio file. The most widely used technique involves the watermark process in either the time domain (also called the special domain in some references) or the frequency domain (or transform domain). Generally, the performances of the transform domain approaches are much better than those of the special domain approaches [2]. The commonly used transform domain approaches are based on discrete cosine transform (DCT) [3, 4], short-term Fourier transform (STFT) [5], discrete wavelet transform (DWT) [6, 7] and cepstrum transform [8].

The watermarking approaches based on the advanced transform domain, specifically the wavelet domain of the audio signal, are adopted in this Master’s thesis.

In the literature, the watermarking approaches that depend on the spatial domain were introduced first. They are simple and easy to design. For example, **Cai and Gopalan** [9], 2014, proposed an approach that depends on the spatial domain. This watermarking approach depends on bit modification of voiced or unvoiced segments, where five consecutive samples in each voiced or unvoiced segment of the original audio signal are selected and replaced by the watermark code. Although the authors have proved the effectiveness of this approach and the attacker cannot view the watermark code, its robustness is insufficient in some applications. Therefore, most authors have concentrated their studies on the approaches based on the transform domain, which are classified as high-robustness watermark approaches. As a result, transform domain approaches were developed.

First, **Khayam** [10]**,** 2003, used DCT to transform a signal in the spatial domain into the frequency domain.

Then, **Chen, Wen-Yuan;Huang.,Shih-Yuan** [11], 2000, suggested a watermarking approach that uses DCT to embed a watermark code into original image data. The authors investigated the performance of the described approach and compared it to its spatial domain counterpart. The principle role of DCT is to divide the original data signal into three band frequencies (i.e. lower-frequency band, middle-frequency band, and high-frequency band). The authors use the lower-frequency band to embed the watermark code.

Next, an improved version of DCT called block-based DCT was suggested by **Namazi, Karami, and Ramazannia** [12], 2012, in this approach, the watermark code was embedded into the middle-frequency band of the original data signal. The middle-frequency band was chosen so that the robustness would be guaranteed when its performance against some signal processing operations such as compression was investigated. The original data signal was partitioned into many blocks and then DCT was performed on each block. The middle frequency band was selected and the watermark code was embedded in the assigned frequencies.

Furthermore, watermarking approaches based on singular value decomposition (SVD) were also suggested in the literature. For example, **Lai** [13], 2013, used SVD in watermarking. This approach uses some visual features of the original data to find out the proper location of the watermark code and shows a good performance.

Some other advanced watermarking approaches based on the wavelet domain were also presented in the literature. **Singh, Dave, and Mohan** [14], 2013, propose an approach to decompose the original information using wavelet transform. The authors showed that this approach can provide good robustness against some signal-processing operations and maintain a high quality of the watermarked signal at the same time.

Hong-yan A., Quan L., and Xue-mei J. [15], 2013, studied the issue of synchronization audio watermarking based on DCT and DWT. The approach is a combination of special and wavelet transformers. The authors mainly tried to improve the safety and robustness of their watermark algorithm. In addition, they demonstrated the effectiveness of the proposed approach through a number of experimental results. They showed that their approach has good safety and robustness against different kinds of attacker, such as AWGN, up and down sampling, and MP3 compression.

Nin and Ricciardi [16], 2013, concentrated their study on digital watermarking and security-related issues in the information society.

Khalil and Adib [17], 2014, developed a new approach for embedding and extracting a watermarking audio signal based on multiple watermark codes by exploring the code division multiple access (CDMA) technique. The CDMA is a well-known and effective technique in the digital communication society, where many users are allowed to transmit simultaneously on the same channel without affecting or disturbing each other. The authors also suggested using multiple watermark codes in the same channel. They mainly wanted to increase the amount of information that can be hidden in an audio signal. They showed that the suggested approach maintains high quality while hiding the amount of information.

The stability issue was investigated by **Zeki, Ibrahim, Haruna, and Ya'u Gital** [18], 2013, who showed that the dynamics of watermark characteristics are unstable after insertion into speech streams. In order to overcome this drawback, the watermark code is inserted in many positions within the speech signal by the spread spectrum method. The authors also found the most suitable locations for inserting the watermark code to ensure a robust watermark.

A robust audio watermarking approach was proposed by **Zhang, Li, Fan, Jiang, Ma, and Hao** [19], 2013, This technique is based on the frequency-domain spread spectrum using a constant amplitude zero autocorrelation (CAZAC) sequence. The authors showed, by means of computer simulation, that the suggested approach provides good robustness and is strong enough for the most common signal processing operations or attacks while maintaining high quality of the audio signal.

An approach based on Word documents was proposed by **Li and Fucheng** [20], 2013, this approach is different from other watermarking approaches such as audio and video. The suggested approach performs the watermarking process by changing the font of the letters or characters in the Word document. The authors also showed its effectiveness and feasibility via a number of computer simulation results.

Wang and Unoki [21], 2013, present an approach for audio watermarking based on the line spectral frequencies (LSFs) of the source audio signal. The line spectral frequencies from each frame were found with the use of linear prediction (LP). Then the watermark codes were inserted into them by using quantization index modulation (QIM). The authors studied the influence of the line spectral frequencies on the audibility or quality of the output signal extensively.

A study of the effect of MPEG compression on audio watermarking was carried out by **Artameeyanant** [22], 2010, who explored the principle of human hearing called the psychoacoustic model.

Elshazly, Fouad, and Nasr [23], 2012, tried to enhance the security and robustness of audio watermarking. The described approach is based on mean-quantization in DWT.

Finally, the use of fingerprinting was proposed by **Kamaladas and Dialin** [24], 2013, this method extracts the acoustic features of the speech signal and saves it as a fingerprint in a database. By using the fingerprint-matching techniques, the speech signals can be successfully identified.

2.3 Why Digital Watermarking?

It is obvious that keeping the watermark in the file header is highly undesirable for security reasons. This is mainly because anyone with a personal computer (PC), a laptop, or any other digital editing workstation would be able to change the intended information to another format and delete the watermark code at the same time. This clearly shows the importance and requirements of using watermarks in multimedia signals.

Figure 2 shows a general block diagram of the watermark embedding process. In this figure, Input Data 1 represents the original audio signal such as the speech signal or music signal, and Input Data 2 represents the watermark code such as a binary image. The watermark data may be produced by a production algorithm, which may use a secret key, a signature, or a combination of several secret keys and the original data. In other words, the standard procedure of watermarking starts with an embedding stage. At this stage, a cover media file is considered, and the watermarking information is embedded using a hidden key.

Both the watermark information and the hidden key have to be selected and must be available prior to the embedding stage [25, 26].

Finally, the output of the watermark algorithm represents the required watermarked data.

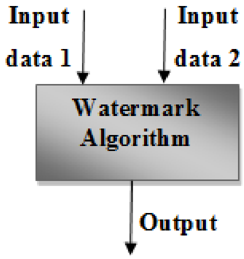

Figure 2: Block Diagram of the Watermarking Process

It is worth mentioning that Input Data 1 and Input Data 2 can be in any of the following data forms: text, image, video, or audio. These inputs as well as the watermark algorithm that will be considered in this thesis are audio-type watermarking. The other types of watermarking algorithms are outside the scope of this thesis.

Furthermore, a watermarking algorithm can be also divided into visible watermarking and invisible watermarking according to human perception [27]. In visible watermarking, the property of visibility is associated with perception by the human eye. In such a case, if the watermark code is embedded in the original information in a way that can be observed or seen without the extraction process, the watermark is called the visible kind. Examples of visible watermarks are logos that are widely used by commercial companies.

On the other hand, invisible watermarking is the approach whereby the code cannot be visualized by the human eye. Thus, it is more difficult to attack or break the code than in the visible approaches. The only thing that requires considerable attention is the issue of maintaining the quality of the original information. The digital watermarked information distributed over the Internet represents one example of invisible watermarking.

In the following, the most important requirements for digital watermarking are summarized [28]:

1. Invisibility: Here the invisibility may point to the similarity between the watermarked signal and the original signal. The watermark code should be invisible or inaudible as in the case of audio signals. In other words, the intended user should observe no visual or audio effect. On the other hand, a watermark code can be embedded in the original signal in a manner that can be easily observed without extraction. This type of watermarking is referred to as a visible watermark [28]. One common example of a visible watermark is logos.

2. Robustness: A watermark method becomes *robust* or strong if it can resist some well-known signal processing operations like filtering, de-noising, and compressing processes. In other words, the watermarked signal and the watermarked code should both be strong and unaffected by the aforementioned signal-processing operations.

3. Capacity: Here, capacity means that the watermarking algorithm may use a certain amount of bits embedded into the intended watermark signal. The number of bits of the watermark code that can be embedded in the intended watermark signal is called the data payload [28]. The data payload in the audio watermarking algorithm represents the number of bits encoded with the speech signal. The payload of the watermarked code should be sufficient to avoid some practical problematic issues.

4. Security: This is the most important issue in the topic under study. An attacker may try to get information regarding the watermark code or even change the watermarked signal. This kind of illegal use is a serious problem and full consideration should be given to it when using watermarking. In other words, for good security it should be hard or even impossible for an attacker to modify or change the watermarked signal without knowing the hidden watermark code.

5. Complexity: The computational complexity of a watermark approach mainly depends on the application. The embedding process of the watermark code can achieved only once and may be performed off-line [28]. Generally, the computational complexity of the encoding process is less important than the complexity of the decoding process. In some applications that require real-time decoding, the computational complexity of the watermark approaches should be as low as possible.

2.4 Watermarking Applications

In this section, we discuss some important applications of digital watermarking [28, 29]. One of the most important practical implementation of digital watermarking is copyright protection. This feature gains more importance in some special applications such as speech or audio watermarking. Generally, in the applications of audio watermarking it is required to add or input the required information regarding the copyright into the original signal without degradation of the quality of the original information. It is worth mentioning that the applications of audio watermarking demand high robustness [30].

The second application is the owner identification. As a proof of ownership, some important information regarding the identification of the owner may be inserted as a watermark code into the original signal. The applications of the owner identification need a high level of security [28, 29].

The third application is copy control. This application has a unique feature to prevent unwanted copying processes through a consumer-control mechanism. This control mechanism prevents unwanted or illegal copying and recording of the information by inserting a special watermark code called a “never-copy” watermark. It can also limit the number of times the information can be copied [28, 29].

The fourth application is the authentication. In this type of application, the aim is to have the possibility of observing or noting any modification of the original information so that the data needed to verify the content must be watermarked. This may be achieved through the use of a fragile watermark. It should be noted that a fragile watermark has low robustness to any modification [28].

The fifth application is fingerprinting. In this application of fingerprinting, the main goal is to track the source of unwanted or illegal copies so that the owner may insert a new and different watermark code into each copy that is given to each available customer [31].

The sixth application is broadcast monitoring. Generally in the media, advertisers use this type of application to be sure that broadcasters will air commercials at the time and location that they want according to the contracts. Watermark codes can be inserting into any form of digital information for broadcasting on network systems [31].

Another application is in biomedicine. In these applications, the watermarking code can be the full name of the patient and some other related personal information, which are unique on X-ray reports or MRI scan reports. This application is very important because it avoids or reduces the misplacement of medical reports, which are very important during treatment [32, 33].

There are also some applications in airports or airline monitoring. The use of watermarking approaches may also be effective in applications of airline-traffic monitoring, where the pilot may communicate with a ground station system via a voice or speech signal. This communication can easily attack. This may result in a breakdown of the communication between the pilot and the ground station. In order to overcome such problems, the flight number may be embedded into the speech signal during the communication between the ground station and the flight pilot. It is well known that the flight numbers are unique, and thus the tracking of flights will become more secure and easy [33, 34].

2.5 Watermarking in the Wavelet Domain

Generally, an advanced watermarking algorithm such as wavelet transform is typically more robust to audio manipulation compared to spatial domain techniques. This is because the transform domain does not use the original audio for embedding the watermark data. In addition, a transform domain algorithm spreads the watermark data over all parts of the speech signal. Additionally, frequency-domain-based techniques can embed a higher number of bits for watermarking. It is also more robust against attack. Furthermore, most audio signals can be easily transformed into the frequency domain.

Some transforms such as DCT and DWT are commonly used for watermarking in the frequency domain. In this thesis, we mainly use the DWT watermarking algorithms. The main reason to consider the DWT watermarking algorithms is that several multimedia standards such as JPEG2000 and MPEG-4 are based on the DWT [2, 3]. These new standards have brought new requirements such as progressive low-bit-rate transmission and region-of-interest coding. The following section gives more details and explanations about the wavelet transformations used.

2.6 Wavelet Transformations

One-dimensional (1D) signals such as speech can be analysed by using wavelet transformation. It is well known that wavelet transformations are widely used to compress data and to suppress noise. In the literature, this process is known as wavelet de-noising. Wavelet transformation of the 1D signal contains the information regarding the low-frequency content of the speech signal. This low-frequency content is called the *approximation coefficients*, while the information regarding the high-frequency content of the speech signal is called the *detail coefficients*. The wavelet transformation of the signal using the matrix method is described in the following sections.

2.7. Haar Transformation

For simplicity of presentation, let us assume a sinusoidal signal with a certain number of samples equal to *N*. In this case, the Haar matrix (*HM*) with size $N \times N$ and with the diagonal matrices filled up with the matrix given below [32].

$$\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{bmatrix}$$

$$HM = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \cdots & 0 & 0 \\ \frac{1}{2} & -\frac{1}{2} & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & & \frac{1}{2} & -\frac{1}{2} \end{bmatrix}_{NxN} \quad (2.1)$$

Also for simplicity, let us assume that $N = 8$ samples. In this case, the *HM* can be written as

$$HM = \begin{bmatrix} 0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.5 & -0.5 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.5 & 0.5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.5 & -0.5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.5 & 0.5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.5 & -0.5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & -0.5 \end{bmatrix}_{8x8} \quad (2.2)$$

Let us also assume that the signal that needs to be transformed consists of eight samples as in the following:

$$Signal = [S_1 \quad S_2 \quad S_3 \quad S_4 \quad S_5 \quad S_6 \quad S_7 \quad S_8] \quad (2.3)$$

Now, the HM given by Equation (2.2) is multiplied by the signal samples given by Equation (2.3). The result is called *first-level* decomposition, as shown in the following:

$$First\ Level = [S_1 \quad S_2 \quad S_3 \quad S_4 \quad S_5 \quad S_6 \quad S_7 \quad S_8].\begin{bmatrix} 0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.5 & -0.5 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.5 & 0.5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.5 & -0.5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.5 & 0.5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.5 & -0.5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & -0.5 \end{bmatrix} \tag{2.4}$$

Then, the result of the first-level decomposition of the Haar transformation is

$$App.Coff._{First\ Level} = \left[\frac{1}{2}(S_1 + S_2) \quad \frac{1}{2}(S_3 + S_4) \quad \frac{1}{2}(S_5 + S_6) \quad \frac{1}{2}(S_7 + S_8)\right] \tag{2.5}$$

These samples represent the average samples and they are commonly called approximation coefficients of the tested signal at the first level of decomposition. Meanwhile the following samples,

$$Det.Coff._{First\ Level} = \left[\frac{1}{2}(S_1 - S_2) \quad \frac{1}{2}(S_3 - S_4) \quad \frac{1}{2}(S_5 - S_6) \quad \frac{1}{2}(S_7 - S_8)\right] \tag{2.6}$$

are called the detail coefficients of the tested signal at the first level of decomposition.

Next, the above approximation coefficients of the tested signal which are obtained at the first level ($App.Coff._{First\ Level}$) are further decomposed using the Haar transformation matrix to obtain a new set of approximation and detail coefficients for the second level as in the following:

In this case, the *HM* in the second level of the signal decomposition is a 4 × 4 matrix:

$$HM_{Second\ Level} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} & -\frac{1}{2} \end{bmatrix}_{4x4} \tag{2.7}$$

Then the matrix ($HM_{Second\ Level}$) is multiplied by the approximation coefficients ($App.Coff._{First\ Level}$) which are represented by Equation (2.5) to obtain a new set of approximation coefficients of the tested signal at the second level of decomposition, as in the following:

$$App.Coff._{Second\ Level} =$$

$$\left[\frac{1}{2}(S_1+S_2) \quad \frac{1}{2}(S_3+S_4) \quad \frac{1}{2}(S_5+S_6) \quad \frac{1}{2}(S_7+S_8)\right] . \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & \frac{1}{2} & -\frac{1}{2} \end{bmatrix}_{4x4} \tag{2.8}$$

The result at this level of signal decomposition is

$$App.Coff._{Second\ Level} = \left[\frac{1}{4}(S_1+S_2+S_3+S_4) \quad \frac{1}{4}(S_5+S_6+S_7+S_8)\right] \tag{2.9}$$

Following the same procedure as above, we can get the detail coefficients at the second level of decomposition of the tested signal:

$$Det.Coff._{Second\ Level} = \left[\frac{1}{4}(S_1-S_2-S_3-S_4) \quad \frac{1}{4}(S_5-S_6-S_7-S_8)\right] \tag{2.10}$$

This process of signal decomposition can be repeated to any certain level. For ease of presentation, the Haar wavelet transformation and its approximate and detail coefficients of the speech signal are shown in Figure. 3. The parameters **a** and **b** which are shown in this figure represent the scale function and the wavelet function respectively.

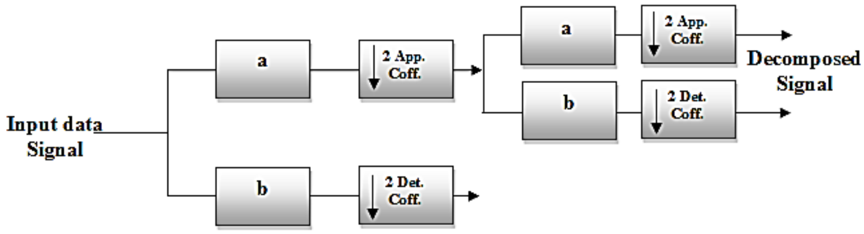

Figure 3: Block Diagram of the Haar Wavelet Transformation.

It is worth mentioning that the approximation coefficients at the first and second levels of the signal decomposition represent the low-frequency information derived from the tested signal, whereas the detail coefficients at the first and the second levels represent the high-frequency information derived from the tested signal.

All of the aforementioned coefficients

(that is, $App.Coff._{First\ Level}$, $App.Coff._{Second\ Level}$, $Det.Coff._{First\ Level}$, $Det.Coff._{Second\ Level}$)

contribute to reconstructing the original tested signal. This means that it is possible to reconstruct the original signal using these aforementioned coefficients of the tested signal.

The process of the reconstruction of the original signal is carried out by using the inverse Haar matrix (*IHM*). This process is summarized as follows:

1. First, the elements of the approximation $App.Coff._{Second\ Level}$ and detail coefficients $Det.Coff._{Second\ Level}$ at the second level are concatenated into a vector as in the following:

$$\left[\frac{1}{4}(S_1+S_2+S_3+S_4)\quad \frac{1}{4}(S_5+S_6+S_7+S_8)\quad \frac{1}{4}(S_1-S_2-S_3-S_4)\quad \frac{1}{4}(S_5-S_6-S_7-S_8)\right] \tag{2.11}$$

2. The inverse Haar transformation matrix (IHM) is applied:

$$IHM_{Second\ Level} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}_{4x4} \tag{2.12}$$

3. Then the multiplication process between the vector in step 1 and the matrix in step 2 is performed to get $App.Coff._{First\ Level}$ and $Det.Coff._{First\ Level}$.
4. Next, the inverse transformation matrix ITM2 is applied:

$$IHM_{First\ Level} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}_{8x8} \tag{2.13}$$

5. Finally, the vector obtained in step 3 above is multiplied by the matrix $IHM_{First\ Level}$ to reconstruct the original signal.

2.8. Results of Applying the Haar Transformation

In order to illustrate the abovementioned Haar transformation, consider the following sinusoidal signal:

$$x(n) = \sin(2\pi n) + \sin(2\pi 100 n) \tag{2.14}$$

In this signal, the number of samples is chosen to be equal to 512 samples and the sampling frequency Fs is chosen to be 512. The Haar transformation according to the aforementioned procedures is applied to this signal. The approximation and detail coefficients are obtained as described in the above equations. Figures 4 to 5 show the approximation coefficients (i.e., low-frequency information) and the detail coefficients (i.e., high-frequency information) at the second level of decomposition, while Figure 6 shows the reconstruction process of the original sinusoidal signal. The sinusoidal signal is reconstructed using inverse Haar transformation. From Figure 6, it can be clearly seen that the reconstructed and original signals are in very good agreement, which means that the reconstruction process has been done very precisely.

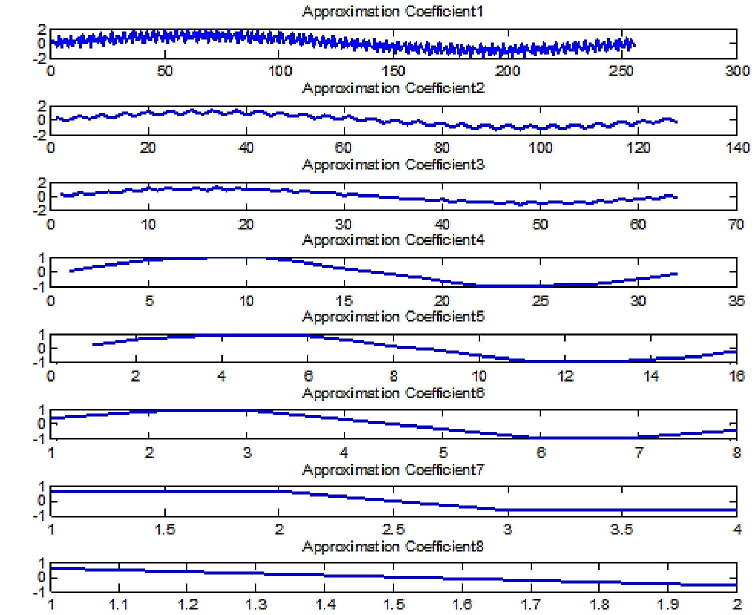

Figure 4: Approximation Coefficients Obtained Using Haar Transformation

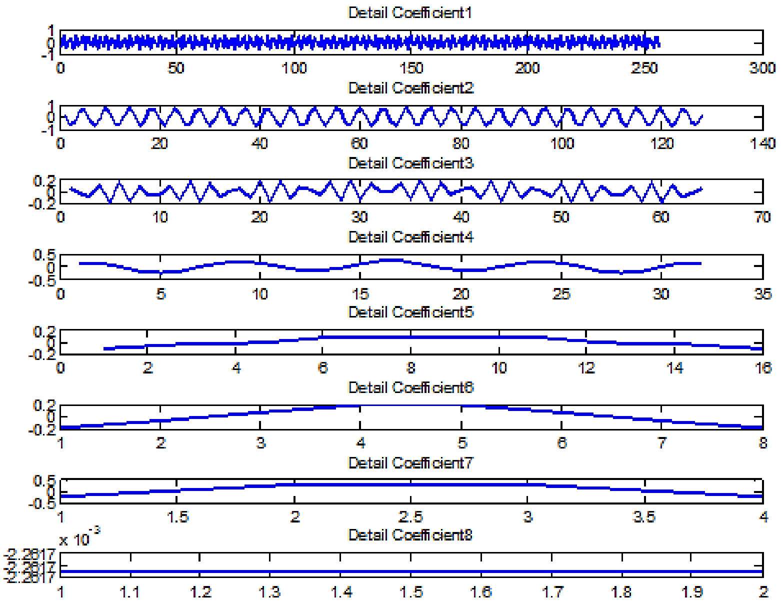

Figure 5: Detail Coefficients Obtained Using Haar Transformation

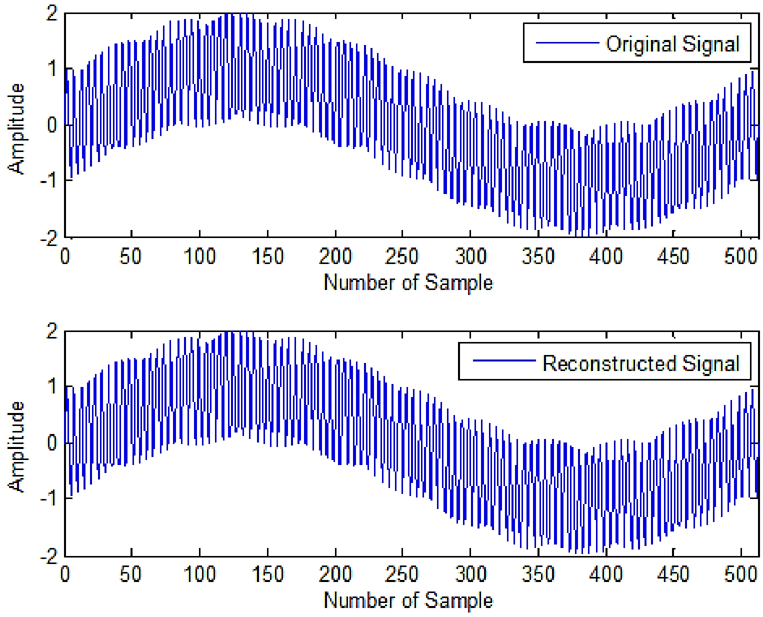

Figure 6: Original and Reconstructed Sinusoidal Signals Using Inverse Haar Transformation

2.9. Daubechies-4 Transformations

In this section, the same steps will be used to perform Daubechies-4 transformation. Here, the diagonal of the Daubechies-4 transformation matrix will be filled with

$[(1 + \sqrt{3}) / 4\sqrt{2}]$ $[(3 + \sqrt{3}) / 4\sqrt{2}]$ $[(3 - \sqrt{3}) / 4\sqrt{2}]$ $[(1 - \sqrt{3}) / 4\sqrt{2}]$

$[(1 - \sqrt{3}) / 4\sqrt{2}]$ $-[(3 - \sqrt{3}) / 4\sqrt{2}]$ $[(3 + \sqrt{3}) / 4\sqrt{2}]$ $-(1 + \sqrt{3}) / 4\sqrt{2}]$

Also, as in Section 2.7, let we consider a signal that consists of N samples. Here, the same steps are used to obtain the approximation and detail coefficients for the Daubechies-4 transformation case. Similarly, to recover the original signal, the inverse Daubechies matrix is formed.

2.10. Results of Applying Daubechies-4 Transformation

In order to illustrate the abovementioned Daubechies-4 transformation, we considered the same sinusoidal signal as in (2.14). However, here the number of samples was chosen to be 128 and the sampling frequency Fs was chosen to be 128. The Daubechies-4 transformation is applied to this signal according to the aforementioned procedures. The approximation and detail coefficients are obtained as described in the above equations. Figures 7 to 8 show the approximation coefficients (i.e., low-frequency information) and the detail coefficients (i.e., high-frequency information) at the second level of decomposition, while Figure 9 shows the reconstruction process of the original sinusoidal signal. The sinusoidal signal is reconstructed using inverse Daubechies-4 transformation. From Figure 9, it can be clearly seen that the reconstructed and original signals are in very good agreement, which means that the reconstruction process has been done very precisely.

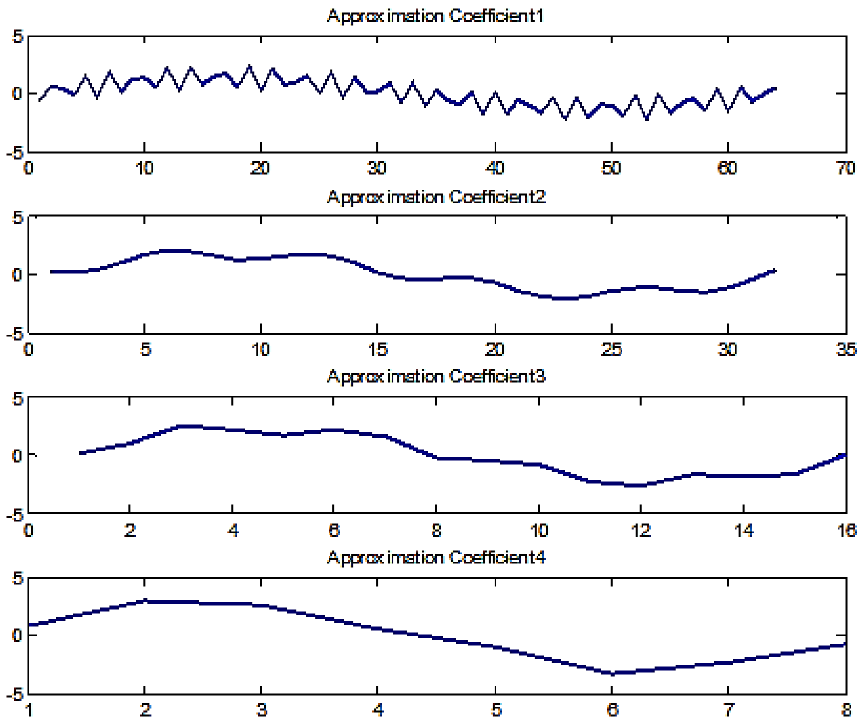

Figure 7: Approximation Coefficients Obtained Using Daubechies-4 Transformation

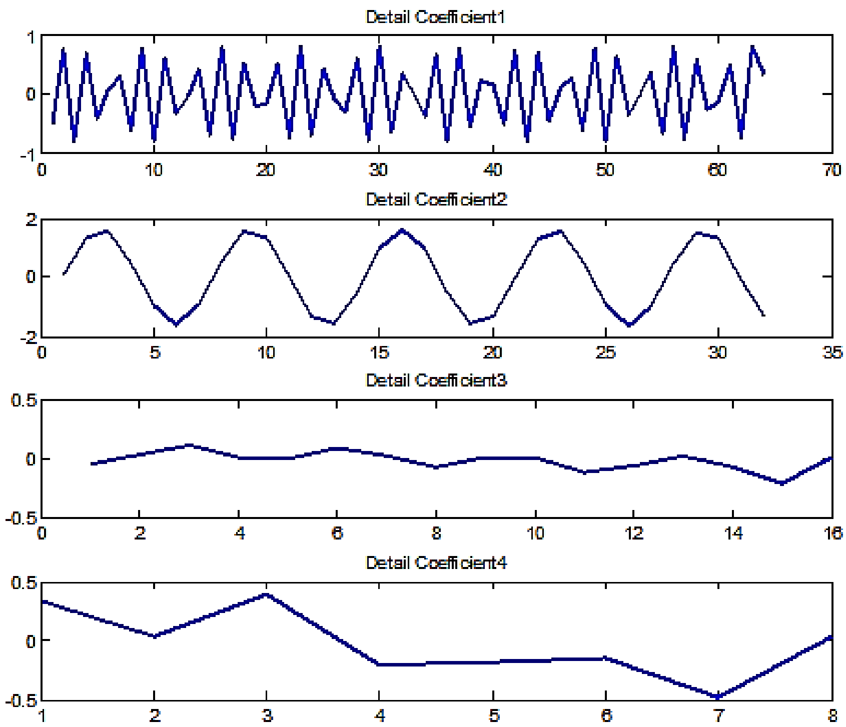

Figure 8: Detail Coefficients Obtained Using Daubechies-4 Transformation.

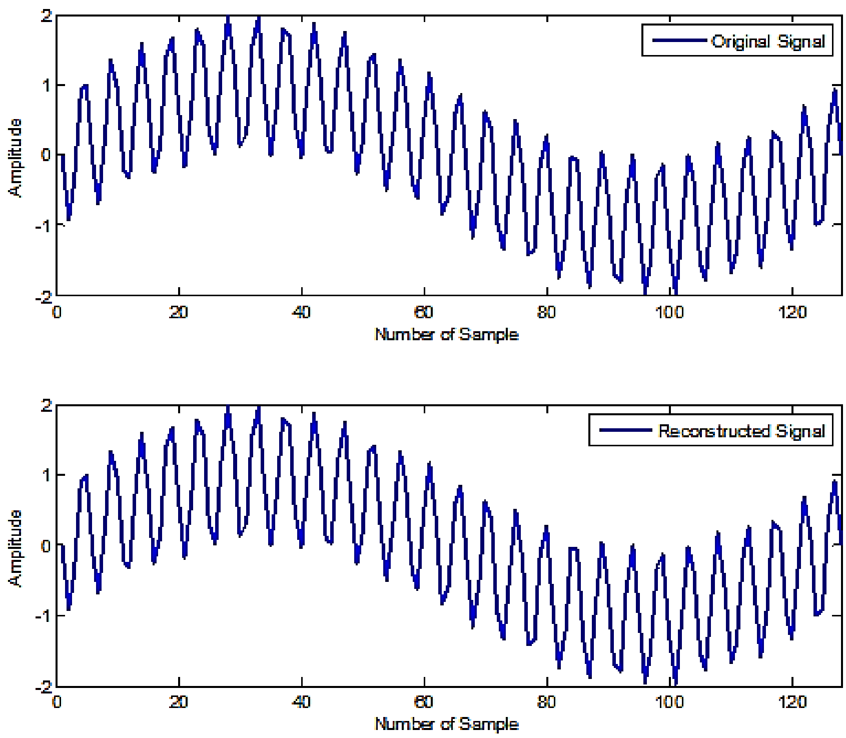

Figure 9: Original and Reconstructed Sinusoidal Signal Using Inverse Daubechies-4 Transformation

CHAPTER 3

STRUCTURE AND ANAYSIS OF THE PROPOSED WATERMARK APPROACH

First, since the wavelet transform approach, the Haar and Daubechies-4 transformations in particular have been widely used for watermarking in the frequency domain; these transformations have been extensively explained and presented in the previous chapter.

In this chapter, we mainly focus on the process of hiding a watermark code such as a binary image in an audio signal such as a speech or music signal. In this thesis, only binary images are considered as watermark codes, while all other types of images such as JPEG and MPEG are not considered. This is mainly because binary images contain a smaller number of pixels (where the values of the pixels are either 0 or 1 and the total number of the pixels may be easily chosen during the creation process of the binary image). By hiding these pixels in the recorded speech signal in a proper way, the original recorded speech signal will not much affected and its quality will remain at an acceptable level. That is why we only considered binary images. Moreover, in this chapter, the process of creation of specific binary images is described. Also, the process of hiding those binary images in the wavelet domain of the recorded speech signals is also presented.

3.1 Main Processes of Watermarking

Figure 10 shows a block diagram of the embedding process in the wavelet transform domain. First, the input audio signal is recorded by Matlab software and then transformed using Haar or Daubechies-4 transformations. It should be mentioned that it is not only the two aforementioned transformations that can be used (in other words, any other frequency domain transformation such as DCT can be also applicable). After creating the watermark code (or binary image) and specifying its pixels, this binary image is embedded in a transformed domain of the recorded audio signal. In other words, the pixels of the watermark code are properly inserted into the approximate and detail coefficients. Finally, inverse wavelet transformation is performed on the transformed watermarked audio signal.

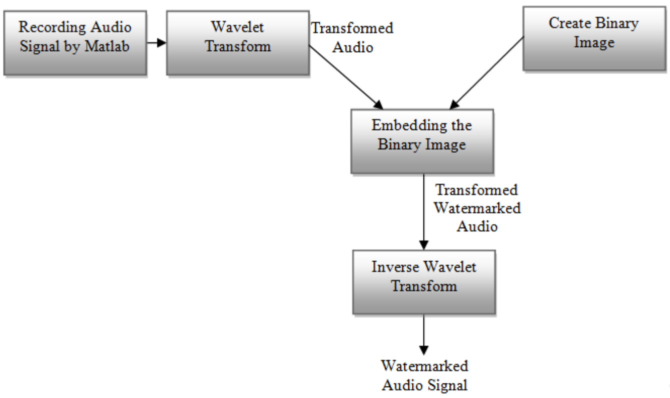

Figure 10: Block Diagram of the Watermark Embedding Process

The watermark extraction process is the inverse procedure of the watermark embedding process as shown in Figure 11. It can be seen from this figure that in order to extract the pixels of the binary image from the watermarked audio signal, first the watermarked and the original recorded audio signals are transformed using the wavelet transform. Second, the transformed original audio signal is subtracted from the transformed watermarked audio signal. This is because the binary image is the difference between the original audio signal and the watermarked audio signal. Finally, the similarity between the original watermark code (binary image) and the extracted watermark code is evaluated.

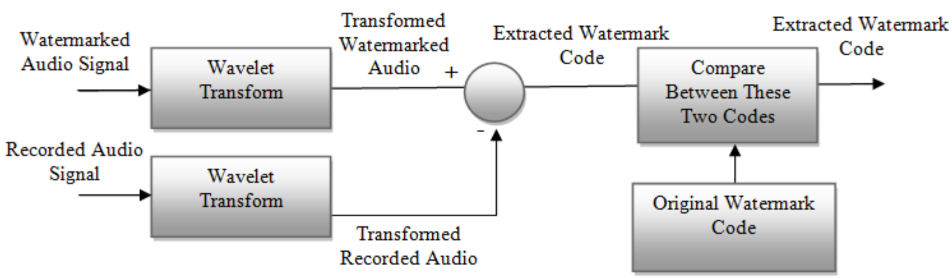

Figure 11: Block Diagram of the Watermark Extracting Process

From Figures 10 and 11, it should be noted that the transformation process (that is, the block of wavelet transform) is based on Ref. [32].

3.2 Principles of the Proposed Watermarking Approach

As mentioned before, the described watermarking approach consists of two processes as follows:

- Protection Process: Embedding the pixels of the binary image into samples of the recorded speech signal in a proper way so that the quality of the speech signal is preserved.
- Identification Process: Extracting the binary image from the watermarked speech signal.

More details about these two processes are given below. For the purpose of clearness and better presentation, Figure 10 is redrawn as Figure 12 to better emphasize the process of embedding the pixels of the binary image into samples of the recorded speech signal.

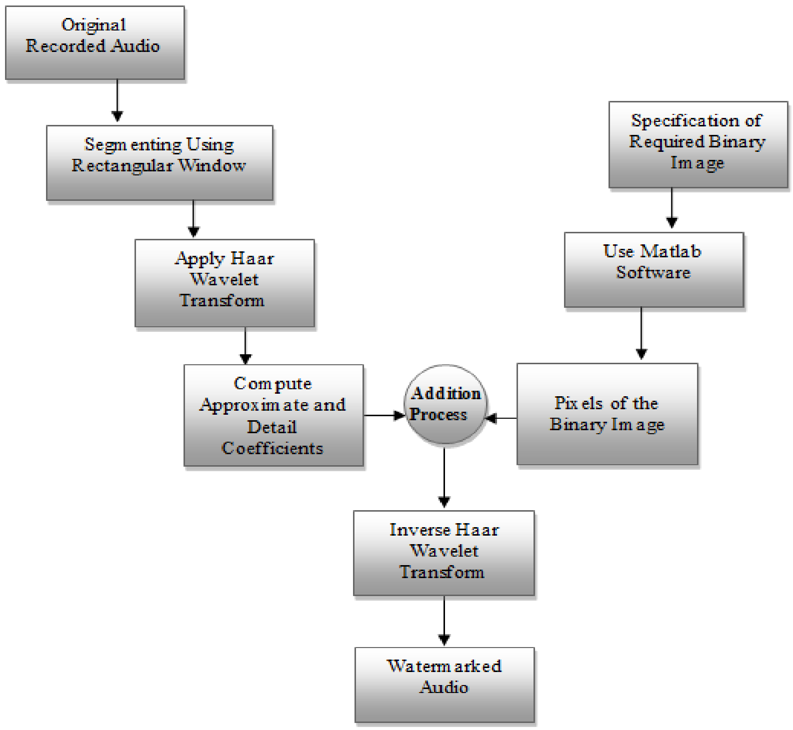

Figure 12: Block Diagram of the Proposed Watermarking Approach to Hide a Binary Image in a Recorded Audio Signal

According to Figure 12, the embedding process that is used in this thesis for binary image watermarking in a speech signal consists of the following steps:

Step 1: The required audio signal that needs to be watermarked for the purpose of protection is prepared. This audio signal is recorded by Matlab software and sampled with a specific sampling rate equal to 11025 Hz. In order to achieve this step, the following Matlab commands are used.

```
clear all; clc; close all;
Fs = 11025; %  sampling rate
y = wavrecord (n,Fs)
wavwrite (y,Fs,'D:\Cankaya.wav')
wavplay(y,Fs)
```

On the other hand, the binary image is created by the following Matlab command

```
I = imread('rakan.bmp');
imshow(I)
title('Binary Image');
```

Step 2: Then the recorded audio signal is divided into segments, where each segment consists of 4487 samples. Every segment of the recorded speech signal is transformed or decomposed using either Haar or Daubechies-4 wavelet transformation or any other transformation. For more details about these transformations, see Chapter 2 of this thesis. The process starts by inserting the first pixel of the binary data collected from the binary image (because it is a binary image, the value of each of its pixels is either 1 or 0) into the third-level detail coefficients that are obtained using wavelet decomposition of the first segment of the recorded speech signal. This is done by changing the values of the third-level detail coefficients such that the mean or average of the third-level detail coefficients is modified to a new value. This new value may be represented by $m + e$ if the binary value is ‘1’ or a value of $m - e$ if the binary value is ‘0’. Here the parameter m

represents the mean of the third-level detail coefficients and the parameter *e* represents a constant number. Its value is chosen to be equal to the value of one fifth of the energy of the third-level detail coefficients. Note that the value of the variance should remain the same so that the quality of the recorded speech signal is preserved. The process of inserting the watermark code into the wavelet domain of the speech signal is based on the idea of Ref. [7], while the Matlab code used to perform this insertion process is adopted from [32].

Step 3: This process is repeated for the other segments of the recorded speech signal in order to hide the complete pixels obtained from the binary image.

Step 4: After completing the above steps, the result is that the pixels of the required watermark code or binary image will be completely hidden in the wavelet domain of the recorded speech signal.

Step 5: For the purpose of identification, the hidden watermark binary code can be recovered easily by comparing the mean of the corresponding detail coefficients computed before and after hiding, as shown in Figure 11. If the value of the average of the third-level detail coefficient of the specific segment corresponding to the original recorded speech signal is greater than the average of the third-level detail coefficients of the respective segment corresponding to the watermarked speech signal, the value of the pixel will be considered as ‘1’; otherwise, its value will be considered as ‘0’. All these estimated values of the pixels will be stored to construct or recover the hidden watermark code.

Step 6: Note that the total number of samples (or period) of the original recorded speech signal is chosen such that all the binary pixels collected from the binary image are hidden properly in the recorded speech signal.

It is worth mentioning that in this way the length of the original recorded speech signal used for hiding the binary image data is set to be equal to 11488 samples.

It is repeated 100 times so that the length of the recorded speech signal becomes equal to 1148800 samples. The size of the binary image (total number of pixels) used in this thesis is chosen to be equal to 45 × 45. The binary image is stored at the rate of 1 pixel in each segment that consists of 256 samples of the recorded speech signal.

The flowchart of the Matlab program used to implement the proposed watermark approach is shown in Figure 13. The experimental results of the proposed watermark approach are presented and discussed in the following chapter.

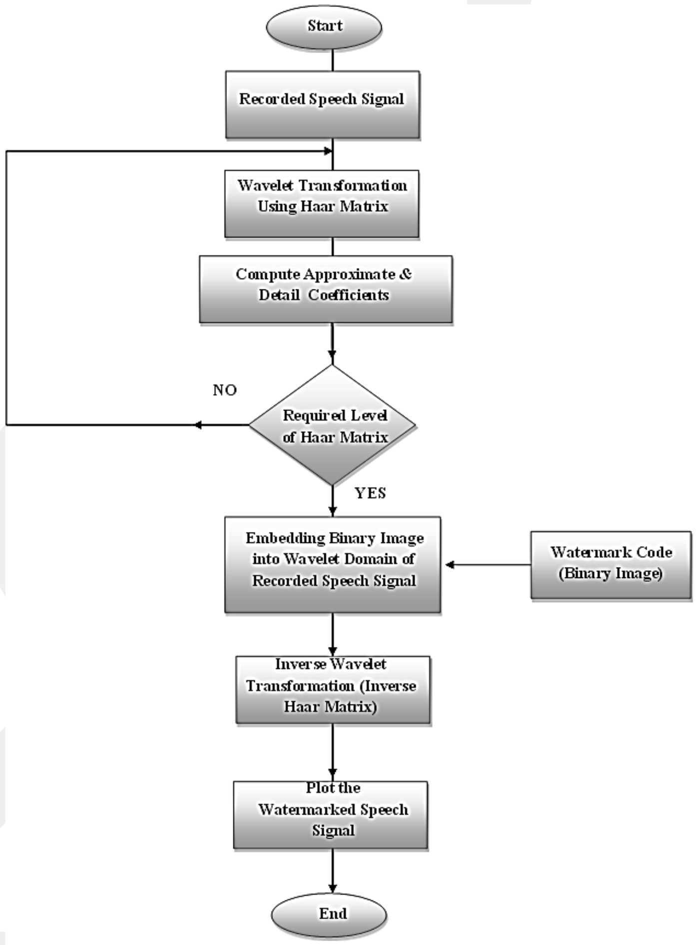

Figure 13: The flowchart of the Matlab program used to implement the proposed watermark approach

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Results of the Proposed Watermarking Approach

In order to validate the performance of the described approach of watermarking, extensive computer simulations carried out by means of Matlab software are presented in this chapter. Regarding the audio signals, this research work used recorded speech signals of 2 s length. Moreover, some music signals were also used. Generally, the sampling frequency was chosen to be equal to 11025 Hz. The original recorded speech and music signals were decomposed up to the fourth level using either Haar or Daubechies-4 wavelet matrix transformations and both approximate and detail coefficients were selected to embed the pixels of the watermark code or binary image. Here, the first binary image is like a square geometrical shape. Figure 14 shows the original recorded speech signal of a sentence or word "rakan". This figure also shows the watermarked speech signal after embedding the binary image or watermark code. The difference between the original and watermarked speech signals is also displayed in this figure. For this particular example, the watermark code or binary image of 45 × 45 pixels is shown in Figure 15.

Figure 16 shows the results of watermarking a speech signal of a sentence or word "cankaya" with the binary image "square". In another experiment, we record a music signal and we want to watermark it. The music signal that is used is a melody signal, which is an audio signal but is completely different from a speech signal. This melody signal is played and we used Matlab commands to record it. In this case, the binary image is chosen to be in the shape of "rakan". Figures 17 and 18 show the results of watermarking a melody music signal with the binary image "rakan".

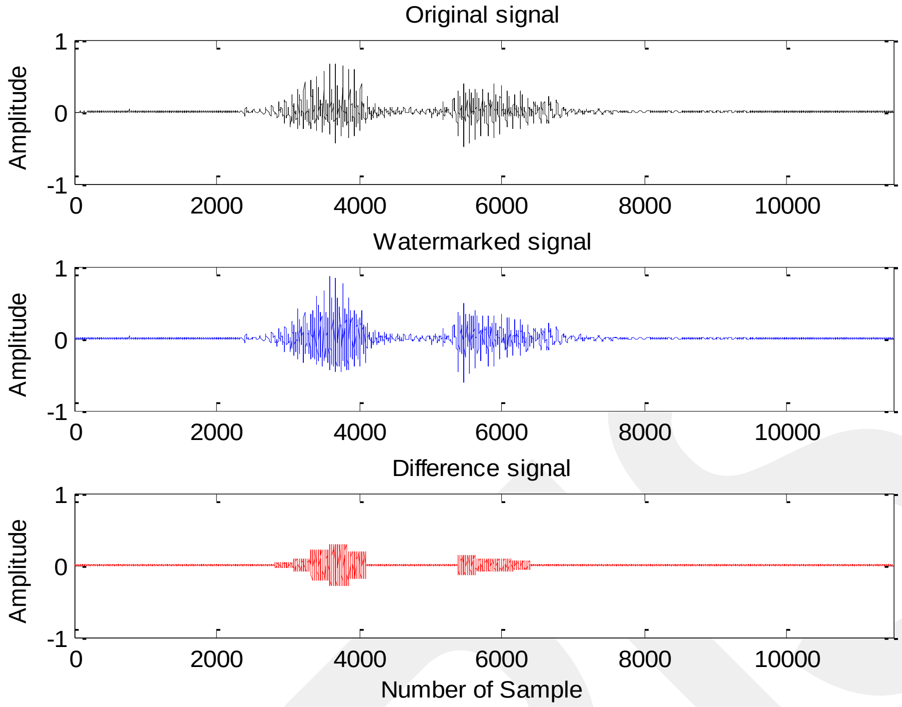

Figure 14: Speech signal "rakan" before and after watermarking with the binary image "square"

The signal shown in the top of this figure represents the recorded speech signal "rakan" without the watermark code, while the middle signal represents the watermarked speech signal (the output signal of the proposed approach which is shown in Chapter 3, Figure 12). This signal contains the binary image "square", which is invisible.

The signal on the bottom of Figure 14 represents the difference between the recorded speech signal and the watermarked speech signal. This difference signal is one way to show the performance of the proposed watermark approach. For good performance, its amplitude should be as small as possible but it can never be zero since the pixels of the binary image have been added to the samples of the recorded speech signal.

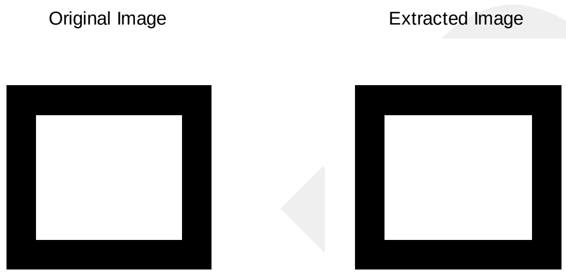

Figure 15: Getting the binary image from the watermarked speech signal

The figure on the left side of Figure 15 represents the binary image that will be used for the purpose of watermarking in the embedding process, while the figure on the right side represents the watermark code extracted during the extraction process, which is explained in Chapter 3, Figure 11.

It can be seen that the two figures (on the left and right sides) are identical to each other. This is exactly true for the case where none of the signal processing operation attackers were considered.

On the other hand, the extracted watermark code will be slightly different from the original one when considering some attackers such as AWGN.

Figure 16 shows the watermarking process of another recorded speech signal, "cankaya", with the binary image "square". Here, the same observation as for Figure 16 is noted. Also, we note that the amplitude of the difference signal is higher than that of Figure 14.

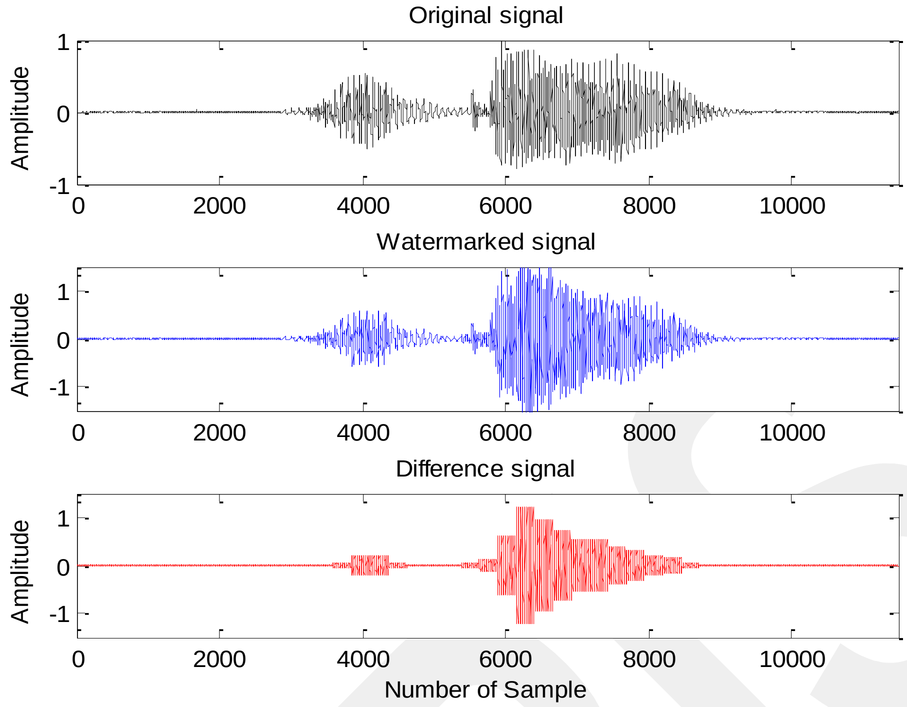

Figure 16: Speech signal "cankaya" before and after watermarking with the binary image "square"

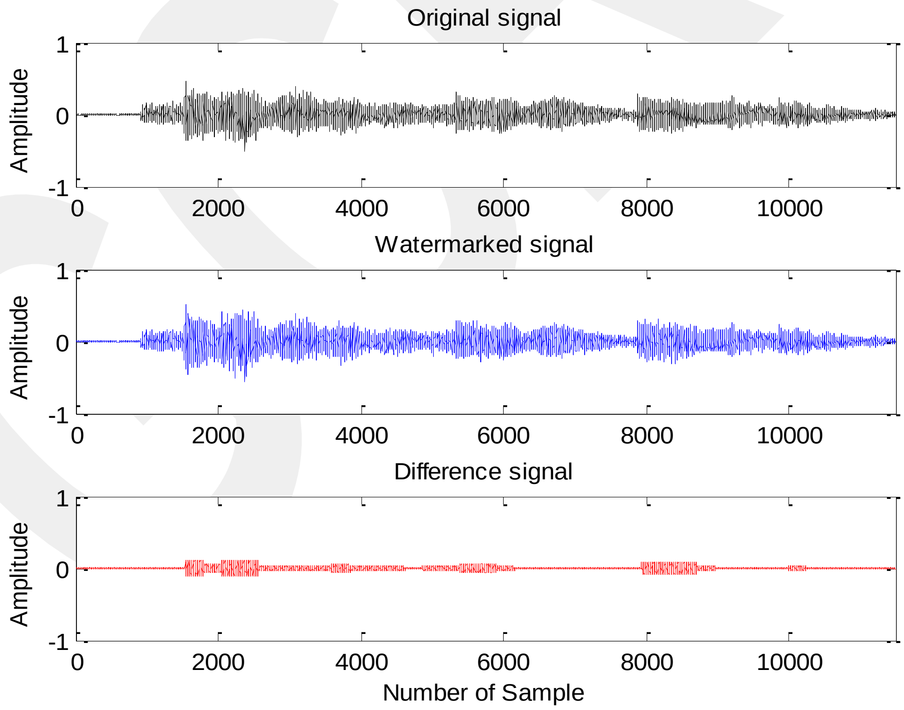

Figure 17: Music signal "melody" before and after watermarking with the binary image "rakan"

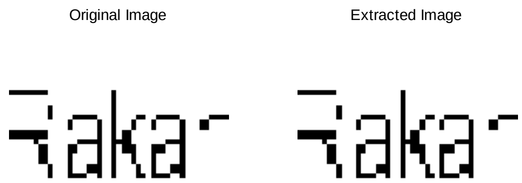

Figure 18: Getting the binary image from the watermarked music signal

Figures 17 and 18 represent the results of another type of audio signal, the music signal. This music signal is chosen to be a melody, which is played back by an audio player and then recorded by Matlab software. We chose the recording time to be only 2 s so that the number of samples would be moderate and the run time of the Matlab code would be not too long. The main observations from these two figures are as follows:

The difference signal between the recorded melody signal and the watermarked melody signal is small. This means that the quality and audibility of the watermarked melody signal are good. This is true since the waveform of the watermarked melody signal is identical to that of the recorded melody signal.

In this example, the binary image of the watermark code is chosen to be "rakan". The number of pixels is chosen to be 45 × 45, and thus some pixels of the word "rakan" have been omitted.

Also, the hidden binary image is recovered or extracted from the watermarked melody signal and compared with the original one.

The Matlab code used to get the above results is adopted from [32]. Appendix A shows the Matlab code used to obtain the results depicted in Figures 14 to 18.

It is worth mentioning that the quality of the watermarked audio signal could be further improved by considering a new audio signal with a large number of samples. In this case, the relative amount between the numbers of pixels of the binary image inserted into the samples of the audio signal will be large enough to further increase the quality of the watermarked audio signal. Similarly, we may also reduce or increase the number of pixels of the binary image and note its effect on the watermarked signal.

4.2 Performance Comparison of the Proposed and Related Watermarking Approaches

In order to fully validate the performance of the proposed approach, it should be compared with some other existing watermarking approaches. In addition, it is also necessary to investigate the performance of the proposed watermarking approach under different signal processing operations (attackers). The most common attackers considered in this thesis are AWGN, filtering, and compression.

For comparison purposes, we need to define some essential performance measures. The most commonly used measures are the Signal-to-Noise Ratio (SNR) and Normalized Correlation (NC).

The SNR evaluates the quality of the watermarked audio signal, while the NC measures the similarity (or correlation) between the original watermark code (the created binary image) and the extracted watermark code. In mathematical equations, these two performance measures are defined as [7]:

$$SNR = 10\ log \frac{\sum_{n=0}^{N-1} S(n)^2}{\sum_{n=0}^{N-1}\left[S(n) - S(\acute{n})\right]^2} \tag{4.1}$$

where $S(n)$ represents the original recorded speech or music signal, $S(\acute{n})$ represents the watermarked speech or music signal (i.e., the output of the proposed watermark approach), and $S(n) - S(\acute{n})$ represents the difference signal that was plotted previously in Figures 16, 18, and 19. The variable N stands for the total number of samples in the recorded speech signal, which is chosen to be 11448 by Matlab.

$$NC = \left| \frac{\sum_{i=1}^{I} \sum_{j=1}^{J} B(i,j) * B(\acute{i},\acute{j})}{\left(\sum_{i=1}^{I} \sum_{j=1}^{J} \left(B(i,j) * B(\acute{i},\acute{j})\right)\right)^{0.5}} \right| \quad (4.2)$$

where $B(i,j)$ represents the original watermark code created (binary image), $B(\acute{i},\acute{j})$ represents the hidden watermark code which is recovered during the extraction process, and the variables I and J stand for the pixel's location.

It is worth mentioning that, in the ideal case (no attackers), the value of the NC is 1 and the value of the SNR is about 50 dB.

Test Audio Signal	Watermark Approach	Without Attackers		AWGN Attack		Compression		Low Pass Filtering		High Pass Filtering	
		SNR in dB	NC	SNR in dB	NC	SNR in dB	NC	SNR in dB	NC	SNR in dB	NC
Speech	DCT reported in [11]	45.9	1	18.7	0.63	16.7	0. 81	15.9	0.48	12.3	0.34
Music		43.5	1	19.8	0.72	16.9	0.87	16.9	0.47	17.7	0.33
Speech	DWT reported in [14]	49.8	1	22.3	0.71	21.9	0.89	21.7	0.57	21.1	0.55
Music		49	1	22.7	0.79	22.3	0.91	23.5	0.61	22.1	0.64
Speech	DCT+DWT reported in [15]	52.6	1	27.5	0.99	27.9	0.97	28	0.82	25.8	0.72
Music		55	1	28.2	0.99	27.7	0.97	27.9	0.89	24.9	0.78
Speech	Proposed Approach Using Haar	50	1	25.11	0.89	24.8	0.96	23.6	0.81	23.2	0.73
Music		51	1	25	0.94	24.8	0.95	24.3	0.8	22.9	0.72
Speech	Proposed Approach Using DB4	50.4	1	26.05	0.93	25.9	0.98	25.9	0.84	24.6	0.77
Music		55.1	1	27.4	0.97	28	0.99	26.4	0.89	26.1	0.74
Speech	Mitra's Approach [28]	50	1	20.7	0.87	20.	0.95	19.9	0.74	16.8	0.52
Music		51	1	23.4	0.89	22	0.91	21.6	0.76	15.9	0.56

Table 1: Performance Comparison of the Proposed and Related Watermarking Approaches under Different Signal Processing Operations (Attackers)

From this table, several notes may be observed:

- All the watermarking approaches including the proposed approach perform quite well under the no-attacks condition.
- The proposed watermarking approach based on both Haar and Daubechies-4 transformations has superiority in its performance in terms of both SNR and NC compared to some other existing watermark approaches.
- Only the watermark approach based on DCT + DWT has better performance than the proposed watermark approach in all cases of attackers.
- The performance in terms of the SNR and NC of all approaches including the proposed watermarking decreases dramatically for the filtering (especially high-pass filter) attackers.
- The process of watermark-code (binary image) recovery becomes difficult under some operations of signal-processing attackers. This leads to a requirement to search for new approaches that are more robust.
- It is clear from this table (SNR values in rows 9–12) that the effectiveness of the proposed watermark approach for maintaining the quality of the watermarked speech or music signals is achieved.
- Generally, audio watermarking is harder than image watermarking due to quality concerns. Since the quality of the speech signals is maintained, the main objectives of this thesis are achieved.

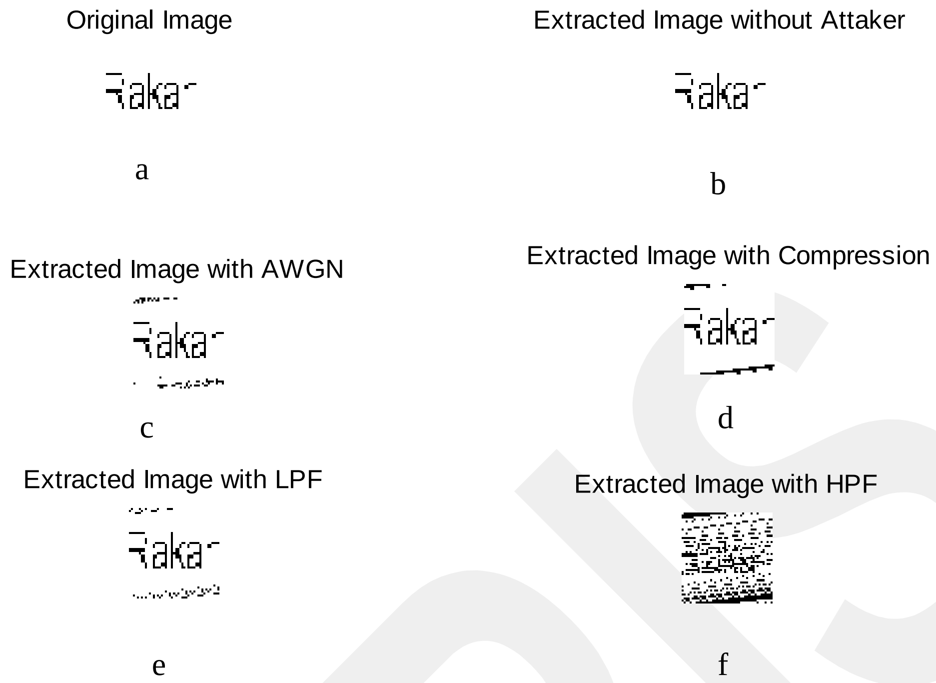

Figure 19: Performance Comparisons of Different Watermarking Approaches in Extracting the Hidden Code "Rakan" and under AWGN Attackers.

In this figure, (a) represents the original binary image, (b) represents the binary image extracted by the proposed approach under the no-attacks condition (the NC value is equal to 1), (c) represents the extracted binary image under an AWGN attacker (NC = 0.76), (d) represents the extracted binary image under a compression attacker (NC = 0.75), (e) represents the extracted binary image under a low-pass filter attacker (NC = 0.96), and (f) represents the extracted binary image under a high-pass filter attacker (NC = 0.67).

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

5.1 Conclusions

Audio watermarking is a newly advancing field of study and its importance is rapidly increasing. Positive and concrete benefits gathered from obtainable experimental results presented in Chapter 4 increase the popularity of audio watermarking. Application fields of digital watermarking expand too. Although it seems to fit the audio recording field best, watermarking also applies to biomedical, modern, and secure communication systems.

This study shows a basic yet useful application of watermarking employing the fundamentals and algorithms of digital audio watermarking.

Watermarking approaches have received a lot attention in the current and last decades. This is mainly because of the fast development of the technology, as there is more demand to transmit a huge amount of data over the Internet. Watermarking can be employed in digital media such as text, image, video, and audio. Audio watermarking is more difficult than video or image watermarking due to some dynamical characteristics phenomena of the human auditory system or hearing compared to the human eye or visual system.

Nowadays, audio watermarking is an interesting topic and has become a new line of research around the world. In this thesis, a simple application of watermarking is applied to speech and music signals and is limited to a binary image watermark code. The proposed watermarking approach was implemented on real recorded audio signals. Moreover, the proposed approach as well as some related watermarking approaches that are considered in this research work is in the frequency domain, which is more efficient and has more advantages than any other domain. It is well known that time-domain watermarking approaches have many disadvantages compared to the frequency-domain-based watermarking approaches. Its greatest disadvantages are that it has less bit capacity and is not robust enough for some signal-processing applications such as filtering and compression operations.

On the other hand, frequency- or transform-domain-based watermarking approaches have proved their effectiveness and robustness for some signal-processing operations or attackers. In this thesis, the performances of some common transforms such as DCT and DWT for achieving digital audio watermarking are compared. The digital wavelet transforms include Haar and Daubechies-4. The effectiveness of the proposed watermarking approach was demonstrated by watermarking two different audio signals: speech and melody music. The experimental results show the power of the proposed approach compared to some other existing approaches where the quality of the watermarked speech signal is preserved. In addition, the watermark code (binary image) was recovered during the extraction process with an acceptable value of the normalized correlation (NC) even under an attack. Thus, the proposed watermarking approach may be considered as a robust approach. The attackers that are considered in the experimental results of this thesis are some operations of the signal processing such as AWGN, filtering, and MP3 compression.

5.2 Future Work

In this section, we discuss some future works in which new lines of research work may be opened. The first line of research may include the use of neural networks in audio watermarking. The use of neural networks may raise the complexity of the algorithm, as discussed in Chapter 2. However, an improvement in the security and some other good features may be obtained by the use of neural networks.

The second line of future research may concentrate on making the proposed approach more practical by modifying it in such a way that the recorded speech signal is not required for the extraction process to recover the hidden binary image. In addition, the proposed approach may also be applied to video or image watermarking.

The third line of future research may include the use of an effective encryption algorithm to encrypt the watermark code. This line of research is desirable in some applications that require high security.

Further research can be carried out on deploying an effective watermarking approach in tracking systems such as CCTV where it is necessary to embed a watermark code in the recorded video clips. In such applications, the security and protection of the recorded video sequences are the main challenging problems.

This list of future works may open new horizons in this field of audio watermarking.

REFERENCES

1. **Li X., Zhang M., & Zhang R., (2004),** "*A New Adaptive Audio Watermarking Algorithm*", in Proceedings. 5th World Congress on Intelligent Control and Automation, WCICA 4, Hangzhou, China, pp. 4357–4361.

2. **Sruthi N., Sheetal A. V., & Elamaran V., (2014),** "*Spatial and Spectral Digital Watermarking with Robustness Evaluation*", in Proceedings of the International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), pp. 500–505.

3. **Potdar V. M., Han S., & Chang E., (2005),** "*A Survey of Digital Image Watermarking Techniques*", in IEEE Proceedings of the 3rd International Conference on Industrial Informatics (INDIN 2005), pp. 1–8.

4. **Jiansheng M., Sukang L., & Xiaomei T., (2009),** "*A Digital Watermarking Algorithm Based on DCT and DWT*", in IEEE Proceedings of the International Symposium on Web Information Systems and Applications, Nanchang, P. R. China. pp. 67-75.

5. **Sonoda K., & Sek A., (2013),** "*Digital Watermarking Method Based on STFT Histogram*", in IEEE Proceedings of the Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 287–290.

6. **Tang X., Niu Y., Yue H., & Yin Z., (2005),** "*A Digital Audio Watermark Embedding Algorithm with WT and DCT*", in Proceedings of MAPE 5, Beijing, China, pp. 970–973.

7. **Kaengin S., Pathoumvanh S., & Airphaiboon S., (2008),** "*Binary Image Watermarking on Audio Signal Using Mean-Quantization and Wavelet Transform*", in Proceedings of ISBME 2008, Bangkok, Thailand, pp. A-18.

8. **Seitz J., (2005),** Digital Watermarking for Digital Media. Information Science Publishing, London. pp. 119-124.

9. **Cai D., & Gopalan K., (2014),** "*Audio Watermarking Using Bit Modification of Voiced or Unvoiced Segments*", in IEEE Proceedings, pp. 501–506.

10. **Khayam S. A., (2003),** The Discrete Cosine Transform (DCT): Theory and Application, Michigan State University. pp. 203-209.

11. **Chen W-Y & Huang S.-Y., (2000)**, Digital Watermarking Using DCT Transformation, pp.98.

12. **Namazi F., Karami M. R., & Ramazannia S. B., (2012),** "*Block Based Adaptive Image Watermarking Scheme Using Visual Perception Model in DCT Domain*", International Journal of Computer Applications, vol. 4, pp. 41–45.

13. **Lai C. C., (2011),** "*An Improved SVD-Based Watermarking Scheme Using Human Visual Characteristics*", Optics Communications, vol. 14, pp. 938–944.

14. **Singh A. K., Dave M., & Mohan A., (2013),** "*Performance Comparison of Wavelet Filters against Signal Processing Attacks*", in IEEE Proceedings of the 2nd International Conference on Image Information Processing, pp. 695–698.

15. **Hong-yan A., Quan L., & Xue-mei J., (2013),** "*Synchronization Audio Watermarking Algorithm Based on DCT and DWT*", in IEEE Conference Anthology, pp. 1–4.

16. **Nin J., & Ricciardi S., (2013),** "*Digital Watermarking Techniques and Security Issues in the Information and Communication Society*", in IEEE Proceedings of the 27th International Conference on Advanced Information Networking and Applications Workshops, pp. 1553–1558.

17. **Khalil M., & Adib A., (2014),** *"Embedding and Extracting Multiple Watermarks in Audio Signals using CDMA*", in IEEE Proceedings. pp. 117-126.

18. **Zeki A. M., Ibrahim A. A., Haruna C., & Ya'u Gital A., (2013),** "*Investigating the Dynamics of Watermark Features in Audio Streams*", in IEEE Proceedings of International Symposium on Industrial Electronics and Applications, Kuching, Malaysia. pp. 442-446.

19. **Zhang P., Li Y., Fan Y., Jiang J., Ma X., & Hao Q., (2013),** "*Robust Audio Watermarking Based on Frequency-Domain Spread Spectrum using CAZAC Sequence*", in IEEE Proceedings of the Sixth International Conference on Advanced Computational Intelligence, Hangzhou, China, pp. 23–26.

20. **Li C., & Fucheng Y., (2013),** "*The Study on Digital Watermarking Based on Word Document*", in IEEE Proceedings of the International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC), Shenyang, China, pp. 2265–2268.

21. **Wang S., & Unoki M., (2013),** "*Watermarking Method for Speech Signals Based on Modifications to LSFs*", in IEEE Proceedings of the Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 283–286.

22. **Artameeyanant P., (2010),** "*Wavelet Audio Watermark Robust Against MPEG Compression*", SICE Annual Conference, Kagawa University, Japan, pp. 1375–1378.

23. **Elshazly A. R., Fouad M. M., & Nasr M. E., (2012),** *"Secure and Robust High Quality DWT Domain Audio Watermarking Algorithm with Binary Image*", in IEEE Proceedings, pp. 207–212.

24. **Kamaladas M. D., & Dialin M. M., (2013),** "*Fingerprint Extraction of Audio Signal Using Wavelet Transform*", in IEEE Proceedings of the International Conference on Signal Processing, Image Processing and Pattern Recognition (ICSIPR), pp. 308–312.

25. **Chan A. K., Liu S. J., & Chui C. K., (1998),** "*Wavelet Toolware Software for Wavelet Training*", Academic Press, San Diego. pp. 71-76.

26. **Chen B., & Wornell G. W., (2001),** "*Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding*", IEEE Transactions on Information Theory, vol. 47, no. 4, pp. 1423–1443.

27. **Hofbauer K., & Hering H., (2007),** "*Noise Robust Speech Watermarking with Bit Synchronization for the Aeronautical Radio*", LNCS 4567, Springer-Verlag Berlin Heidelberg, pp. 252–266.

28. **Abbasfard M., (2009),** "*Digital Image Watermarking Robustness: A Comparative Study*", M.Sc. thesis, Department of Computer Engineering, Delft University of Technology, The Netherlands. pp. 33-37.

29. **Ravula R., (2010),** "*Audio Watermarkıng Using Transformatıon Technıques*", M.Sc. thesis, Electrical Engineering, Graduate Faculty of the Louisiana State University and Agricultural and Mechanical College, USA. pp. 119.

30. **Zhou Z., & Zhou L., (2007),** "*A Novel Algorithm for Robust Audio Watermarking Based on Quantification DCT Dom*ain", Third International Conference on International Information Hiding and Multimedia Signal Processing, vol. 1, pp. 441–444.

31. **Katzenbeisser S., & Petitolas F., (2004),** Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, no. 2.

32. **Gopi E. S. (2007),** Algorithm Collections for Digital Signal Processing Applications Using Matlab, Springer, Netherlands, vol. 190.

33. **Vassiliadis S., Wong S., Gaydadjiev G., Bertels K., Kuzmanov G., & Panainte E. M. (2004),** "*The Molen Polymorphic Processor*", IEEE Transactions on Computers, vol. 190, pp. 1363–1375.

APPENDINCES

APPENDIX A

This appendix shows the Matlab program of the proposed watermarking approach which has the following processes:

A1. Inserting Process

```
%%%% This Code Perform the Inserting Process Accorrding to the Block Diagram of
%%%% Figure 12 in the Thesis
close all; clc; clear all

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%   Without Attacker
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
original_signal= wavread ('D:\original_music.wav');original_signal_size=size(original_signal)
original_signal=repmat(original_signal,100,1);% this command replicate 100 times original cankaya
wave
AA_size=size(original_signal)
original_signal=original_signal';
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%   First Attacker: AWGN
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%snr=40; % signal to noise ratio
%original_signal = awgn(original_signal,snr);
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%   Second Attacker: Comparession
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%aaa = lpc(original_signal,3); % find the coffecients of the compressor
%original_signal = filter(aaa,1,original_signal); % The output is Compressed Watermarking Signal
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%   Third Attacker: Low and High Filtering
%%%%%%%%%%%%%%%%%%

%bb = fir1(48,[0.01 0.99]);    % Low Pas Filter
%original_signal = filter(bb,1,original_signal);
%bb = fir1(48,0.29,'high');   % High Pass Filter
%original_signal = filter(bb,1,original_signal);
```

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%

%%%%%%%%% Performing the Segmantation and finds approxmate and detial coff of wavelet
transform   %%%%%%%%%%%
len=fix(length(original_signal)/256) % the fraction parts after division will be zero
for k=1:1:len-1
temp=original_signal((k-1)*256+1:1:(k-1)*256+256);
col{k}=daub4water(temp);% This function will finds approxmate and detial coff of wavelet transform
end

%%%%%%%% read the created watermark code   %%%%%%%%%
I=imread('rakan.bmp');I_size=size(I)
figure
imshow(I);title('Original Image')
I=I(1:1:45,1:1:45)
I=reshape(I,1,45*45); I_length=length(I)

%%%%%%% This Part of code has been taken from Ref [32]
for k=1:1:length(I)
switch I(k)
case 0
 temp=col{k}{2}{3};
 e=sum(temp.^2)/5;
 m=mean(temp); % average value
 v=var(temp);  % variance
 col{k}{2}{3}=mean_var_norm(temp,(m-e),v);
case 1
 temp=col{k}{2}{3};
 e=sum(temp.^2)/5;
 m=mean(temp);
 v=var(temp);
 col{k}{2}{3}=mean_var_norm(temp,(m+e),v);
end
end
s=256;
watermarked_signal=[];
for k=1:1:length(I)
approx=col{k}{1};
det=col{k}{2};
app=approx{log2(s)-2};
for i=(log2(s)-2):-1:1
a=[app;det{i}];
a=reshape(a,1,size(a,1)*size(a,2));
a=[ a(length(a)-1:1:length(a)) a];
app=createdaubinvmatrix(length(a)-2)*a';
app=app';
end
watermarked_signal=[watermarked_signal app];
end
%watermarked_signal1=watermarked_signal;
```

```
%save watermarked_signal1 watermarked_signal1 % save the data of watermarked signal
%%%%%% Plot the results   %%%%%%%%%%%
figure
subplot(3,1,1)
plot(original_signal(1:1:11488),'k');
axis([0 11488 -1 1]);
%xlabel('Number of Sample');
ylabel('Amplitude ');
%legend ('Original Signal');
title('Original signal')
subplot(3,1,2)
plot(watermarked_signal(1:1:11488),'b');
axis([0 11488 -1 1]);
ylabel('Amplitude ');
title('Watermarked signal');
wavwrite(watermarked_signal,11025,'D:\Repeated_music_with_watemarkrcode_rakan.wav')
NN=11488;
AA=wavread('D:\Repeated_music_with_watemarkrcode_rakan.wav', NN);
wavwrite(AA,11025,'D:\music_with_watemarkrcode_rakan.wav')
subplot(3,1,3)
plot(watermarked_signal(1:1:11488)-original_signal(1:1:11488),'r')
axis([0 11488 -1 1]);
xlabel('Number of Sample');
ylabel('Amplitude ');
title('Difference signal')

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%% Calculate the value of SNR According to eq 4.1
%%%%%%%%%%%
AA=original_signal.^2;
sum1=sum(AA); % sum of samples of the original signal
diff=watermarked_signal(1:1:11488);
diff2=diff.^2;
sum2=sum(diff); % sum of samples of the difference signal

SNR=5*log10(abs(sum1/sum2))
```

A2. Extracting Process

```
%%%% This Code Perform the Extracting Process Accorrding to the Block Diagram of
%%%% Figure 11 in the Thesis
% size of the Binary image is 45x45
clear all; clc; close all;
original_signal= wavread ('D:\original_music.wav');
original_signal=repmat(original_signal,100,1);
original_signal=original_signal'; % take the transpose
len=fix(length(original_signal)/256);
for k=1:1:len-1
temp=original_signal((k-1)*256+1:1:(k-1)*256+256);
```

```
col1{k}=daub4water(temp);
end
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%   Without Attacker
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

load watermarked_signal % watermarked cankaya with square code
original_signal=watermarked_signal;
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%   First Attacker: AWGN
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%snr=40; % signal to noise ratio
%original_signal = awgn(original_signal,snr);

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%   Second Attacker: Comparession
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%aaa = lpc(original_signal,3); % find the coffecients of the compressor
%original_signal = filter(aaa,1,original_signal); % The output is Compressed Watermarking Signal

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%   Third Attacker: Low and High Filtering
%%%%%%%%%%%%%%%%%%
%bb = fir1(48,[0.2 0.8]);    % Low Pas Filter
%original_signal = filter(bb,1,original_signal);
%bb = fir1(48,0.31,'high');   % High Pass Filter
%original_signal = filter(bb,1,original_signal);

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%% This Part of code has been taken from Ref [32]
len=fix(length(original_signal)/256);
for k=1:1:len
temp=original_signal((k-1)*256+1:1:(k-1)*256+256);
col2{k}=daub4water(temp);
end
temp=[];
for k=1:1:45*45
m1=mean(col1{k}{2}{3});
m2=mean(col2{k}{2}{3});
if(m1>m2)
temp=[temp 0];
else
temp=[temp 1];
end
end
temp1=reshape(temp,45,45);
```

```
%%%%%%%% Plot the original binary image %%%%%%%%%
I=imread('rakan.bmp');
I_size=size(I);
figure (1)

%subplot (1,2,1)
imshow(I);title('Original Image')

%%%%%%%% Plot the extracted binary image %%%%%%%%%
%subplot(1,2,2)
figure (2)
imshow(temp1);title('Extracted Image with attaker LPF')
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%% Calculate the value of nc
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
sum1_I=sum(I);
sum2_I=sum(sum1_I) % sum of the original binary image
sum1_E=sum(temp1);
sum2_E=sum(sum1_E) % sum of the extracted binary image

Nc=abs(sum2_E/sum2_I)  % Find the Value of Normalized correlation according to eq. 4.2
```

APPENDIX B

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: RASHID, Rakan Saadllah

Date and Place of Birth: 06 April 1983, Ninawa

Marital Status: Married

Phone: +90 536 596 07 27

Email: c1279508@cankaya.edu.tr

EDUCATION

Degree	**Institution**	**Year of Graduation**
M.Sc.	Çankaya Univrsity., Information Technology	2014
B.Sc.	Alhadba Univrsity., Computer Science	2006
High School	Al-Kndi High School	2002

WORK EXPERIENCE

Year	Place	Enrollment
2006 July	Bardarash Technical Institute. Department of The Computer System	Lecturer
2010 May	IREX Org.	Trainer

FOREIGN LANGUAGES

Kurdish, Arabic, English, Beginner Turkish.

HOBBIES

Football, Travel, Swimming.