Bachelor of Science in Computer Science & Engineering

Audio Watermarking Based on Discrete Tchebichef Transform and Singular Value Decomposition

by

Anjan Halder

ID: 1404048

Department of Computer Science & Engineering

Chittagong University of Engineering & Technology (CUET)

Chattogram-4349, Bangladesh.

April, 2021

Audio Watermarking Based on Discrete Tchebichef Transform and Singular Value Decomposition

Submitted in partial fulfilment of the requirements for
Degree of Bachelor of Science
in Computer Science & Engineering

by

Anjan Halder
ID: 1404048

Supervised by

Dr. Kaushik Deb
Professor
Department of Computer Science & Engineering

Chittagong University of Engineering & Technology (CUET)
Chattogram-4349, Bangladesh.

The thesis titled **'Audio Watermarking Based on Discrete Tchebichef Transform and Singular Value Decomposition'** submitted by ID: 1404048, Session 2018-2019 has been accepted as satisfactory in fulfilment of the requirement for the degree of Bachelor of Science in Computer Science and Engineering to be awarded by the Chittagong University of Engineering and Technology (CUET).

Board of Examiners

____________________________ Chairman

Dr. Kaushik Deb
Professor
Department of Computer Science and Engineering
Chittagong University of Engineering and Technology (CUET)

____________________________ Member (Ex-Officio)

Dr. Md. Mokammel Haque
Professor and Head
Department of Computer Science and Engineering
Chittagong University of Engineering and Technology (CUET)

____________________________ Member (External)

Dr. Md Ibrahim Khan
Professor
Department of Computer Science and Engineering
Chittagong University of Engineering and Technology (CUET)

Declaration of Originality

This is to certify that I am the sole author of this thesis and that neither any part of this thesis nor the whole of the thesis has been submitted for a degree to any other institution.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. I am also aware that if any infringement of anyone's copyright is found, whether intentional or otherwise, I may be subject to legal and disciplinary action determined by Dept. of CSE, CUET.

I hereby assign every rights in the copyright of this thesis work to Dept. of CSE, CUET, who shall be the owner of the copyright of this work and any reproduction or use in any form or by any means whatsoever is prohibited without the consent of Dept. of CSE, CUET.

Signature of the candidate

Date:

Acknowledgements

First and foremost, I want to express my gratitude to God for providing me with the health and well-being that allowed me to finish this project. I'd like to express my heartfelt appreciation to my respected project supervisor, Dr. Kaushik Deb, Professor, Department of Computer Science Engineering, Chittagong University of Engineering Technology for providing me the perfect guidance, encouragement, instructive suggestions with all of the requisite facilities for study and thesis preparation. I'd like to take this opportunity to express my heartfelt gratitude to Dr. Asaduzzaman, Head and Professor of the Department, Department of Computer Science Engineering, Chittagong University of Engineering Technology, for the kind encouragement. I am also thankful to our external, Dr. Md Ibrahim Khan, Professor, Department of Computer Science Engineering, Chittagong University of Engineering Technology, for his support and feedback on our project. I'd like to take this opportunity to thank all of my Department's faculty members and seniors for their assistance and encouragement. I'd like to express my gratitude to my parents for their unwavering love, motivation, and attention. I'd like to express my gratitude to everyone who has contributed to this project, whether directly or indirectly.

Abstract

In the present world, Digitalization in information and technology has been promoted in many fields like telemedicine, banking, shopping, office work, broadcasting etc. The availability of data transmission through internet has been increased because of the increasing speed of internet. Nowadays hospital, bank, telecommunication require a huge data transmission in shortest time. The transmitted data can be corrupted during transmission through internet and the copyright of the data can be infringed. For this, data transmission requires more safety. The process of hiding invisible data in multimedia material such as images, audio, video, and text is known as digital watermarking. Spatial domain and frequency domain watermarking techniques can be used to embed watermark in a digital content. In terms of imperceptibility and robustness, frequency domain techniques have proven to be more efficient. DWT, DCT, DFT are most commonly used frequency domain approaches used in digital watermarking. Based on Discrete Tchebichef Transform (DTT), we proposed an audio watermarking method. In our proposed method, the host audio was divided into some blocks. The grayscale watermark image was converted into binary values. DTT was applied on the every block of audio. After that, Singular Value Decomposition (SVD) was applied. Then we embedded watermark to the host audio with embedding equation. With the extraction algorithm, watermark was extracted as it is. We have also applied several attacks such as AWGN, Resampling, Requantization, Low pass filter, Invertion, Cropping, MP3 Compression etc. From the experiment result and comparative analysis with other existing methods, we observed that our proposed audio watermarking scheme achieves good quality and we can recover the watermark exactly. It also shows excellent robustness and resists all kind of attacks.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

Digital watermarking is a technique for protecting information by inserting certain information into multi-media items such as images, video, and audio. It is used to protect copy-right information. It gives the authenticity of owner rights. It is done with minimum perceptual disturbance.

In the present world, Digitalization in information and technology has been promoted in many fields like telemedicine, banking, shopping, office work, broadcasting etc. The availability of data transmission through internet has been increased because of the increasing speed of internet. Nowadays hospital, bank, telecommunication require a huge data transmission in shortest time. The transmitted data can be corrupted during transmission through internet. The wide amount of transmitted data can be modified and the copyright of the data can be infringed. For this, data transmission requires more safety.

Depending on the application, the watermark must either be robust or fragile. If even small changes to a watermark cause it to fail to be detected, it is called fragile. 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. Semi-fragile watermarking is a hybrid of fragile and robust watermarking. It allows some content preserving modification while is sensitive against malicious modification. For these reasons, semi fragile watermarking is suitable tamper detection and image authentication.

Recently much importance has been given to content tampering detection using the digital watermark technique. Because there is no need for using separate file or data for detecting tampering and the process is fairly secure. To detect tampering and protect digital data from malicious manipulation various novel watermarking scheme has been proposed in the literature.

1.2 Difference between cryptography, steganography and watermarking:

Cryptography means sender converts plain text to cypher text by using encryption key and other side receiver decrypts the cypher text to plain text using decryption key. In this process, there remains no host to hide information. So, Cryptography is not so secure to hide information.

Steganography means hiding information into a cover image without altering the information. In this process, there is a cover image to hide information. But this procedure is also not so secure.

Watermarking is a method of incorporating knowledge into multi-media objects such as images, video and audio to protect the information. But in this process, the hiding information is also altered or scrambled to make it more secure.

1.3 Basic Concept of Digital Watermarking

The digital watermark is the information that will be encoded in a signal, and the host signal is the signal where the watermark will be embedded. Watermark embedding, attack, and watermark extraction are the three main steps in a watermarking scheme.

An algorithm embraces the host and data to be embedded and generates a watermarked signal.

The watermarked signal is then transmitted or processed, normally over the internet or another network medium to another user. Attack or tampering occurs when this individual or the medium by which it is transmitted makes a change.

Extraction, also known as detection, is an algorithm that extracts the watermark from an attacked or watermarked signal. The watermark is still present and can be extracted if the signal was not altered during transmission. Figure 1.1 clearly describes the watermarking life cycle.

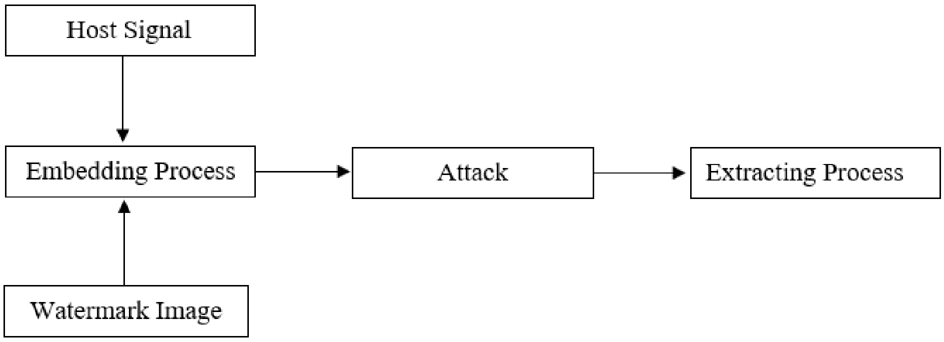


Figure 1.1: Watermarking life cycle

1.4 Types of Digital Watermarking

In terms of implementation areas and uses, there are several different forms of watermarking techniques. Generally they are divided into the following categories:

1.4.1 According to Host Media

According to attached media/host signal there can be five types of watermarking approaches and they are:

- Image watermarking: This is used to mask unique details in images so that it can be detected and extracted later to prove the author's ownership.
- Video watermarking: This applies a watermark to the video stream in order to monitor video applications. It's a form of image watermarking that's been extended. This approach necessitates real-time extraction and compression robustness.
- Audio watermarking: Due to internet music and MP3, audio watermarking has become one of the most common and hot topics.
- Text watermarking: This applies a watermark to PDF, DOC, and other text files in order to avoid text changes. The font form, as well as the space between

characters and line spaces, are used to embed this watermark.

• Graphis watermarking: It adds a watermark to 2D or 3D computer graphics to signify that they are protected by copyright.

1.4.2 According to Robustness

According to robustness there can be three types of watermarking approaches and they are:

1.4.2.1 Robust Watermarking

The aim of a robust watermarking algorithm is to mix an imperceptible data with host signal that can be obtained even after modification. Robust watermarking has applications in many areas such as:

• Evidence of ownership and identity: A watermark containing the content owner's identification details may be inserted in the host media to prove or recognize copyright ownership.

• Transaction tracking/fingerprinting: The owner can insert a unique watermark, into each copy of the media which for example identifies the recipient and used to trace the source for redistribution that is not permissible.

• Copy control/prevention: Another common piracy scenario is illegal copying or recording. One possible solution is to provide a never-copy watermark that, when detected by the recording device's detector, prevents further recording.

• Broadcast monitoring: Marketers can track whether or not the advertisements they have paid for are transmitted by the broadcasters according to the contracts by embedding a watermark that is to be broadcasted along with the host media in the advertising applications.

1.4.2.2 Fragile Watermarking

Fragile watermarks are vulnerable to both malicious and non-malicious manipulations, and are supposed to be fully lost when manipulated. They can be used for the following purposes:

- Authentication: Through embedding a fragile watermark that marks the source or producer in the media, legitimate recipients of the marked media may search for the existence of the source's or producer's watermark and verify the validity of the received media.

- Content-integrity verification: The inclusion of a delicate watermark in the original media enables the content's legitimacy to be checked by the appropriate parties. Fragile watermarking is used in medical image archiving, media monitoring of criminal cases, and accident scene capture for insurance and forensic purposes.

1.4.2.3 Semi Fragile Watermarking

Only when the manipulations on the watermarked media are considered malicious by the schemes are these watermarks meant to be fragile. Semi-fragile watermarking scheme plays an important role in facilitating authentication and content-integrity verification for multimedia applications where content-preserving operations are popular. The ability to differentiate between content-preserving operations and malicious attacks is a difficult challenge for semi-fragile schemes.

1.4.3 According to Perceptibility

- Imperceptible: When the original cover signal and the marked signal are perceptually indistinguishable, the digital watermark is said to be imperceptible.

- Perceptible: If the presence of a digital watermark in the marked signal is visible, it is called perceptible.

1.4.4 According to Domain

There are two forms of watermarking methods, depending on the domain:

- Spatial domain: The pixels of one or two randomly selected subsets of images are modified in this domain. It loads the raw data directly into the image pixels. Some of its algorithms are based on LSB and SSM Modulation.

- Frequency domain: This method is also known as transform domain. The original values of those frequencies are modified. DCT, DWT, and DFT are some of the most widely used transform domains.

1.4.5 According to Detection Process

According to detection process there are two types of watermarking approaches and they are:

- Non-blind watermarking: It needs original media for watermark detection.

- Blind watermarking: It does not include original media, but it does necessitate a more advanced watermark technology.

1.5 Properties of Digital Watermark

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

- Imperceptibility: If the original signal and the marked signal are perceptually indistinguishable, the digital watermark is imperceptible. It is not detectable by bare human eyes or ear. It remains hidden in content and can be detected only by authorized agencies. A digital watermark is said to be perceptible if its presence in the marked signal can be detected.

- Security: The watermarking procedure should be secured. It can depend on secret keys to ensure protection, but not on the algorithm's confidentiality, so pirates cannot detect or delete the 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: The watermark should be robust to some degree of manipulation. Practically no perfect method has been proposed so far that can withstand against all kind of attacks or signal processing operations. But a robust watermark should be able to withstand the basic operation and some attacks to a reasonable limit.

1.6 Applications

Watermarking is used for:

- Copyright Protection
- Copy Protection
- Digital right Management
- Temper Proofing
- Broadcast Monitoring
- Fingerprinting
- Access Control
- Media Application
- Image and Content Authentication
- Automation and Privacy Control
- Media Forensics
- Communication Enhancement
- Content Protection for Audio and video Content
- Content Filtering
- Communication of Ownership and Objects
- Document and Image Security
- Locating Content Online
- Improve Auditing

1.7 Motivation

In the recent years, it becomes very problematic to have right ownership details as newer means to copy and attack audio has emerged. So, it creates the need of watermarking for authenticating the ownership of the audio.

1.8 Objective of Proposed Schema

- To develop an algorithm for a robust audio watermarking.
- To completely recover the original image from the watermarked audio.

- To embed a grayscale image into audio file so that the owner can get a way to hide more information than previous methods.
- To develop a more robust watermarking method against any intentional and unintentional attack.

1.9 Contribution of the thesis

There are many watermarking techniques have been published. But not enough in audio watermarking. Again, in Discrete Tchebichef Transform (DTT), no audio watermarking techniques have been published yet.

In this thesis, we have proposed an audio watermarking technique in DTT.

Most of audio watermarking techniques, binary image has been used as watermark. But in this thesis, we have used grayscale image as watermark.

1.10 Thesis Organization

This thesis is divided into six chapters. This chapter briefly discussed a general watermarking scheme and its properties and its basic concepts along with 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 image and audio watermarking and tamper detection of images are 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 well-known properties and performance metric.

Chapter 6 concludes the thesis with mentioning the goal achieved by this research work and future recommendations.

Chapter 2

Literature Review

2.1 Introduction

In the modern communication system, the rate of using digital devices like computers, multimedia players and other communication medias are rapidly increasing thoroughly. So, a huge amount of data is being shared and stored through internet or other mediums. Naturally, such wide amount of digital data is creating security and ownership problem as digital multimedia resources can easily be edited by various software tools and anyone can claim the ownership.
Digital watermarking is used as an effective tool to ensure the authenticity of the real owner or resources. Digital Watermarking mainly tracks down the unauthorized copies. The main feature of Digital Watermarking lies in it's embedding process. If a watermark is embedded successfully then it will remain in the signal forever. So, Digital Watermarking ensures the detection of original ownership, tampering and protect digital data from malicious manipulations.
To ensure the copyright protection of the audio signal and to stop audio tempering a new kind of Watermarking was introduced which is known as Audio Watermarking.
Here in this context, we have proposed an audio watermarking scheme.

2.2 Related Literature Review

In literature, many watermarking algorithms have been proposed for hiding information. Normally digital watermarking has three techniques such as fragile watermark technique, semi-fragile watermark technique and robust watermark technique. Basically, most of the algorithms are developed for robust watermark technique. Some basic watermarking techniques such as DCT, DWT etc. have been discussed in [1], [2] and [3].

In general, digital watermarking techniques are classified into two categories according to the processing domain of the host signal. They are: spatial domain watermarking and transform or frequency domain watermarking.

In spatial domain methods, watermarking is performed by modifying the pixels values in the host image which is considered as a straightforward method. The watermarking algorithm in spatial domain is generally fragile to common image processing operations or attacks. Some spatial domain watermarking techniques have been discussed in [4] ,[5] and [6].

However, in frequency domain methods, the watermark is embedded into transformed coefficients of the image. Frequency domain methods are found to be more robust and complex than spatial domain ones. Also they are visually more convenient to human and have higher imperceptibility and capacity. The computational cost is higher in the frequency domain methods. So, it is better to develop an algorithm for watermark embedding in frequency domain.

All kinds of digital media may be protected in order to guarantee ownership and copyrights identification and hence watermarking can be applied on digital videos, audios, images or documents.

Image watermarking techniques are those techniques where host signal is a image. Image can be color or grayscale. Many image watermarking techniques have been published. Of them, Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform(DWT) are well known. DWT watermark techniques are discussed in [7] and [8]. DCT watermark technique is discussed in [9]. In [10], A watermarking technique was published where DCT and DWT techniques are used in a body. This method was far better than previous methods. Some other image watermarking techniques are discussed in [11], [12], [13] , [14], [15], [16], [17], [18] and [19].

Audio watermarking is a watermarking technique where host signal is an audio. Nowadays many researchers are trying to use audio as host of the watermark due to some reasons. For example, it is difficult for a attacker to imagine that watermark information is hidden in an audio file than an image file. Again not enough audio watermarking techniques have been published yet. For these reasons, we have proposed an audio watermarking method.

In Audio watermarking, many transformation techniques have been published. Like image watermarking, basic audio watermarking techniques are DCT, DWT, DFT and so on. DCT watermarking technique have been discussed in [20] and [21]. In [20], audio file was divided into some subsection. Then Discrete Cosine Transform (DCT) was applied in every subsection. Then image watermark was embedded into the higher energy value in every subsection.

DWT watermarking technique have been discussed in [22] and [23]. In [23], two level Discrete Wavelet Transform was applied an audio file. Then grayscale image watermark was embedded into detail sub-band which was found after two level DWT. Some other audio watermarking techniques have been published in [24], [25], [26], [27], [28], [29] and [30].

In [31], Discrete Tchebichef Transform (DTT) was published for image watermarking. Here image was first divided into blocks. Then DTT was applied in each block. After that, watermark image was embedded into the blocks. However, DTT is far better than DCT. Again DCT is very common in audio watermarking. DTT has not been used in any audio watermarking technique yet. For this reason, we have proposed an audio watermarking method in DTT.

Decomposition is a method where one single value will be decomposed into two or more values. For this reason, we get twice or thrice number of given values after decomposition. So, it is more secure to embed watermark into decomposed values. Many decomposition techniques have been stablished in mathematics.

Different types of decomposition techniques also used in digital watermarking. Singular value decomposition (SVD) [1], [8], [10], [17], [24], [27] is used in most of the proposed schemes. Other decomposition technique includes QR decomposition [14] and [26], LU decomposition [32], schur decomposition [33] and so on.

Among all decompositions, SVD is best. Because, it is a very easy way to decompose in SVD. In SVD, values are decomposed into three parts and multiplying those values it gets back to the original values. Largest singular values are always found in the first position. For those reasons, we have used SVD as decomposition in our proposed watermarking scheme.

2.3 Conclusion

In audio watermarking, grayscale image is used as watermark in a little amount of techniques that have been published. As we know that it has more watermark information in a grayscale image than a binary image, we have used grayscale image as watermark in our proposed scheme.

2.3.1 Implementation Challenges

1. Increasing the embedding capacity.
2. Recovering the watermark image exactly after extraction.
3. Increasing robustness and imperceptibility.
4. Embedding a grayscale image as watermark.

Chapter 3

Methodology

3.1 Introduction

From the previous chapter it can be seen that not only many image watermarking schemes but also many audio watermarking schemes have been proposed. Problem with image watermarking schemes is the distortion between the watermarked image and the cover image caused by data hiding process. Any distortion in the original image can cause a large problem in some sensitive issues such as military images, medical images. It is necessary to get the original image back after extracting the watermark image. So, it is relatively better to hide data in audio as it is more secure. This watermarking scheme allows the user to hide a grayscale image into an audio file. For this reason, the watermark can be huge size if the owner wants. It is desired that the watermarking will be enough imperceptible and robust. This thesis proposes an audio watermarking method where the watermark is a grayscale image.

3.2 Background Information

The proposed method uses Discrete Tchebichef Transformation for the watermarking purpose. To understand the proposed method clearly some basic knowledge about the transformation and the related background information regarding the process is necessary.

3.2.1 Discrete Cosine Transformation

In mathematics, the Two Dimentional Discrete Cosine Transform follows the following equation:

$$B(p,q) = \alpha(p)\alpha(q)\sum_{m=0}^{K-1}\sum_{n=0}^{L-1} A(m,n)cos(\frac{\pi(2m+1)p}{2K})cos(\frac{\pi(2n+1)q}{2L}) \quad (3.1)$$

if p=0, then $\alpha(p) = \sqrt{1/K}$
$otherwise, \alpha(p) = \sqrt{2/K}$

Where ,

B(p,q)= Audio amplitude value after Discrete Cosine Transform.

A(m,n)= Audio amplitude value before Discrete Cosine Transform.

3.2.2 Discrete Tchebichef Transformation

In mathematics, the Two Dimentional Discrete Tchebichef Transform follows the following equation:

$$B(p,q) = \alpha(p)\alpha(q)\sum_{m=0}^{K-1}\sum_{n=0}^{L-1} A(m,n)cos(\frac{\pi(2m+1)p}{2K})cos(\frac{\pi(2n+1)q}{2L}) \quad (3.2)$$

if p=0, then $\alpha(p) = \sqrt{1/K}$
$otherwise, \alpha(p) = \sqrt{2/K}$

if p=0, then

$$T(p,q) = \frac{B(p,q)}{\sqrt{2}} \quad (3.3)$$

otherwise,

$$T(p,q) = B(p,q)\sqrt{\frac{2}{K}} \quad (3.4)$$

Where ,

T(p,q)= Audio amplitude value after Discrete Tchebichef Transform.

A(m,n)= Audio amplitude value before Discrete Tchebichef Transform.

3.2.3 Inverse Discrete Tchebichef Transformation

It is completely reverse process of Discrete Tchebichef Transform. The mathematical formula is given below:

if p=0, then

$$B(p,q) = T(p,q)\sqrt{2} \tag{3.5}$$

otherwise,

$$B(p,q) = \frac{T(p,q)}{\sqrt{\frac{2}{k}}} \tag{3.6}$$

$$A(m,n) = \sum_{p=0}^{K-1}\sum_{q=0}^{L-1} \alpha(p)\alpha(q)B(p,q)cos(\frac{\pi(2m+1)p}{2K})cos(\frac{\pi(2n+1)q}{2L}) \tag{3.7}$$

if p=0, then $\alpha(p) = \sqrt{1/K}$
$otherwise, \alpha(p) = \sqrt{2/K}$

Where ,

T(p,q)= Audio amplitude value before Inverse Discrete Tchebichef Transform.

A(m,n)= Audio amplitude value after Inverse Discrete Tchebichef Transform.

3.2.4 Singular Value Decomposition (SVD)

In SVD transformation, A given matrix is decomposed into three matrices. For example, Let A be a PxP matrix with SVD of the form

$$A = USV^T \tag{3.8}$$

where U and V are orthogonal PxP matrices and S is a PxP diagonal matrix with non-negative elements.

$$A = \begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ \\ \end{vmatrix}$$

$$then, U = \begin{Vmatrix} -0.2148 & 0.8872 & 0.4082 \\ 0.5206 & 0.2496 & -0.8165 \\ -0.8263 & -0.3879 & 0.4082 \end{Vmatrix}$$

$$V = \begin{Vmatrix} -0.4797 & -0.7767 & -0.4082 \\ -0.5724 & -0.0757 & 0.8165 \\ -0.6651 & 0.6253 & -0.4082 \end{Vmatrix}$$

$$S = \begin{Vmatrix} 16.8481 & 0 & 0 \\ 0 & 1.0684 & 0 \\ 0 & 0 & 0.0000 \end{Vmatrix}$$

3.3 Proposed Watermarking Method

The proposed method is divided into two parts. They are watermark embedding, watermark extraction. At first a grayscale image is selected as original watermark. The host audio in divided into frames each having 8x8 samples/frame. After scrambling the watermark, the 32x32 grayscale image will be embedded into the host audio after Discrete Tchebichef Transform and Singular Value Decomposition. In the extraction process, we used reversible approach to recover the original image exactly.

3.3.1 Scrambling Method

First of all a grayscale watermark image of size MxN with L bit per pixel was selected for embedding. Every pixel was converted into binary L bit sequence. Number of L binary images of size MxN was made with the corresponding binary sequence. For example, All the first binary values of MxN image made the first binary image.

Then all the two dimentional images converted into one dimentional binary sequences. Another different binary sequences were generated according the equation below:

Y(i+1)=exp(-a(Y(i))2)+b.

If Y(i)>T then, Z(i)=1.

Otherwise, Z(i)=0.

Where y(1) , a ,b parameters are predefined by the owner. T is a predefined threshold.

With the exclusive-OR operation of above binary sequence and one dimentional binary image we got scrambled binary sequences.

Every binary sequence will be merged together with reverse position again and we will get scrambled image.

Descrambling method is completely reverse process of scrambling method.

3.3.2 Watermark Embedding Process

The watermark embedding process has been showed in fig [3.1] and can be described as follows:

1. Divide the host audio signal into frames of 8x8 samples/frame.
2. Apply Discrete Tchebichef Transform into each frame of host audio signal.
3. Apply Singular Value Decomposition into the signal.
4. Apply scrambling method into the grayscale watermark image.
5. Convert the scrambled watermark into a binary sequence.
6. Then the scrambled watermark will be embedded into the S part of SVD decomposed audio signal using the equation below:

if W(a,b)= 1, then

$$S - part - embedded(a,b)(1,1) = S - part(a,b)(1,1) + Alpha; \tag{3.9}$$

Here,
W(a,b)= Watermark sequence Value.
Alpha= A small value which does not affect the signal too much.
S-part= S part of SVD decomposed audio signal.

7. Apply Inverse Singular Value Decomposition to the embedded audio matrix.
8. Apply Inverse Discrete Tchebichef Transform to the signal.
9. Reconstruct the signal and get the audio format signal.

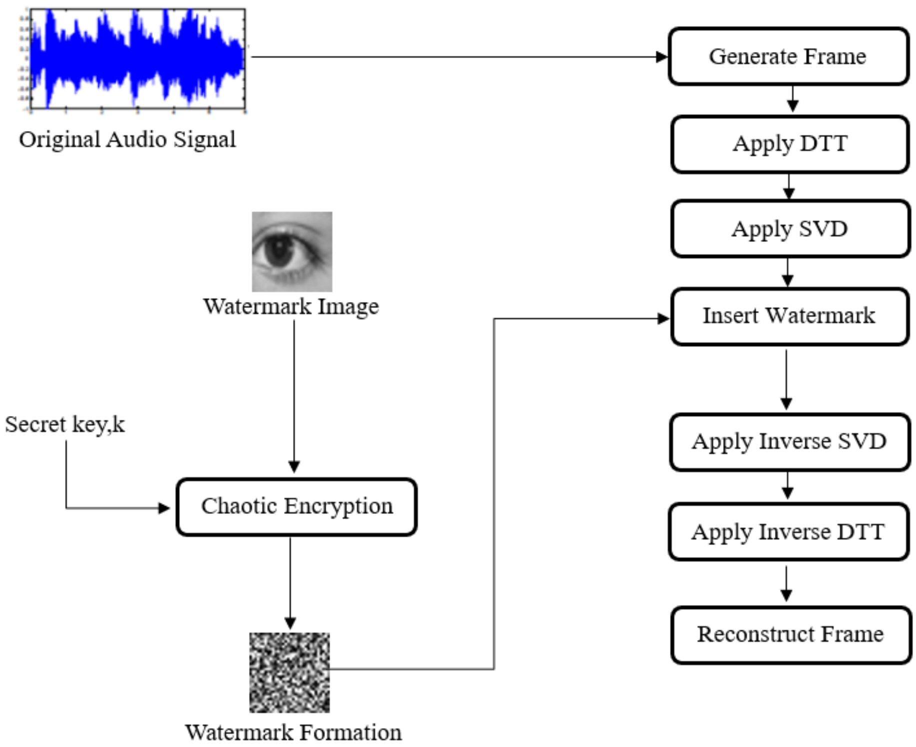


Figure 3.1: Watermark embedding process of the proposed scheme

3.3.3 Watermark Extraction Process

The watermark extraction process has been showed in Figure [3.2] and it can be described as follows:

1. Divide the watermarked audio signal into frames of 8x8 samples/frame.

2. Apply Discrete Tchebichef Transform into each frame of watermarked audio signal.

3. Apply Singular Value Decomposition into the signal.

4. With the comparison of watermarked audio and host audio we can get back the watermark image binary sequence. The equation is below:

if (S-part(a,b)(1,1) - S-part-host(a,b)(1,1)>=B)

$$W(a, b) = 1; \tag{3.10}$$

Here,

S-part= S part of SVD decomposed watermarked audio signal.

S-part-host= S part of SVD decomposed host audio signal.

B= A small value.

W(a,b)= Binary sequence of extracted image.

5. Binary Sequence will be converted into grayscale image.
6. After Descrambling, extracted grayscale image will be found.

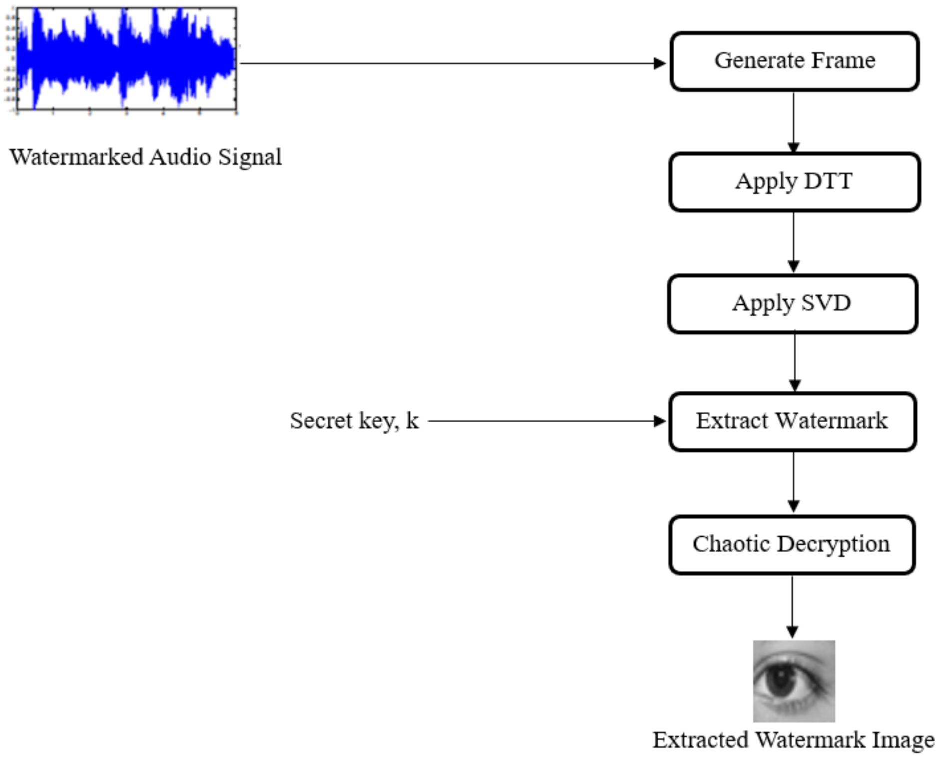


Figure 3.2: Watermark extraction process of the proposed scheme

Chapter 4

Implementation

4.1 Host Audio Used for Simulation

For simulation, two different audios have been used as host. The audios are

a) Hey Jude.wav

b) Toms diner.wav

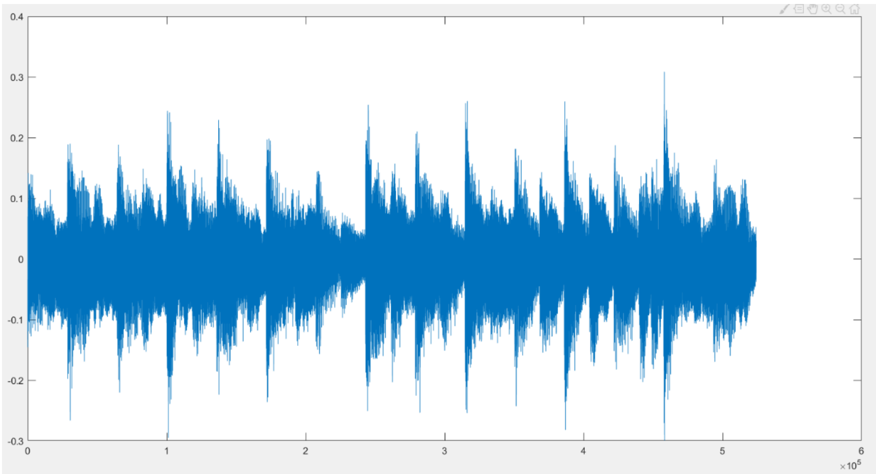


Figure 4.1: Hey Jude.wav

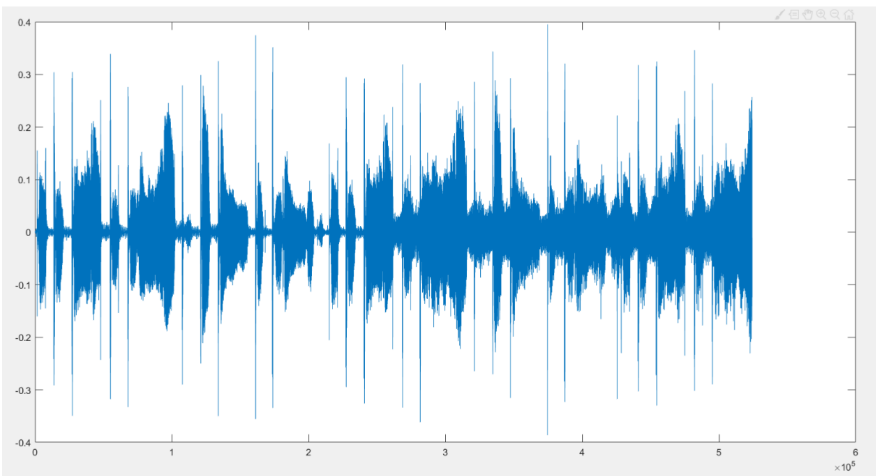


Figure 4.2: Toms Diner.wav

4.2 Watermark Image Used for Simulation

In this experiment, we have used a 32x32 grayscale image as the watermark.

Figure 4.3: Watermark image

4.3 Experimental Result:

After simulation, watermarked audio:

Hey Jude.wav:

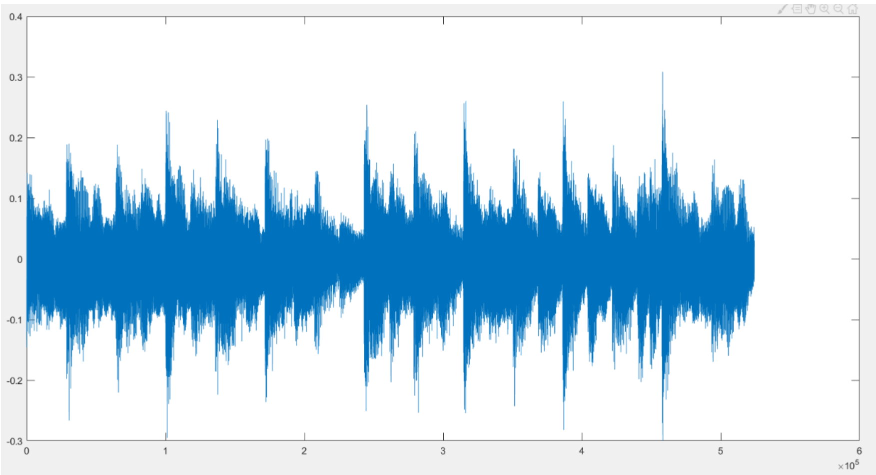


Figure 4.4: Watermarked Audio(Hey Jude.wav)

Toms Diner.wav:

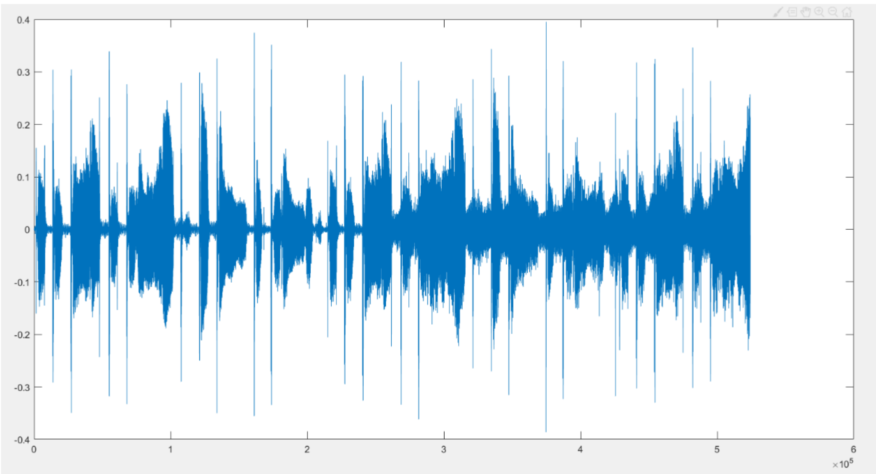


Figure 4.5: Watermarked Audio(Toms Diner.wav)

After simulation, the extracted watermark image:

Figure 4.6: Extracted Watermark image

Comparison of original image and extracted image:

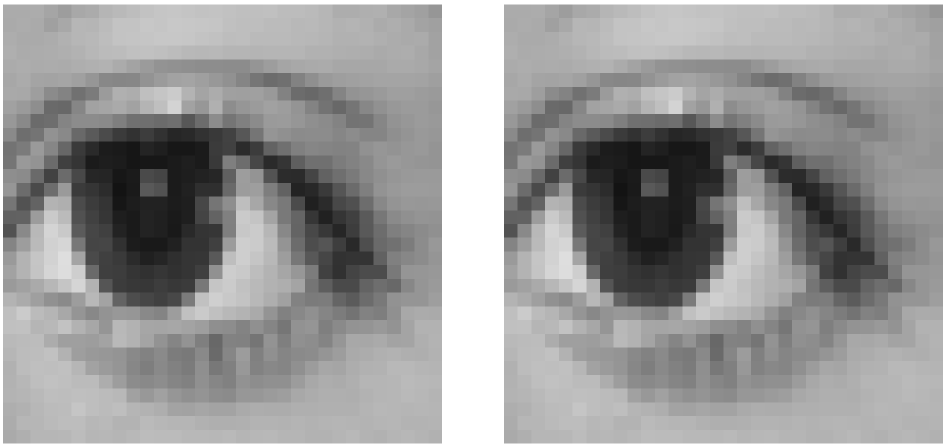


Figure 4.7: Original Image and Extracted Watermark Image

4.4 Attacks Applied on Simulation

In order to test the efficiency of the scheme various attacks were applied. They are the following:

1. Cropping: 1000 samples were removed from the watermarked audio signal and replaced these samples by the original signal.

2. Invertion: All the sample values were inverted of the watermarked audio signal that means positive values turned into negative values and negative values turned into positive values.

3. Echo addition: An echo signal is added to the watermarked audio signal.

4. Resampling: The Frequency Sampling Rate was made half of it's original value and resampled back to original Frequency Sampling Rate.

5. Re-quantization: The 16 bit watermarked audio signal was quantized down to 8bits/sample and again re-quantized back to 16bits/sample.

6. Noise Reduction: Background noise was removed down to 10 decibel.

7. Low Pass Filter: All the frequency of above 22000Hz was removed in this section.

8. MPEG-1 Compression: The watermarked audio signal was compressed at a bit rate of 128kbps and then decompressed back to the wave format.

9. Additive White Gaussian Noise: AWGN was added to the signal.

4.5 Experimental Environment

- Processing software: Matlab 2018b.
- Attack software:

1. Cool Edit Pro v2.0.
2. Audacity.

4.6 Normalized Correlation Coefficient (NC)

Normalized correlation coefficient (NC) is mainly used to obtain the similarity between the original watermark and the extracted watermark. In order to evaluate the value of NC, the extracted image used as watermark W* is compared based on the similarity with the original watermark W.

The NC is calculated by the following equation:

$$NC\ (W,W^*) = \frac{\sum_{i=1}^{I} w(i) \cdot w^*(i)}{\sqrt{\sum_{i=1}^{I} w(i) \cdot w(i)}\sqrt{\sum_{i=1}^{I} w^*(i) \cdot w^*(i)}}$$

4.7 Bit Error Rate (BER)

The bit error rate is used to evaluate the accuracy of watermark detection after applying attacks.

The BER is calculated by following equation:

$$BER(W, W^*) = \frac{\sum_{i=1}^{M} \sum_{i=1}^{M} W(i,j) \oplus W^*(i,j)}{M \times M}$$

4.8 Peak Signal to Noise Ratio (PSNR)

The peak signal-to-noise ratio (PSNR) is mainly used to check the characteristics of the watermarked signal. It is denoted as:

$$SNR = 10log_{10} \frac{\sum_{n=1}^{N} X^2(n)}{\sum_{n=1}^{N} [X(n) - X^*(n)]^2}$$

Chapter 5

Results and Discussions

5.1 Imperceptibility Analysis

There are mainly 2 major techniques for evaluating the Imperceptibility of the watermarked audio signal such as subjective listening test and objective test. Objective difference grade (ODG) is generally measured with the help of software packages. Again Subjective difference grade (SDG) generally measured with the help of human listeners.

Objective quality of watermarked audio signal is measured by PSNR values. After embedding the PSNR values are calculated. Low PSNR value means low quality and High PSNR value means good quality. In this thesis, the imperceptibility is measured with the help of PSNR values.

Table 5.1: PSNR comparison among conventional method.

Audio	Proposed	DWT-SVD [8]	DCT-SVD[34]
Hey Jude.wav	59.3554	49.7637	42.3030
Toms diner.wav	63.7832	36.3834	35.4635

The calculation of PSNR value is done after the embedding procedure. The PSNR ranges from 59 to 64 are good quality. Here average value is 61.57 which is much impressive for the proposed method. So the method provides better imperceptibility and ensures the good audio quality. From the table 5.1, it is observed that this new method produces better result than those existing methods.

5.2 Robustness Analysis

The measuring of robustness mainly depends on the similarity between the original watermark W and the extracted watermark W*. Two different parameters such as the Normalized Correlation Coefficient (NC) and Bit Error Rate (BER) is used to measure the robustness of a watermarked audio. Several intentional and unintentional attacks were performed on watermarked audio to test the robustness of the proposed watermarking method, such as Additive White Gaussian Noise, Requantization, Cropping, Noise Reduction, Echo addition, Invertion etc.

The testing is done on 2 different audios and the extracted watermark images are similar to the original watermark. This clearly shows the higher robustness performance of the proposed method against different kinds of attacks.

It is observed that the proposed method have standard NC and BER.

Table 5.2: NC and BER value for the proposed method (Hey Jude.wav).

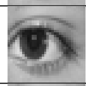
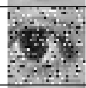
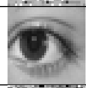
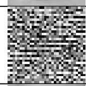
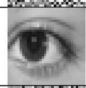
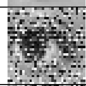
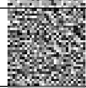
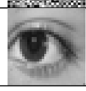
Attack	NC	BER	Extracted Watermark
No Attack	1	0	
Cropping	1	0	
Invertion	1	0	
Echo Adding	0.9574	0.0740	
Resampling	1	0	
Requantization	0.8367	0.3972	
Noise Reduction	1	0	
Low Pass Filter	0.9236	0.1569	
MPEG-1 Compression	0.8294	0.5042	
AWGN	0.9999	0.0016	

Table 5.3: NC and BER value for the proposed method (Toms diner.wav)

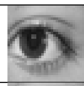
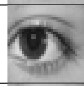
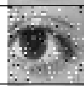
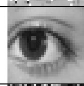
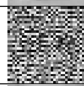
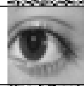
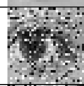
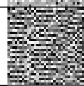
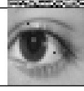
Attack	NC	BER	Extracted Watermark
No Attack	1	0	
Cropping	1	0	
Invertion	1	0	
Echo Adding	0.9822	0.0493	
Resampling	0.9942	0.0085	
Requantization	0.8350	0.4032	
Noise Reduction	1	0	
Low Pass Filter	0.9401	0.1392	
MPEG-1 Compression	0.8076	0.5037	
AWGN	0.9993	0.0007	

Table 5.4: Comparison value of NC for the different methods (Hey Jude.wav).

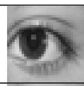
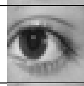
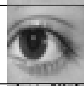
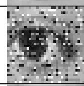
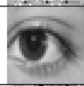
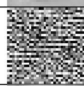
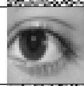
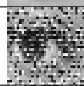
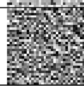
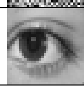
Attack	NC(Proposed)	NC(DWT-SVD)	NC(DCT-SVD)	Extracted Watermark
No Attack	1	1	1	
Cropping	1	0.9049	0.9202	
Invertion	1	1	1	
Echo Adding	0.9574	0.8055	0.8755	
Resampling	1	-	-	
Requantization	0.8367	0.8156	0.8666	
Noise Reduction	1	0.7775	0.8756	
Low Pass Filter	0.9236	-	-	
MPEG-1 Compression	0.8294	-	-	
AWGN	0.9999	0.9175	0.9265	

Table 5.5: Comparison value of NC for the different methods (Toms diner.wav)

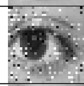
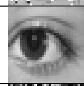
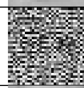
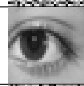
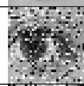
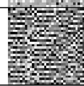
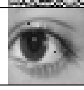
Attack	NC(Proposed)	NC(DWT-SVD)	NC(DCT-SVD)	Extracted Watermark
No Attack	1	1	1	
Cropping	1	0.9049	0.9202	
Invertion	1	1	1	
Echo Adding	0.9822	0.8055	0.8755	
Resampling	0.9942	-	-	
Requantization	0.8350	0.8156	0.8666	
Noise Reduction	1	0.7775	0.8756	
Low Pass Filter	0.9401	-	-	
MPEG-1 Compression	0.8076	-	-	
AWGN	0.9993	0.9175	0.9265	

Table 5.6: Comparison value of BER for the different methods (Hey Jude.wav).

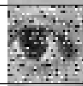
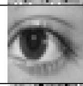
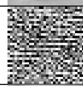
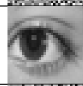
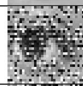
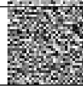
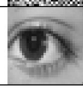
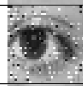
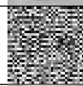
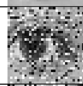
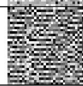
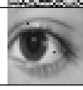
Attack	BER(Proposed)	BER(DWT-SVD)	BER(DCT-SVD)	Extracted Watermark
No Attack	0	0	0	
Cropping	0	0.1338	0.1094	
Invertion	0	0	0	
Echo Adding	0.0740	0.1782	0.1862	
Resampling	0	-	-	
Requantization	0.3972	0.1856	0.1556	
Noise Reduction	0	0.2229	0.1657	
Low Pass Filter	0.1569	-	-	
MPEG-1 Compression	0.5042	-	-	
AWGN	0.0016	0.2550	0.0890	

Table 5.7: Comparison value of BER for the different methods (Toms diner.wav)

Attack	BER(Proposed)	BER(DWT-SVD)	BER(DCT-SVD)	Extracted Watermark
No Attack	0	0	0	
Cropping	0	0.1338	0.1094	
Invertion	0	0	0	
Echo Adding	0.0493	0.1782	0.1862	
Resampling	0.0085	-	-	
Requantization	0.4032	0.1856	0.1556	
Noise Reduction	0	0.2229	0.1657	
Low Pass Filter	0.1392	-	-	
MPEG-1 Compression	0.5037	-	-	
AWGN	0.0007	0.2550	0.0890	

From table 5.2 and 5.3, it is observed that for both the audio, BER and NC values are in acceptable range. For the Hey Jude.wav the NC value is between 0.83 to 1 and for Tom diner.wav the NC value is between 0.83 to 1. So, this method shows better robustness.

Again from table 5.4, 5.5, 5.6 and 5.7, it is observed that the proposed method has better NC and BER values than the existing ones.

Chapter 6

Conclusion

6.1 Conclusion

In this thesis, an audio watermarking method based on Discrete Tchebichef Transform (DTT) and Singular Value Decomposition (SVD) has been proposed. The proposed method is computationally fast, blind, robust, imperceptible and secured. This method introduces a new watermarking technique for embedding watermark which is very popular and rare nowadays. A new algorithm for this technique is introduced here. The proposed method is based on Discrete Tchebichef Transform which is still not used in the field of audio watermarking method. Again grayscale image is used as watermark. So, it can be told that this method is a unique one.

The method has produced high quality watermarked audio and also effectively extract the watermark image after various attacks to ensure copyright protection. These results verify that the proposed watermarking method can be a suitable candidate for audio watermarking.

6.2 Future Work

We have done an audio watermarking technique in digital watermarking using Discrete Tchebichef Transform. The proposed method opens some new opportunity in digital watermarking in frequency domain. Here watermark image is a grayscale image. By modifying this algorithm color image can be used as watermark in future. Besides, new watermarking methodology can be introduced with this transform in future.

References

[1] H. Kumar and S. Kumar, 'Techniques of digital watermarking,' (cit. on pp. 11, 12).

[2] M. Singh, A. Singhal and A. Chaudhary, 'Digital image watermarking techniques: A survey,' *International journal of computer science and telecommunications*, vol. 4, no. 6, 2013 (cit. on p. 11).

[3] L. K. Saini and V. Shrivastava, 'A survey of digital watermarking techniques and its applications,' *arXiv preprint arXiv:1407.4735*, 2014 (cit. on p. 11).

[4] T. Sarkar and S. Sanyal, 'Digital watermarking techniques in spatial and frequency domain,' *arXiv preprint arXiv:1406.2146*, 2014 (cit. on p. 11).

[5] N. Nikolaidis and I. Pitas, 'Robust image watermarking in the spatial domain,' *Signal processing*, vol. 66, no. 3, pp. 385–403, 1998 (cit. on p. 11).

[6] G. Voyatzis and I. Pitas, 'Chaotic watermarks for embedding in the spatial digital image domain,' in *Proceedings 1998 International Conference on Image Processing. ICIP98 (Cat. No. 98CB36269)*, IEEE, vol. 2, 1998, pp. 432–436 (cit. on p. 11).

[7] Z. Dawei, C. Guanrong and L. Wenbo, 'A chaos-based robust wavelet-domain watermarking algorithm,' *Chaos, Solitons & Fractals*, vol. 22, no. 1, pp. 47–54, 2004 (cit. on p. 11).

[8] K. A. Darabkh *et al.*, 'Imperceptible and robust dwt-svd-based digital audio watermarking algorithm,' *Journal of Software Engineering and Applications*, vol. 7, no. 10, p. 859, 2014 (cit. on pp. 11, 12, 27).

[9] Z. Liu, L. Xu, T. Liu, H. Chen, P. Li, C. Lin and S. Liu, 'Color image encryption by using arnold transform and color-blend operation in discrete cosine transform domains,' *Optics Communications*, vol. 284, no. 1, pp. 123–128, 2011 (cit. on p. 11).

[10] B. Wang, J. Ding, Q. Wen, X. Liao and C. Liu, 'An image watermarking algorithm based on dwt dct and svd,' in *2009 IEEE International Conference on Network Infrastructure and Digital Content*, IEEE, 2009, pp. 1034–1038 (cit. on pp. 11, 12).

[11] S. Tsai and S. Yang, 'A fast dct algorithm for watermarking in digital signal processor,' *Mathematical Problems in Engineering*, vol. 2017, 2017 (cit. on p. 11).

[12] Y. Zou, X. Tian, S. Xia and Y. Song, 'A novel image scrambling algorithm based on sudoku puzzle,' in *2011 4th International Congress on Image and Signal Processing*, IEEE, vol. 2, 2011, pp. 737–740 (cit. on p. 11).

[13] C.-H. Chou and T.-L. Wu, 'Embedding color watermarks in color images,' *EURASIP Journal on Advances in Signal Processing*, vol. 2003, no. 1, pp. 1–9, 2003 (cit. on p. 11).

[14] Q. Su, G. Wang, X. Zhang, G. Lv and B. Chen, 'An improved color image watermarking algorithm based on qr decomposition,' *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 707–729, 2017 (cit. on pp. 11, 12).

[15] W. Lu, H. Lu and F.-L. Chung, 'Robust digital image watermarking based on subsampling,' *Applied mathematics and computation*, vol. 181, no. 2, pp. 886–893, 2006 (cit. on p. 11).

[16] N. A. Abu, F. Ernawan, N. Suryana and S. Sahib, 'Image watermarking using psychovisual threshold over the edge,' in *Information and Communication Technology-EurAsia Conference*, Springer, 2013, pp. 519–527 (cit. on p. 11).

[17] J. Liu, X. Niu and W. Kong, 'Image watermarking based on singular value decomposition,' in *2006 International Conference on Intelligent Information Hiding and Multimedia*, IEEE, 2006, pp. 457–460 (cit. on pp. 11, 12).

[18] K.-C. Liu, 'Colour image watermarking for tamper proofing and pattern-based recovery,' *IET image processing*, vol. 6, no. 5, pp. 445–454, 2012 (cit. on p. 11).

[19] K. C. Liu, 'Moment-preserving based watermarking for color image authentication and recovery,' in *IACSIT Hong Kong Conferences*, 2012, pp. 139–143 (cit. on p. 11).

[20] G. Zeng and Z. Qiu, 'Audio watermarking in dct: Embedding strategy and algorithm,' in *2008 9th International Conference on Signal Processing*, IEEE, 2008, pp. 2193–2196 (cit. on p. 12).

[21] Y. Yan, H. Rong and X. Mintao, 'A novel audio watermarking algorithm for copyright protection based on dct domain,' in *2009 Second International Symposium on Electronic Commerce and Security*, IEEE, vol. 1, 2009, pp. 184–188 (cit. on p. 12).

[22] 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 (cit. on p. 12).

[23] A. Al-Haj, L. Bata and A. Mohammad, 'Audio watermarking using wavelets,' in *2009 First International Conference on Networked Digital Technologies*, IEEE, 2009, pp. 398–403 (cit. on p. 12).

[24] W. Al-Nuaimy, M. A. El-Bendary, A. Shafik, F. Shawki, A. E. Abou-El-azm, N. A. El-Fishawy, S. M. Elhalafawy, S. M. Diab, B. M. Sallam, F. E. Abd El-Samie *et al.*, 'An svd audio watermarking approach using chaotic encrypted images,' *Digital Signal Processing*, vol. 21, no. 6, pp. 764–779, 2011 (cit. on p. 12).

[25] S.-K. Lee and Y.-S. Ho, 'Digital audio watermarking in the cepstrum domain,' *IEEE Transactions on Consumer Electronics*, vol. 46, no. 3, pp. 744–750, 2000 (cit. on p. 12).

[26] P. K. Dhar, 'A blind audio watermarking method based on lifting wavelet transform and qr decomposition,' in *8th International Conference on Electrical and Computer Engineering*, IEEE, 2014, pp. 136–139 (cit. on p. 12).

[27] P. K. Dhar and T. Shimamura, 'Blind audio watermarking in transform domain based on singular value decomposition and exponential-log operations,' *Radioengineering*, vol. 26, no. 2, pp. 552–561, 2017 (cit. on p. 12).

[28] W.-N. Lie and L.-C. Chang, 'Robust and high-quality time-domain audio watermarking based on low-frequency amplitude modification,' *IEEE transactions on multimedia*, vol. 8, no. 1, pp. 46–59, 2006 (cit. on p. 12).

[29] 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 (cit. on p. 12).

[30] Y. Luo, D. Peng, Y. Sang and Y. Xiang, 'Dual-domain audio watermarking algorithm based on flexible segmentation and adaptive embedding,' *IEEE access*, vol. 7, pp. 10 533–10 545, 2019 (cit. on p. 12).

[31] R. Noor, A. Khan, A. Sarfaraz, Z. Mehmood and A. M. Cheema, 'Highly robust hybrid image watermarking approach using tchebichef transform with secured pca and cat encryption,' *soft computing*, vol. 23, no. 20, pp. 9821–9829, 2019 (cit. on p. 12).

[32] O. Jane and E. Elbaşi, 'A new approach of nonblind watermarking methods based on dwt and svd via lu decomposition,' *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 22, no. 5, pp. 1354–1366, 2014 (cit. on p. 12).

[33] E. W. K. Full, S. Metkar and H. C. Kamble, 'Image watermarking by schur decomposition,' *Int J Inf Comput Technol*, vol. 4, pp. 1155–1159, 2014 (cit. on p. 12).

[34] G. Suresh, N. Lalitha, C. S. Rao and V. Sailaja, 'An efficient and simple audio watermarking using dct-svd,' in *2012 International Conference on Devices, Circuits and Systems (ICDCS)*, IEEE, 2012, pp. 177–181 (cit. on p. 27).