CANKAYA UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
MATHEMATICS AND COMPUTER SCIENCE

MASTER THESIS

RADON TRANSFORM BASED ROBUST NON-BLIND WATERMARKING

OMER SIDDIK

FEBRUARY 2013

Title of Thesis: **Radon Transform Based Robust Non-Blind Watermarking**

Submitted By **Omer SIDDIK**

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 mathematics and computer 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 of degree Master of Science (M.S.) in Mathematics and Computer Science.

Dr.Ersin ELBAŞI
Supervisor

Examination Date: 15/02/2013

Examining Committee Members

Dr.Ersin ELBAŞI (TÜBİTAK)

Assist.Prof. Dr. Abdül Kadir GÖRÜR (Çankaya Univ.)

Assist.Prof. Dr. Reza ZARE HASSANPOUR (Çankaya Univ.)

STATEMENT OF NON PLAGIARISM

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 : ÖMER SIDDIK

Signature :

Date : 15.02.2013

ACKNOWLEDGMENTS

I would like to express the deepest appreciation to my supervisor **Dr.Ersin ELBAŞI** who has attitude and substance of genius: he continually convincingly conveyed a spirit of adventure in regard to research and regard to teaching.

I would like extend my thanks to my family and special my parents for there for eternal love support and trust me. Without them i would never come up to this stage.

Finally, i offer my sincere thanks to my friends and my lovers for supporting me in this study.

ABSTRACT

RADON TRANSFORM BASED ROBUST NON-BLIND WATERMARKING

SIDDIK, Omer

M.S. Department of Mathematics and Computer Science

Supervisor: Dr.Ersin ELBAŞI

February 15, 76 pages

The purpose of digital watermarking is to attempt to solve the copyright ownership problem for all multimedia data which can be image, audio or video. The main objective of this thesis is to design a robust method of image watermarking for copy protection and copyright protection.

The thesis consists principally from an overview of watermarking algorithm, types of watermarking, watermarking requirements. Further the watermarking techniques that are used in embedding. There are many watermarking techniques discussed in spatial domain and transform domains. The spatial domain watermarking algorithms still not resistant to lossy compression image, shed noise in the image and most operations of image processing. On the other hand, frequency domain watermarking techniques can embed more bits for watermark and the watermarked images are more robust to attack. Otherwise, in frequency domain we can embed more bits and more resistance to the attacks. However, comparing watermarking in DWT with watermarking in DCT, DWT has a number of advantages that led us to focus in discrete wavelet transform from other types of same domain.

In this thesis, there are three different watermarking methods proposed in different levels DWT based on radon transform. All proposed methods are requires the presence of original image for watermark extraction. Each method is various

from the other from the way of embedding the watermark, the number of watermarks that embedded and in which level the watermark embedded. Moreover, the watermarked image and attacked images measured by the PSNR that measuring the noise ratio in each image. Finally, we attempt to extract the watermark and attacked image, to determine the proportion of the deterioration that occurred after the attack or the embedding process.

Keywords: Watermarking, Discrete Wavelet Transform, Radon Transform.

ÖZET

RADON TRANSFORM TEMELLİ GİZLİ OLMAYAN DAYANIKLI FİLİGRANLAR

SIDDIK, Omer

M.S. Matematik ve Bilgisayar Bilimleri Bölümü

Danışman: Dr. Ersin ELBAŞI

Şubat 15, 76 sayfa

Dijital filigran oluşturmanın amacı görüntü, ses ya da video olabilen tüm dosyaların telif hakkı sahipliği problemlerini ortadan kaldırmaktır. Bu tezin ana konusu kopya ve telkih hakkı koruması ile ilgili görüntü filigranının sağlam bir tasarımını oluşturmaktır.

Bu tez genel olarak filigran algoritmalarının, filigran çeşitlerinin ve filigran gerekliliklerinin genel tanıtımlarından oluşmaktadır. Sonra da gömmede kullanılan filigran teknikleri yer almaktadır. Uzamsal ve dönüşüm alanlarındaki tartışılan birçok filigran teknikleri vardır. Uzamsal alanlardaki filigran algoritmaları yitimli sıkıştırma görüntüleri, görüntüdeki ses dağıtımı ve görüntü işleme operasyonlarının çoğunda hala yeterince dirençli değiller. Diğer tarafta ise frekans etki alanlı filigran teknikleri filigranlar için daha çok bit gömebilir ve bu filigranlarla korunan görüntüler saldırılara karşı daha dayanıklıdırlar. Aksi takdirde (başka bir deyişle), frekans etki alanlarına daha fazla bit gömebilir ve saldırılara karşı daha dirençli hale getirebiliriz. Ancak, DWT filigran basma, DCT filigran basma ile kıyasla, bizi DWT ile aynı etki alanında bulunan diğer alanlardan ziyade, gizli dalgacıklı transformuna yönlendiren ve odaklayan birçok avantajı bulunmaktadır.

Bu tezde DWT'nin farklı seviyelerinde Radon transform temeline dayandırılan üç farklı filigran metodu sunulmaktadır. Tüm sunulan metotlar var olan

orijinal görüntü filigran çıkarma için gereklidir. Her bir metot diğerinden filigran gömme, gömülen filigran sayısı ve filigranın gömülme seviyeleri arasında farklılıklar göstermektedir. Ayrıca, her bir görüntüde PSNR tarafından ölçülen filigran görüntüsü ve saldırılan görüntülerin ses oranlarını da içermektedir. Son olarak da gömme işlemi ya da saldırı sonrası meydana gelen bozulma oranını belirlemek için filigran ve saldırılan görüntüleri ayırmayı denedik.

Anahtar kelimeler: Filigran basmak, Gizli Dalgacık Transformu, Radon Transformu,

TABLE OF CONTENTS

TRANSFORM DOMAIN WATERMARKING ALGORITHIMS AND RADON TRANSFORM ALGORITHM

WATERMARKING ALGORITHMS USING DWT BASED ON RADON TRANSFORM

CONCLUSION AND FUTURE WORK

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS / ABBREVIATIONS

RST	Rotation, scaling and translation
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
IDWT	Inverse Discrete Wavelet Transform
ISBN	International Standard Book Number
ISRC	International Standard Recording Code
LSB	Least Significant Bit
MSE	Mean Squared Error
PSNR	Peak Signal to Noise Ratio
HVS	Human Visual System

INTRODUCTION

The rapid progress of computer technology led to increase concerns on the security of multimedia. In addition, the evolution of the internet has become easy way to access and manipulate the contents of the media. These problems led to interests in watermarking which involves embedding an invisible data (logo or signature) into original data to maintain the ownership copyright.

There are many types of watermarking techniques that can be classified depending on different respects. For instance the form of the contents can be image, audio or video, or the classification on the area of work which can be spatial or transform domain, or it may depends on the type of information which are blind, semi-blind or non-blind and many other types. [2]

For more details the Cox et al. in [41] and Katzenbeisser and Petitcolas in [23] are describes several applications.

Watermarking What For?

The techniques of copyright protection and copy protection for all multimedia (image, audio and video) are divided in two fields: Encryption and watermarking. [43]

The purpose of Encryption techniques is to protect the data that transferred from the sender to the receiver. Moreover, the receiver decrypts the data and matches them with the original data. These techniques confined to provide the protection just during transmission process. [44]

The watermarking techniques can represent by embedding a secret imperceptible data into original data which can be logo or seal of organization for signify the ownership. The digital watermarking aims to enforcement the law and copy protection for the digital media parts from unauthorized people.

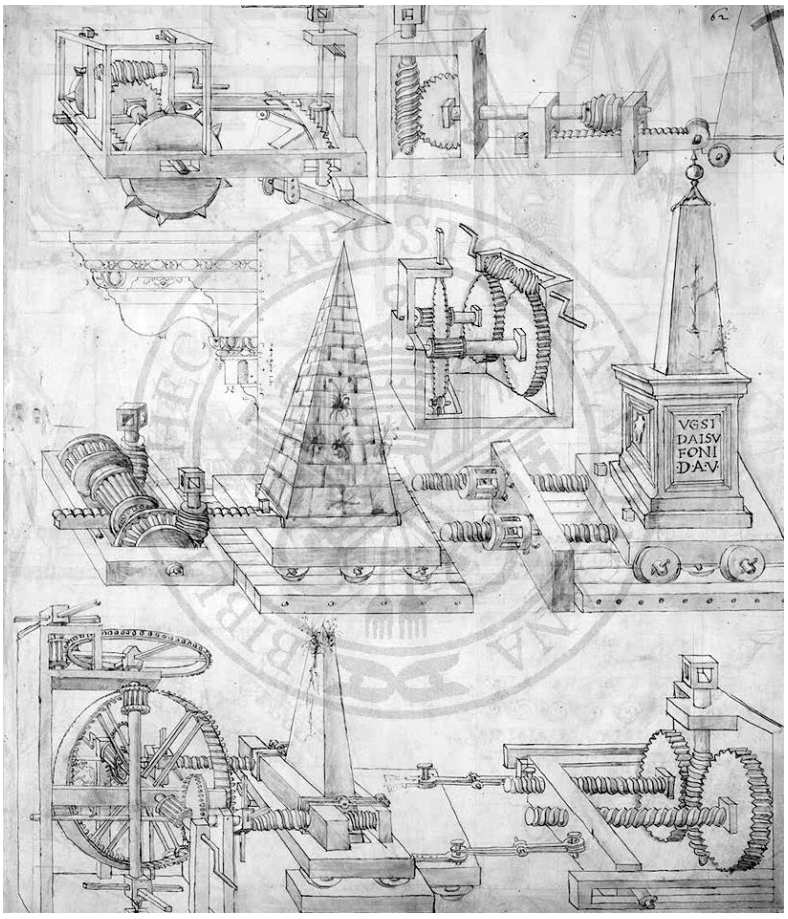


Figure: Perceptible watermark embedded in a figure

In chapter two we will use the term watermarking for all this applications.

Thesis layout

In chapter one, we discuss the types and methods of data hiding, the watermark requirements, watermarking types, watermark application, watermarks processes, watermarking algorithms, watermarking techniques, watermarking attacks and evaluation in watermarking.

In chapter two, we discuss the transform domain watermarking algorithms and Radon transform algorithm, transform domain watermarking algorithm, transform domain embedding and extraction, Discrete Wavelet Transform and properties of wavelet transform, then we discuss the radon transform and the inverse Radon transform.

In chapter three, we will explain the watermarking algorithms using DWT based on Radon transform and then the three methods with the experimental results which are:

1. Multi Watermarking With Radon Transform and First Level DWT Decomposition.

2. Radon Transformation Based Multi Watermarking Using Second Level DWT Decomposition.

3. Radon Transformation Based Multi Watermarking Using Second Level DWT Decomposition.

In chapter four, the conclusion and the future work.

CHAPTER I

1.1 TYPES AND METHODS OF DATA HIDING

Methods of information hiding are dividing into two types: cryptography and steganography. The term cryptography means “secret writing” and steganography means “cover writing”.

Cryptography is a method of sending messages in characteristically forms that only receiver can read the message. The message that send (plain text) is convert to masked message (cipher text) before sending the message, this process is called enciphering (encryption) and the inverse of this process is called deciphering (decryption). This method protects the message contents from the sender to the receiver.

Steganography is a method for hiding the message themselves by using devising astute methods and cannot be detected. The steganography is wider than cryptography and there is no theory for steganography. The steganography is origin from the biological and physiological. [1]

- **Watermarking** is hiding information in image that human eye cannot detect it in a difficult manner to detect and remove. There are many watermarking techniques that used to embed images and extract the embedded image. [3]

1.2 THE WATERMARK REQUIREMENTS:

1. **Invisibility**: In most embedded watermark application the embedding process does not affect to the quality of original image. The invisibility of embedded watermark is if human cannot distinguish between the original image data and embedded image data.[6]

2. **Capacity of watermark**: The information and quantity which stored in the watermark, depends on the type of application used the copy protection, and copyright protection [6], ownership and Intellectual rights. The owner can embed the data based on ISBN (international standard book number) or embed data on ISRC (international standard recording code**).** [7]

3. **Robustness**: Embedded images must have the ability to resistance against most types of attacks and embedded image cannot be detected [7].

4. **Security**: The parties must be authorized to access to the parts concerned and supposed to know the method that used to embed and cannot be accessed for unauthorized people, strength of security is in the selection of key. [3].

1.3 WATERMARKING TYPES

The visible, invisible and fragile watermarks are watermarking general types:

1. **Visible watermark:** Is a translucent image overlaid onto the cover image as shown in figure 1.1. (b) . The watermark appears visible to the viewer and may be logo or seal.

2. **Invisible watermark:** In invisible watermarking the embedded data is not perceptible and cannot detect by human eye as shown in figure 1.1.(c). [4]

3. **Dual watermark:** Is a collection of a visible watermark and an invisible watermark. A visible watermark is inserted in the cover image and then an invisible watermark is added to the visible-watermarked image. This process is called dual watermarked image. Invisible watermarking is the most robust type. [5]

(a) (b) (c)

(d)

Figur1.1. a. Cover image b. visible watermarked image, c. Invisible watermarked image

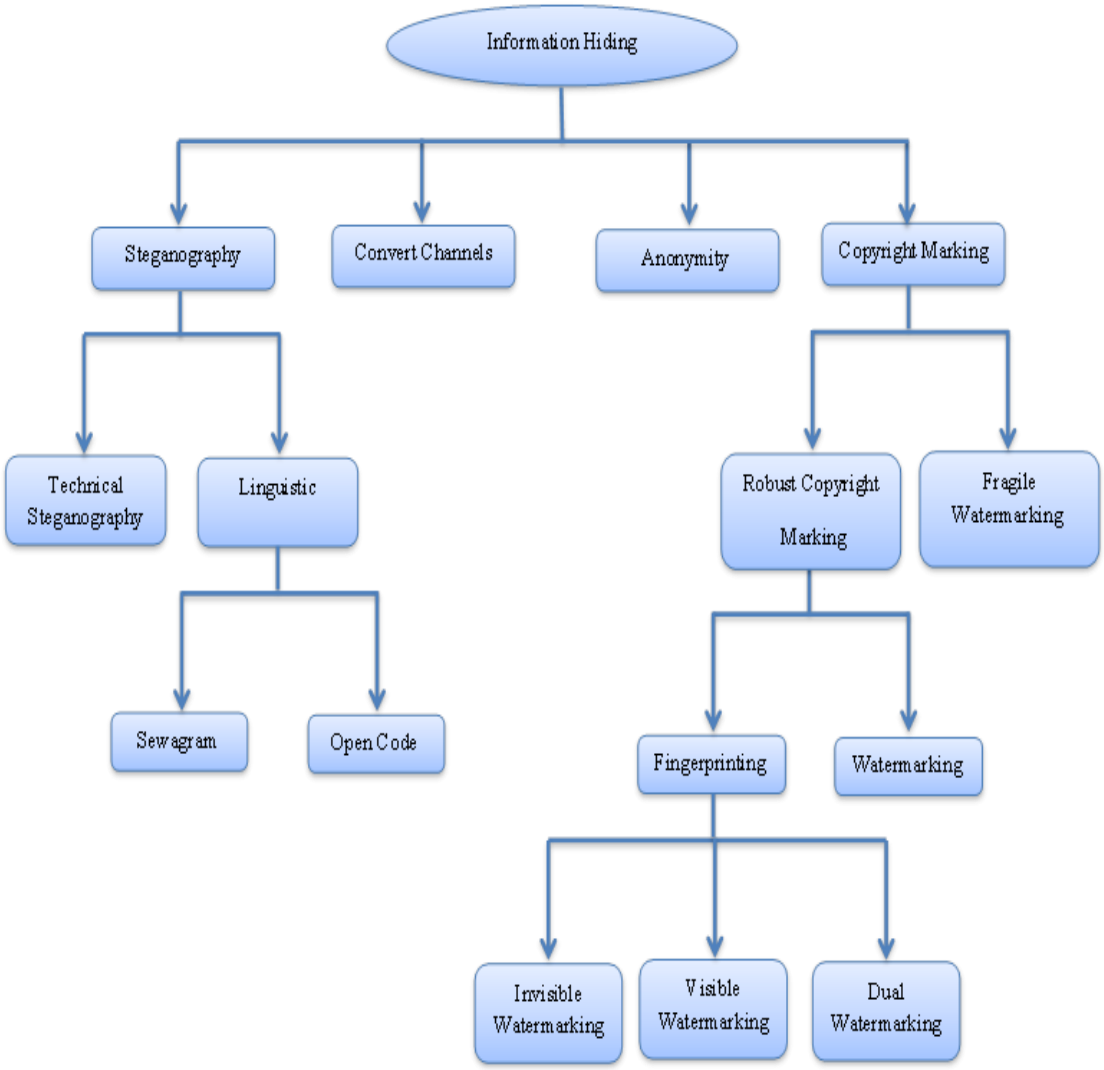


Figure1.2. Information hiding techniques

1.4 WATERMARK APPLICATION

Digital watermarking has many applications. In this part we focus in some more common application of digital watermarking.

Copyright protection: The most common applications of watermarking are copyright protection and needs high robustness and the main purpose is to insert copyright information like rules, data and copying into the image without loss of quality. [16]

Owner Identification: The embedded watermark data can prove the ownership by identification the information of the content owner. This kind of application needs high security. [16]

Copy Control: These techniques of copy protection is used to consumer control mechanism and prevent unauthorized copying of the content by inserting a never-copy watermark and decreasing the number of copying times. [16]

Authentication /Content Verification: The purpose of authentication is to be able to detect any change or modification of the data. This information required to authenticate the content that be watermarked. The fragile watermark is used in this application which has low robustness to the modification. [16]

Transactional Watermarks/Fingerprinting: The purpose of fingerprinting is to prevent the source of using unauthorized copies; therefore the owner can embed a different key into each copy. [16]

Broadcast Monitoring: This kind of application is to ensure that the commercials are aired by the broadcasters at the time and location that they want according to the contracts. Watermarks can be embedding in any type of data to broadcast on the network, which are able to monitor distribution channels to track the content in the time and the place that they appear [16].

1.5 WATERMARK PROCESSES

Embedding and Extraction

Watermark Embedding: Embedding is the process of hiding a data in cover image this data can be logo or seal. Scheme below is shown the watermark embedding. [3]

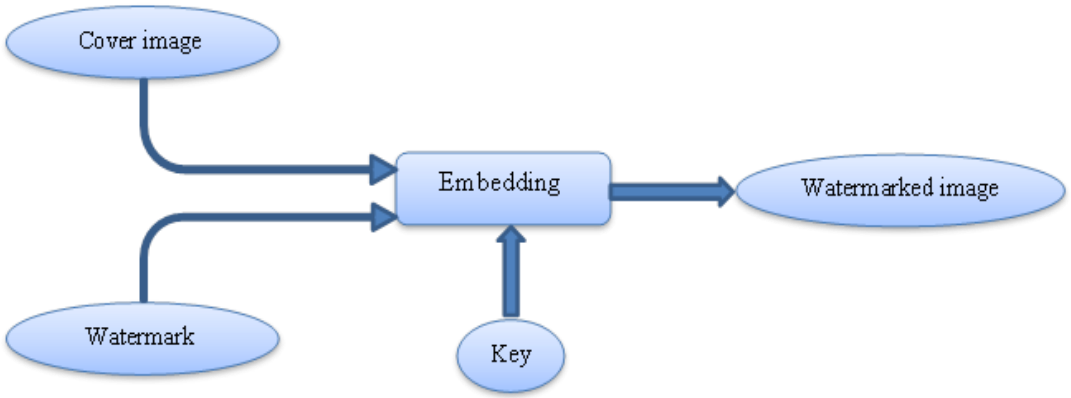


Figure 1.3 watermark embedding

Watermark Extraction: Extraction is the process of obtaining the embedded image from watermarked image. This process is used for checking the existence of the watermark. Scheme below is shown the watermark extraction. [3]

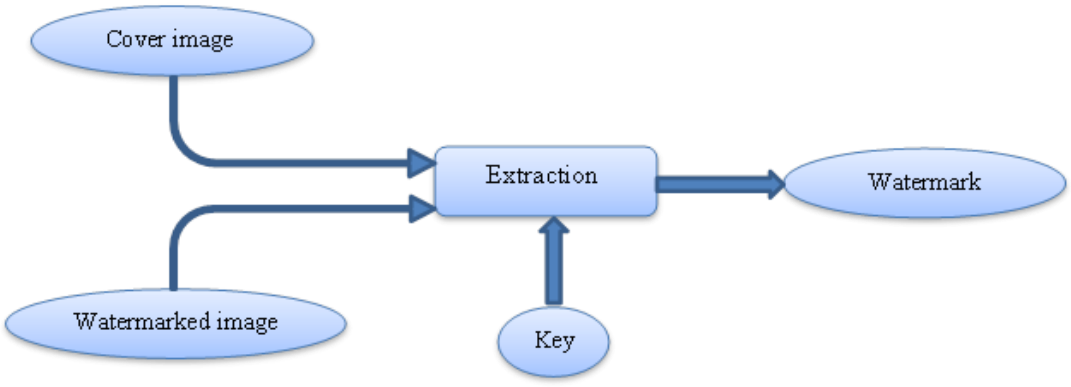


Figure 1.4 watermark extraction

1.6 WATERMARKING ALGORITHMS

Watermark algorithms are classified based on the information detection. They are as follows:

Blind or Public Watermarking: In blind watermarking, the detection process has no need for original image to detect the watermark. Only the secret key is required.

Non-Blind or Private Watermarking: In non-blind or private watermarking, the information of the original image is required in the watermark detection. [16]

Semi-Blind Watermarking: In semi-blind watermarking, occasionally the watermark detection may require the original image. Some watermarking algorithms require the original signal after adding the watermark, which is called published watermarked signal.

1.7 WATERMARKING TECHNIQUES

Techniques of watermarking are separate in two approaches: Spatial domain and frequency domain, this technique is also called transform domain. [9]

Spatial Domain

These types of watermarking are selected the pixels of an image randomly and modified them. This technique is unreliable for media operations.

LSB (Least Significant Bit) method: The Least Significant Bit is the common application method of spatial domain watermarking that lies in modifying the cover image signal. [11]

Transform Domain

The transform domain is similar to spatial domain watermarking but varies in modifying the coefficients of the image.

1. **Discrete Cosine Transforms (DCT):** The spatial domain data points are converted to the sum of sine and cosine waveforms with different capacity in the transform domain. [12, 13]
2. **Discrete Fourier Transform (DFT):** Cosine function has used only for real numbers. There are eight different variants of DCT with some modifications between them. [13]
3. **Discrete Wavelet Transform (DWT):** The signal is decomposed into a set of basic wavelets by replacement the lower frequencies at various resolutions. [14]

The differences between spatial domain and transform domain methods is the spatial domain watermarking has disadvantage, which is the cropping attack may remove the watermark from the watermarked image. [15] The following figure 1.5 illustrates the classification of watermarking algorithms.

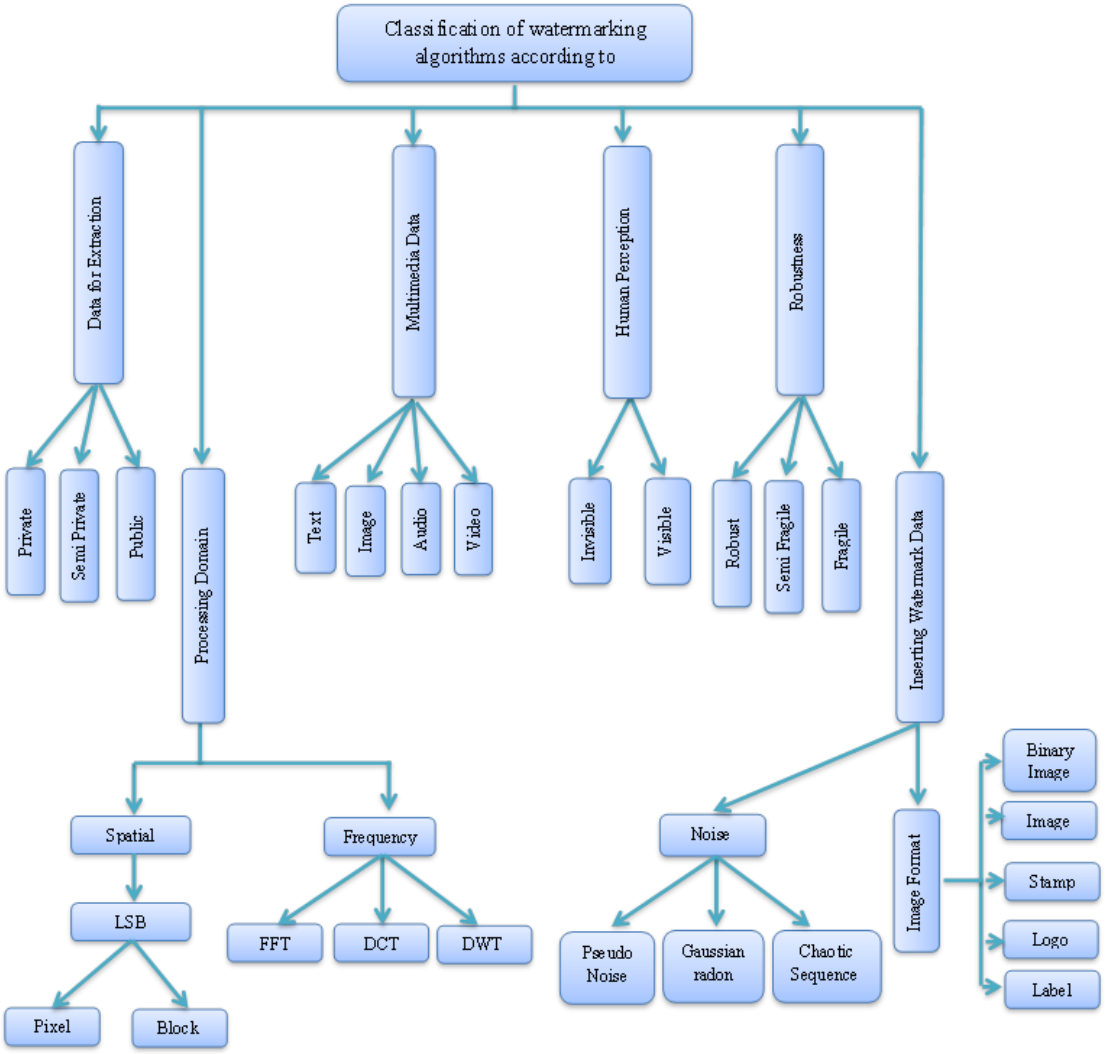


Figure 1.5 .Classification of watermarking techniques

1.8 WATERMARKING ATTACKS

There are so many contributions that have been studied in security. One of the contributions is reported by Craver. [17] Aims at the ownership claim established with the help of non-blind linear watermarking algorithms like Cox el al. [18] The watermark should have high reliability of watermark detection.

The watermark detection process has been robust to the alterations in the host image for both unintentional and intentional distortions. [19] The operations on watermarked multimedia may have effect to the watermarking algorithms or destroy it.

These types of operations are called attacks. The Image, audio, and video multimedia are stored in loss compressed format.

These compressions are divided into important and unimportant parts of data and ignore the unimportant parts. This distortion may damage the watermark data. [16] The aim of attacks is not always to remove or destroy the watermark but aims to disable the detection. Distortions are limited to not producing excessive damages. Otherwise, could not use the watermarked object. These distortions could also introduce damage to the performance of the system. [20]

The best-known watermarking attacks, which may be intentional or unintentional that depends on the application are:

Cropping: This application is one of common attacks in many cases which eliminate a small portion of watermarked image or from parts frames of video sequence. [20]

Compressions: Generally it is unintentional attack that appears often in multimedia applications. The compression used currently in all the audio, video and image that distributed via internet. The watermark requires resistance to different levels of compression. This advisable the watermark embedding performs in the same domain for compression take places. [20]

Collusion: A number of authorized receivers of the image should not be able to come together and use the differently watermarked copies to generate a watermarked copy of the image. [23]

Histogram Equalization: This application is used for increasing the details of an image are lacking in contrast. It modifies the intensity levels in the image to conform to some desired histogram. [23]

Gamma Correction: Gamma correction is used to adjust the color difference. The differences in the display monitor for same color image displayed may be leads to look different. [23]

Rotation: Change the rotation of the image either clockwise or counter clockwise. [20]

Scaling: Change the size of the image, for example, if a watermarked image size is 256 * 256, it is resized to 128 * 128 and then to 256* 256. [20]

Rewatermarking: Embedding another watermark to an image.

Denoising attacks: Image denoising attacks is an additive noise relative to the original image. Main types are local median, midpoint, trimmed mean filtering, wiener filtering, and hard and soft thresholds. [22]

Filtering: Filtering attacks are high pass; low pass filtering, Gaussian and sharpening filtering. Low-pass filtering does not introduce significant deterioration in watermarked images, but can affect to the performance. The watermark should be designed to have most of its energy in the frequencies which filters change the least. These changes are to design a watermark has robustness to the most filters that may be applied to the watermarked image. [21]

1.9 EVALUATION IN WATERMARKING

The visual quality metrics are used as a measurement of distortions that added by watermarking process. The difference in visual quality can be distinguished by the data due to embedding of the watermark and the watermarked data due to attacks performed on it. One of the important requirements of the visual quality is the high probability of the data degradation due to the watermarking operation are not affected to the visual quality .Two commonly measurements that are used to determine the error between images are: Mean Square Error (MSE) and PSNR. [20]

Mean Squared Error (MSE): is the old measurement type that used to confirm control and quality of images. The mean squared error (MSE) is defined as:

$$MSE = \frac{1}{N}\sum^{N}(F_i' - F_i)^2$$

Where F is the original image, and F_i' is the output signal of the watermarked image.

Peak Signal to Noise Ratio (PSNR): The PSNR is most commonly used for measuring the quality of image watermarking. The PSNR is a ratio between the maximum value of a signal and the noise in watermarked image. It is most easily defined due to the mean squared error (MSE).

$$PSNR = 10\, log_{10}\ \frac{255^2}{MSE}$$

Where i is the sum over and j is denote the sum over all image pixels. Increasing in PSNR value is increasing reliability in compression. In general when the PSNR is 40 dB or larger, then the two images are virtually cannot distinguished by human observers. The transformed image is almost identical to the original. [24]

CHAPTER II

TRANSFORM DOMAIN WATERMARKING ALGORITHIMS AND RADON TRANSFORM ALGORITHM

2.1 TRANSFORM DOMAIN WATERMARKING ALGORITHMS

Spatial domain and transform domain are the main processing domains that have been proposed in watermarking algorithms. The watermark technique that based on the spatial domain is separate the watermark data to be embedded in the pixel value. That means this approach uses small changes in the pixel value intensity. The main idea of this approach is to embed the watermark in the least significant bit of image pixels. [25] The watermark data should inserted in a reliable and robust way via modification the significant portions of low frequency components of images. In other words, an image is divided into the same size of blocks and a certain watermark data is added with the sub-blocks. [26] Nevertheless, the disadvantages of the spatial domain are still having low-bit capacity and less robustness to lossy compression. [27] Transform domain watermarking techniques have more robust to the image manipulation from the spatial domain techniques, because the transform domain watermarking is not use the original image for embedding the watermark data. [16]

2.1.1 TRANSFORM DOMAIN EMBEDDING AND EXTRACTION

1. **Embedding**: The block diagram below is the transform domain watermark embedding. The embedding process is as follows:

A. The image is transformed using transform domains which are DWT or DCT.

B. The watermark data is embedded in a transformed image (watermark data is inserted into transformed coefficients).

C. Inverse transform is performed on the transformed watermarked image. [28.29]

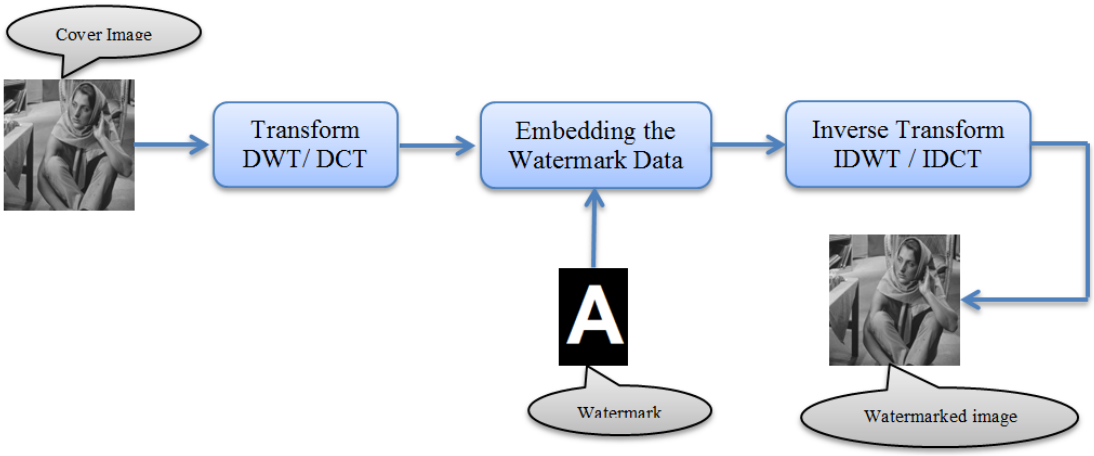


Figure 2.1 Transform Domain Embedding

2. **Extracting**: The watermark extraction process is the inverse procedure of the watermark embedding process as it drawn in diagram below. To extract the watermark data from the watermarked image:

A. The watermarked and the original image are transformed using the DCT or DWT.

B. The transformed image is extracted from the transformed watermarked image.

C. The difference between the original image and the watermarked image is the watermark data. [28,29]

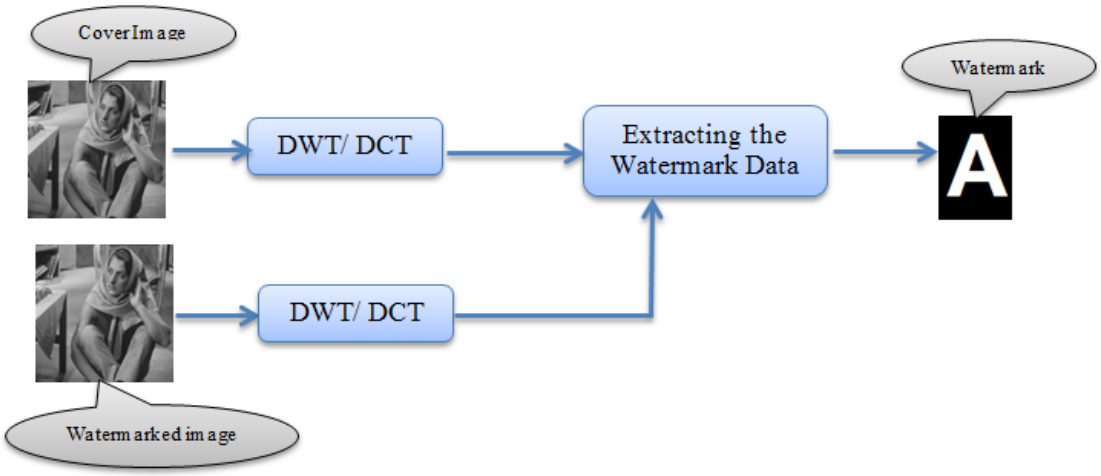


Figure 2.2 Transform Domain extractions

2.2 DISCRETE WAVELET TRANSFORM

In this section the basic idea of the Discrete Wavelet Transform (DWT) for one dimensional and two dimensional signals are described.

2.2.1 1D Discrete Wavelet Transform

To understand the basic idea of the DWT we focus on one dimensional signal. A DWT is split the signal into two parts, *high frequency* and *low frequency*. The high frequency part contains large edge components of the signal. The process of splitting the low frequency into high and low frequency is continued until the signal has been entirely decomposed. Generally, there are five decomposition steps for compression and watermarking applications. Moreover, the original signal can be reconstructed from the DWT coefficients. The reconstruction process is called the Inverse Discrete Wavelet Transform (IDWT). The signal is passed through a set of high pass filters and passed through a set of low pass filters to analyze the high and the low frequencies. The low-pass and high-pass filter pair are called analysis filter-bank. [16, 32]

Mathematically, the DWT and IDWT can be expressed as follows. Let

$$H(W) = \sum_K h_k \,.\, e^{-\,jkw}$$

And

$$G(W) = \sum_K g_k \,.\, e^{-\,jkw}$$

A signal *f (n)* can be decomposed recursively as:

$$f_{j-1}^{low}(k) = \sum_n h_{n-2k} \,.\, f_j(n)$$

And

$$f_{j-1}^{high}(k) = \sum_n g_{n-2k} \,.\, f_j(n)$$

The signal in each level is split in two and passed through the filters f_{j-1}^{low} low pass and f_{j-1}^{high} high pass.

The perfect reconstruction coefficient becomes:

$$f_j^{low} = \sum_k h_{n-2k} \,.\, f_{j-1}^{low}(k) + \sum_k g_{n-2k} \,.\, f_{j-1}^{high}(k)$$

To ensure the above IDWT and DWT relationship, the following orthogonally condition on the filters *H (w)* and *G (w)* most needed is:

$$|H(W)|^2 + |G(W)|^2 = 1$$

Which is known as the *Haar wavelet* filter.

2.2.2 2D Discrete Wavelet Transform

The 2D DWT is computed by performing low-pass and high-pass filtering of the image pixels. The low-pass is denoted h and a high-pass filter is denoted by g. The figure 2.3 is depicts the three levels of the 2D DWT decomposition. At each level, the high-pass filter generates detailed image pixels information, while the low-pass filter produces the coarse approximations of the input image. [31, 16]

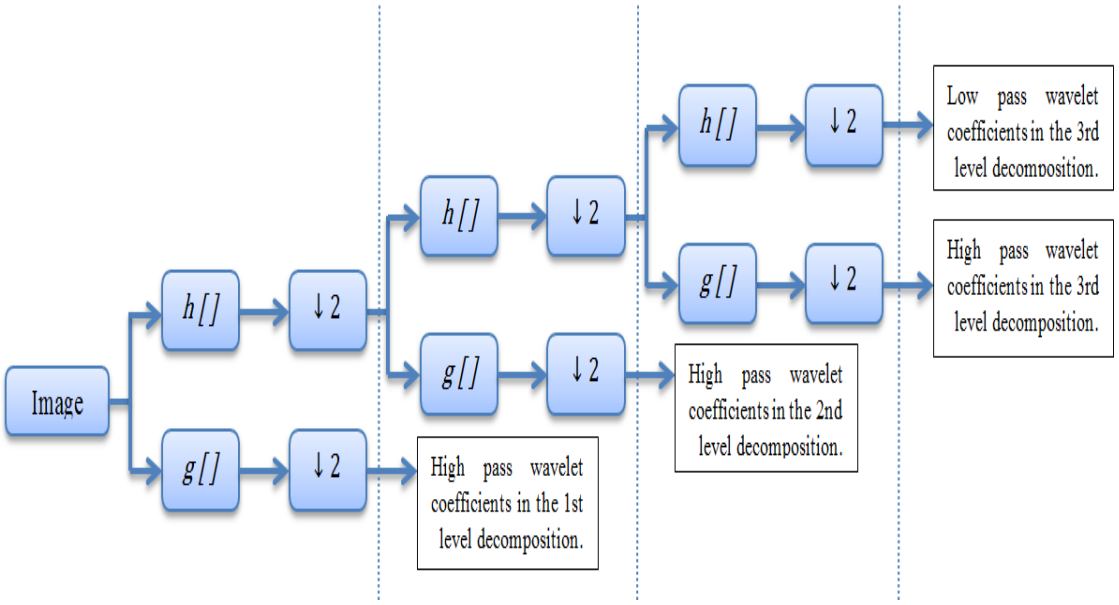
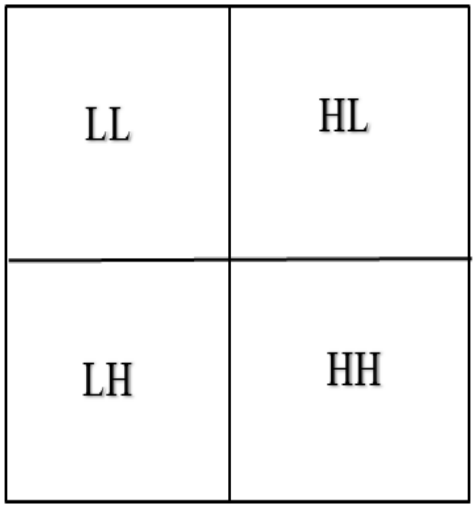


Figure 2.3 .Three level 2D DWT decomposition of an input image using filtering approach

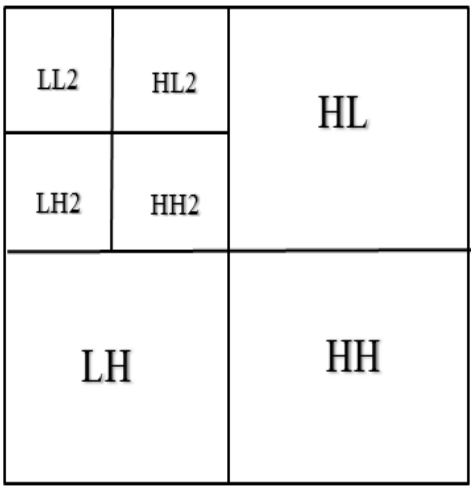
Where *h* and *g* are variables denote the low-pass and high-pass filters. The notation of (↓ 2) refers to down-sapling of the output coefficients by two. [33]

In this way an image can be decomposed into *pyramidal structure* as shown in figure 2.4. The DWT separates image into a lower resolution image *low-low* (LL), and horizontal *high-low* (HL), vertical *low-high* (LH) and diagonal *high-high* (HH) detail components. The amounts of DWT coefficients are larger in the lowest bands (LL) at each level of decomposition. Embedding the watermark in the higher level bands increases the robustness of the watermark. The high frequency bands can easily identify the edges and texture. Figure 2.4 shows the three levels DWT decomposition of Barbara. [23, 30]



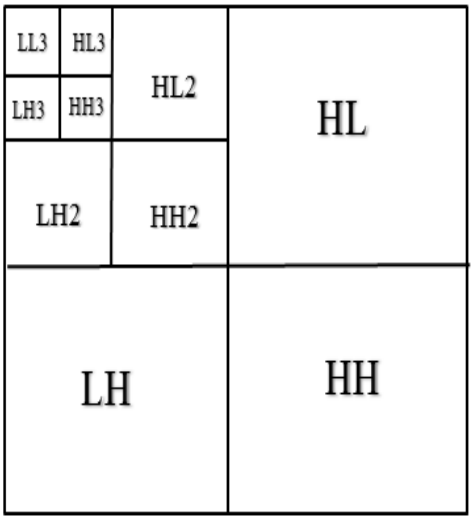
Layout of bands at first level decomposition

First level DWT decomposition of Barbara

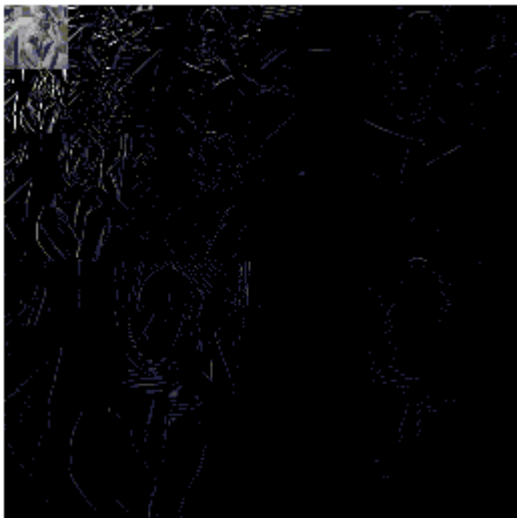


Layout of bands at second level decomposition

Second level DWT decomposition of Barbara



Layout of bands at third level decomposition



Third level DWT decomposition of Barbara

Figure 2.4: Three-level DWT decomposition of Barbara image.

2.3 PROPERTIES OF WAVELET TRANSFORM

Comparing the watermarking in DWT with watermarking in DCT, it has a number of advantages:

1. The DWT is a multi-resolution describes the image. Thus the image can be processed sequentially from a low resolution to the higher resolutions and viewed in different levels of resolution. [21]
2. The DWT is closer to the human visual system (HVS) than the DCT, as it separates the signal into individual bands, which can be processed separately. [34]
3. The images processed by DWT with high compression ratio are less damage than those processed at the same bit rate by the DCT.
4. The data structure that generates from DWT is known as scale space representation. Hence, the high frequency signals are located in the pixel domain and the low frequency signals are located in the frequency domain.
5. The spatial resolution of the DWT increases with frequency, which means the frequency resolution is independent of the frequency in the DCT domain, it is inversely proportional to frequency in the DWT. [3]

2.4 RADON TRANSFORM

The Radon transform is named after the Austrian mathematician Johann Radon that he showed the description of the function in terms of its projections and the Radon transform is the mapping from the function into the projections. Radon transform is used to compute the projection of an image f (x, y) for a given angles it can compute the projection of the image along the given angles. The resulting projection is the sum of the intensities of pixels in each direction. [35]

Radon transform is using in many applications in science and engineering. Radon transform is has good feature of transforms the information from two dimensional image into a string of one dimensional projections because many applications can be performed on the one dimensional data faster than the two dimensional image. Radon transform has many advantages especially in linear

feature detection such as the ability to detect line width and has robustness in noisy images. [36, 37]

The Cartesian rectangular coordinates of the distance and angels *(t,θ)* are mapping the Radon transform and it's known as polar coordinates. [35] Figure 2.5 illustrates the 1D projection *P (t,θ)* of the 2D function *f(x, y)* and the *P (t,θ)* is gives the Radon transform of the function *f(x, y)* where

$$P(t,\theta) = R(t,\theta)[f(x,y)] = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)\,\delta(t - x\cos\theta - y\sin\theta)dx\,dy$$

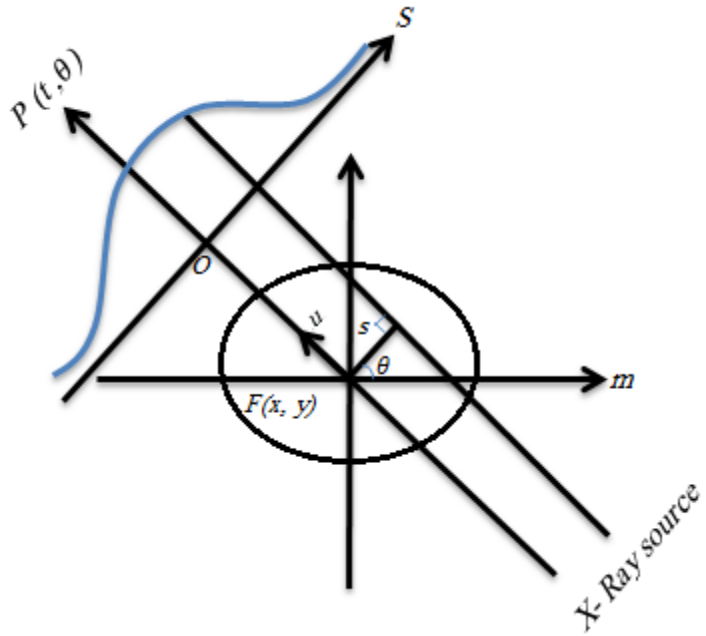


Figure 2.5. Schematic illustration of Radon transform in tomography

The source and sensor are rotated around the center of the object θ degrees. Intensity of ray for each angle q from the source ray is passed from the sensor and it repeats the operation for the number of angles θ is generally given as [0:180].

In image processing, the Radon transform has some advantages are as the following: [38].

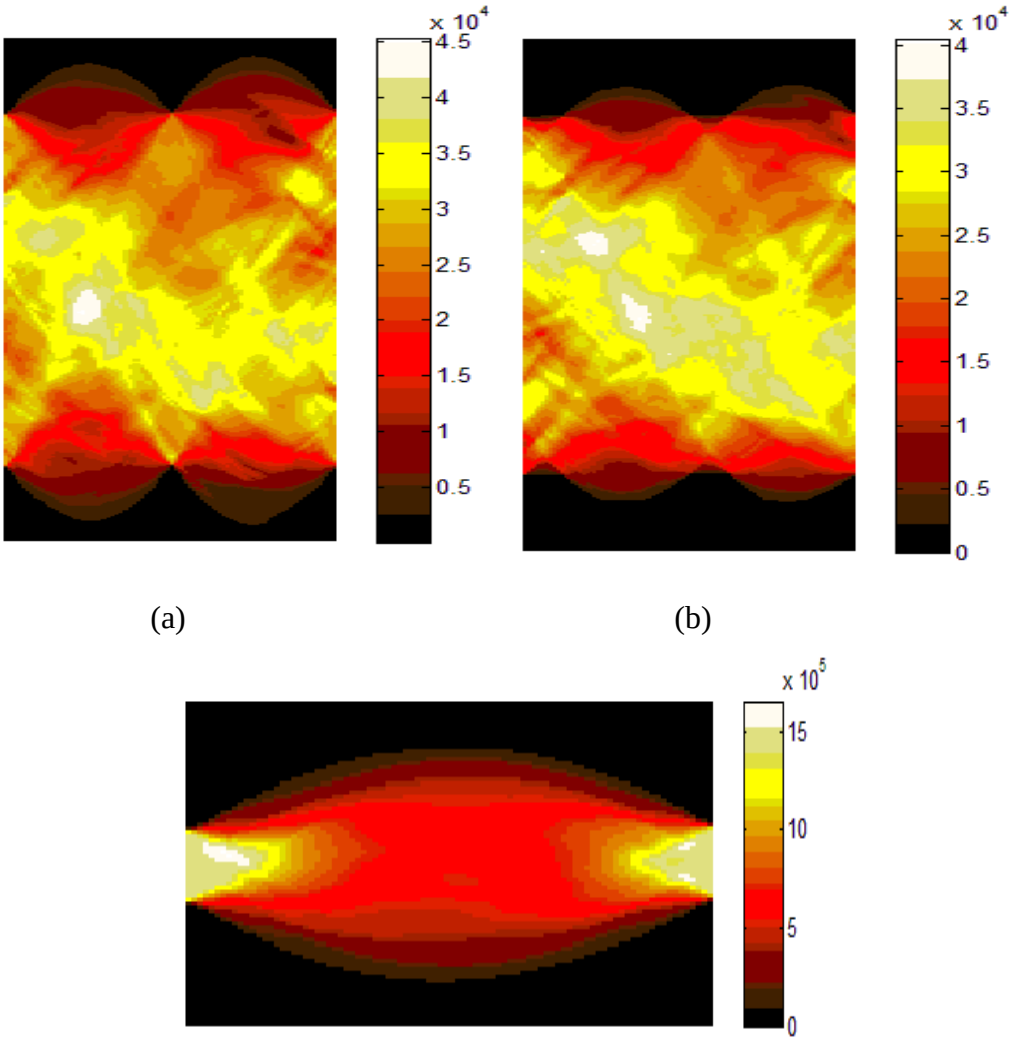
1. If the image rotated θ angle, the Radon transform will shift same amount.

$$I(x\ \cos\emptyset\ - y\ \sin\emptyset\ , x\ \sin\emptyset + y\ \cos\emptyset) \leftrightarrow \mathrm{R}\ (\mathrm{x}, \theta + \emptyset\ )$$

2. If the image scale p factor, the Radon transform will scale same factor.

$$I(\ px\ , py\ ) \leftrightarrow \frac{1}{p}\ R(\ pX, \theta\ )$$

Example1. The Radon transforms of the image Barbara rotated (20) and scaled (20) the results of Barbara images are shown in fig 2.6.



(a) (b)

(c)

Figure 2.6 Radon transforms for (a) Barbara image (b) Barbara image rotated 20 degrees (c) Barbara image scaled 20 factors

Comparing the original image with the Radon transform of the rotated and scaled the image we see it shifted 20 degree to right in fig 2.6.b and scaled 0.2 factor in fig 2.6.c

2.5 THE INVERSE RADON TRANSFORM

The inverse Radon transform (IRT) is used the set of projection to rebuild an image [35]. Rebuilding problem is to finding the Inverse Radon transform of g(s,θ). [39]

$$g(s,\theta) \triangleq Rf, \quad -\infty < s < +\infty \ , \ 0 \leq \theta < \pi$$

The Inverse Radon transform is:

$$f(x,y) = \frac{1}{2\,\pi^2} \int_0^{\pi} \int_{-\infty}^{+\infty} [\left(\frac{\partial g}{\partial s}\right) (s\,,\theta)]\, ds\, d\theta\,,$$

$$x\ \cos\theta + y\ \sin\theta - s$$

In Polar coordinates

$$fp(r,\emptyset) \triangleq f\ (\ r\ \cos\theta\ , r\sin\theta\ )$$

$$f(x,y) = \frac{1}{2\pi^2} \int_0^{\pi} \int_{-\infty}^{+\infty} [\left(\frac{\partial g}{\partial s}\right) (s\,,\theta)]\, ds\, d\theta\ ,$$

$$r\ \cos(\ \theta - \ \emptyset\ ) - s$$

The Inverse Radon transform is generated as follows:

1. The each projection $g(s,\theta)$ is passes through one dimensional filter, which frequency is$|\varepsilon|$.
2. The result of $g(s,\theta)$is back projected to produce$f(x,y)$.

Backprojection algorithm is used to compute the inverse Radon transform. This algorithm forms an approximation of the original image based on the projections in

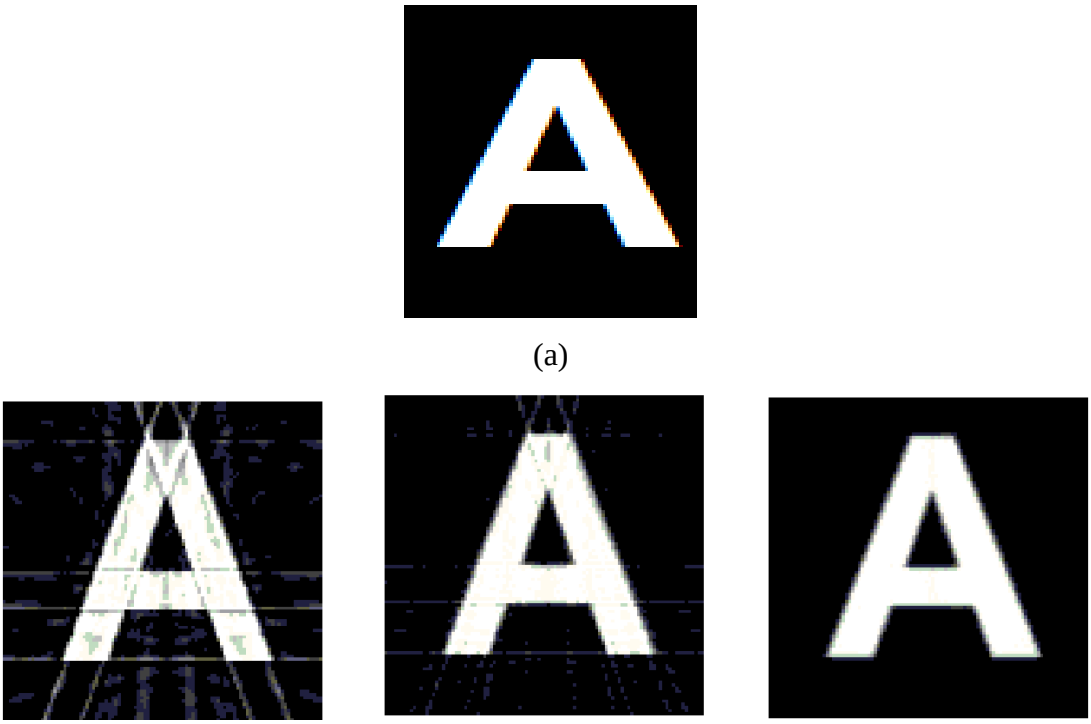
the columns. For more accurate result can be obtained by using more projections in the rebuilding process. Whenever the number of projection is approaching the length of theta the rebuilding image will have more accurately approximates the original image [37].

Occasionally, the noise can be exposure in the projections. In this case the window filters are used to remove the high frequency noise and attenuate it.

The inverse Radon transform has many windowed filters as shown below:

value	Descreption
Ram-Lak	Cropped Ram-Lak or ramp filter. This is the default. The frequency response of this filter is |f|. Because this filter is sensitive to noise in the projections, one of the filters listed below might be preferable. These filters multiply the Ram-Lak filter by a window that deemphasizes high frequencies.
Shepp-Logan	Multiplies the Ram-Lak filter by a sinc function
Cosine	Multiplies the Ram-Lak filter by a cosine function
Hamming	Multiplies the Ram-Lak filter by a Hamming window
Hann	Multiplies the Ram-Lak filter by a Hann window
None	No filtering. When you specify this value, iradon returns unfiltered backprojection data.

The example below explains how to reconstruct an image from parallel projection data with test image logo A. We use three different sets of theta values. First we set 18 projections, the second 36 projections, and the third has 90 projections to compute the Radon transform. Finally, reconstruct the image from the projection data. The following figure shows the results of all three reconstructions.



(a)

(b) (c) (d)

Figure 2.7. (a) Original image (b) reconstructed image from 18 projections (c) reconstructed image from 36 projections (d) reconstructed image from 90 projections

Notice the image in figure 2.7 (b), which was rebuild from only 18 projections has the least accurate obvious. The image figure 2.7 (c), which was reconstructed from 36 projections, is more efficient; however it is still unclear enough to excellence the small deterioration in the lower part of the image. The figure 2.7 (d), reconstructed using 90 projections, the result is most closely similar to the original image. That means when the number of projections is comparatively small the reconstruction can include some parts from the backprojection.

CHAPTER III
WATERMARKING ALGORITHMS USING DWT BASED ON RADON TRANSFORM

Multimedia watermarking is divided into three major schemes:

1. Spatial domain watermarking is the basic type which embeds a visible logo or stamp to selected pixels in cover image.

2. Transform domain watermarking which are DCT, DWT or DFT.

3. Compressed domain watermarking that embeds only in audio or video. A video watermarking is still open research; video watermarking should satisfy to some requirements in embedding such as transparency, robustness, blind, free-from deadlock problem, public key detection, etc.

Watermarking algorithms using DWT based on Radon transform schemes, we used semi-blind watermarking. In this chapter we will talk about DWT watermark insertion algorithms using Radon transform and experimental results in images as follows:

1. Multi watermarking with Radon transform and first level DWT decomposition.

2. Radon transformation based multi watermarking using second level DWT decomposition.

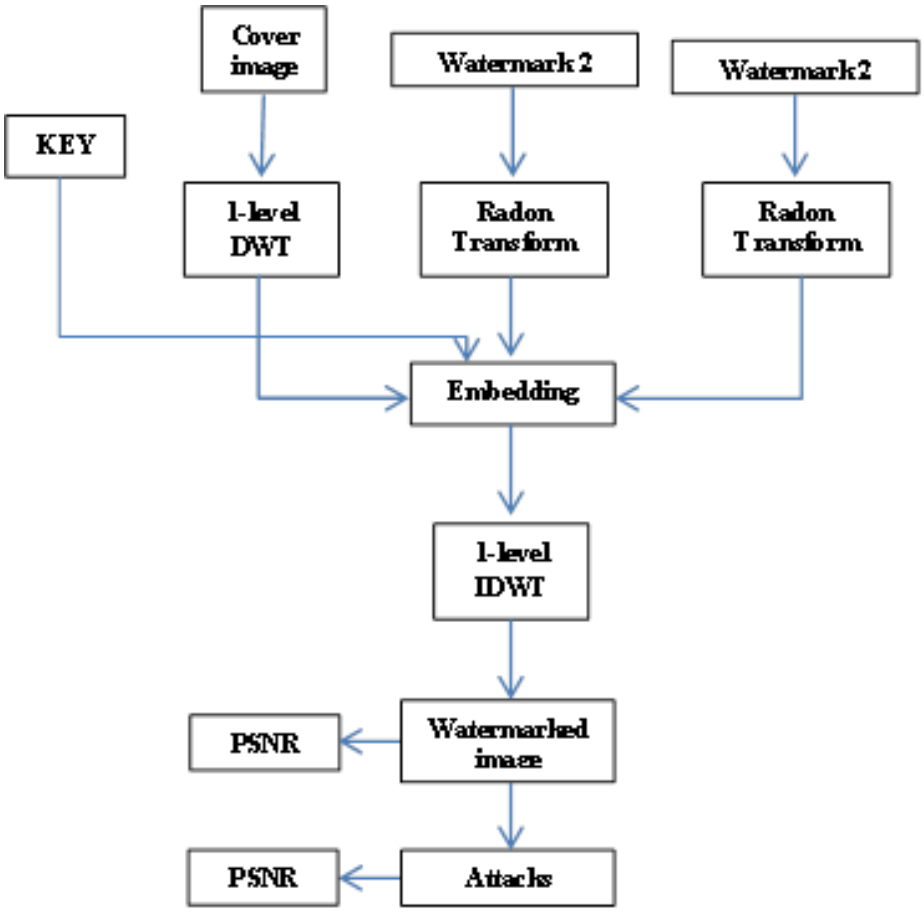
3. Watermarking with third level DWT decomposition based on Radon transform.

3.1 MULTI WATERMARKING WITH RADON TRANSFORM AND FIRST LEVEL DWT DECOMPOSITION

In this section the watermarking method is used the wavelet transform and Radon transform which mixture Radon transform and first level Discrete Wavelet Transform which embed the watermark in the low pass band .The point privacy transform into the line privacy by the Radon transform and the wavelet transform has capability in dealing with the point privacy.

The watermark embedding and extraction algorithms can be summarized as follows:

Watermark Embedding:



The steps are:

1. Convert the cover image into grayscale image and resize the result into 256 * 256

2. Apply DWT to the cover image to separate the image into four bands and use LL and HH sub bands for embedding.

3. Apply Radon transform with theta 0:2:179 to the watermark1 and watermark2.

4. Resize the two results to the old size which is 128 * 128 before the embedding process.

5. Use the embedding method to embed the watermark1 and watermark2 into the LL and HH respectively.

$$\boldsymbol{LL(i,j) = LL(i,j) + RE * R(i,j)};$$

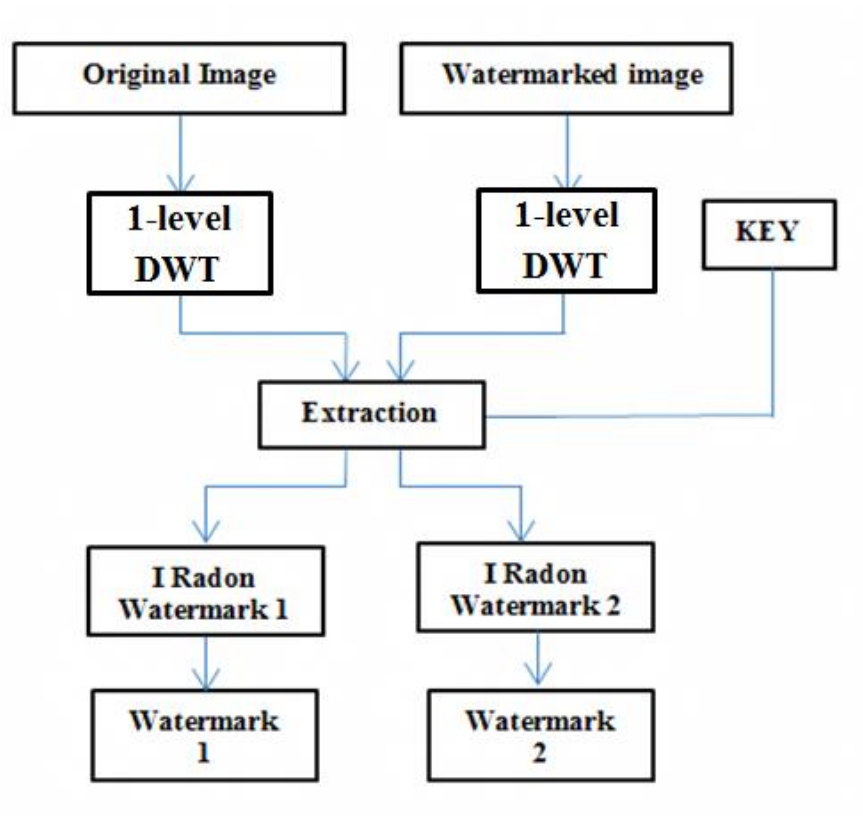
$$\boldsymbol{HH(i,j) = HH(i,j) + RE * R1(i,j)};$$

The R is the Radon transform of the first watermark. The R1 is the Radon transform of the second watermark; RE is the key which is 0.05.

6. Compute the inverse DWT to reconstruct the image (watermarked image).

Watermark Extracting:

The steps of extracting the watermarks from the watermarked image are the inverse steps of embedding method.



The steps are as follows:

1. Compute 1-level DWT decomposition to watermarked image or attacked image to separate the image into four bands and get the LL and HH bands.

2. Compute 1-level DWT decomposition to the original image to separate the image into four bands and get the LL and HH bands.

3. Apply the extraction method with the key to extract the embedded watermarks from LL and HH

$$\boldsymbol{hLL(i,j) = (hLL(i,j) - LL1(i,j))/RE};$$
$$\boldsymbol{hHH(i,j) = (hHH(i,j) - HH1(i,j))/RE};$$

4. Resize obtained $\boldsymbol{hLL(i,j)}$and $\boldsymbol{hHH(i,j)}$ to Radon size before the inverse Radon transform.

5. Compute Inverse Radon transform for $\boldsymbol{hLL(i,j)}$ and $\boldsymbol{hHH(i,j)}$ to reconstruct watermark 1 and watermark 2.

In this section, the watermark is embedded to the low frequency (LL) band of the image and the high frequency (HH) together. In above paper the value of RE and that we assume it as the key is chosen as 0.05. In our extension to the DWT-based approach [40], we embed the two watermarks in two bands (LL and HH) using same scaling factors for the bands.

Each level of decomposition results four bands of data which are LL, HL, LH, and HH. The LL subband can be decomposed to get another four subbands. This process is continued until reach the number of levels that determined. Figure 3.1 shows first level of decomposition of Barbara to be watermarked.

(a) (b)

Figure 3.1: (a). First Level DWT Decomposition, (b).First Level DWT Decomposition of Barbara

3.1.1 Experimental results:

In this method, we used the MATLAB R2011a as performing program. The code is applied to many images like cameraman, Lena and goldhill but the tested image is Barbara as shown in figure 3.2 which is 512*512. The sizes used in the two watermarks are 128*128 as shown in figure 3.2.

Original Barbara

Watermarked Barbara (PSNR = 43.1546)

Two watermarks

Figure 3.2: Embedding in Barbara Image

Matlab was used for all attacks. many different attacks like Gaussian noise, Mean filter, Resize, rotate, equalization, intensity adjustment and Gamma correction are applied to the watermarked image as shown in figure 3.3 [41] .

Gaussian noise
(Mean = 0, variance = 0.001)

Median Filtering
(Window size=3x3)

Scaling
(256→ 128 → 256)

Rotation
(20 Degree)

Histogram Equalization
(Automatic)

Intensity Adjustment
([L=0 H=0.8] , [B=0 T=1])

Gamma Correction
(1.5)

PSNR values before and after attacks for proposed method are shown in table 3.1:

Table 3.1

PSNR VALUE OF BARBARA	
WATERMARKED IMAGE	**43.1546**
ATTACKS	
GAUSSIAN NOISE	**29.8321**
MEAN FILTER	**28.5504**
SCALING	**28.3933**
ROTATE	**12.0599**
EQUALIZATION	**17.4939**
INTENSITY ADJUSTMENT	**18.2578**
GAMMA CORRECTION	**17.8500**

Extraction

The following are the watermarks extracted from attacked images.

1. Extract watermarks from the original image:

PSNR value (59.0972)

PSNR value (50.0951)

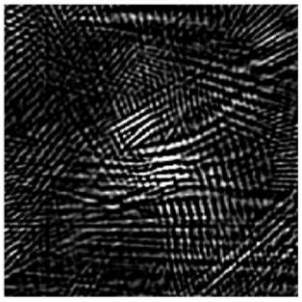
2. Extracted watermarks from the image attacked by Gaussian noise:

PSNR value (42.1003)

PSNR value (42.3350)

3. Extracted watermarks from the image attacked by mean filter:

PSNR value (42.5009)



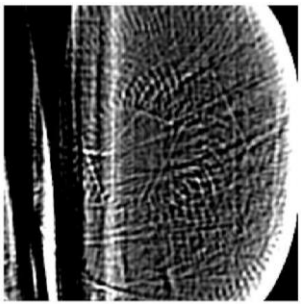
PSNR value (36.0771)

4. Extracted watermarks from the image attacked by scaling:

PSNR value (40.5411)

PSNR value (35.4980)

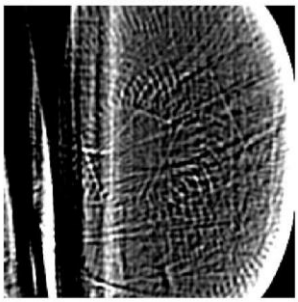
5. Extracted watermarks from the image attacked by rotation:



PSNR value (31.9972)

PSNR value (40.5941)

6. Extracted watermarks from the image attacked by intensity adjustment:



PSNR value (38.8965)

PSNR value (40.9805)

7. Extracted watermarks from the image attacked by equalization:

PSNR value (36.4552)

PSNR value (39.6941)

8. Extracted watermarks from the image attacked by Gamma correction:

PSNR value (41.2964)

PSNR value (45.1315)

In this part, digital watermark based on wavelet transform and Radon transform is proposed algorithm .This method has good performers in invisibility for embedding watermark. Moreover proposed method has good robustness to the Gaussian attack, mean filter attack, scaling attack, rotation attack, equalization attack, intensity attack and Gamma attack. The process of digital watermark embedding in this paper is simple and the ability to embed two different watermarks at the same time.

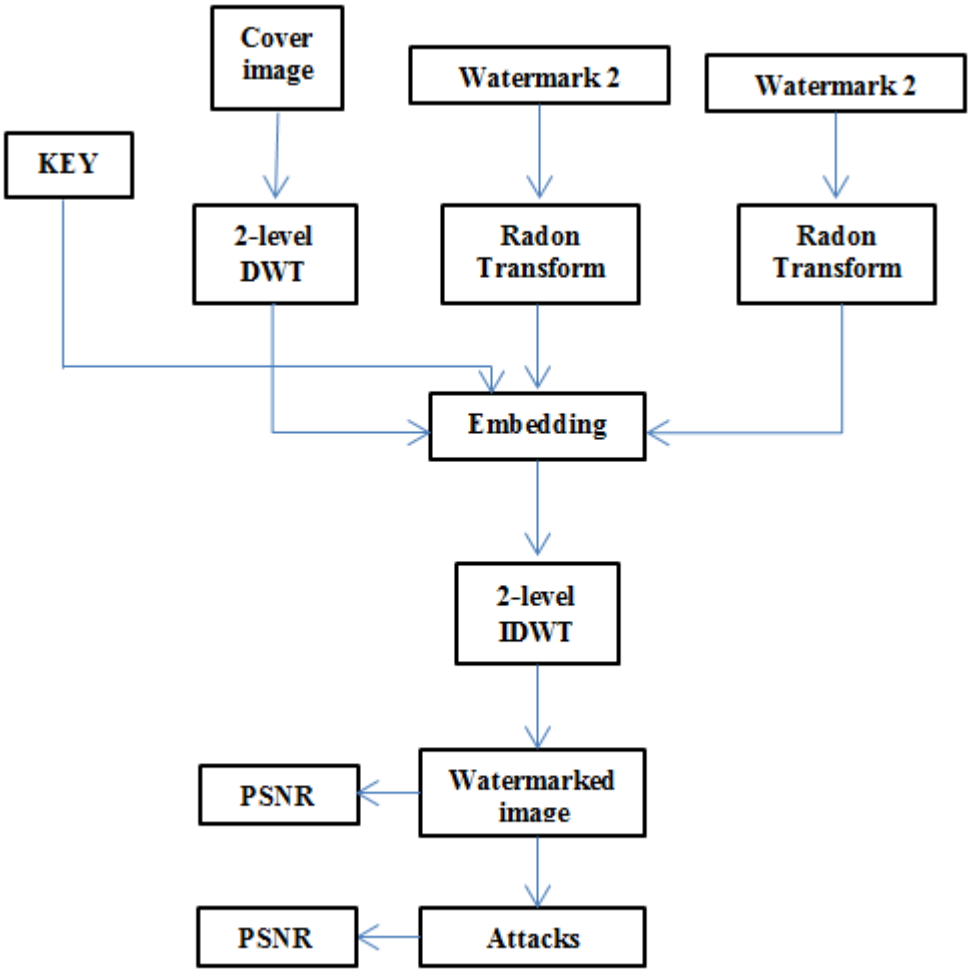
3.2 RADON TRANSFORMATION BASED MULTI WATERMARKING USING SECOND LEVEL DWT DECOMPOSITION

In this section, we used the semi-blind watermark which is used the secret key for extract or detect the embedded watermark. The basic idea of Radon transform in this paper is to convert the 2-D image information to 1-D image and embed it in the second level of DWT in (HH2) and (HL2) of the low frequency (LL) band.

This method is used to obtain more security to the watermark and make it difficult as possible to detect and good robustness to the attacks.

The watermark embedding and extraction algorithms can be summarized as follows:

Watermark Embedding:



Watermark embedding steps are:

1. Resize the image to 256*256 and convert the image to gray scale image X.

2. Resize the watermarks to 64*64 W1 and W2.

3. Separate the image by the second level DWT decomposition for the low frequency and use the HL2 and HH2 for embedding.

4. Radon transforms to the watermark W1 and W2.

5. Resize the W1 and W2 to 64*64.

6. Embed the W1 and W2 into the second level DWT with HL2 and HH2 sequentially and use the key RE which is 0.05 scale factor in this paper.

$$\boldsymbol{R(i,j) = RE * R(i,j) + HL2(i,j);}$$

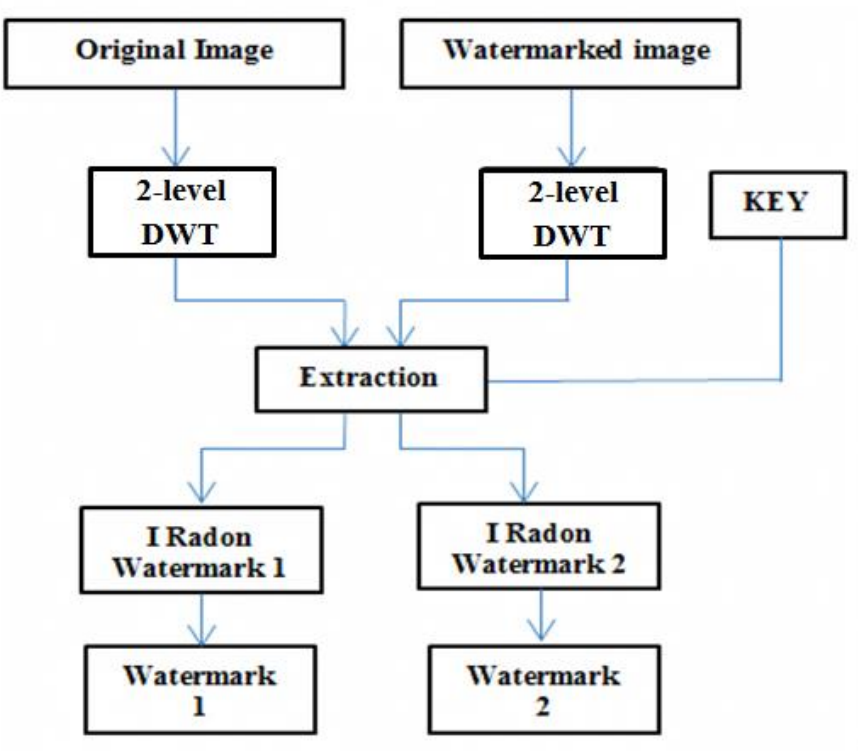
$$\boldsymbol{R1(i,j) = RE * R1(i,j) + HH2(i,j);}$$

7. Replace the old HL2 and HH2 with new R and R1.

8. Compute the inverse second level DWT to obtain the watermarked image A0.

Watermark Extraction:

The steps of extracting the watermarks from the watermarked image are the inverse steps of embedding method.



The steps are as follows:

1. Compute the second level DWT for the watermarked image or attacked image.

2. Compute the second level DWT for the original image.

3. Extract the HL2 and HH2 of watermarked image from original image using the key RE which is 0.05.

$$HL2 = HL2 - hHL2\ /RE$$
$$HH2 = HH2 - hHH2\ /RE.$$

4. Resize the results of extracting to 367*90 (the size of the watermarks after the Radon transform.

5. Radon transform to HL2 and HH2 to get the watermarks.

3.2.1 Experimental Results

The experimental results are implemented on Barbara 512*512 resized to 256*256 image shown in figure 3.4.a and the two watermarks are 256*256 resized to 64*64 image as shown in figure 3.4.c and the key is 0.05 .the watermarked image is shown in figure 3.4 The PSNR is **49.2532**.

a. Original Barbara

b. watermarked Barbara (PSNR =49.2532)

c. Two watermarks

Figure 3.3: Embedding in Barbara Image

Matlab was used for all attacks. many different attacks like Gaussian noise, Mean filter, Resize, rotate, equalization, intensity adjustment and Gamma correction are applied to the watermarked image as shown in figure 3.4 .

Gaussian noise
(Mean = 0, variance = 0.001)

Median Filtering
(Window size=3x3)

Scaling
(256 → 128 → 256)

Rotation
(20 Degree)

Histogram Equalization
(Automatic)

Intensity Adjustment
([L=0 H=0.8] , [B=0 T=1])

Gamma Correction
(1.5)

PSNR values before and after attacks for proposed method are shown in Table 3.2.

Table 3.2

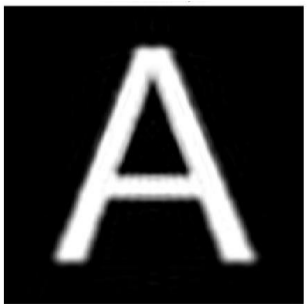
PSNR VALUE OF BARBARA	
WATERMARKED IMAGE	**49.2532**
ATTACKS	
GAUSSIAN NOISE	**29.9481**
MEAN FILTER	**28.6161**
SCALING	**28.5071**
ROTATE	**12.0716**
EQUALIZATION	**17.4773**
INTENSITY ADJUSTMENT	**18.5571**
GAMMA CORRECTION	**17.6297**

Extraction

The following are the watermarks extracted from attacked images.

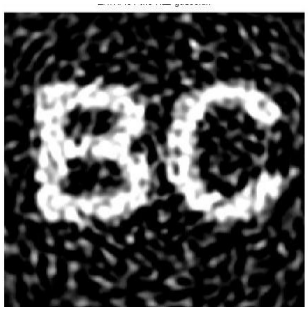
1. Extract watermarks from the original image:

PSNR value (46.6903)

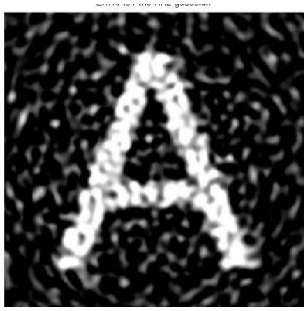


PSNR value (48.0023)

2. Extracted watermarks from the image attacked by Gaussian noise:

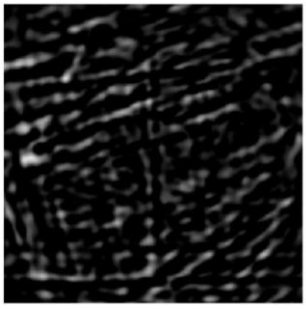


PSNR value (43.5228)

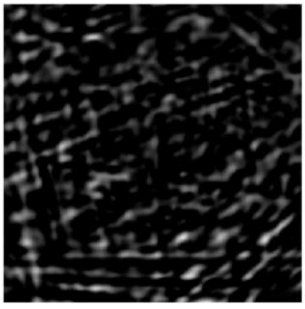


PSNR value (44.2307)

3. Extracted watermarks from the image attacked by mean filter:

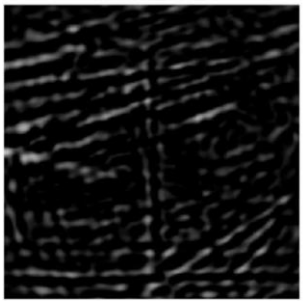


PSNR value (34.2754)

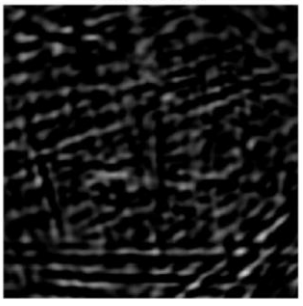


PSNR value (36.7358)

4. Extracted watermarks from the image attacked by scaling:

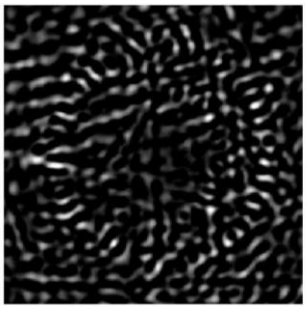


PSNR value (34.9934)

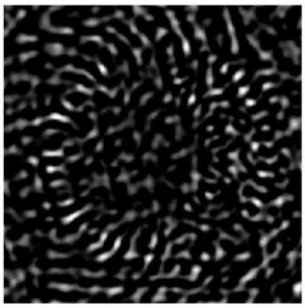


PSNR value (35.9497)

5. Extracted watermarks from the image attacked by rotation:



PSNR value (34.3528)



PSNR value (35.0394)

6. Extracted watermarks from the image attacked by intensity adjustment:

PSNR value (43.5314)

PSNR value (44.9081)

7. Extracted watermarks from the image attacked by equalization:

PSNR value (44.2359)

PSNR value (46.4150)

8. Extracted watermarks from the image attacked by Gamma correction:

PSNR value (43.2007)

PSNR value (45.0714)

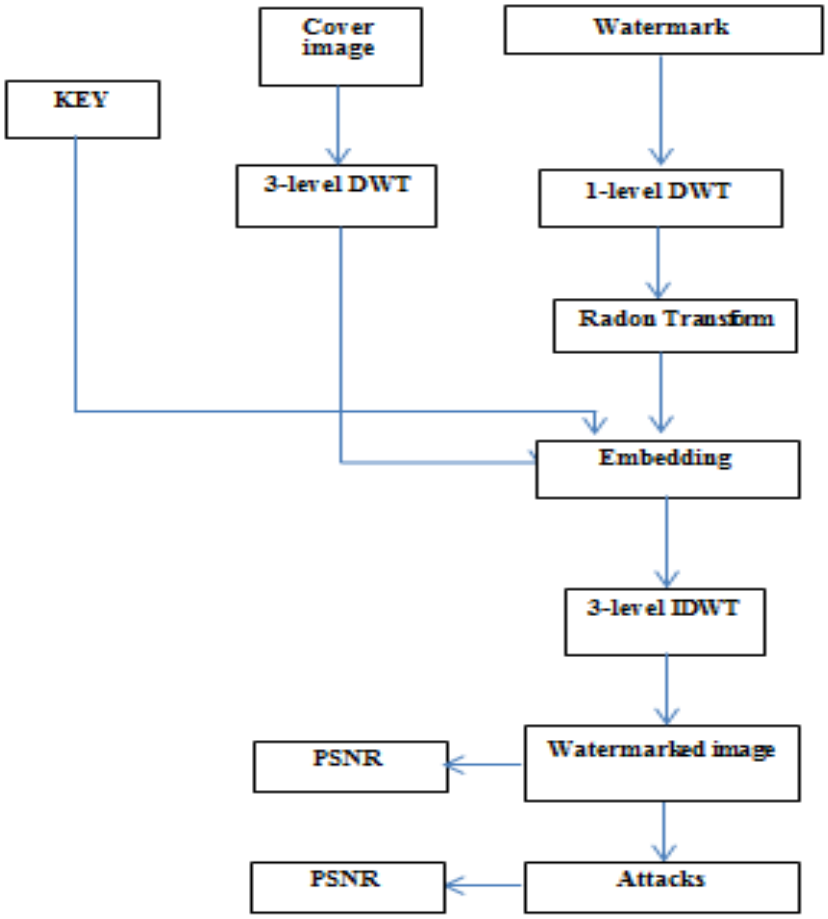
In this method, we proposed a watermarking method based on Radon transform using two watermarks with second level DWT decomposition. The proposed method has more invisibility than the previous algorithm and high robustness to the attacks, Gaussian noise, mean filter, scaling, rotate, equalization, intensity adjustment and Gamma correction. The concept of embedding watermark using Radon transform that granted is very difficult to detect and extract.

3.3 WATERMARKING WITH THIRD LEVEL DWT DECOMPOSITION BASED ON RADON TRANSFORM

In this section, we use the Radon transform with 3 levels DWT decomposition. In the watermark embedding the cover image is converted to 3 levels DWT using the low frequency. After computing the three DWT of the layer we compute the first DWT for the watermark and convert the four bands to Radon transform before the embedding process. The next step is the embedding process which embeds the watermark confidents with the third level DWT LL3, LH3, HL3 and HH3 sequentially. In final step, converts the results to obtain the image with inverse DWT decomposition.

The proposed watermark embedding and extraction algorithms are as follows:

Watermark Embedding



Watermark embedding steps are:

1. Resize the image to 512 * 512 and convert the image to gray scale image X.

2. Resize the watermarks to 128*128 of W.

3. Separate the image by the third level DWT decomposition for the low frequency to use the LL3, LH3, HL3 and HH3 for embedding.

4. Compute the first level DWT for the watermark.

5. Radon transforms to first DWT confidents for the watermark.

6. Resize the all results of the Radon transform to 64*64.

7. Embed the Radon R1, R2, R3 and R4 into the third level DWT with LL3, LH3, HL3 and HH3 sequentially and use the key RE which is 0.001 scale factor in this paper.

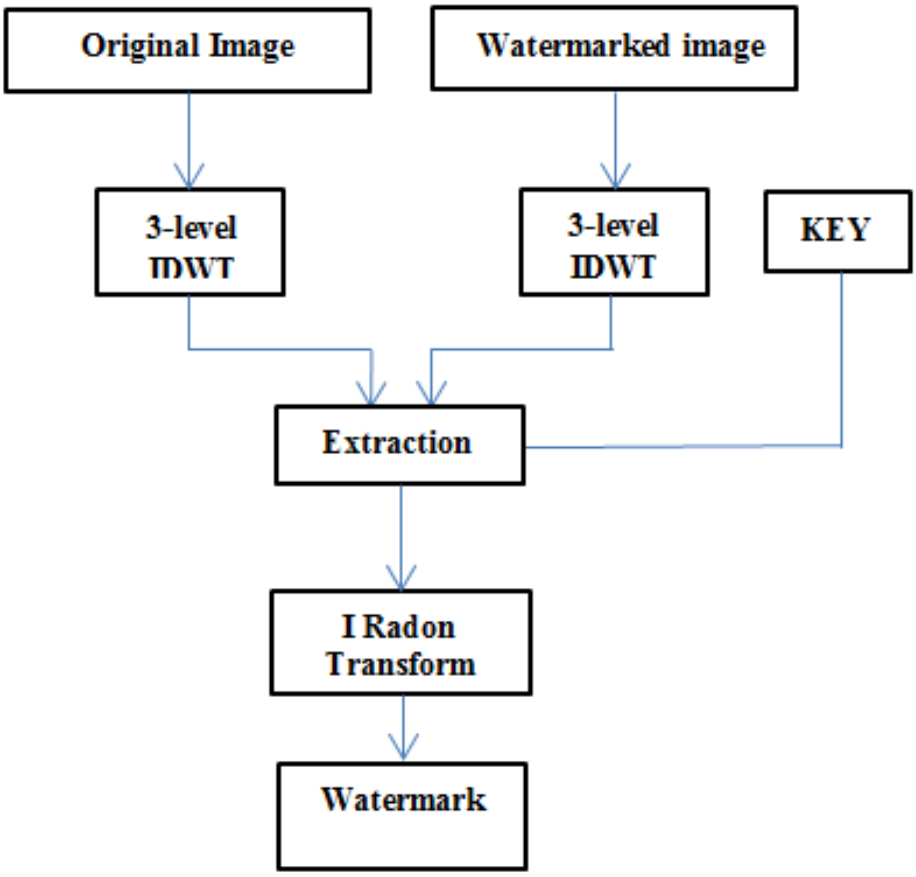
$$\boldsymbol{R1(i,j) = RE * R1(i,j) + LL3(i,j)};$$

8. Replace the old LL3, LH3, HL3 and HH3 with new R1, R2, R3 and R4.

9. Compute the inverse third level DWT to obtain the watermarked image A0.

Watermark Extraction:

The steps of extracting the watermarks from the watermarked image are the inverse steps of embedding method.



The steps are as follows:

1. Compute the third level DWT for the watermarked image or attacked image.

2. Compute the third level DWT for the original image.

3. Extract the LL3, LH3, HL3 and HH3 of watermarked image from original image using the key RE which is 0.001.

$$\boldsymbol{hLL3(i,j) = (hLL3(i,j) - LL33(i,j))/RE};$$

4. Resize the results of extracting $\boldsymbol{hLL3}$ to 207*90 (the size of the watermarks after the Radon transform.

5. Inverse Radon transforms hLL3, hLH3, hHL3 and hHH3 to get the watermark.

3.3.1 Experimental Results

The experimental results are implemented on Barbara 512*512 image shown in figure 3.4 and the two watermark is 256*256 resized to 128*128 image and the key is 0.001 . The PSNR is **45.7278**.

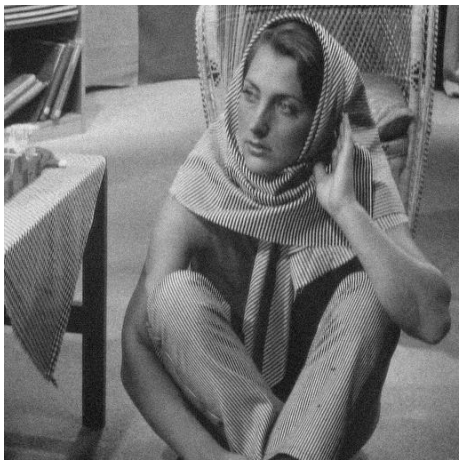
Original Barbara

watermarked Barbara (PSNR = 45.7278)

Watermark

Figure 3.4: Embedding in Barbara Image

Using Matlab many different attacks like Gaussian noise, Mean filter, Resize, rotate, equalization, intensity adjustment and Gamma correction are applied to the watermarked image as shown in figure 3.5 .



Gaussian noise
(Mean = 0, variance = 0.001)

Median Filtering
(Window size=3x3)

Scaling
($256 \rightarrow 128 \rightarrow 256$)

Rotation
(20 Degree)

Histogram Equalization
(Automatic)

Intensity Adjustment
([L=0 H=0.8] , [B=0 T=1])

Gamma Correction
(1.5)

PSNR values before and after attacks for proposed method are shown in Table 3.3.

Table 3.3

PSNR VALUE OF BARBARA	
WATERMARKED IMAGE	**45.7278**
ATTACKS	
GAUSSIAN NOISE	**29.9227**
MEAN FILTER	**25.0134**
SCALING	**24.7021**
ROTATE	**11.7035**
EQUALIZATION	**18.0411**
INTENSITY ADJUSTMENT	**18.2639**
GAMMA CORRECTION	**17.9435**

Extraction

The following are the watermarks extracted from attacked images.

1. Extract watermarks from the original image:

PSNR value (46.6903)

2. Extracted watermarks from the image attacked by Gaussian noise:

PSNR value (44.5228)

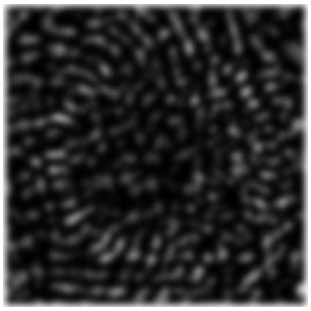
3. Extracted watermarks from the image attacked by mean filter:

PSNR value (34.2754)

4. Extracted watermarks from the image attacked by scaling:

PSNR value (35.4980)

5. Extracted watermarks from the image attacked by rotation:



PSNR value (33.4332)

6. Extracted watermarks from the image attacked by intensity adjustment:

PSNR value (42.9081)

7. Extracted watermarks from the image attacked by equalization:

PSNR value (45.5314)

8. Extracted watermarks from the image attacked by Gamma correction:

PSNR value (44.1315)

In this section, we proposed a watermarking method based on Radon transform using one watermark converted using one level DWT decomposition embedded with third level DWT decomposition of the cover image. The proposed method has good invisibility and high robustness to the attacks, Gaussian noise, mean filter, scaling, rotate, equalization, intensity adjustment and Gamma correction.

CONCLUSION AND FUTURE WORK

Conclusion

In this thesis, the robustness of Discrete Wavelet Transform watermarking algorithms on digital images has been evaluated using seven different attacks. We have proposed three watermarking methods which are based on DWT and Radon transform.

The spatial domain watermarking is not inspected or used because it is extremely sensitive to lossy compression and the most of attacks remove it.

The robustness of the watermarking methods has been measured by comparing the watermarked image or attacked image with the original image. This helped us to measure the amount of damage done by each attack.

In two main instances, the attacks destroy the embedded watermark data.

First, when the watermark data is embedded in high frequency HH components of the images which is proposed in first method. Therefore the noise removal algorithms like median filter destroy it.

Secondly, the watermarking algorithm and the attack are not based on the same operation. This is the case in three methods when scaling and rotation attacks applied in watermarked image.

The experiments is shows that for group of attacks (resizing, adding Gaussian noise, median filtering, and rotation, histogram equalization, intensity adjustment, Gamma correction).

The embedding in the first method has more accurate result in terms of extracting the watermarks from the images attacked by rotation scaling and Mean filter. While the extraction in intensity adjustment, histogram equalization and Gamma correction less accurate result of the two proposed methods.

Another observation is that the embedding using the second level DWT decomposition using Radon transform method is typically better watermarking than the first and the third methods, for both reasons of robustness and invisibility.

Embedding in the second level DWT proved to be highly resistant to most of the attacks than the embedding in the first level DWT, while the PSNR value 49.2532 dB which has the best invisibility. However the extraction in mean filter, scaling and rotation we did not get the results because the attacks removed the watermarks that embedded in the watermarked image.

In addition, as we showed in the third method which embeds the first level DWT of Radon transform in the third level DWT decomposition of cover image has a good invisibility and high security and the most difficult method in detection.

However, the resizing in the Radon stage led to decrease the resistance and the extraction from attacked images.

Future Works

This study described here measured the robustness of the proposed watermarking methods against the seven types of attacks. These attacks are aimed to destroy the watermark data in the image and make the extraction difficult as mentioned in Chapter 3.

Our study can be extended to include more types of attacks and try to measure the robustness of the algorithms against them.

In this study we have used a group of test images for measuring the robustness of each method like (cameraman, Lena, godhill) but we have not classified the images.

Expand the scope of our study we can use images with different frequency and applying them to the attacks.

As well as, Future work will concentrate on finding better methods based on the proposed methods to get better accuracy results in extracting the watermarks.

REFERENCES

[1] Saraju Prasad Mohanty, *Watermarking of Digital Images" A Project Report Submitted in Partial Fulfillment of the Requirement for the degree of Master of Engineering.*

[2] Yusnita Yusof1, Othman O. Khalifa1, (e.g. 1954). *," Imperceptibility and Robustness Analysis of DWT-based Digital Image Watermarking*. 1st ed. Proceedings of the International Conference on Computer and Communication Engineering 2008 May 13-15, 2008 Kuala Lumpur, Malaysia.

[3] Yoseph abate . *Digital image Watermarking " A thesis submitted in partial fulfillment of The requirements for the degree of M..sc.. in computer engineering*.

[4] M. Yeung et al, *Digital Watermarking for High-Quality Imaging", Proc. IEEE First Workshop on Multimedia Signal Processing, Princeton, New Jersey, pp- 357-362, June 1997.*

[5] S. P. Mohanty, et al, *A Dual Watermarking Technique for images", Proceedings*.

[6] P. Chan, M. R. Lyu and R. T. Chin. *Copyright Protection on the Web: A Hybrid Digital Video Watermarking Scheme," Proceedings 13th International World Wide Web Conference, New York.*.

[7] Ian ping li,simon x.young,stephone jaffard ,bruno torresani,john yen , *watermarking wavelet active media technology and information processing" processing of international computer conference.*.

[8] L. Massey "Contemporary cryptology: *An introduction. In Contemporary Cryptology" The Science of Information Integrity, G. J. Simmons, editor, pages New York, IEEE.*

[9] F. Hartung and M. Kutter ,*Multimedia watermarking techniques", Proceedings of the IEEE, Vol. 87, No. 7, pp 1079 – 1107, July 1999.*

[10] Ehsan syed , (e.g. 1954). *Digital Watermarking " The University of Texas at Arlington – Spring 2011*.

[11] M. Barni et al, , (e.g. 1954). *Copyright protection of digital images by embedded unperceivable marks", Image and Vision Computing, pp897-906, Aug 1998.*

[12] .N. Ahmed, et al, , (e.g. 1975). Discrete cosine transform", IEEE Trans. Computers, Vol. 23(1),. *e.g. Jet Powered Motors*.

[13] V. Britanak, *"Discrete Cosine Transform: Properties, Algorithms, Advantages, Applications", Academic Press Publications, ISBN 978-0-12- 373624-6, Boston, 1990.*

[14] J. Cummins, *Steganography and digital watermarking", School of Computer Science, The University of Birmingham, 2004 Website*

[15] Dr.Ersin Elbaşı, ". *A Survey on Digital Image & Video Watermarking", First Portion of Second Examination Report, Graduate Center, CUNY, 2006.*

[16] Mitra Abbasfard , (e.g. 1954). *Digital Image Watermarking Robustness: A Comparative Study" submitted in partial fulfillment of the requirements for the degree of MASTER OF SCIENCE.*

[17] Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal G. Shamoon, *Secure spread spectrum watermarking for multimedia. In Proceedings of the IEEE International Conference on Image Processing, ICIP '97, volume 6, pages 1673 – 1687, Santa Barbara, California, USA, October 1997.*

[18] J. J. K. Ó Ruanaidh, S. Pereira, *A secure robust digital image watermark", In Electronic Imaging: Processing, Printing and Publishing in Colour, SPIE Proceedings, Zürich, Switzerland, May 1998. (SPIE/IST/Europto Symposium on Advanced Imaging and Network Technologies).*

[19] N. Terzija, M. Repges, K. Luck, W. Geisselhardt, *Digital Image Watermarking Using Discrete Wavelet Transform: Performance Comparison of Error Correction Codes", published in Proceedings of the Second IASTED International Conference* .

[20] N. Terzija, W. Geisselhardt, .*Robust Digital Image Watermarking Based on Complex Wavelet Transform", In WSEAS Transactions on Communication, Issue 10, Volume 4, pp 1086-1092, October 2005, ISSN 1109-2742.*

[21] S. Voloshynovskiy, S. Pereira, V. Iquise, T. Pun, *Attack modelling: Towards a second generation benchmark", Signal Processing, 81, 6, pp. 1177-1214, June 2001. Special Issue: Information Theoretic Issues in Digital Watermarking, 2001. V. Cappellini, M. Barni, F. Bartolini, Eds*.

[22] Ersin Elbaşı "MULTIMEDIA SECURITY: DIGITAL IMAGE and VIDEO WATERMARKING "A dissertation submitted to the Graduate Faculty in Computer Science in partial fulfillment of the requirements for the degree of Doctor of Philosophy,2007

[23] S. Katzenbeisser, F.A.P Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking”, Artech House, Boston – London 2000.

[24] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, A Digital Watermark, Proc. IEEE Int. Conf. on Image Processing, Sebtember 1994,.

[25] R. B. Wolfgang and E. J. Delp, A Watermark for Digital Images, Proc. IEEE Int. Conf. on Image Processing, 1996, pp. 219–222.

[26] M. S. Hsieh, D. C. Tseng, and Y. H. Huang, Hiding Digital Watermarks using Multiresolution Wavelet Transform, IEEE Trans. on Industrial Electronics 48 (2006), no. 5, 875–882.

[27] Salwa A.K Mostafa†, A. S. Tolba†† , F. M. Abdelkader†, Hisham M. Elhindy† " Video Watermarking Scheme Based on Principal Component Analysis and Wavelet Transform " IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009 .

[28] Peining Tao, *Digital Image Processing”, First Portion of Second Examination Report, Graduate Center, CUNY, 2004*

[29] M. Ferretti and D. Rizzo, *A Parallel Architecture for the 2D Discrete Wavelet Transform with Integer Lifting Scheme, Journal of VLSI Signal Processing 28 (2001), 165–185*

[30] durga sowjanya, k n h srinivas and p venkata ganapathi "fpga i mplementation of efficient vlsi a rchitecture for fixed poin 1-d dwt using lifting scheme " International Journal of VLSI design & Communication Systems (VLSICS) Vol.3, No.4, August 2012.

[31] P. Sasikala , Dr. R.S.D. Wahidabanu " Robust R Peak and QRS detection inElectrocardiogram using Wavelet Transform" *(IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 1, No.6, December 2010.*

[32] A. K. Jain, Fundamentals of digital image processing, Prentice-Hall, NJ; 1985.

[33] Jayaraman S, Veerakumar T, Esakkirajan S " DIGITAL IMAGE PROCESSING" 2009 tata mcgraw hil education private limited .

[34] Dr. AbdulSattar M. Khidhir ,Mosul Technical Institute, (). *Use of Radon Transform in Orientation Estimation of Printed Text"ICIT 2011 The 5th International Conference on Information Technology*.

[35] . Zhang and I. Couloigner, *Accurate Centerline Detection and Line Width Estimation of Thick Lines Using the Radon Transform", IEEE Trans. On Image Processing..*

[36] Horance H.S Ip ,Oscar C.Au , Howard Leung , Ming Ting Sun , Wei ying ma , shi min Hu, *advances in multimedia information processing – PCM 2007 " 8th pacific rim conference on multimedia Hong Kong ,china ,December 2007 proceedings*

[37] Madhuri a.joshi , *Digital Image Processing An Algorithmic Approach" 2006 by prentice-hall of India private limited, new Delhi*.

[38] E. Elbasi, A. M. Eskicioglu, (). *A DWT-Based Robust Semi-Blind Image Watermarking Algorithm Using Two Bands", IS&T/SPIE's 18th Annual Symposium on Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII Conference, San Jose, CA, January 15–19, 2006*. 1st ed.

[39] R.Dugad, K.Ratakonda, and N. Ahuja, "A new wavelet-based scheme for watermarking images", *Proceedings of the IEEE International Conference on IImage Processing*, ICIP 1998, Chicago, IL, USA, October 1998.

[40] Ersin Elbaşı " Robust multimedia watermarking: Hidden Markov model approach for video sequences " Turk J Elec Eng & Comp Sci, Vol.18, No.2, 2010, c_ TUBITAK

[41] I. J. Cox and M. L. Miller. A review of watermarking and the importance of perceptual modeling. In Proceedings SPIE Electronic Imaging '97, Storage and Retrieval for Image and Video Databases V, San Jose, CA, February 1997.

[42] G. C. Langelaar. Conditional access to television service. In Wireless Communication, the Interactive Multimedia CD-ROM, 3rd edition, Amsterdam, TheNetherlands: Baltzer Science, 1999.

APPENDIX A

Examples for the three proposed methods on Cameraman and Lena images

A. TESTED ON CAMERAMAN IMAGE:

1. Embedding in the Cameraman using first method

Original Cameraman

Watermarked Cameraman (PSNR =43.2230)

Two watermarks

Figure 5.1: Embedding in Cameraman Image using first method

PSNR values before and after attacks for first proposed method are shown in table 5.1:

PSNR VALUE OF CAMERAMAN	
WATERMARKED IMAGE	**43.2230**
ATTACKS	
GAUSSIAN NOISE	**29.8961**
MEAN FILTER	**25.1067**
SCALING	**24.6399**
ROTATE	**10.4928**
EQUALIZATION	**19.0915**
INTENSITY ADJUSTMENT	**17.5106**
GAMMA CORRECTION	**18.8414**

2. Embedding in the Cameraman using second method

Original Cameraman

Watermarked Cameraman (PSNR =49.0118)

Two watermarks

Figure 5.2: Embedding in Cameraman Image using second method

PSNR values before and after attacks for second proposed method are shown in table 5.2:

PSNR VALUE OF CAMERAMAN	
WATERMARKED IMAGE	**49.0118**
ATTACKS	
GAUSSIAN NOISE	**30.0751**
MEAN FILTER	**25.1350**
SCALING	**24.6875**
ROTATE	**10.4949**
EQUALIZATION	**19.1462**
INTENSITY ADJUSTMENT	**17.7347**
GAMMA CORRECTION	**18.6255**

3. Embedding in the Cameraman using third method

Original Cameraman

Watermarked Cameraman (PSNR =45.7211)

Watermark

Figure 5.3: Embedding in Cameraman Image using third method

PSNR values before and after attacks for third proposed method are shown in table 5.3:

PSNR VALUE OF CAMERAMAN	
WATERMARKED IMAGE	**45.7211**
ATTACKS	
GAUSSIAN NOISE	**29.9815**
MEAN FILTER	**32.3221**
SCALING	**31.5713**
ROTATE	**10.4842**
EQUALIZATION	**18.9947**
INTENSITY ADJUSTMENT	**17.5294**
GAMMA CORRECTION	**18.8064**

B. TESTED ON LENA IMAGE:

1. Embedding in the Lena using first method

Original Lena

Watermarked Lena (PSNR =43.1546)

Two watermarks

Figure 5.4: Embedding in Lena Image using first method

PSNR values before and after attacks for first proposed method are shown in table 5.4:

PSNR VALUE OF LENA	
WATERMARKED IMAGE	**43.1546**
ATTACKS	
GAUSSIAN NOISE	**29.8113**
MEAN FILTER	**29.2603**
SCALING	**28.7133**
ROTATE	**11.3705**
EQUALIZATION	**18.9911**
INTENSITY ADJUSTMENT	**17.6715**
GAMMA CORRECTION	**17.9800**

2. Embedding in the Lena using second method

Original Lena

Watermarked Lena (PSNR =49.2532)

Two watermarks

Figure 5.5: Embedding in Lena Image using second method

PSNR values before and after attacks for second proposed method are shown in table 5.5:

PSNR VALUE OF LENA	
WATERMARKED IMAGE	**49.2532**
ATTACKS	
GAUSSIAN NOISE	**30.0214**
MEAN FILTER	**29.3335**
SCALING	**28.8359**
ROTATE	**11.3786**
EQUALIZATION	**18.9957**
INTENSITY ADJUSTMENT	**17.9311**
GAMMA CORRECTION	**17.7553**

3. Embedding in the Lena using third method

Original Lena

Watermarked Lena (PSNR =45.7278)

Watermark

Figure 5.6: Embedding in Lena Image using third method

PSNR values before and after attacks for third proposed method are shown in table 5.6:

PSNR VALUE OF LENA	
WATERMARKED IMAGE	**45.7278**
ATTACKS	
GAUSSIAN NOISE	**29.9012**
MEAN FILTER	**34.6418**
SCALING	**34.7609**
ROTATE	**11.3352**
EQUALIZATION	**18.9949**
INTENSITY ADJUSTMENT	**17.6920**
GAMMA CORRECTION	**17.9702**

APPENDIX B

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, name: SIDDIK, OMER

Nationality: Iraq

Date and place of birth: 18/06/1987, IRAQ / KIRKUK

Marital state: Single

Phone: +905319899381, +9647701317157

Email: omersubhi87@yahoo.com, c1074504@student.cankaya.edu.tr

EDUCATION

Degree	Institution	Year of Graduation
MS	Çankaya Univ. Mathematics and Computer Science	2013
BS	AL Mansour University Collage	2010
High School	Kirkuk	2006

FOREIGN LANGUAGES

Turkish, Arabic, Kurdish, English

HOBBIES

Image Processing, Mathematic, Cars and Football.