An Efficient Digital Image Watermarking System based on Contourlet Transform and Discrete Wavelet Transform

By

Zainab Nouman Yousif Al-Qudsy

Supervised By

Prof. Nidal Shilbayeh

Master Thesis

Submitted in Partial Fulfillment of the

Requirements for the Master Degree

In Computer Science

Department of Computer Science
Faculty of Information Technology
Middle East University
Amman – Jordan

May, 2011

Middle East University

Authorization Statement

I, Zainab Nouman Yousif, authorize Middle East University to supply hardcopies and electronic copies of my thesis to libraries, establishments, or bodies and institutions concerned with research and scientific studies upon request, according to the university regulations.

Name: Zainab Nouman Al-Qudsy

Date: 5/9/2011

Signature: Zainab

II

Middle East University

Examination Committee Decision

This is to certify that the thesis entitled "An Efficient Digital Image Watermarking System based on Contourlet Transform and Discrete Wavelet Transform" was successfully defended and approved in May / 2011.

Examination Committee Members	**Signature**
Dr. Nidal F. Shilbayeh Professor Department of Computer Science Middle East University	
Dr. Hazim A. Farhan Assistant professor Department of Computer Science Middle East University	
Dr. Mohammad E. Malkawi Associate professor Dean of college of Engineering Jadara University	

Acknowledgements

“In the name of Allah the Most Gracious and the Most Merciful”. First of all, my great thanks and appreciations go to my advisor Prof. Nidal Shilbayeh for his guidance, assistance, availability, making critical comments and numerous suggestions to improve this work. Finally, great thanks go to all staff of the faculty of the information technology department for offering me their exceptional Knowledge and experience during the course of our studies.

Dedication

To my parents,

For their taught me the love of knowledge.

To my husband,

For his support throw the years during the course of this work.

To my kids,

For their love and great patience.

Zainab Al-Qudsy

Table of Contents

List of tables

List of Figures

List of Abbreviations

CT	Contourlet Transform
DCT	Discrete Cosine Transform
DFB	Directional Filter Bank
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
GUI	Graphical User Interface
HVS	Human Visual System
HWT	Haar Wavelet Transform
JPEG	Joint Photographic Expert Group
LP	Lapulician Pyramid
LSB	Least Significant Bit
MATLAB	Matrix Laboratory
MSE	Mean Square Error
NCC	Normalized Cross Correlation
PN	Pseudo Random Noise
PSNR	Peak Signal to Noise Ratio

Abstract

The fast and continuous growth in using internet and the simplicity of copy and store processes of (images, audios, videos clips and texts) without pre-authorization from the owner, led to the appearance of digital image watermarking. The proposed system is one of the solutions for patent and copyright protection from those unauthorized users. Furthermore, it prevents unauthorized users from manipulation, illegal use and redistribution of such materials.

There are several available algorithms of digital image watermarking that currently used Discrete Wavelet Transform (DWT) or Contourlet Transform (CT) separately. In this thesis, we propose a new robust and secure system that is based on the combination between two different transforms DWT and CT. The new system has been implemented efficiently and successfully. The experimental results showed that combining two transforms improves the imperceptibility and robustness and provide better results in comparison with other algorithms based only on DWT or CT separately. The proposed system has been tested against five types of common image attacks. Performance evaluation of the proposed system shored improved results in terms of imperceptibility, robustness, and high tolerance against these attacks; accordingly, the system is very effective and applicable.

الملخص

النمو السريع والمتواصل في استخدام الانترنت وسهولة اجراء عمليات النسخ والتخزين للـ(الصور والصوتيات والافلام والنصوص) من دون الحاجة الى اي تفويض سابق من المالك ادى ظهور العلامة المائية للصور الرقمية. ان النظام المقترح هو احد الحلول لحماية الملكية وحقوق الطبع والنسخ من المستخدمين غير المخولين اضافة لذلك منع المستخدمين غير المخولين من التلاعب والاستخدام غير القانوني واعادة التوزيع لمثل هذه المواد .

هنالك الكثير من الخوارزميات للعلامة المائية المتوفرة حاليا تستخدم " Discrete Wavelet Transform (DWT) " او"Contourlet Transform (CT) " كل على انفراد..في هذه الرسالة قد تم اقتراح نظام جديد قوي وامن يعتمد على الدمج بين تحويلين مختلفين " DWT " و" CT " . ان النظام الجديد قد تم تطبيقه بفاعلية ونجاح. اظهرت النتائج التجريبية ان دمج التحويلين يحسن من قابلية الاخفاء وقوة النظام ويعطي نتائج افضل بالمقارنة مع الخوارزميات المعتمدة فقط على" DWT " و " CT" كل على انفراد. ان النظام المقترح قد تم تقييمة باستخدام خمسة انواع معروفة من "Image Attacks" وقد دل تقييم اداء النظام على ان النظام الجديد وبكل تاكيد يحسن النتائج من ناحية قابلية الاخفاء والقوة والمقاومة العالية ضد هذة الانواع من الـ "Attacks " وبالتالي فان النظام عالي الفعالية وممكن تطبيقة.

CHAPTER ONE

INTRODUCTION

Chapter 1

Introduction

1.1 Introduction

Today all users of the internet have the ability to download duplicate and retransmit the multimedia data legally or illegally due to the internet open environment. Many problems arise such as copyright protection and intellectual property. Digital watermarking is one of the possible solutions to solve such a problem. Digital watermarking is a process of hiding secret information called a watermark in original multimedia objects such as digital image, text document, audio and video clips. Researchers in the field of digital watermarking search on effective techniques provide two properties: imperceptibility (watermark not noticeable by viewer), and robustness against attacks that try to remove or destroy watermark.

Early image watermarking algorithms used special domain technique that represents image as pixels. Least Significant Bits (LSB_S) is one of the common methods used in special domain technique. In contrast to the special domain, frequency domain technique can embed more bits of watermark and more robust to attacks; thus, they are more attractive than special domain technique (Hsieh, Tseng, & Huang, 2001). Digital image watermarking utilizes many types of transforms such as Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and Contourlet Transform (CT). The reason of applying two transforms is based on the fact that the combined transform, could make up for the disadvantages of each other, so that effective watermarking approaches could

acquire (Amirgholipour, &Naghsh-Nilchi, 2009).

DWT has been used in digital image watermarking more frequently due to its excellent spatial localization and multiresolution characteristics, which are similar to the theoretical models of the human visual system (Al-Haj, 2007). DWT performance is increased by combining it with another transform.

CT has been developed as an improvement over wavelet. In addition to multiscale and time frequency localization prosperities of wavelet, CT has the capability of capturing directional information such as smooth contours and directional edges. So that, CT is well suited for images like maps were a lot of curves and text are present.

Any digital image watermarking system can be divided into two main subsystems but complimentary to each other: embedding subsystem and extracting subsystem. In embedding subsystem, the watermark is hidden in the original image to obtain watermarked image, and to measure imperceptibility. In extracting subsystem, the output of embedding subsystem (watermarked image) is the input, and the watermark is the extracted, and to measure robustness.

The watermark algorithm can be divided into two types according to whether the original image is required to extract the watermark: blind and non-blind. Blind algorithm does not need the original image in extraction. While, non-blind algorithm needs the original image to extract watermark.

In this thesis, a new suggested blind digital image watermarking algorithm based on combining DWT and CT is introduced and implemented. First, 1, 2, and 3 levels of DWT are applied and watermark is embedded in different sub-bands. Second, the same is done to CT as in DWT above, for the sake of comparison. Finally, DWT technique is improved

by combining it with CT. The main point of this thesis is to find the best subband for embedding which would provide better imperceptibility and robustness at the same time.

1.2. The Statement of the Problem

There are many digital image watermarking techniques utilized to hide secret information in the original image for the purpose of copyright protection and data authentication. The algorithm presented in this thesis, offers a good solution to overcome the problem of attacks after transmitting image through the internet or after performing some image operation like compression or cropping. Therefore, there is an essential need to propose a new improvement of digital watermarking techniques that is robust against different types of attacks and the extracted watermark which can be easily recognized.

1.3. Study Objectives

The following are the main objectives of this thesis:

1. Propose a new robust and secure watermarking algorithm that is based on combination of two powerful watermarking algorithms DWT and CT.
2. The new technique incorporates a high level of robustness and low image quality degradation.
3. The system has been designed and implemented successfully.
4. The implemented system shored a successful extraction method to extract watermark efficiently.
5. The performance of the system has been tested against five types of image attacks.

1.4. Significance of the Study

1. The system may provide a great benefit to medical application. Digital watermark can create hidden label and annotation in medical application since watermark might be used for identical patient records.
2. The system is a suitable solution for the problem of copyright protection and data authentication.
3. The system may be used in banks application. Watermark acts as a digital signature, giving the image a sense of ownership or authenticity.
4. The system may have great significance in fingerprint application because it is invisible and inseparable from the content. This type of application is useful for monitoring and tracing illegally produced copies of digital work.

1.5. Thesis Organization

In addition to this chapter, the thesis is organized as follows: chapter 2 provides an overview of watermarking techniques along with listing and explaining different related works that are mostly related to the proposed system. Chapter 3 describes in detail the system architecture and the different models and algorithms that are used in all parts of the system. Experimental results of the designed system are presented and discussed in detail in chapter 4. Finally, chapter 5 includes conclusion and future work including recommendations.

CHAPTER TWO

Literature Review and Related Works

Chapter 2

Literature Review and Related Works

2.1. Literature Review

2.1.1. Watermarking Definition

Watermarking is a branch of information hiding which is used to hide secret information in multimedia data like digital images, text documents, audios, or video clips. Specifically, a digital image watermark is a label that is embedded inside an image. It acts as a digital signature, giving the image a sense of ownership or authenticity.

2.1.2. Watermarking Applications

Watermark can be used in many applications. Such as:

- Copyright protection

  Watermarking can be used to protect redistribution of copyright material and to prevent unauthorized tampering with multimedia data (audio, video, image, text).

- Fingerprinting

  Associating unique information about each distributed copy of digital content is called fingerprinting, and watermarking is an appropriate solution for that application because it is invisible and inseparable from the content. This type of application is useful for monitoring or tracing illegally produced copies of digital work.

- Medical application

  Digital watermarks can also create hidden labels and annotations in medical applications, and for multimedia indexing and content-based retrieval applications. In the medical application, watermarks might be used for identifying patient records.

- Monitoring broadcast

  Watermarking can also be used for broadcast monitoring which refers to verifying whether the content that support to be broadcast (on TV or Radio) has really been broadcast.

2.1.3. Watermarking Prosperities

When implementing a watermark system, several properties must be observed, which are the following (Emek, &Pazarci, 2005):

- Imperceptibility: an embedded watermark is truly imperceptible if a user cannot distinguish original from the watermarked version.
- Robustness: it should not be possible to remove or alter the watermark without sufficient degradation of the perceptual quality of the host data.
- Payload: the amount of information that can be stored in a watermark depends on the application. Generally, 60 to 70 bits of information should be embedded in the host data.
- Security: according to Kerckhoff's assumption, the security of the encryption techniques must lie in the choice of key. This assumption is also valid for watermark techniques.

2.1.4. General Digital Image Watermarking Framework

All the digital watermarking systems are constructed from two subsystems but complimentary to each other's, these are:

- Embedding subsystem
- Extracting subsystem

Figure 2.1 shows the components of embedding and extracting subsystems.

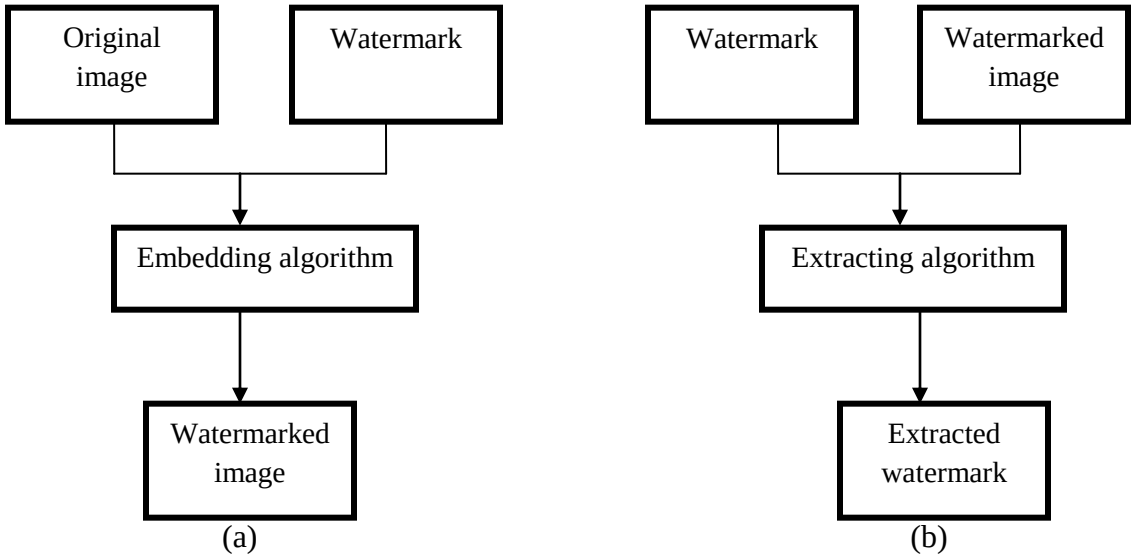


Figure 2.1 :(a) embedding subsystem (b) extracting subsystem

2.1.5. Watermarking Classification

There are different criteria which can be used for classifying watermarking techniques, these are:

2.1.5.1. From the imperceptibility aspect

We can classify watermark system to visible and invisible watermark systems.

- **Visible watermark system:** the watermark can be seen by naked eyes like watermark in dollar bills.
- **Invisible watermark system:** the watermark hides into host image in a way that causes an imperceptible distraction.

2.1.5.2. From the types of domain aspect

Images can be represented in spatial and frequency domains. In the frequency domain, images are represented in terms of their frequencies, while in the spatial domain, images are represented by pixels.

Special Domain Watermarking

Embedding a watermark in the spatial domain scatters the information to be embedded making it hardly detectable. These techniques are advantageous in their resistance to cropping, but they are weak to attacks like noise and compression. The most straightforward way to add a watermark to an image in the spatial domain is to

add a pseudorandom noise pattern to the luminance values of its pixels. Several methods are based on this principle (Emek, &Pazarci, 2005).

Frequency or Transform Domain Watermarking

Embedding a watermark in a transform domain proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital Watermarking algorithms. Commonly used frequency-domain transforms include the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Haar Wavelet Transform (HWT) and Contourlet Transform (CT) (Shilbayeh,&Alshamary, 2010).

In general, the frequency-based approaches are better than the spatial-based ones based on the following observations:

• In the frequency domain, more bits of watermark can be embedded into the original image.

• In the frequency domain, watermarked image being more robust to attacks.

1. The Discrete Wavelet Transform based techniques (DWT)

Discrete Wavelet Transform (DWT) based techniques are more powerful and popular since DWT has a number of advantages over other transforms including space-frequency localization, multi resolution representation, superior HVS modeling, linear complexity and adaptively. It locates regions of high frequency or middle frequency to embed information imperceptibly. Even though, DWT is popular, powerful and familiar among watermarking techniques, it has its own limitations in capturing the directional information such as smooth contours and the

directional edges of the image. This problem is addressed by contourlet transformation (CT) (Khalighi,&Rabiee, 2009).

2. The Contourlet Transform based techniques (CT)

CT was developed as an improvement over wavelet. We select CT for watermark embedding because it captures the directional edges and smooth contours better than other transforms. Since the human visual system is less sensitive to the edges, embedding the watermark in the directional sub-band improves the imperceptibility of the watermarked image, but it is hardly robust. To achieve robustness we can embed the watermark in the lowpass image of the contourlet decomposition. However the imperceptibility of the watermarked image degrades.

3. The Discrete Cosine Transform (DCT) (Amirgholipour, &Naghsh-Nilchi, 2009)

The discrete cosine transforms (DCT) is a technique for converting a signal into elementary frequency components. It represents an image as a sum of sinusoids of varying magnitudes and frequencies. With an input image, x, the coefficients for the output "image," y, is:

$$y(u,v)=\sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha_u\alpha_v\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}x(m,n)\cos\frac{(2m+1)u\prod}{2M}\cos\frac{(2n+1)v\prod}{2N}\ldots\ldots\ldots \quad \mathbf{2.1}$$

Where

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{2}} & u = 0 \\ 1 & u = 1,2,...,N-1 \end{cases}$$

$$\alpha_v = \begin{cases} \frac{1}{\sqrt{2}} & v = 0 \\ 1 & v = 1,2,...,N-1 \end{cases}$$

The input image, x, is N pixels wide by M pixels high; x(m,n) is the intensity of the pixel in row m and column n. y(u,v) is the DCT coefficient in row u and column v of the DCT matrix.

DCT domain watermarking segments the image into non-overlapping blocks of 8x8 and applies DCT to each of the blocks which results with three frequency sub-bands: low, mid and high frequencies in each block as shown in Figure 2.2. Much of the signal energy lies at low frequencies which contain the most important visual parts of the image, and the high frequency components are easily removed through compression and noise attacks. The watermark is embedded by modifying the coefficients of the middle frequency bands so that the visibility of the image will not be affected and the watermark will not be removed by compression.

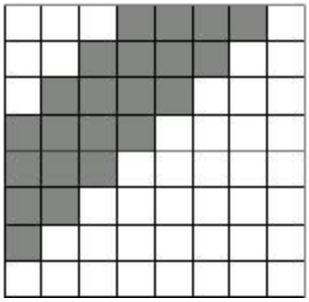


Figure 2.2: DCT Transformation of *8x8* blocks

The image is reconstructed by applying inverse DCT to each block using the three frequency sub-bands' coefficients including the modified coefficients according to equation 2.2.

$$x(m,n) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}\alpha_u\alpha_v y(u,v)\cos\frac{(2m+1)u\prod}{2M}\cos\frac{(2n+1)v\prod}{2N} \quad \text{..... 2.2}$$

DCT based watermarking techniques are more robust compared to simple spatial domain watermarking techniques.

2.1.5.3. From a blind and non-blind aspect

Extraction can be done with the presence of the original image or the absence of the original image depending on the watermarking system.

- Blind watermarking system: system does not require the original image in order to extract the watermark

- Non-Blind watermarking system: system requires access to the original image in order to decode the watermark.

2.1.6. Evaluation of Digital Image Watermark System

Digital watermarking systems are evaluated with respect to two parameters; Imperceptibility (visibility) and Robustness. A description of each parameter and the metrics used to evaluate it is illustrated in the following subsections.

2.1.6.1. Imperceptibility (Visibility)

The watermark signal should be imperceptible to the end user who is viewing the watermarked image. This means that the perceived quality of the image should not be distorted by the presence of the watermark and a user should not be able to differentiate between watermarked and original image.

As a measure of the quality of a watermarked image, Peak Signal to Noise Ratio (PSNR) is used.

To compute the Peak signal to noise ratio, first we need to compute the Mean Square Error (MSE) (Al-Haj, 2007):

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left\|I(i,j) - K(i,j)\right\|^2 \quad \text{.....} \quad \textbf{2.3}$$

Where I is the original image, K is the watermarked image that contain m by n pixels,

PSNR calculated according to the following equation:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX^{2}_{I}}{MSE}\right) = 20 \cdot \log_{10}\left(\frac{MAX_{I}}{\sqrt{MSE}}\right) \text{.....} \quad \mathbf{2.4}$$

Here, MAX_I is the maximum pixel value of the image. Once the PSNR exceeds some value, the errors become undetectable to human viewers. Conversely, the human visual system seems to have a saturation effect as well. Once the image quality falls below a certain level, the image simply looks bad.

2.1.6.2. Robustness

One of the most important requirements of a watermarked image is to be robust against several attacks. Attacks are classified into two main categories; *Geometrical attacks* and *Watermark Removal attacks*. We describe these two attack types and present some examples.

1. <u>Geometrical Attacks</u>

Geometrical attacks do not actually remove the embedded watermark itself, but intend to distort the watermark detector synchronization with the embedded information.

The detector could recover the embedded watermark information when perfect synchronization is regained. Here are the geometric attacks that are used to evaluate this thesis:

- **Rotation**

Rotates the image by a certain angle degrees, in clockwise or counter clockwise direction. For the image shown in figure 2.3, Rotation by 60° in a counter clockwise direction will give the image shown in figure 2.4. The image is cropped to include only the central portion of the rotated image and is the same size as the original image.

Figure 2.3: Original Lena Image

Figure 2.4: Rotated Lena Image by 60º

- **Cropping**

Cropping is the process of removing selected pixels from a digital image.

This is a very common attack since in many cases the attacker is interested in a small portion of the watermarked object, such as parts of a certain picture. With this in mind, in order to survive, the watermark needs to be spread over the dimensions where this attack takes place. When the image shown in figure 2.3 is cropped from 4 corners, the result is shown in figure 2.5.

Figure 2.5: Cropped Lena Image from four sides

2. Watermark Removal Attacks

These attacks change the features of the image by adding or manipulating the values of the matrices that represent the image.

Here are the signals processing attacks that are used to evaluate this study:

- **Gaussian White Noise**

An amount of noise of mean M and Variance V is added to every part of the picture. This means that each pixel in the noisy image is the sum of the true pixel value and a random Gaussian distributed noise value. When noise of Mean = 0.0, Variance = 0.01 is added to the image in figure 2.3, the result is as shown in figure 2.6.

Figure 2.6: Lena Image with additive Gaussian Noise

- **Dithering**

Full-color photographs may contain an almost infinite range of color values. Dithering is the most common means of reducing the color range of images.

Dithering is the process of putting side by side pixels of two colors to create the illusion that a third color is present. There are two parameters to be specified in Dithering: *Qm*and *Qe*. *Qm* specifies the number of quantization bits to use along each color axis for the inverse color map.

Qe specifies the number of quantization bits to use for the color space error calculations. If *Qe*<*Qm*, dithering cannot be performed. When the image in figure 2.3 is dithered with *Qm* = 5, *Qe* = 15 the result is shown in figure 2.7.

Figure 2.7: Dithered Lena Image with *Qm* = 5, *Qe*=15

- **JPEG Compression:**

This is generally an unintentional attack which appears very often in multimedia applications. Practically, all the images that are currently being distributed via Internet have been compressed. Image compression is minimizing the size in bytes of a graphics file without degrading the quality of the image to an unacceptable level. The reduction in

file size allows more images to be stored in a given amount of disk or memory space. It also reduces the time required for images to be sent over the Internet or downloaded from Web pages. The name JPEG stands for Joint Photographic Experts Group, the name of the committee who created the standard. Image compression can be lossy or lossless. Images are compressed by a certain "Quality" which is a number between 0 and 100; higher numbers mean quality is better (less image degradation due to compression). When the image in figure 2.3 is converted to JPEG with Lossy Compression and Quality = 50, the result is shown in figure 2.8.

Figure 2.8: JPEG Compressed Lena Image

2.1.7 Correlation-Based Technique (Portdar,V.,Han,S.& Chang,E.2005)

A technique for watermark embedding is to exploit the correlation properties of additive pseudo-random noise patterns as applied to an image. A pseudo-random noise (PN) pattern W(x,y) is added to the cover image I(x,y), according to the equation shown below in equation 2.5.

$$I_w(x,y) = I(x,y) + k * W(x,y) \quad \text{.....2.5}$$

Where, k denotes a gain factor, and I_W the resulting watermarked image. Increasing *k* increases the robustness of the watermark at the expense of the quality of the watermarked image. To retrieve the watermark, the same pseudo-random noise generator algorithm is seeded with the same key, and the correlation between the noise pattern and possibly watermarked image computed. If the correlation exceeds a certain threshold T, the watermark is detected, and a single bit is set. This method can easily be extended to a multiple-bit watermark by dividing the image up into blocks, and performing the above procedure independently on each block.

2.2. Related Works

Digital Image watermarking is the image processing field that is severely considered in the last few years due to rapid development in the digital multimedia technologies. In this section we illustrate several related works in order to determine the major research techniques and methodologies used. In the following literature survey describes the previous work done on digital watermarking:

Hsieh, Tseng, & Huang, (2001) the researchers proposed an image accreditation technique by embedding digital watermarks in images. The technique based on wavelet transform and embeds a watermark with visual recognizable patterns by modifying the frequency part of the images. In the proposed approach, the original image is decomposed into wavelet coefficient. Then, multi-energy watermarking based on the qualified significant wavelet tree is used to achieve the robustness watermarking.

Candik, Matus, & Levicky, (2001) in their paper, they presented a technique for the digital watermarking of still images based on the wavelet transform. The watermark (binary image) is embedded into an original image in its wavelet domain. The original unmarked image is required for watermark extraction. The method of embedding of digital watermarks in wavelet transform domain was analyzed and verified on grey- scale static images.

Lin, (2001) the study proposed a multi-purpose watermarking method that integrates robust, fragile and semi-fragile watermarking. The watermarking information generated by DWT and embedded into DWT subbands as a watermarked image.

Do, & Vetterli, (2005) in their work, they introduced a new image decomposition scheme called CT which is more effective in representing smooth contours in different directions of an image than DWT.

Emek, & Pazarci, (2005) they proposed a new watermarking algorithm using DWT prior to the DCT to provide better imperceptibility in harmony with the human visual system. Their algorithm showed resistance to common signal processing operation

Jaylakshmi, Merchant, & Desai (2006) the researchers proposed a new method of non-blind digital image watermarking in contourlet domain. In this method the number of directions in the band pass image is doubled at every other scale of decomposition according to curve scale relation and the simulation results which prove that contourlet domain watermarking is well suited for image like maps where a lot of curves and texts are inherently present.

Al-Haj, (2007) the researcher described imperceptible and robust combined DWT-DCT digital image watermarking algorithm and the performance evaluation result show that combining the two transform improves the performance of the watermarking algorithm that are based solely on the DWT transform.

Shu, et. al., (2008) the study proposed a blind watermarking algorithm in the translation invariant circular semantic contourlet transform (TICSCT) domain. Experimentation shows that this domain has higher capacity than wavelet and special domain and robustness and imperceptibility are improved.

Yingkun, et al., (2008) in this paper, they developed a new filter bank based on non subsample contourlet and wavelet hybrid transform (NSCWHT) and study its application. They proposed a new image watermarking based on developed NSCWHT. The experiment shows that their algorithm provides an imperceptibility better than the one based on DWT, but is not quite robust to geometrical attacks.

El-rube', et. al., (2009) their paper investigated the role of CT versus DWT in providing robust image watermarking. Two measures are utilized in the comparison between wavelet based and contourlet based methods, peak signal to noise ratio (PSNR) and normalized cross correlation (NCC).

Hajjara, Abdallah, & Hudiab, (2009) in their study, they have proposed novel watermarking technique using biorthogonal wavelets. The technique is highly robust against non-geometric attacks. The watermark is extracted fairly accurately even if the watermarked images are almost destroyed.

Jiansheng, Sukang, & Xiaomei, (2009) the authors in their work proposed an algorithm of digital image watermarking based on DCT and DWT according to the characteristics of the human vision. In their algorithm the information of the digital watermark is transform using DCT embedded in the original image which is transform using DWT then embedding information of the digital watermark in the high frequency band of the original image transformation.

Zhu, Campus, & Xiao (2009) a blind watermarking algorithm is proposed in which extraction algorithm is designed according to the method of maximum likelihood estimation. This paper carries on the static analysis to the high frequency subband coefficient of wavelet and contourlet transform .The extraction does not need original image neither does it need the original watermark information. The Algorithm is one kind of real sense blind watermark algorithm.

Khalighi, & Rabiee, (2009) in their paper, suggested a new non-blind multiresolution watermarking method for still image based on the CT. In their approach, they embedded the grayscale image into the highest frequency subband of the host image in its contourlet domain. They demonstrate that this method enables is to embed more amount of data without degrading the perceptibility and robustness.

Amirgholipour, & Naghsh-Nilchi, (2009) they developed a new robust digital image watermarking algorithm based on join DWT-DCT transforms. A binary watermarked logo is scrambled by Arnold cat map and embedded in the certain coefficient sets of a 3-level DWT transformed of a host image. Then, DCT of each selected DWT subband is

computed and the PN-sequences of the watermark bits are embedded in the middle frequencies coefficient of the corresponding DCT block.

Ghannam, & Abuo-Chadi, (2009) in this paper, they clarified the advantages by CT versus the DWT. Prove that the contourlet domain is suitable for image like maps.

Shu, et al., (2009) this paper proposed a watermarking algorithm in the frequency domain based on the selection of a high frequency range containing a large amount of information. The selected high frequency range contributes to the imperceptibility of the watermark while the robustness against compression is achieved because the selected frequency range contains large amount of information. The entropy-based algorithm is used to find the host tree of the wavelet based contourlet packet transform (WCPT).

Shilbayeh, & Alshamary, (2010) the researchers presented a new robust and secure hybrid watermark technique based on HWT and DWT. The proposed method is constructed by cascading two different but complementary techniques. Performance evaluation of the proposed method showed improved result of imperceptibility, robust and security in comparison with other systems**.**

Meena, & muthivadhan, (2010) their paper considered two techniques that protect fingerprint biometric data using digital watermarking techniques which are based on DWT. They conclude that both techniques provide adequate security to the fingerprint data without degrading visual quality. Further, the verification performance after dewatermarking is also analyzed.

CHAPTER THREE

THE COMBINED DWT-CT

BASED

DIGITAL WATERMARKING

Chapter 3

THE COMBINED DWT-CT BASED DIGITAL WATERMARKING

3.1. Introduction

In this chapter, we will present a new image watermarking algorithm based on combining two transforms; DWT and CT. Watermarking is done by modifying the coefficients of carefully selected DWT sub-band, followed by applying CT on the selected sub-band.

The reason for applying the two transforms is based on the fact that combined transforms could compensate for the drawbacks of each other, resulting in effective watermarking. Although most work in the field of digital image watermarking focuses on utilizing DWT due to its excellent spatial-frequency localization and multiresolution properties. CT began to gain some interest for capability of capturing directional information such as smooth contours and directional edges (Ghannam, &Abuo-Chadi, 2009).

There are different techniques that can be used to embed the watermark, but since using the spatial domain gives us fragile watermarks that are not robust against the attacks, we decided to work on the frequency domain because we are searching for watermarking algorithms that are robust against different kinds of attacks such the Geometrical and Removal attacks, without affecting the quality of the watermarked image, so we were trying to solve the conflict between robustness and imperceptibility.

Figure 3.1 shows the sequence of the techniques we used in our thesis.

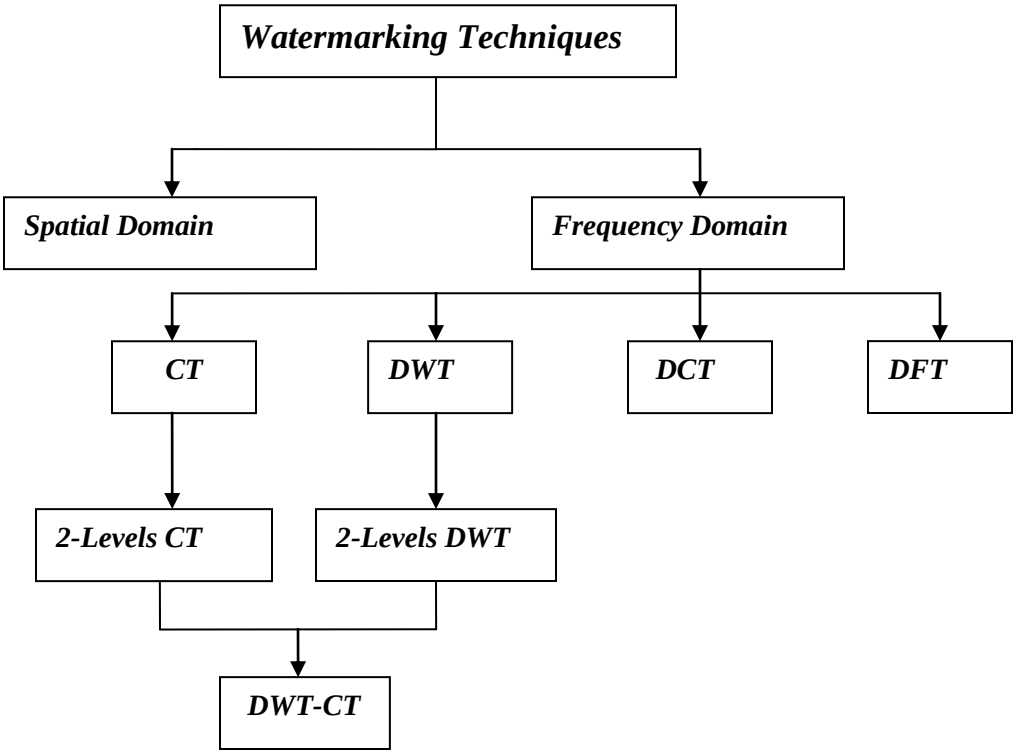


Figure 3.1: Watermarking Techniques Used

The proposed system has been designed and implemented to use the DWT and the CT algorithm separately and the new suggested combined algorithm DWT-CT for the purpose of testing the robustness and the imperceptibility. Section 3.2 explains how we use the DWT watermarking algorithm. Section 3.3 explains how we use the CT watermarking algorithm. Section 3.4 explains how we use the combined DWT-CT watermarking algorithm.

3.2. Discrete Wavelet Transform

DWT for digital image is a mathematical formula which converts an image from special domain to frequency domain. The basic idea DWT of an image is described as follows. Decompose a given image into four subbands (LL1, HL1, LH1, and HH1). LL1 is the lower resolution approximation image as well as horizontal HL1, vertical LH1 and diagonal HH1 detail components. To obtain the next wavelet level for example the HL1 is further decomposed into another four subbands (LL2, HL2, LH2, and HH2). This decomposition can be repeated several times. Figure 3.2 shows the example of two levels wavelet decomposition subbands.

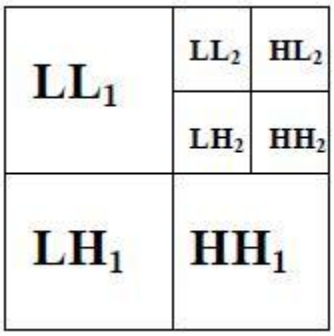
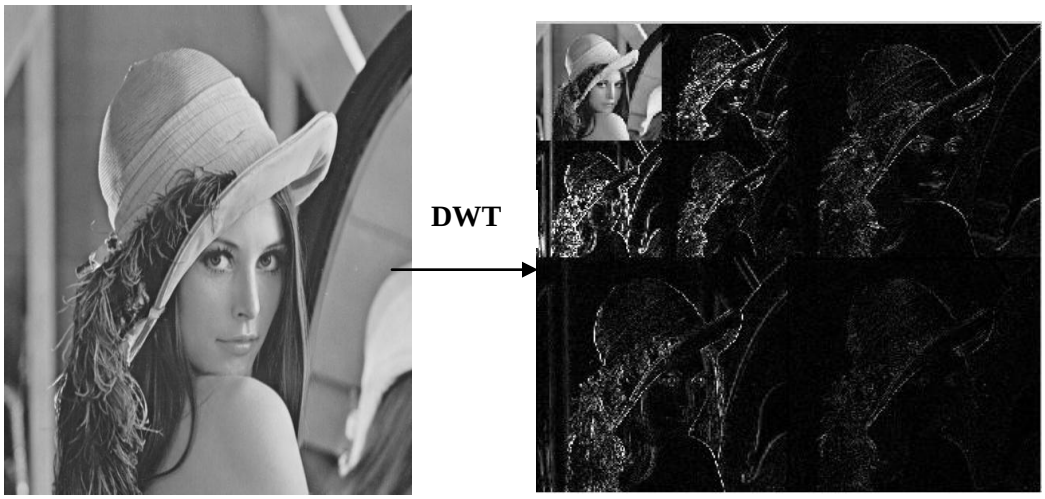


Figure 3.2: Two level DWT decomposition

Furthermore, from these DWT coefficients, the original image can be reconstructed by performing Inverse Discrete Wavelet Transform of an image called IDWT. The DWT of an image introduces a sequence of coefficients map in subbands. An original 512×512 Lena image and its DWT decomposition shown in figure 3.3.



(a) (b)

Figure 3.3: A real two–level DWT decomposition. (a) The original 512×512 Lena image (b) Its DWT decomposition.

The DWT for digital image is implemented by passing it through a serious of wavelet filters called analysis filter bank, some common example of wavelet filters are Haar, daubechies, orthogonal, and Bi-orthogonal filters. The basic idea of DWT implementation is to decompose the given image by low pass (LP) and high pass (HP) filters followed by down sampling first of rows and then columns. The output of the low pass filter gives the approximation coefficients sub-band (LL), which are the high-scale, low frequency components whose content is the most important part of the signal. The output of the high pass filter gives the detail coefficients sub-bands (LH, HL, and HH), which are the low-scale, high frequency components. The result of the DWT decomposition can be expressed in the following equation 3.1 (Candik, Matus, &Levicky, 2001).

$$cI_j = cI_{j+1} + cD_{j+1}^{(h)} + cD_{j+1}^{(v)} + cD_{j+1}^{(d)} \quad \text{…...3.1}$$

The process of image decomposition after applying two levels DWT is shown in figure 3.4.

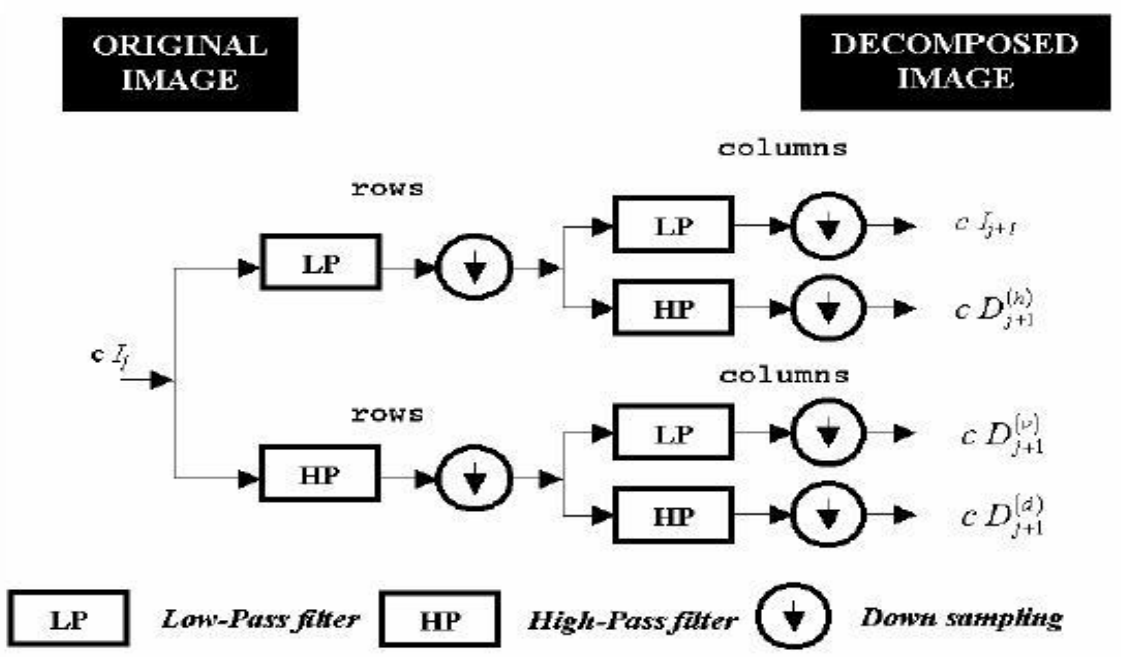


Figure 3.4: Wavelet decomposition of image (Candik, Matus, & Levicky, 2001).

The reconstruction process of IDWT is shown in figure 3.5.

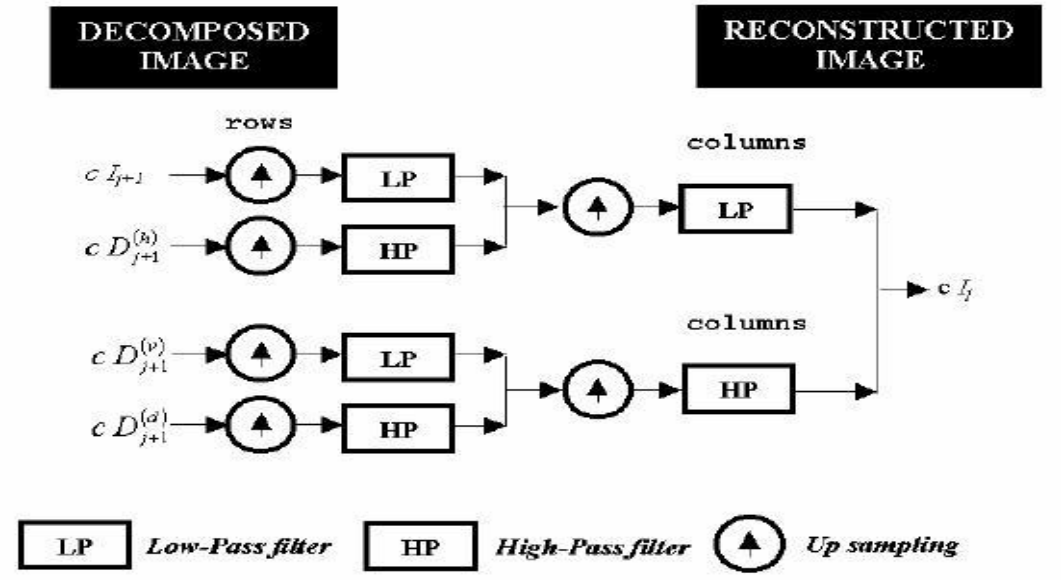


Figure 3.5: Image reconstruction (Candik, Matus, & Levicky, 2001).

DWT Watermarking is based on two facts:-

1. Much of the signal energy lies at low-frequencies sub-band which contains the most important visual parts of the image.

2. High frequency components of the image are usually removed through compression and noise attacks.

The watermark is therefore embedded by modifying the coefficients of the middle frequency sub-band so that the visibility of the image will not be affected and the watermark will not be removed by compression (Al-Haj, 2007).

3.2.1. Discrete Wavelet Transform Watermarking Algorithm

The watermarking algorithm consists of two algorithms; watermark embedding and watermark extraction. The two algorithms are described in the following subsections:

3.2.1.1. Embedding Algorithm Based on DWT

The watermark embedding algorithm is shown in figure 3.6. I adapted DWT algorithm from (Al-Haj, 2007) and made some adjustments represented in the following steps:

Step1: Apply DWT to decompose the original image into four non-overlapping multi-resolution sub-bands:LL1, HL1, LH1, and HH1.

Step2: Apply DWT again to HL1 to get four smaller subbands and choose the HL2 subband for embedding process.

Step3: Re-formulate the gray-scale watermark image into a vector of zeros and ones.

Step4: Generate uncorrelated pseudorandom sequence (*pn_sequence*) which is used to embed the watermark bit 0. Size of (*pn_sequence*) must be equal to the size of chosen subband for embedding.

Step5: Modify the coefficients of the chosen subband by embedding *pn_sequence* with the gain factor k according to the equation

$$X = X + K * pn\text{-}sequance \quad \ldots\ldots\ldots\ldots\ldots\ldots 3.2$$

Where X is the coefficient of the selected subband and k is the gain factor .we should find the suitable gain factor which gives best tradeoff between visibility and robustness.

Step6: Perform inverse discrete wavelet transform (IDWT) using the selected sub-bands of each level and modified coefficient and produce the watermarked image.

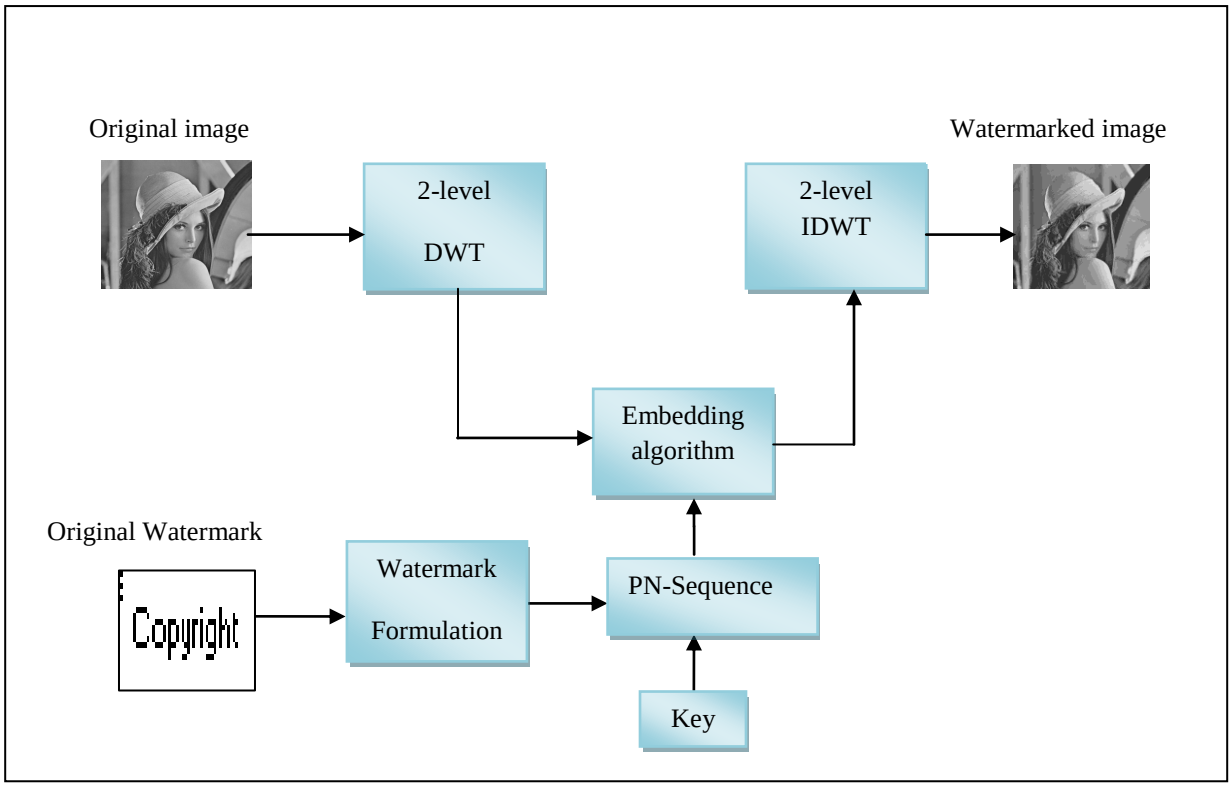


Figure 3.6: DWT Watermark embedding block diagram

3.2.1.2. Extracting Algorithm Based on DWT

The DWT watermark algorithm is a blind watermarking algorithm, and thus the extraction does not need the original image. The watermark extraction algorithm is shown in figure 3.7. I adapted DWT algorithm from (Al-Haj, 2007) and made some adjustments represented in the following steps:

Step1: Apply DWT to decompose the Watermarked image into four non-overlapping multi-resolution subbands: LL1, HL1, LH1, and HH1.

Step2: Apply DWT again to HL1 to get four smaller subbands and choose the HL2 sub-band.

Step3: Re-formulate the gray-scale watermark image into a vector of zeros and ones.

Step4: Generate uncorrelated pseudorandom sequence (*pn_sequence*) using the same seed used in the watermark embedding algorithm.

Step5: Calculate the correlation of the chosen subband with the generated pseudorandom sequence by (m) times, where (m) is the length of watermark vector.

Step6: Calculate the mean of the correlation and compare it with each value of the correlation value that we calculated in step 5.

Step7: If the calculated values of the correlation are greater than the mean, then the extracted watermark equals 0, otherwise 1.

Step8: Reconstructed the watermark using the extracted watermark bits, and compute the similarity between the original and extracted watermarks.

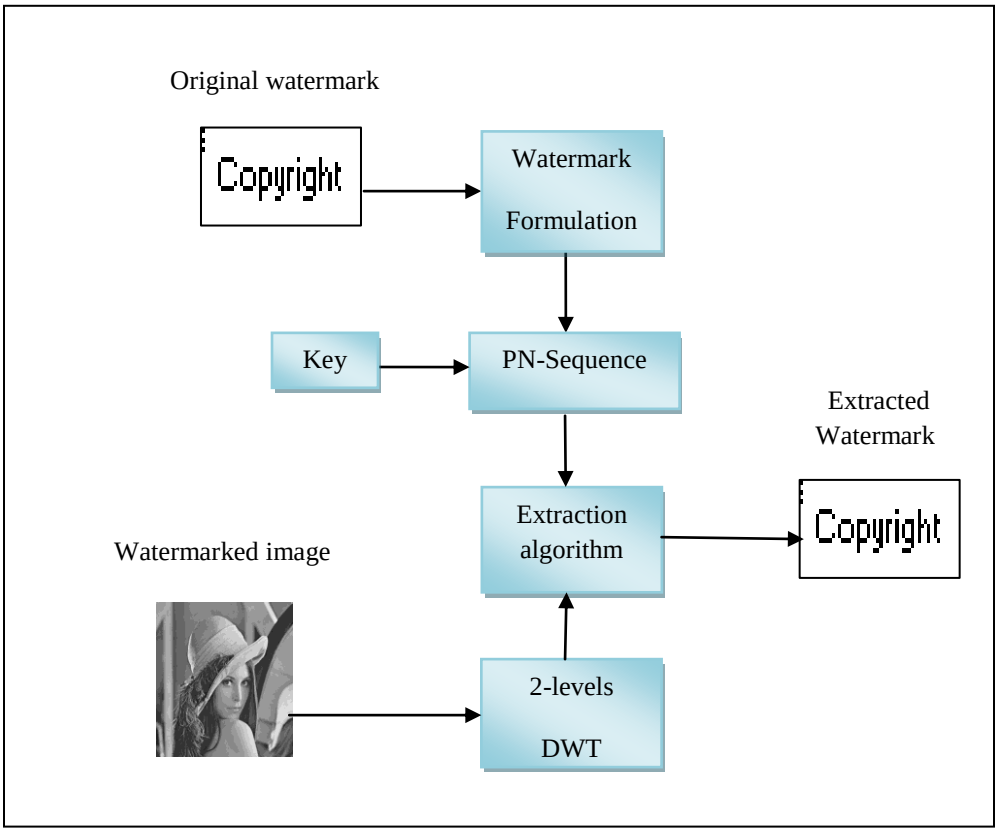


Figure 3.7: DWT Watermark extraction block diagram

3.3. Contourlet Transform

CT is one of the geometrical image transforms, which represents images containing contours and textures. The CT introduced by (Do, & Vettrli, 2005) is more effective in representing smooth contours in different directions of an image than DWT. The CT is a multi-resolution and directional decomposition of signal using two main steps: Lapalician Pyramid (LP) decomposition and Directional Filter Bank (DFB) decomposition. In LP step an image is decomposed into low pass image and band pass image. Each band pass image is further decomposed by DFB step. In CT the number of directional subbands after applied n levels equal 2^n, where, n=1, 2, 3…is shown in figure 3.8.

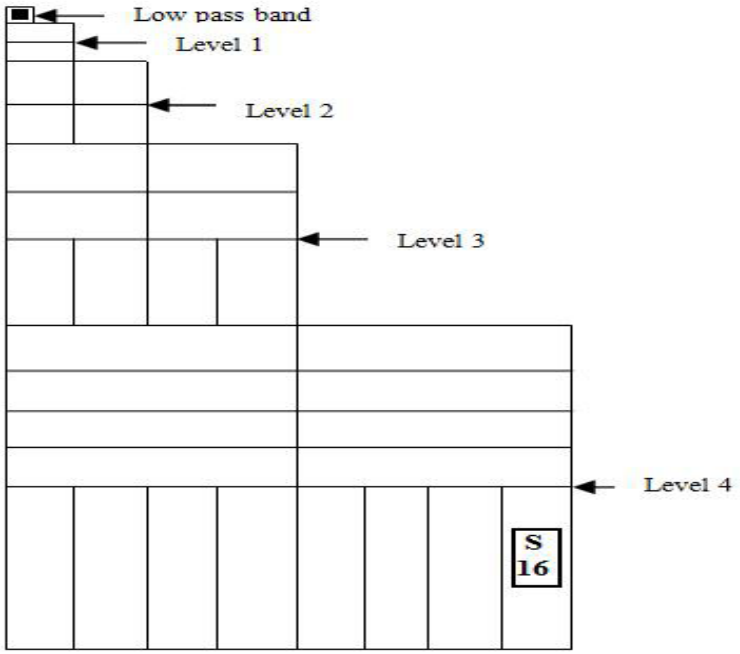


Figure 3.8: Contourlet decomposition (El-rube', et al., 2009)

The contourlet transform based Watermarking could compensate for the drawbacks of wavelet transform based watermarking since it captures the directional edges and smooth contours better than other transforms and the human visual system is less sensitive to the edge**(**Khalighi, &Rabiee, 2009**).** The effective watermarking scheme should have essential

properties, robustness and imperceptibility which are in conflict with each other. Watermarking based on CT should take care of two facts:-

1. To improve the imperceptibility, we should perform embedding the watermark in the directional sub-band of the contourlet decomposition, but it is hardly robust.

2. To achieve robustness, we should embed the watermark in the lowpass image of the contourlet decomposition, but the imperceptibility of the watermarked image degrades. In contourlet decomposition, both LP decomposition and DFB decomposition with 'pkva' filters are used. Figure 3.8 shows the image of two-level CT about the of 512×512 Lena.

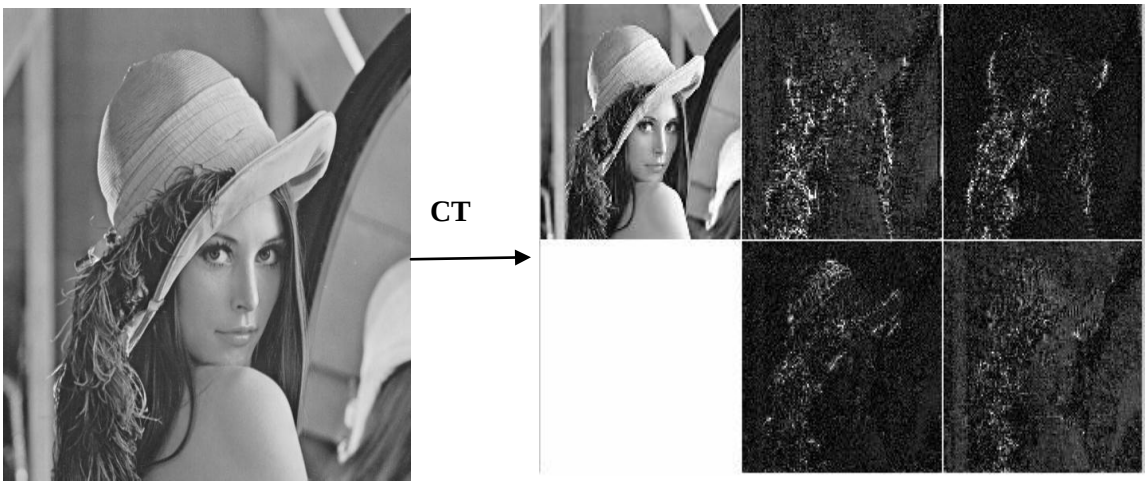


Figure 3.9: A real two –level CT decomposition. (a) The original 512×512 Lena image. (b) Its CT decomposition.

The contourlet filter bank is constructed by two filter stages, a LP and DF (Ghannam, & Abuo-Chadi, 2009) as shown in figure 3.10. The LP decomposes the image octave radial-like frequency bands to capture the point discontinuities, while the DFB decomposes each LP detail band into many directions (a power of 2) to link these point discontinuities into linear structures.

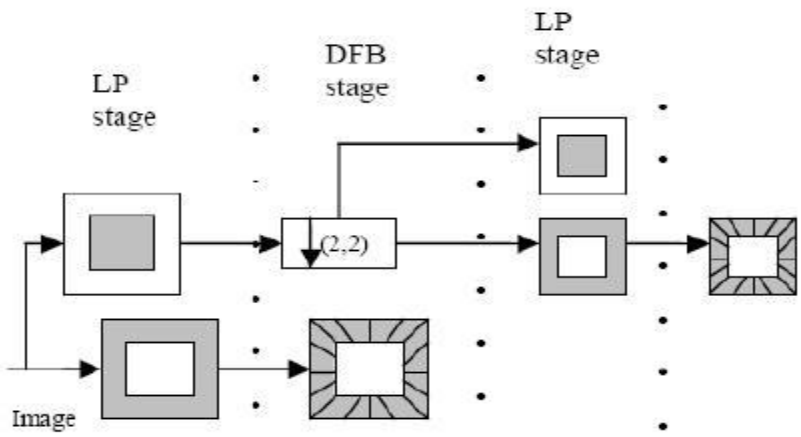


Figure 3.10: Contourlet Filter Bank (Ghannam, & Abuo-Chadi, 2009)

LP has the distinguishing feature that each pyramid level generates only one bandpass image which does not have scrambled frequencies. This frequency scrambling happens in the wavelet filter bank when a highpass channel, after down sampling, is folded back into the low frequency, and thus its spectrum is reflected. In the LP, this effect is avoided by only down sampling the lowpass channel. Figure 3.11 shows one level LP decomposition. It generates a down sampled low pass version of the original and the prediction, resulting in a bandpass image.

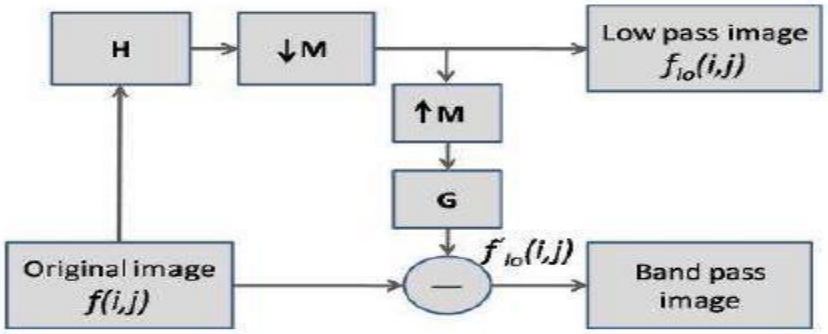


Figure 3.11: one level LP Decomposition (Ghannam, &Abuo-Chadi, 2009)

The directional filter bank is critically sampled filter bank that can decompose image into any power of two's number of directions. The DFB is efficiently implemented via a l-level tree structured decomposition that leads to 2^l subbands with wedge–shaped frequency partition as shown in Figure 3.12.

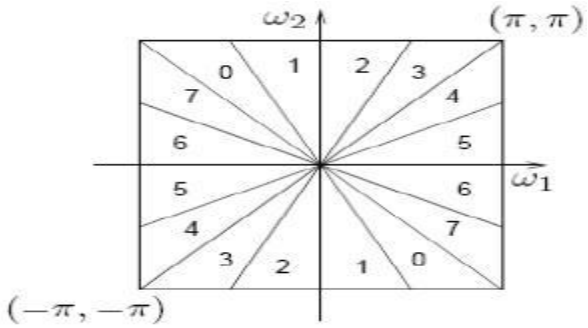


Figure 3.12: DFB Frequency partitioning (l=3) (Ghannam, &Abuo-Chadi, 2009*)*

3.3.1. Contourlet Transform Watermarking Algorithm

The watermarking algorithm consists of two algorithms; watermark embedding and watermark extraction. The two algorithms are described in the following subsections:

3.3.1.1. Embedding Algorithm Based on CT

The watermark embedding algorithm is shown in figure 3.13 and described in details in the following steps.

Step1: Read original image and decompose it by applying 3-levels CT to get 8 subbands. Choose one of subbands to embed watermark image on it.

Step2: Read the watermark image and convert it to vector of zero and one.

Step3: Create zero-mean pseudorandom sequence (pn_sequance) for watermark bit 0.

Step4: Modify the coefficient of the selected subband in step 1 with pn-sequance and gain factor by applying the following equation

X=X+K**pn-sequance*……..**3.1**

Where X is the coefficient of the selected sub-band and k called the gain or the seed factor. We should find the suitable gain factor which gives best tradeoff between visibility and robustness.

Step5: Perform inverse contourlet transform (ICT) using the selected subbands of each level and modified coefficient and produce the watermarked image.

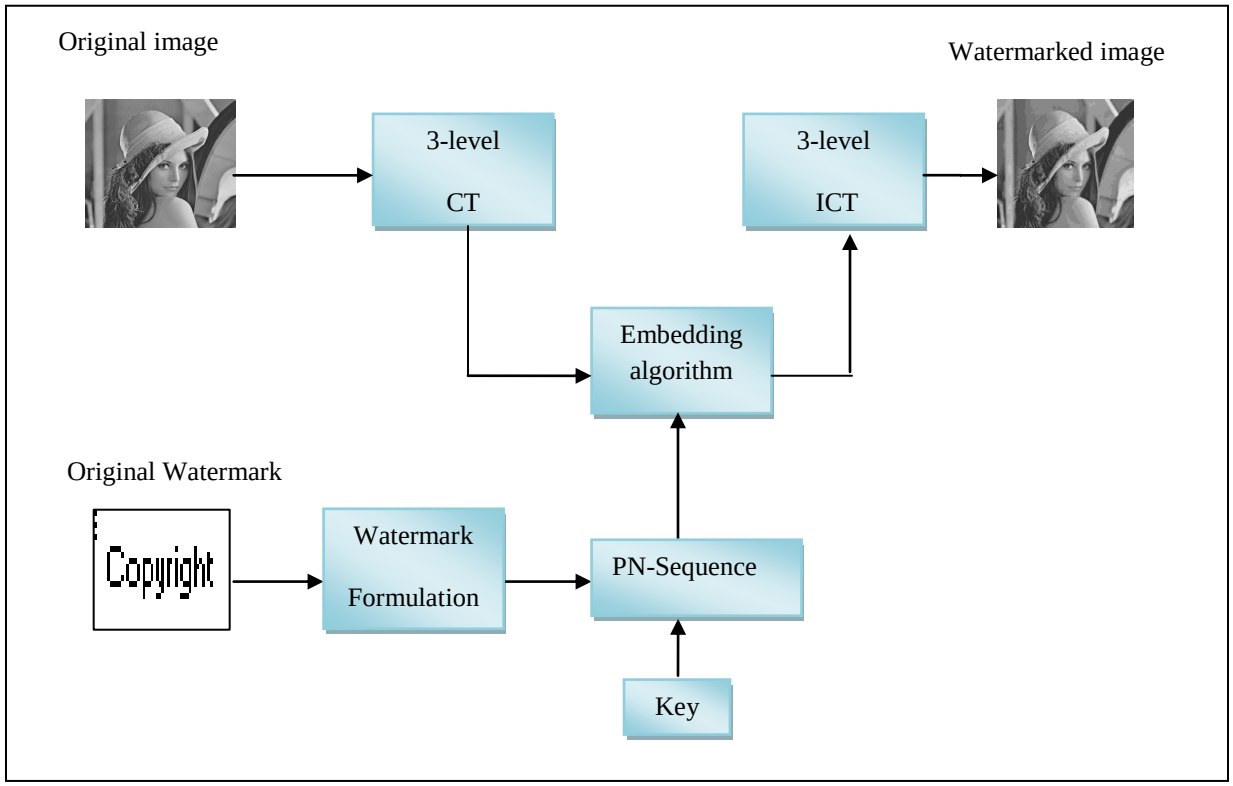


Figure 3.13: CT Watermark embedding block diagram

3.3.1.2. Extracting Algorithm Based on CT

The CT watermark algorithm is a blind watermarking algorithm, and thus the extraction does not need the original image. The watermark extraction algorithm is shown in figure 3.14, and described in detail in the following steps:

Step1: Decompose watermarked image which is obtained from embedding algorithm by applying 3-level CT transformation and choosing the same sub-band used in embedding algorithm after apply the same level of transformation.

Step2: Read the watermark image and convert it to vector of zero and one.

Step3: Create a zero-mean pseudorandom sequence (pn_sequance) for watermark bit 0 by using the same gain factor used in embedding algorithm.

Step4: Calculate the correlation of the chosen sub-band with the generated pseudorandom sequence by "m" times, where "m" is the length of watermark vector.

Step5: Calculate the mean of the correlation and compare it with each value of the correlation value that we calculated in step 4**.** If the calculated values of the correlation one greater than the mean then the extracted watermark equals 0, otherwise 1.

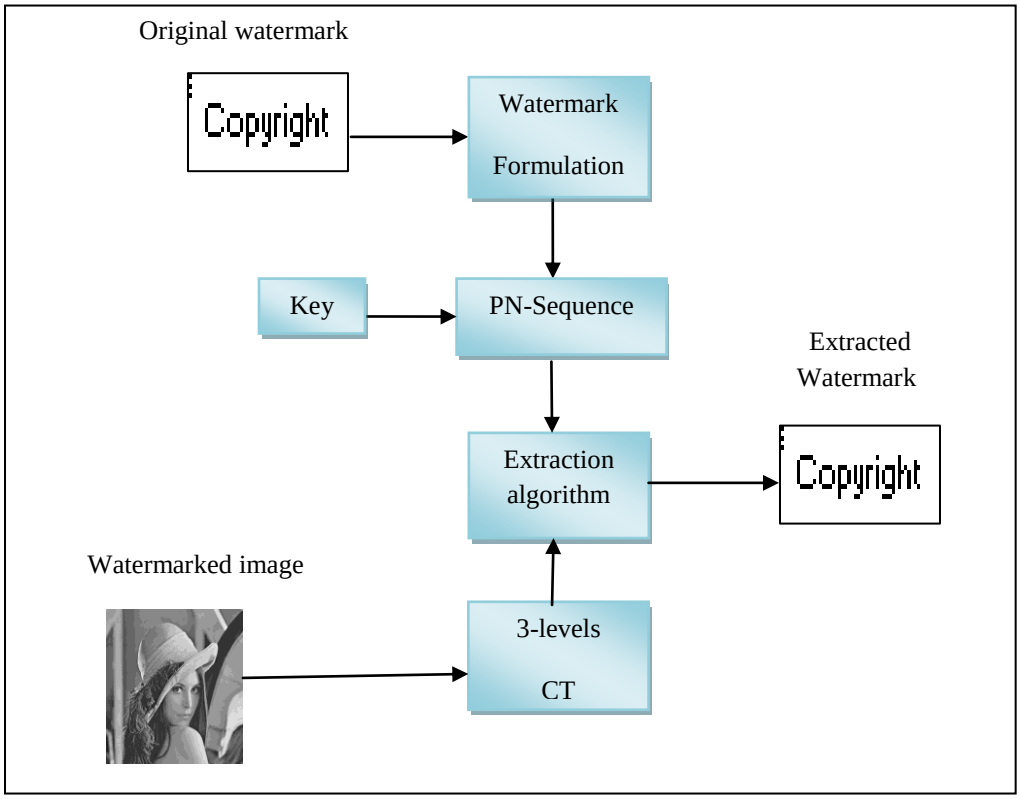


Figure 3.14: CT Watermark extraction block diagram

3.4 The Combined DWT-CT Algorithm

A new image watermarking algorithm will be presented by combining DWT and CT to develop a blind image watermarking algorithm to provide better visibility and higher robustness against variety of attacks. First, we applied a 2-level DWT to the image by choosing mid-mid sub-band. The selection to the mid-mid subband shored better results in imperceptibility. Second, we applied CT to the chosen subband to study their effects.

The main reason of combing DWT and CT is to minimize the drawbacks of each of them separately. Most researchers in the field of digital watermarking focuses on using DWT due to its excellent spatial localization and multi-resolution properties, which are similar to the theoretical models of human visual system. However, there are two drawbacks associated with DWT. First, it lacks shift invariance, which means small shift in input signal that can cause big changes in the energy distribution of the wavelet coefficients. Second, the DWT has poor directional selectivity, which is evident from the impulse responses of the filters of the individual sub-bands. Figure 3.15 shows Lena's image after applying 2-level DWT followed by 2-level CT.

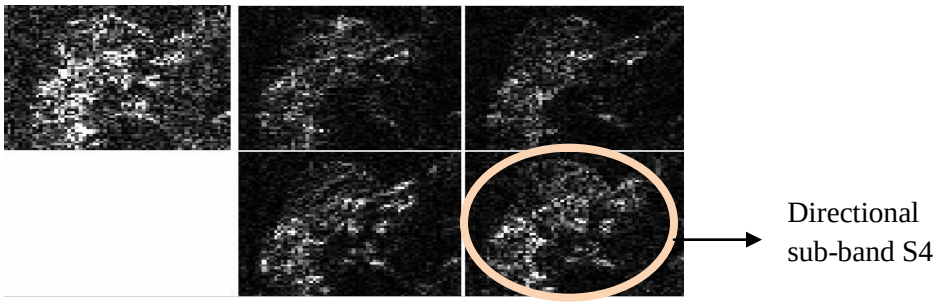


Figure 3.15: 2-level DWT followed by 2-level CT

3.4.1. The combined DWT-CT Watermarking Algorithm

The watermarking algorithm consists of two algorithms; watermark embedding and watermark extraction. The two algorithms are described in the following subsections:

3.4.1.1. Embedding Algorithm Based on DWT-CT

The watermark embedding algorithm is shown as block diagram in figure 3.16 and described in details in the following steps.

Step1: Apply DWT to decompose the original image into four non-overlapping multi-resolution sub-bands:LL1, HL1, LH1, and HH1.

Step2: Apply DWT again to HL1 to get four smaller sub-bands and choose the HL2 sub-band for further decomposition using CT.

Step3: Apply 2-level CT to selected sub-bands in step 2. Then select directional sub-bands to embed the watermark on it.

Step4: Re-formulate the gray-scale watermark image into a vector of zeros and ones.

Step5: Generate uncorrelated pseudorandom sequence (*pn_sequence*) that will be used in embedding the watermark bit 0. Size of (*pn_sequence*) must be equal to the size of the chosen sub-band.

Step6: Modify the coefficients of the chosen sub-band by embedding *pn_sequence* with the gain factor k according to the equation

X=X+K**pn-sequance*……..3.2

Where X is the coefficient of the selected sub-band and k is the gain factor .We should find a suitable gain factor which gives the best tradeoff between visibility and robustness.

Step7: Perform ICT using the selected sub-bands of each level followed by performed IDWT and modified coefficient to produce the watermarked image.

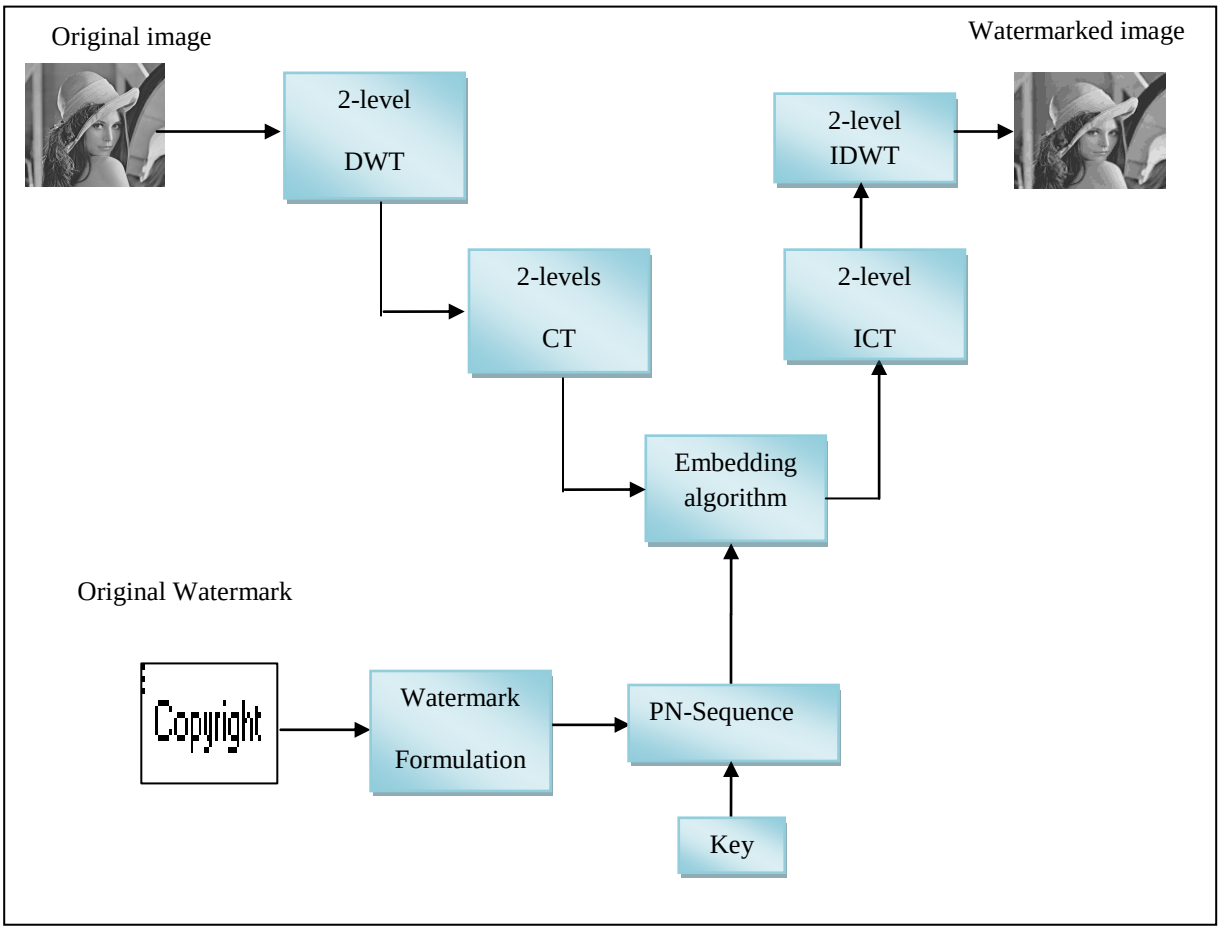


Figure 3.16: DWT-CT Watermark embedding block diagram

3.4.1.2. Extracting Algorithm Based on DWT-CT

The DWT-CT watermark algorithm is a blind watermarking algorithm, and thus the extraction does not need the original image. The watermark extraction algorithm is shown in figure 3.17, and described in detail in the following steps:

Step1: Apply DWT to decompose the watermarked image which is obtained from the embedding algorithm to get four non-overlapping multi-resolution sub-bands: LL1, HL1, LH1, and HH1.

Step2: Apply DWT again to HL1 to get four smaller sub-bands and select the HL2 sub-band for further decomposition by applying CT.

Step3: Apply 2-level CT to the selected sub-bands in step 2. Select directional sub-bands to embed the watermark on it.

Step4: Re-formulate the gray-scale watermark image into a vector of zeros and ones.

Step5: Generate uncorrelated pseudorandom sequence (*pn_sequence*) using the same seed used in the watermark embedding algorithm.

Step6: Calculate the correlation of the chosen sub-band with the generated pseudorandom sequence by m times, where m is the length of watermark vector.

Step7: Calculate the mean of the correlation and compare it with each value of the correlation value that we calculated in step 6.

Step8: If the calculated values of the correlation are greater than the mean, then the extracted watermark is equals 0, otherwise 1.

Step 9: Reconstruct the watermark using the extracted watermark bits, and then compute the similarity between the original and extracted watermark.

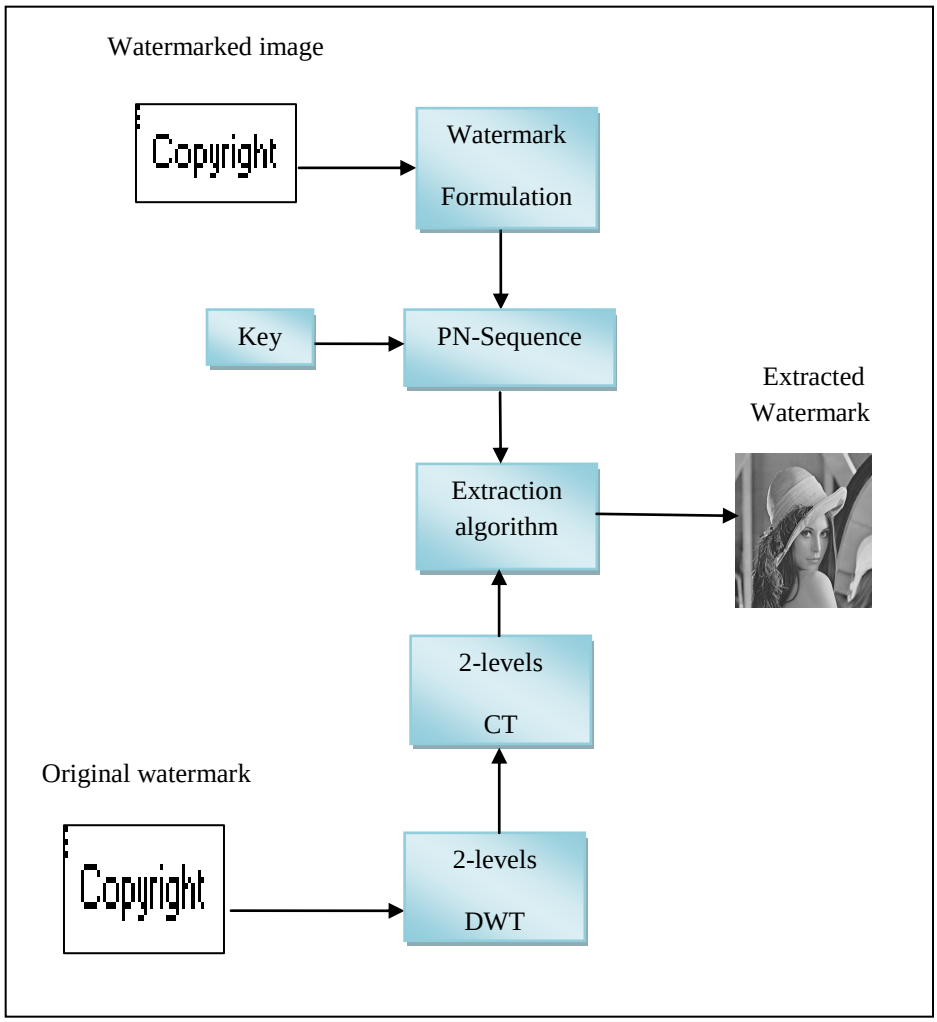


Figure 3.17: DWT-CT Watermark extraction block diagram

CHAPTER FOUR

Experimental Results and Discussion

Chapter 4

Experimental Results and Discussion

4.1. Experimental Results

In this chapter, the combined DWT-CT algorithm has been tested and evaluated. Also, DWT and CT algorithms has been tested and evaluated separately for the sake of comparison.

In section 4.2, performance evaluation of the wavelet based algorithm has been tested after performing 1, 2, and 3 level decomposition of the original image and the coefficients of the diagonal detail band are selected for watermark embedding. Performance evaluation of the contourlet based algorithm has been tested after performing 1, 2, and 3 levels of decomposition and choosing the directional subband for embedding is discussed in section 4.3. Experimental results of the combined DWT and CT are explained in section 4.4.

The performance of the watermarking algorithm is usually evaluated with respect to two properties: imperceptibility and robustness. In each section, the implementation of the algorithm is evaluated by using two measures: Peak Signal to Noise Ratio (PSNR) which measures imperceptibility and the Normalized Cross Correlation (NCC) which measures robustness.

As a sample watermark, we chose the Image shown in figure 4.1. The size of this image is *50 x 20.* We used the "Lena" image shown in figure 4.2 as the original image in which we embedded the watermark. The size of this image is 512 x 512.

Figure 4.1: Sample Watermark

Figure 4.2: Original Image

4.2. DWT based watermarking

In order to evaluate the algorithm performance of blind watermark detection in the wavelet transform domain, we study the imperceptibility of the watermarked image and the robustness of this algorithm to different kinds of attacks.

- **Imperceptibility**

We carried out the watermark embedding algorithm based on DWT domain only. Applied 1-level DWT of the Lena image produced 256×256 sub-bands: LL_1, LH_1, HL_1, and HH1. Since embedding the watermark beyond the watermark in LH_2 or HH_2 is more effective. The coefficient of the LH2 or HH_2 sub-band is selected for embedding process. We evaluate the imperceptibility of the DWT algorithm by measuring PSNR for different sub-bands as shown in table 4.1.

Original image	Watermarked image					
	1-DWT (LH_1)	1-DWT (HH_1)	2-DWT (LH_2)	2-DWT (HH_2)	3-DWT (LH_3)	3-DWT (HH_3)
						
	PSNR=71.28	**PSNR=71.28**	**PSNR=80.21**	**PSNR=77.12**	**PSNR=83.26**	**PSNR=100.97**

Table 4.1: the PSNR values at different DWT sub-bands

- ## Robustness

To verify the robustness of the DWT algorithm the watermarked images were distorted by adding *Gaussian noise*, *Rotation, Cropping, Compression using JPEG compression and dithering.* After the watermarked image was attacked, the watermark was extracted from the attacked image, and the robustness of this algorithm was tested by comparing the original watermark with the extracted watermark. The effect of each one of the attacks is presented below:

- **Effect of Gaussian Noise**

When adding the Gaussian Noise to the watermarked image, we fixed the value of the variance to zero and changed the value of the mean; the results of the chosen sub-band are shown below. When embedding in the Mid-Mid (LH_2) sub-band, the attacked watermarked image at different values of the mean is shown in figure 4.3 and the extracted watermark and the correlation values between the original and the extracted watermark at different values of the mean are shown in figures 4.4 and 4.5 respectively.

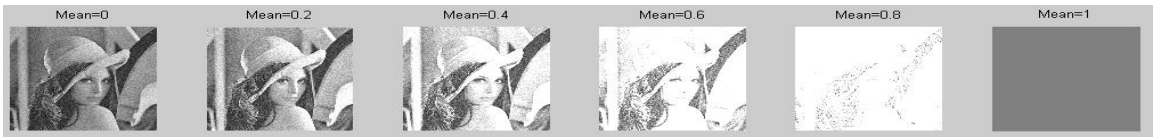


Figure 4.3: the attacked watermarked image by noise based on DWT

Figure 4.4: the extracted watermark image after noise based on DWT

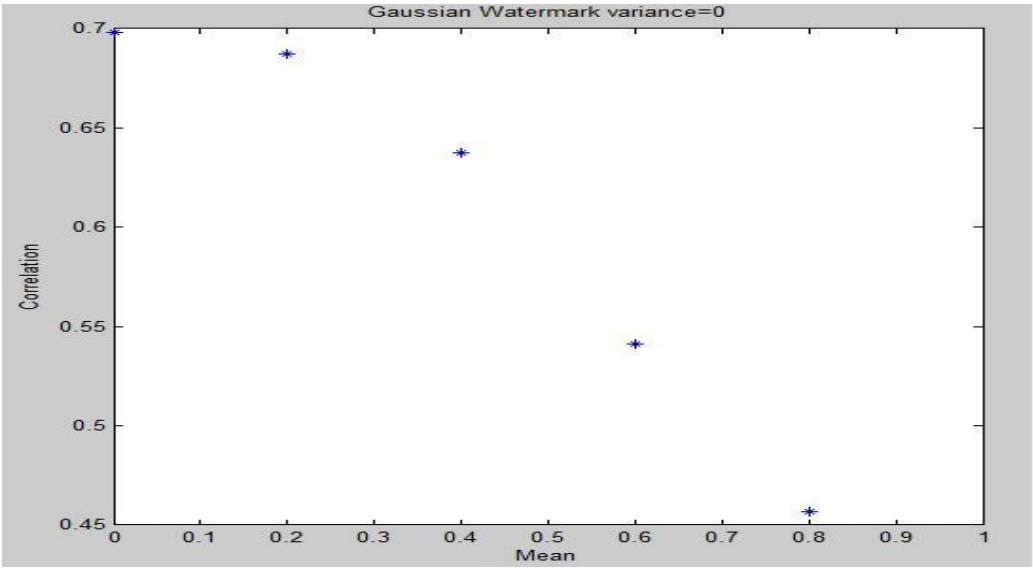


Figure 4.5: Correlation due to noise attacks based on DWT

- **Effect of Rotation**

We rotated the watermarked image by different angles from 0 to 300 anti-clockwise. When the Mid-Mid (LH_2) sub-band was chosen to embed the watermark in, the attacked watermarked image at different values of the angles is shown in figure 4.6 and the extracted watermark and the correlation values between the original and the extracted watermark at different values of angles are shown in figures 4.7 and 4.8 respectively.

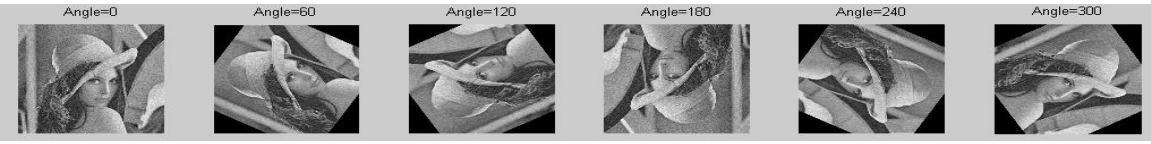


Figure 4.6: the attacked watermarked image by rotation based on DWT

Figure 4.7: the extracted watermark image after rotation based on DWT

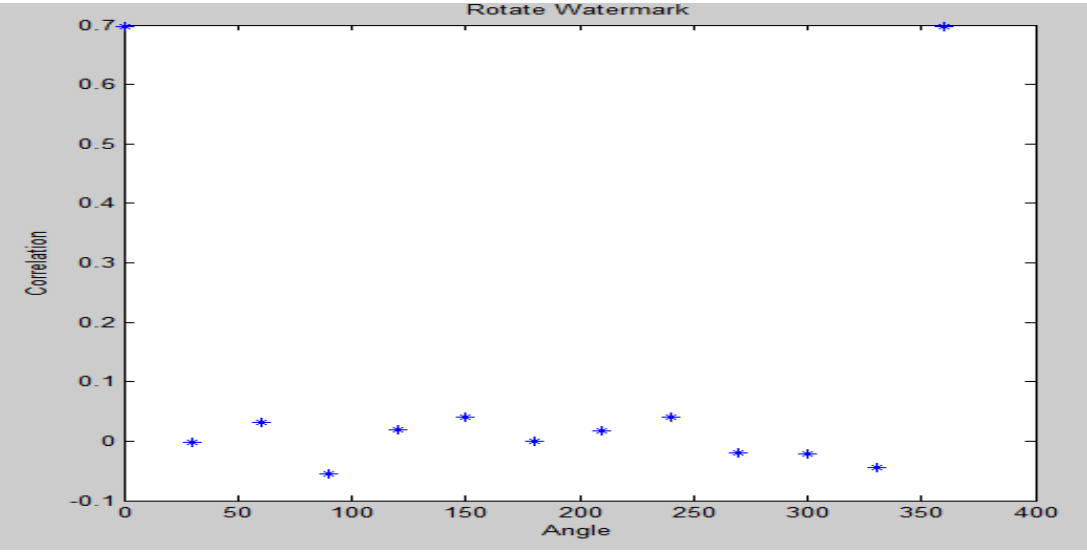


Figure 4.8: Correlation due to rotation attacks based on DWT

- **Effect of Cropping**

We cropped the watermarked image by different block sizes. When the Mid-Mid (LH_2) sub-band was chosen to embed the watermark in, the attacked watermarked image at different values of the block size is shown in figure 4.9 and the extracted watermark and the correlation values between the original and the extracted watermark at different values of the block size are shown in figures 4.10 and 4.11 respectively.

Figure 4.9: the attacked watermarked image by cropping based on DWT

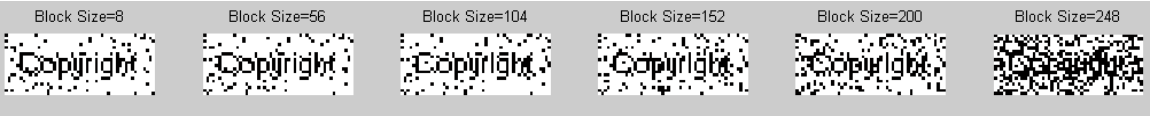


Figure 4.10: the extracted watermark image after cropping based on DWT

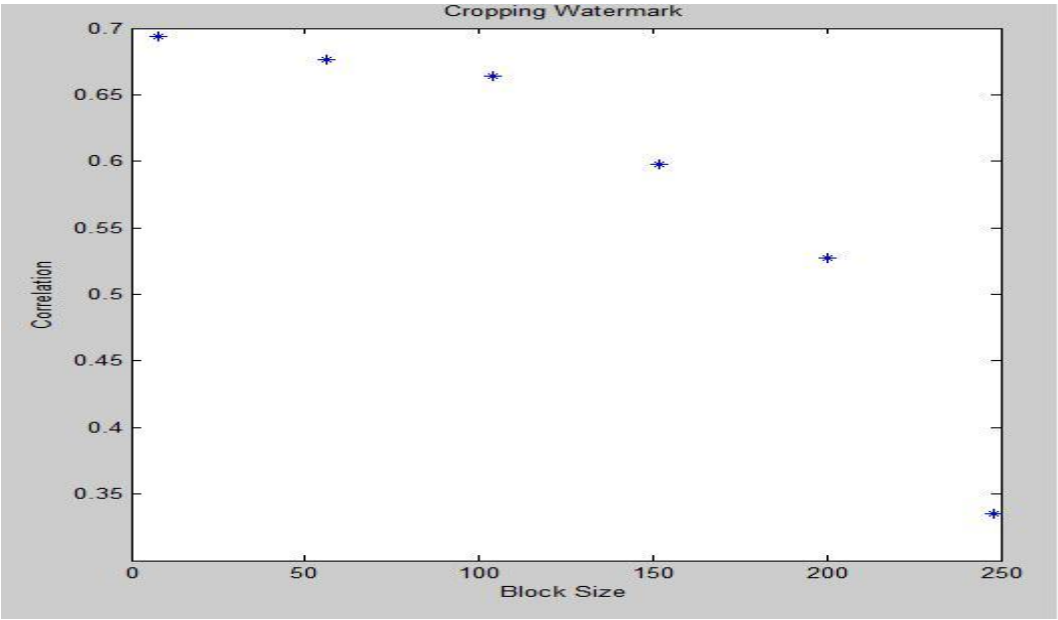


Figure 4.11: Correlation due to cropping attacks based on DWT

- **Effect of JPEG Compression**

We compressed the watermarked image using lossy compression at different Quality values. When the Mid-Mid (LH_2) sub-band was chosen to embed the watermark in, the attacked watermarked image at different values of the quality is shown in figure 4.12 and the extracted watermark and the correlation values between the original and the extracted watermark at different values of quality are shown in figures 4.13 and 4.14 respectively.

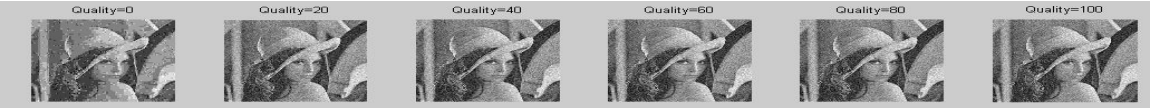


Figure 4.12: the attacked watermarked image by JPEG compression based on DWT

Figure 4.13: the extracted watermark image after JPEG compression based on DWT

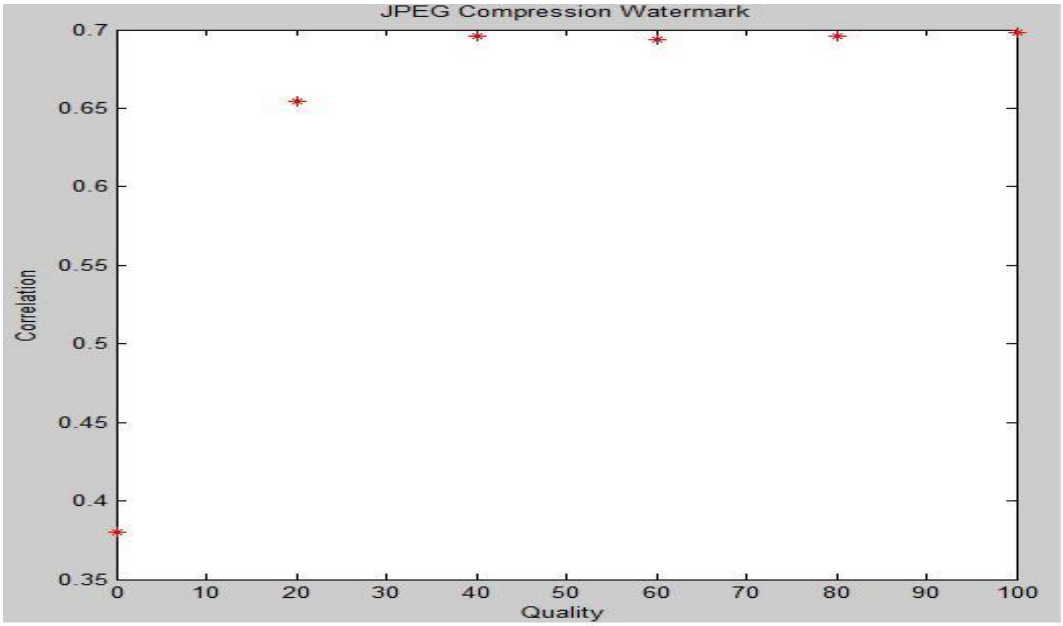


Figure 4.14: Correlation due to JPEG compression attacks based on DWT

- **Effect of Dithering**

We dithered the watermarked image by fixing the value of *Qe* at 5 and changed the value of *Qm.*, where *Qm* specifies the number of quantization bits to use along each color axis for the inverse color map, and *Qe* specifies the number of quantization bits to use for the color space error calculations. When the mid-mid sub-band was chosen to embed the watermark in; the attacked watermarked image at different values of Qm is shown in figure 4.15 and the extracted watermark and the correlation values between the original and the extracted watermark at different values of the Qm are shown in figures 4.16 and 4.17 respectively.

Figure 4.15: the attacked watermarked image by dithering based on DWT

Figure 4.16: the extracted watermark image after dithering based on DWT

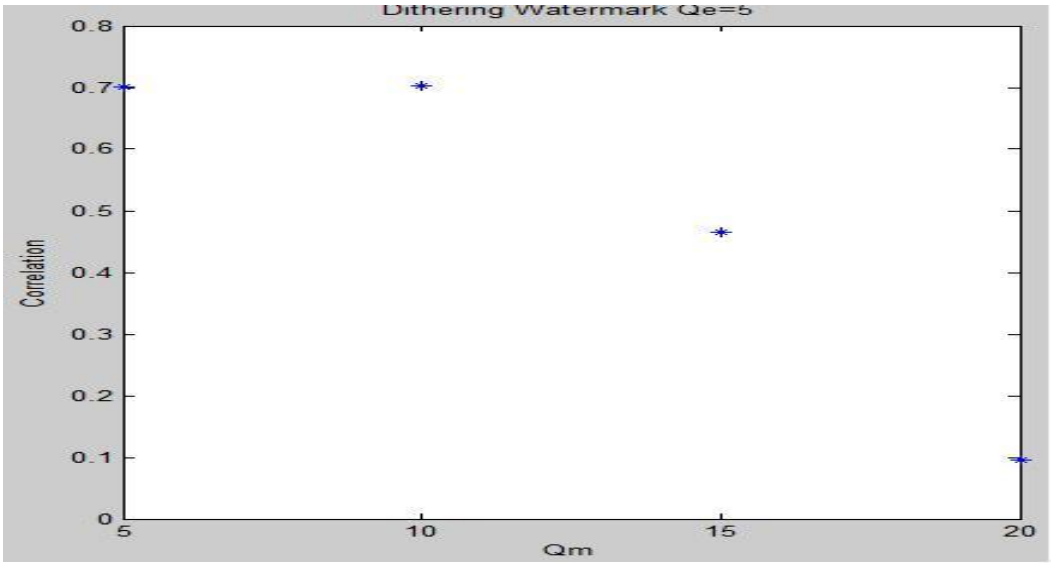


Figure 4.17: Correlation due to dithering attacks based on DWT

Table 4.2 shows the results of Correlation between the original watermark and the watermark extracted from the attacked watermarked image by Geometrical Attacks: Rotation and Cropping.

Algorithm	**Correlation**							
	Rotation Angle				**Cropping Block Size**			
	60	**120**	**240**	**300**	**8**	**104**	**152**	**200**
2-DWT Mid-Mid	0.031	0.041	0.0067	-0.021	0.691	0.664	0.591	0.526

Table 4.2: Correlation values due to geometrical attacks for DWT

After that we measure the robustness against the Watermark Removal Attacks: Gaussian Noise, JPEG Compression, and Dithering. Table 4.3 shows the results of Correlation between original watermark and the watermark extracted from the attacked watermarked image after applying removal attacks.

Algorithm	**Correlation**								
	Gaussian Noise Mean			**Compression Quality**			**Dithering *Qm***		
	0	**0.04**	**0.08**	**0**	**40**	**80**	**5**	**10**	**15**
2-DWT Mid-Mid	0.698	0.698	0.698	0.380	0.695	0.695	0.700	0.702	0.465

Table 4.3: Correlation values due to removal attacks for DWT

4.3. CT- Based Watermarking

The performance of this algorithm was evaluated by studying the imperceptibility of the watermarked image and the robustness of this algorithm to different kinds of attacks.

- **Imperceptibility**

The imperceptibility of this algorithm was tested by calculating the PSNR between the original image and the watermarked image shown in table 4.4.

We embedded the watermark image in each sub-band after applying 1-level CT. We compared the imperceptibility of this algorithm with the 2 and 3 levels CT. We noticed that any change in the low frequency affected the imperceptibility of the image. In table

4.4 we compared the results obtained from embedded watermark image in different sub-bands of 1, 2, and 3 levels CT.

Original image	**Watermarked image**								
	1-CT Sub 0	1-CT Sub 1	1-CT Sub 2	2-CT Sub 0	2-CT Sub 1	2-CT Sub2	2-CT Sub3	2-CT Sub 4	3-CT Sub 8
									
	PSNR= 70.62	PSNR= 69.22	PSNR= 69.93	PSNR= 70.60	PSNR= 72.41	PSNR= 71.41	PSNR= 72.16	PSNR= 73.21	PSNR= 76.88

Table 4.4: the PSNR values at different CT subbands

We notice that best choice of embedding is 3-level in directional sub-band since it produced better result in imperceptibility and we continued the work on 3-level CT.

- ## Robustness

We studied the robustness of embedding in directional sub-bands of 3-level CT. The robustness was determined by applying different kinds of attacks to the watermarked image.

- **Effect of Gaussian Noise**

When adding the Gaussian Noise to the watermarked image, we fixed the value of the variance to zero and changed the value of the mean; the results of the chosen sub-bands are shown below. When embedding in the directional sub-band of 3-level CT, the attacked watermarked image at different values of the mean is shown in figure 4.18 and

the extracted watermark and the correlation values between the original and the extracted watermark at different values of the mean are shown in figures 4.19 and 4.20 respectively.

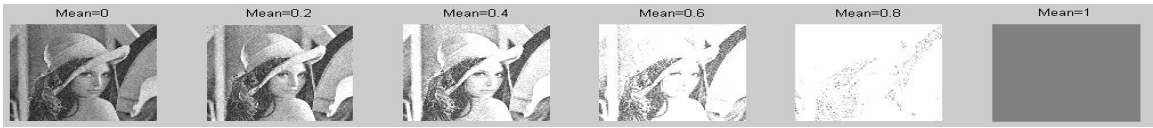


Figure 4.18: the attacked watermarked image by noise based on CT

Figure 4.19: the extracted watermark image after noise based on CT

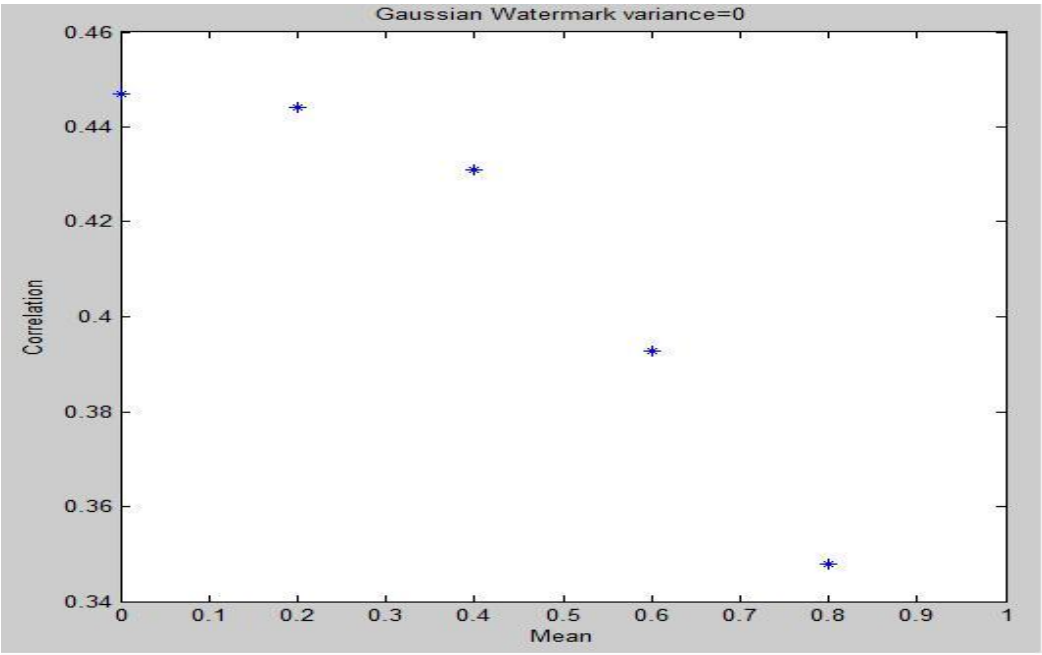


Figure 4.20: Correlation due to noise attacks based on CT

- **Effect of Rotation**

We rotated the watermarked image by different angles from 0 to 300 anti-clockwise. When directional sub-band of 3-level CT was chosen to embed the watermark in, the attacked watermark image with different values of angles shown in figure 4.21 and the extracted watermark and the correlation values between the original and the extracted watermark at different values of angles are shown in figures 4.22 and 4.23 respectively.

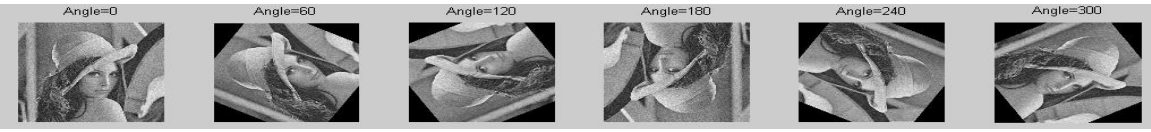


Figure 4.21: the attacked watermarked image by rotation based on CT

Figure 4.22: the extracted watermark image after rotation based on CT

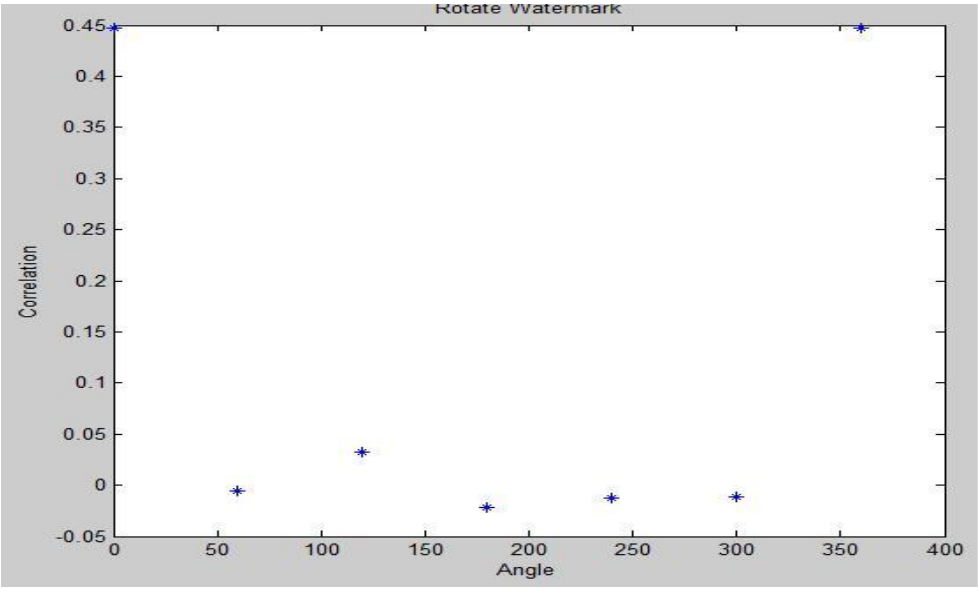


Figure 4.23: Correlation due to rotation attacks based on CT

- **Effect of Cropping**

We cropped the watermarked image by different block sizes. When the directional sub-band of 3-level CT was chosen to embed the watermark in, the attacked watermarked image at different values of the block size is shown in figure 4.24 and the extracted watermark and the correlation values between the original and the extracted watermark at different values of the block size are shown in figures 4.25 and 4.26 respectively.

Figure 4.24: the attacked watermarked image by cropping based on CT

Figure 4.25: the extracted watermark image after cropping based on CT

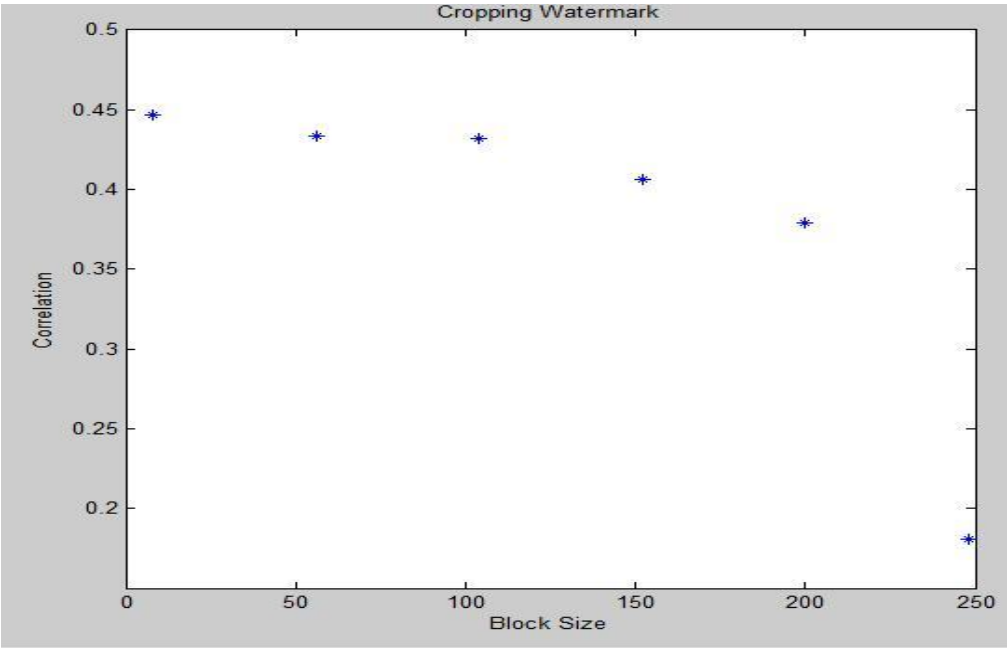


Figure 4.26: Correlation due to cropping attacks based on CT

- **Effect of JPEG Compression**

We compressed the watermarked image using lossy compression at different Quality values. When the directional sub-band of 3-level CT sub-band was chosen to embed the watermark in, the attacked watermarked image at different values of the quality is shown in figure 4.27 and the extracted watermark and the correlation values between the original and the extracted watermark at different values of quality are shown in figures 4.28 and 4.29 respectively.

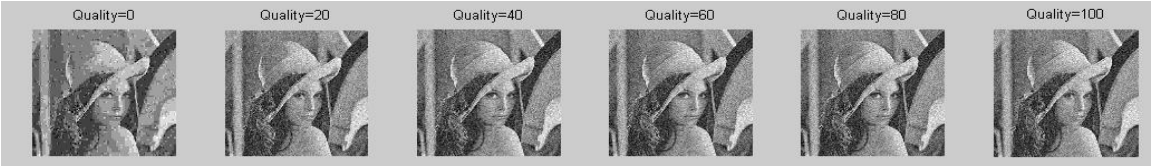


Figure 4.27: the attacked watermarked image by JPEG compression based on CT

Figure 4.28: the extracted watermark image after JPEG compression based on CT

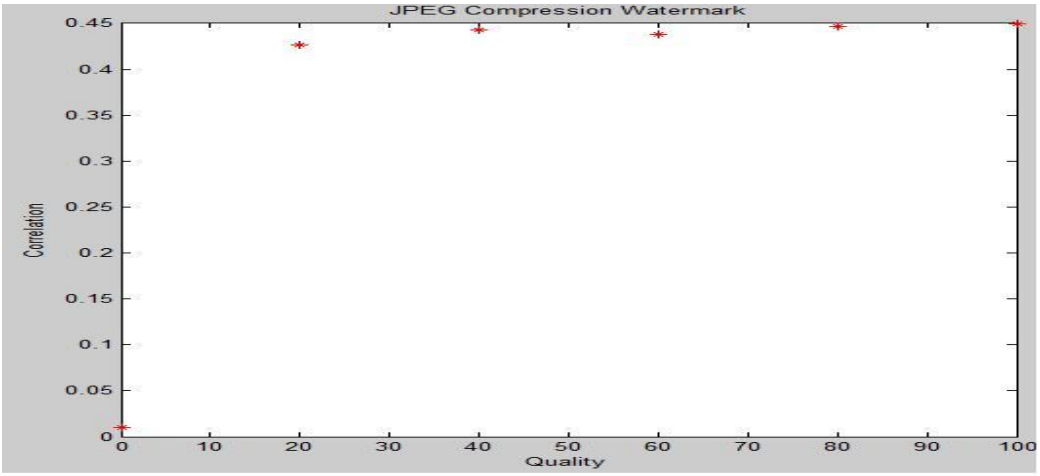


Figure 4.29: Correlation due to JPEG compression attacks based on CT

- **Effect of Dithering**

We dithered the watermarked image by fixing the value of *Qe* at 5 and changed the value of *Qm.*, where *Qm* specifies the number of quantization bits to use along each color axis for the inverse color map, and *Qe* specifies the number of quantization bits to use for the color space error calculations. When directional sub-band of 3-level CT was chosen to embed the watermark in; the attacked watermarked image at different values of Qm is shown in figure 4.30 and the extracted watermark and the correlation values between the original and the extracted watermark at different values of the Qm are shown in figures 4.31 and 4.32 respectively.

Figure 4.30: the attacked watermarked image by dithering based on CT

Figure 4.31: the extracted watermark image after dithering based on CT

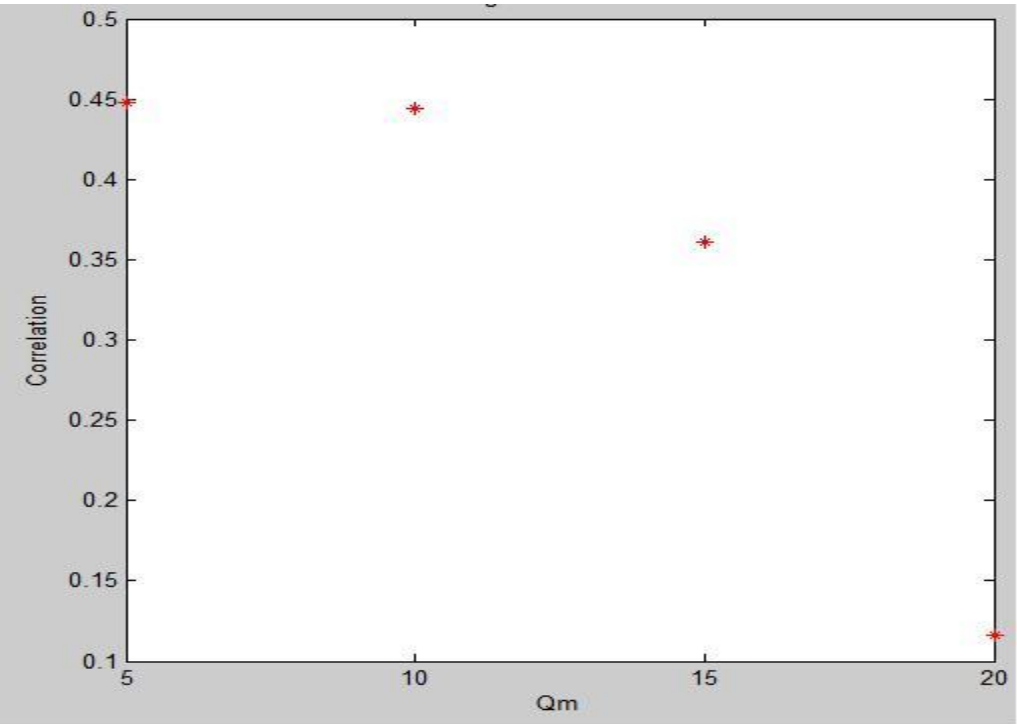


Figure 4.32: Correlation due to dithering attacks based on CT

Table 4.5 shows the results of Correlation between the original watermark and the watermark extracted from the attacked watermarked image by Geometrical Attacks: Rotation and Cropping.

Algorithm	**Correlation**							
	Rotation Angle				**Cropping Block Size**			
	60	**120**	**240**	**300**	**8**	**104**	**152**	**200**
3-level CT	0.311	0.309	-0.303	-0.314	0.443	0.431	0.401	0.385

Table 4.5: Correlation values due to geometrical attacks for CT

After that we measure the robustness against the Watermark Removal Attacks: Gaussian Noise, JPEG Compression, and Dithering. Table 4.6 shows the results of Correlation between original watermark and the watermark extracted from the attacked watermarked image after apply removal attacks.

Algorithm	**Correlation**								
	Gaussian Noise Mean			**Compression Quality**			**Dithering *Qm***		
	0	**0.04**	**0.08**	**0**	**40**	**80**	**5**	**10**	**15**
3-level CT	0.446	0.446	0.445	0.309	0.443	0.446	0.447	0.444	0.366

Table 4.6: Correlation values due to removal attacks for CT

4.4. DWT-CT Based Watermarking

The performance of this algorithm was evaluated by studying the visibility of the watermarked image and the robustness of this algorithm to different kinds of attacks.

- **Imperceptibility**

The visibility of this algorithm was tested by calculating the PSNR between the original image shown in figure 4.34 (a) and the watermarked image. When embedding in the Mid-Mid sub-band of 2-level DWT followed by apply 2-level CT. The watermarked image is shown in figure 4.34 (b) with the PSNR value equal to 88.112.

Figure 4.33: (a) Original Image

Figure 4.33(b)
Watermarked Image (WWCC)
PSNR=88.112

- ## Robustness

Testing the robustness of the combined DWT-CT algorithm is done by adding attacks to watermarked images (*Gaussian noise, Rotation, Cropping, Compression using JPEG compression and dithering).* The performance of the watermark extraction is measured by the NCC value. The effect of each one of these attacks is presented below:

- **Effect of Gaussian Noise**

For adding the Gaussian noise to the watermarked image, we fixed the value of the variance at zero and changed the mean. When the 2-levels DWT are followed by applying 2-levels CT and directional sub-band was chosen to embed the watermark in, the attacked watermarked image at different values of the mean is shown in figure 4.34 and the extracted watermark and the correlation values between the original and the

extracted watermark at different values of the mean are shown in figures 4.35 and 4.36 respectively.

Figure 4.34: the attacked watermarked image by noise based on DWT-CT

Figure 4.35: the extracted watermark image after noise based on DWT- CT

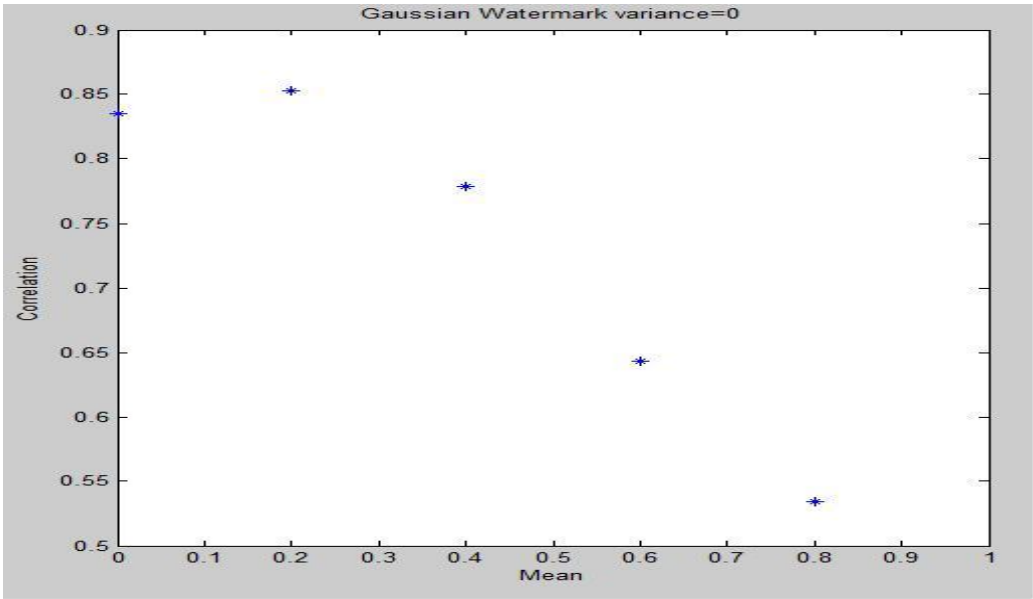


Figure 4.36: Correlation due to noise attacks based on DWT-CT

- **Effect of Rotation**

We rotated the watermarked image by different angles from 0 to 300 anti-clockwise. When the 2-level DWT followed by applying 2-level CT and directional sub-band was chosen to embed the watermark in, the attacked watermark image with different values of angles shown in figure 4.37 and the extracted watermark and the correlation values between the original and the extracted watermark at different values of angles are shown in figures 4.38 and 4.39 respectively.

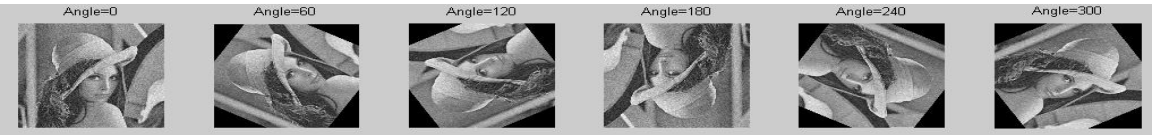


Figure 4.37: the attacked watermarked image by rotation based on DWT- CT

Figure 4.38: the extracted watermark image after rotation based on DWT- CT

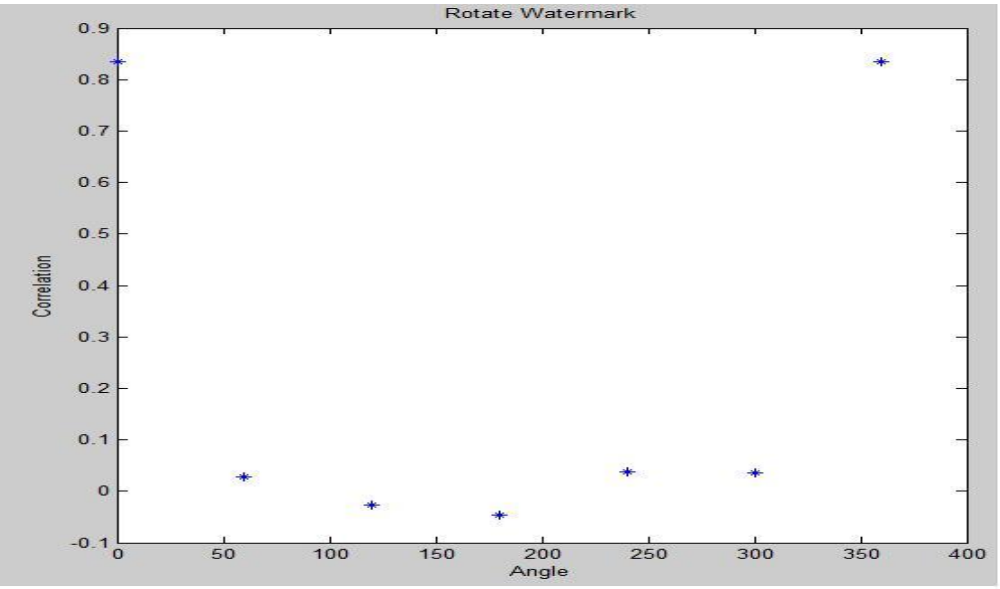


Figure 4.39: Correlation due to rotation attacks based on DWT-CT

- **Effect of Cropping**

We cropped the watermarked image by different block sizes. When the 2-levels DWT followed by applying 2-levels CT and directional sub-band was chosen to embed the watermark in, the attacked watermarked image at different values of the block size is shown in figure 4.40 and the extracted watermark and the correlation values between the original and the extracted watermark at different values of the block size are shown in figures 4.41 and 4.42 respectively.

Figure 4.40: the attacked watermarked image by cropping based on DWT- CT

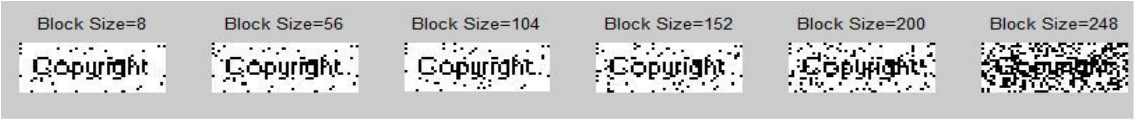


Figure 4.41: the extracted watermark image after cropping based on DWT- CT

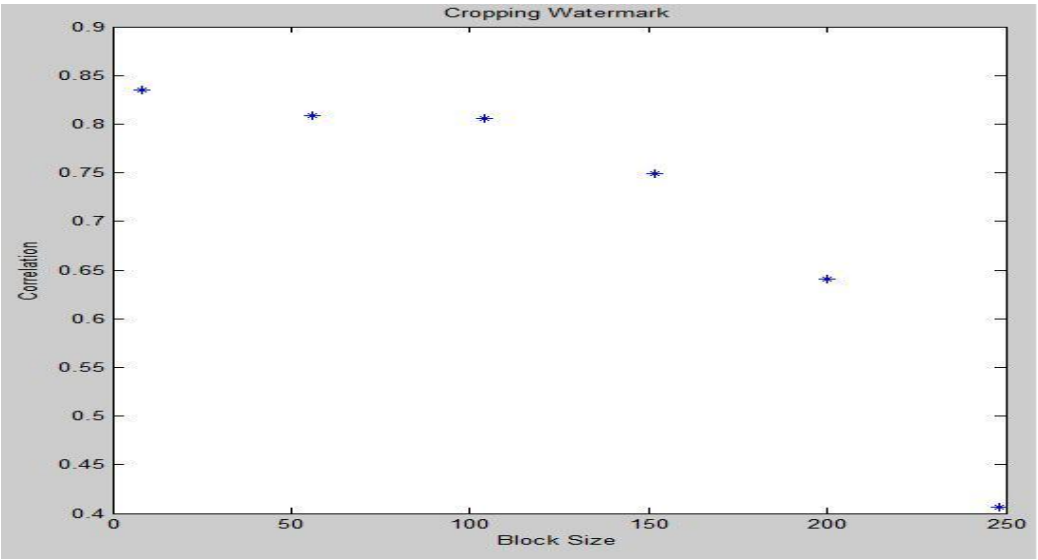


Figure 4.42: Correlation due to cropping attacks based on DWT-CT

- **Effect of JPEG Compression**

We compressed the watermarked image using lossy compression at different Quality values. When the directional sub-band of 2-level DWT followed by 2-level CT was chosen to embed the watermark in; the attacked watermarked image at different values of the quality is shown in figure 4.43 and the extracted watermark and the correlation values between the original and the extracted watermark at different values of quality are shown in figures 4.44 and 4.45 respectively.

Figure 4.43: the attacked watermarked image by JPEG compression based on DWT-CT

Figure 4.44: the extracted watermark image after JPEG compression based on DWT- CT

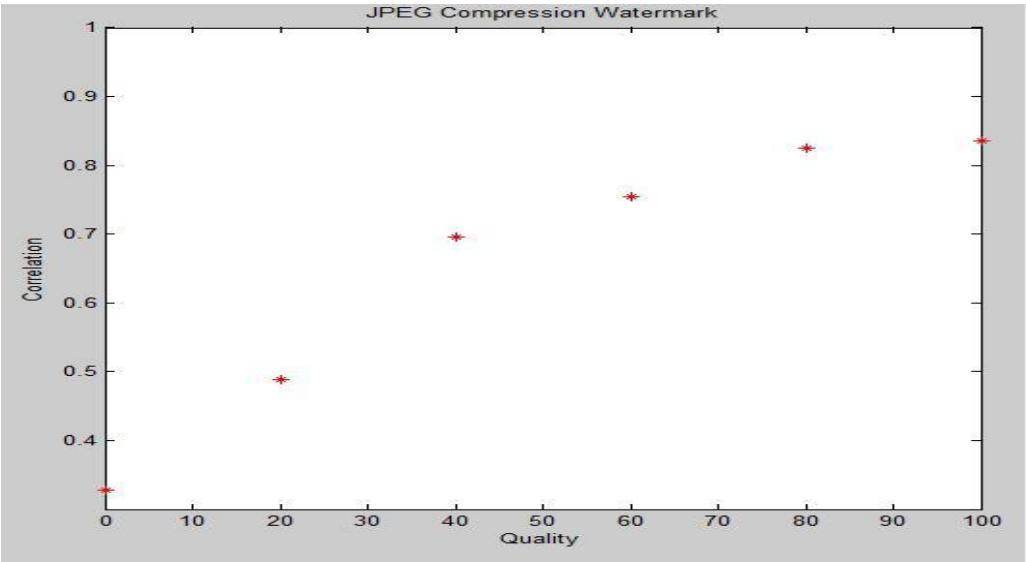


Figure 4.45: Correlation due to JPEG compression attacks based on DWT-CT

- **Effect of Dithering**

We dithered the watermarked image by fixing the value of *Qm* at 5 and changed the value of *Qe.*, where *Qm* specifies the number of quantization bits to use along each color axis for the inverse color map, and *Qe* specifies the number of quantization bits to use for the color space error calculations. When directional sub-band of 2-level DWT followed by 2-level CT was chosen to embed the watermark in; the attacked watermarked image at different values of Qm is shown in figure 4.46 and the extracted watermark and the correlation values between the original and the extracted watermark at different values of the Qm are shown in figures 4.47 and 4.48 respectively.

Figure 4.46: the attacked watermarked image by dithering based on DWT- CT

Figure 4.47: the extracted watermark image after dithering based on DWT- CT

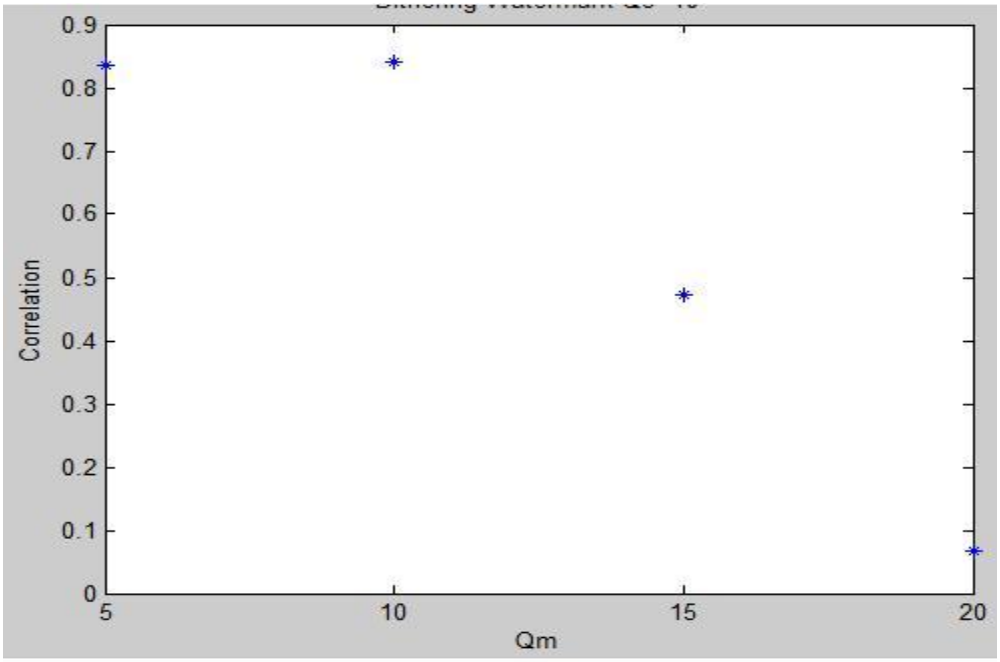


Figure 4.48: Correlation due to dithering attacks based on DWT- CT

Table 4.7 shows the results of Correlation between the original watermark and the watermark extracted from the attacked watermarked image by Geometrical Attacks: Rotation and Cropping.

Algorithm	**Correlation**							
	Rotation Angle				**Cropping Block Size**			
	60	**120**	**240**	**300**	**8**	**104**	**152**	**200**
DWT-CT	0.028	-0.063	0.051	0.037	0.831	0.805	0.759	0.635

Table 4.7: Correlation values due to geometrical attacks for DWT-CT

After that we measure the robustness against the Watermark Removal Attacks: Gaussian Noise, JPEG Compression, and Dithering. Table 4.8 shows the results of Correlation between original watermark and the watermark extracted from the attacked watermarked image after apply removal attacks.

Algorithm	**Correlation**								
	Gaussian Noise Mean			**Compression Quality**			**Dithering *Qm***		
	0	**0.4**	**0.8**	**0**	**40**	**80**	**5**	**10**	**15**
DWT-CT	0.835	0.838	0.835	0.327	0.695	0.825	0.835	0.841	0.472

Table 4.8: Correlation values due to removal attacks for DWT-CT

4.5. Discussion

The objective of this thesis is to design and an implement improved system which is concerned with copyright protection for digital images using watermarking .The main requirements for an efficient digital image watermarking system are imperceptibility and robustness.

This thesis was divided into three parts. In the first part, we start our work by implementing digital image watermark system based on DWT only. In the second part, we implemented system based on CT only. In the final part, we tried to improve these techniques by combining them together. The following steps explain briefly the three algorithms that are used in this thesis:-

- **DWT**

In this algorithm, 1, 2, and 3 levels of DWT to the original image were applied, it is noticed that embedding in the low frequency gave low imperceptibility, so we decided to continue our work in a high frequency. We notice that embedding in high frequency sub-band does not violate the imperceptibility requirements of watermarking, however, compression might remove high frequency sub-band that contains the watermark. So we decide to continue the work in the diagonal sub-band of 2 levels of DWT since it provides better results of imperceptibility.

- **CT**

In this algorithm, the watermark image was embedded after applying 1-level CT. We compared the imperceptibility of this method with 2 and 3 levels of CT. We notice that that the best choice of embedding in the next steps is directional sub-band of 2- level of CT since they produce better results in the imperceptibility.

- **DWT-CT**

In the first step of this algorithm, we applied 2-level DWT to the original image and chose the mid-mid sub-band (LH2) to apply CT. In the second step, we applied 2-level CT and embeded the watermark in the directional sub-band.

Each algorithm was evaluated by testing the imperceptibility and calculating the PSNR between the original image and watermarked image. We also tested the robustness by applying geometrical and removable attacks, and then calculate the correlation between the original and extracted watermark. Following is a discussion of the system after applying the three algorithms, and comparing the results with relevant works.

We compared our results of the three algorithms: DWT, CT and the combined DWT-CT. First we compared the visibility of the three algorithms. Table 4.9 shows the PSNR values of the three algorithms.

Original Image	Watermarked Image		
	2-DWT	3-CT	DWT-CT
	 PSNR = 80.21	 PSNR = 76.88	 PSNR = 88.11

Table 4.9: Evaluation the PSNR values after applying three algorithms

We compared the robustness of the three algorithms for different attacks. First we applied Geometrical Attacks: Rotation and Cropping. The results of Correlation values between the original watermark and the extracted watermark from the attacked watermarked image are shown in table 4.10.

Algorithm	Correlation							
	Rotation Angle				Cropping Block Size			
	60	120	240	300	8	104	152	200
2-DWT	0.031	0.041	0.0067	-0.021	0.691	0.664	0.591	0.526
2-CT	0.311	0.309	-0.303	-0.314	0.443	0.431	0.401	0.385
DWT-CT	0.028	-0.063	0.051	0.037	0.831	0.805	0.759	0.635

Table 4.10: Evaluation correlation values due to geometrical attacks for three algorithms

Then we applied watermark removal attacks: Gaussian Noise, JPEG Compression and Dithering. The results of correlation values between the original watermark and the extracted watermark from the attacked watermarked image are shown in table 4.11.

Algorithm	**Correlation**								
	Gaussian Noise Mean			**Compression Quality**			**Dithering *Qm***		
	0	**0.04**	**0.08**	**0**	**40**	**80**	**5**	**10**	**15**
2-DWT	0.698	0.698	0.698	0.380	0.695	0.695	0.700	0.702	0.465
2-CT	0.446	0.446	0.445	0.309	0.443	0.446	0.447	0.444	0.366
DWT-CT	0.835	0.838	0.835	0.327	0.695	0.825	0.835	0.841	0.472

Table 4.11: Evaluation correlation values due to removal attacks for three algorithms

At the beginning, we tested the performance of applied DWT and CT algorithm separately for the sake of comparison before combining them. First, the results we obtained for the DWT algorithm only, gave a PSNR value 80.21 and we found that this algorithm was not robust against rotation and cropping attacks. Second, the results after applying CT algorithm only gave a PSNR value 76.88 and algorithm was not robust to different types of image attacks. Finally, we evaluated imperceptibility of the combined DWT-CT algorithm which gave a PSNR value 88.11 and the combination DWT-CT algorithm improves robustness since it produced better robust against Gaussian noise ,

cropping and dithering attacks. Accordingly, the results of our system are compared to relevant works of others in the field of watermarking. Table 4.12 shows some comparative results of different methods of digital image watermarking.

Name	Methodology	Imperceptibility	Robustness
Al-Haj, (2007)	Combined DWT-DCT Digit Image Watermarking	PSNR=97.072	Robust against Gaussian noise and cropping
Shilbayeh, &Alshamary, (2010)	Cascading HWT-DWT Digit Image Watermarking	PSNR=37.52	Invert and Gaussian noise
Amirgholipour,& Naghsh-Nilchi, (2009)	Jointed DWT-DCT Digit Image Watermarking	PSNR=37.88	Robust against Gaussian noise, compression Blurring & cropping
DWT-CT	Combined DWT-CT Digit Image Watermarking	PSNR=88.11	Robust against Gaussian noise Dithering & cropping

Table 4.12: Evaluation results of different related works of digital image watermark

Al-Haj, (2007), found that the combined DWT-DCT watermarking algorithm outperforms the conventional DWT only against the Gaussian noise and cropping attacks, and imperceptibility evaluation produced a PSNR value 97.072. Shilbayeh, & Alshamary, (2010), the researchers presented a new robust and secure hybrid watermark technique based on HWT and DWT. This method achieved a PSNR value 37.52 and the system robust to invert and gaussian noise. Amirgholipour, & Naghsh-Nilchi, (2009) developed a new robust digital image watermarking algorithm based on join DWT-DCT transforms. It is clear from table 4.12 that our algorithm shows a significant improvement in imperceptibility compared to Shilbayeh, & Alshamary, (2010) and Amirgholipour, & Naghsh-Nilchi, (2009), and is more robust compared with all previous works.

CHAPTER FIVE

Conclusion, Future work and Recommendations

Chapter 5

Conclusion, Future work and Recommendations

5.1. Conclusion

Discrete Wavelet Transform (DWT) and Contourlet Transform (CT) have been applied efficiently and successfully in many digital image watermarking systems. In this thesis, we introduce a new algorithm of digital image watermarking based on combination between DWT and CT. Watermarking was done by embedding the watermark in the two level-DWT of original image followed by two level-CT on the carefully selected subband. The combination improves the system performance. The system was tested using five common types of image attacks. It achieved a PSNR value 88.11 and provided a high resistance to JPEG compression, add noise and dithering.

Compared with other existing watermarking systems, our system is more robust and more imperceptible. Classical watermarking system is particularly compared based on DWT, using the same embedding strategy, the imperceptibility of the system is better than DWT and stronger robustness than based on DWT only. So we reached our goal by implementing an efficient algorithm that doesn't degrade the visibility of original image and at the same time, is robust against the attacks.

5.2. Future Work and Recommendations

To conclude this thesis, in light of relevant work presented in this thesis, the following are recommended by the researcher:

1. In this thesis there was a tradeoff between imperceptibility and robustness. Increasing the gain factor *K* in three algorithms gave better robustness but affected the imperceptibility of the watermarked image. In the future, an algorithm can be implemented to choose the best gain factor which compromises these two requirements.
2. Increase the payload of the system by increasing the size of the watermark image.
3. Increase the ability of the system to cover other file types such as text, audio, and video clips files.
4. Use neural networks to determine the best region in original image to perform the embedding process.

References

1. Al-Haj, A. (2007), Combined DWT-DCT Digital Image Watermarking, ***Journal of Computer Science***, Vol. 3, No. 9, pp. 740-746.
2. Amirgholipour, S. & Naghsh-Nilchi, A. (2009), Robust Digital Image Watermarking Based on Joint DWT-DCT***, International Journal of Digital Content Technology and its Applications,*** Vol.3, No. 2.
3. Candik, M., Matus, E. & Levicky, D. (2001), Watermarking in Wavelet Transform Domain***, Radioengineering,*** Vol. 10, No. 2.
4. Do, M. &Vetterli, M. (2005), TheContourlet Transform: An Efficient Directional Multiresolution Image Representation***, IEEE Transactions on Image Processing Image Processing***, pp. 2091-2106.
5. Duan ,G. , TS, H. & Zhao, X. (2008), A Novel non-redundant Contourlet Transform for Robust Image Watermarking against non-geometrical and geometrical Attacks, ***5th International Conference on Visual Information Engineering,***PP. 124-129.
6. Duncan D., Po, Y. & Minh, D. (2006), Directional Multiscale Modeling of Images Using the Contourlet Transform, ***IEEE Transactions on Image Processing,*** Vol.15,, No. 6, pp. 1610- 1620.
7. El rube', I. ,Abou el Nasr, M. , Naim,M. & Farouk, M. (2009), Contourlet Versus Wavelet Transform for Robust Digital Image Watermarking Technique***, wordAcademy of Science, Engineering and Technology 60.***

8. Emek, S. & Pazarci, M. (2005) ," A Cascade DWT-DCT Based on Digital Watermarking Scheme", (on-line),available: http://www.eurasip.org/Proceedings/Eusipco

9. Ghannam,S. & Abou-chadi, F. (2009), Contourlet Verses Wavelet Transform: A Performance Study for a Robust Image Watermarking,. ***Second International Conference Applications of Digital Information and Web Technologies, on the 2009. ICADIWT '09***

10. Hajjara, S. ,Abdallah, M. & Hudaib, A. (2009),Digital Image Watermarking using Localized Biorthogonal Wavelets , ***European Journal of Scientific Research*** , Vol. 26, No. 4, pp. 594-608.

11. Hsieh, M., Tseng, D. & Huang, Y. (2001), Hiding Digital Watermarks Using Multiresolution Wavelet Transform, ***IEEE Transactions on Industrial Electronics***, Vol.48, No.5,pp. 875-882.

12. Jayalakshmi, M., Merchant, S. & Desia, B.(2006),Digital Watermarking in Contourler Domain, ***The 18th International Conference on Pattern Rocognition***.

13. Jiansheng, M., Sukang, L. &Xiaomei,T. (2009), A Digital Watermarking Algorithm based on DCT and DWT, ***International Symposium on Web Information System and Applications***, pp.104-107.

14. Khalighi, S. & Rabiee, H. (2009),"A Contourlet-based Image Watermarking Scheme with High Resistance to Removal and Geometrical Attacks", (On-Line), available:http://www.hindawi.com/journals/asp

15. Kundur, D. & Hatzinakos, D.(2004), Towards robust logo watermarking using multiresolution image fusion principles, ***IEEE Tranactions A. on ImageProcessing***, Vol.6,, No. 1, pp. 185– 198.

16. Lin, C. (2001), Multipurpose Digital Watermarking Method Integrating Robust, Fragile and Semifrigle Watermarking **, *International Journal of Innovative Computing , International and Control***, Vol.6,No.7,PP.3023-3036.

17. Lin, T. & Delp, J. (1999), A review of Data Hiding in Digital Images,***Image capture system conference***,PP.274-278.

18. Meena, C. & muthivadhan, D. (2010), A Comparative Study on Fingerprint Protection using Watermarking Ttechniques, ***Global Journals of Computer Science and Technology***, Vol. 9,No.5.

19. Potdar, M., Han, S. & Chang, E.(2005), A Survey of Digital Image Watermarking Techniques, ***IEEE International Conference on Industrial Informatics***, pp. 709-716, Perth, Australia.

20. Paquet, A.(2001), Multiresolution Watermark based on Wavelet Transform for Digital Images, ***projectreport, university of British,*** Columbia, Canada.

21. Riazifar, N. & Yazdi, M. (2009), Effectiveness of Contourlet Vs. Wavelet Transform on Medical Image Compression: A Comparative Study, ***World Academy of Science, Engineering and Technology.***

22. Shilbayeh N. & Ashimary A. (2010), Digital Watermark System Based on Cascading Haar Wavelet Transform and Discrete Wavelet Transform, ***Journal of Applied Science***, Vol.10, No.19,pp. 2168-2186.

23. Shu, Z., Wang, S., Deng, C. , Liu, G. & Zhang, L.(2008), Watermarking Algorithm based on Contourlet Transform and Human Visual Model, ***International Conference on Embedded Software andSystems.***PP.348-352.

24. Tsai, M. & Hung, H.(2005). DCT and DWT based Image Watermarking Using Subsampling, ***IEEE Fourth International Conference on Machine Learning and Cybernetics***, pp. 5308-5313,China.

25. Voloshynovskiy, S., Pereira , S. & Pun, T.(2001), Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks, ***Comm. Magazine***, Vol.39, No.8,pp. 118-126.

26. Wie-Zhu, X. ,Campus, S. & Xiao, L. (2009), Research of Blind Watermark Detection Algorithm Based on Wavelet and Contourlet Transform Domain. ***International Conference, E-Business and Information System Security, 2009.EBISS '09.***

27. Yingkun, H., Chunxia, Z., Mingxia, L. & Deyun, Y.(2008), The Nonsubsampled Contourlet-Wavelet Hybrid Transform: Design and Application to Image Watermarking, ***2008 International Conference on computer Science and Software Engineering.***

28. Zaboli, S. & Shahram, M.(2007), A Non-Blind Adaptive Image Watermarking Approach Based On Entropy in Contourlet Domain, ***IEEE International Symposium on Industrial Electronics,***Spain**.**