EFFICIENT DIGITAL IMAGE WATERMARKING TECHNIQUES BASED ON DISCRETE COSINE TRANSFORM AND DISCRETE WAVELET TRANSFORM

SK. Alamgir Hossain S.M. Mohidul Islam

Computer Science and Engineering Discipline
Khulna University
Bangladesh
February 2007

EFFICIENT DIGITAL IMAGE WATERMARKING TECHNIQUES BASED ON DISCRETE COSINE TRANSFORM AND DISCRETE WAVELET TRANSFORM

By

SK. Alamgir Hossain

Roll: 020216

And

S.M. Mohidul Islam

Roll: 020219

submitted in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering (CSE) at

Khulna University
Khulna-9208, Bangladesh
February 2007

Khulna University

Computer Science and Engineering Discipline

The undersigned hereby certify that they have read and recommend to the computer Science and Engineering Discipline for acceptance a thesis entitled "EFFICIENT DIGITAL IMAGE WATERMARKING TECHNIQUES BASED ON DISCRETE COSINE TRANSFORM AND DISCRETE WAVELET TRANSFORM" by SK. Alamgir Hossain and S.M. Mohidul Islam in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering (CSE)

of Science in Computer Science and Engineering (Co	SE)
	Dated: 27 th February 2007
Dr. Rameswar Debnath	Supervisor
Associate Professor	
Computer Science and Engineering Discipline	
Dr. Md. Rafiqul Islam	External Examiner
Professor	
Computer Science and Engineering Discipline	
Dr. Md. Rafiqul Islam	Head of the discipline
Professor	
Computer Science and Engineering Discipline	

Abstract

In this thesis we propose a digital image watermarking technique based on DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform). A digital watermark is a digital signal or pattern inserted into a digital image that must be invisible, permanent and detectable after intentional or unintentional image processing attacks such as scaling, cropping, rotation, compression etc. Digital image watermarking is necessary for protecting copyright of digital images i.e., the ownership and the right of the author of those images, in the Internet, CD, DVD etc. The DCT, or DWT help to separate an image into spectral sub-bands of differing importance (with respect to the image's visual quality). Most of the images, after transformation the majority of signal energy are carried by just a few of the low order DCT, or DWT coefficients. For invisibility the watermark should be embedded with the higher order DCT, or DWT coefficients of the original image. But the watermark may increase the value of the coefficients significantly which deteriorate image visual quality. For this reason, the watermark is first converted into a special form (in our method a binary sequence) then applied on the selected coefficients. Experimental results show that better performance can be achieved using our proposed method in case of multiple watermarking, scaling and compression attack. We also present results which demonstrate the robustness of the method against some other common image processing attacks such as cropping and rotation.

Acknowledgement

First of all we would like to thank Almighty ALLAH the merciful, the gracious who has given us the ability, intelligence and energy to accomplish the thesis works.

We would like to express our cordial regard to our supervisor Dr. Rameswar Debnath for his suggestion, proper guidance and continuous encouragement through out the course of the study. His inspiration and careful observation are beneficial to reach at this stage.

We want to thank our external examiner Dr. Md. Rafiqul Islam for his proper review and evaluation of our work. His instructions and guidance helped us to perform necessary modifications and improvements to our thesis.

Moreover, we would like to thank all our respective teachers of CSE discipline for their suggestions, valuable advice and their sincere co-operation of this thesis. We also thank all our friends and those who helped, inspired and gave us mental support at different stages in different moment.

Table of Contents

Chapter	Title	Page
	List of Figures List of Tables	vi vii
I	Introduction	1
	1.1 Introduction 1.2 Motivation	1 2 3
	1.3 Challenges in This Area1.4 Objective of Our Study1.5 Organization of the Thesis	3 3 3
II	Overview of Digital Watermarking	5
	 2.1 Introduction 2.2 Digital Watermarking 2.2.1 What is Digital Watermark? 2.2.2 The Purpose of Digital Watermarking 2.2.3 Visible vs. Invisible Digital Watermarks 2.2.4 Requirements of Digital Watermarking 2.2.5 Techniques for Digital Watermarking 2.2.6 Limitations of Digitals Watermarking 2.2.7 Applications of Digital Watermarking 2.2.8 Different Kinds of Attacks in Digital Watermarking 2.3 Digital Image Watermarking 2.3.1 Several Time Domain Methods and Their Problems 2.3.2 Several Frequency Domain Methods and Their Problems 2.4 Conclusion 	5 5 5 6 6 7 7 8 8 8 9 10 10 11
III	Discrete Cosine Transform and Discrete Wavelet Transform Techniques	13
	 3.1 Discrete Cosine Transform (DCT) 3.1.1 What is DCT? 3.1.2 The One and Two-Dimensional DCT 3.1.3 Comparison to DFT 3.2 Discrete Wavelet Transform (DWT) 3.2.1 What is DWT? 3.2.2 Details about DWT 3.2.3 Comparison to DFT 3.3 Conclusion 	13 13 14 16 16 17 17 18
1 V	An Efficient Digital Image Watermarking Technique Based on Discrete Cosine Transform	19
	 4.1 Introduction to the Technique 4.2 Proposed DCT Based Technique 4.2.1 Watermark Embedding process 4.2.2 Watermark Detecting process 4.3 Experimental Results 4.3.1 Determining the Scaling Parameter K 4.3.2 Scaling 4.3.3 JPEG Compression 	19 22 23 24 24 25 25 26

4.3.4 Cropping 4.3.5 Rotation 4.3.6 Performance on Random Watermark test 4.3.7 Performance on Multiple Watermarks 4.4 conclusion	26 27 27 28 28
An Efficient Digital Image Watermarking Technique Based on Discrete Wavelet Transform	29
5.1 Introduction	29
5.2 Proposed DWT Based Technique	29
5.2.1 Watermark Embedding Process	29
5.2.2 Watermark Detecting Process	30
	30
	31
	31
	32
	32
	33
	34
	34
5.4 conclusion	35
Concluding Remarks	36
Bibliography	37
Appendix A List of the Accepted Papers Related to This Thesis	A-I R-I
	4.3.5 Rotation 4.3.6 Performance on Random Watermark test 4.3.7 Performance on Multiple Watermarks 4.4 conclusion An Efficient Digital Image Watermarking Technique Based on Discrete Wavelet Transform 5.1 Introduction 5.2 Proposed DWT Based Technique 5.2.1 Watermark Embedding Process 5.2.2 Watermark Detecting Process 5.3 Experimental Results 5.3.1 Determining the Scaling Parameter K 5.3.2 Scaling 5.3.3 JPEG Compression 5.3.4 Cropping 5.3.5 Rotation 5.3.6 Performance on Random Watermark Test 5.3.7 Performance on Multiple Watermarks 5.4 conclusion Concluding Remarks Bibliography

List of Figures

Figure No	Name of the Figure	Page
1.1	American \$20 bill	2
1.2	A generic watermarking system	2
3.1	(a) Arrangement of DCT coefficients (b) Reordering of DCT coefficients	14
3.2	Block diagram of 2D-DCT transform	15
3.3	Two dimensional DCT basis functions ($N = 8$). Neutral gray represents zero, white represents positive amplitudes, and black represent negative amplitude	15
3.4	2-D DCT compared to the DFT	16
3.5	Arrangement of DWT coefficients	17
4.1	After taking DCT frequency distribution in the proposed method	23
4.2	Block diagram of watermark embedding process	23
4.3	Block diagram of watermark detecting process	24
4.4	(a) Sample watermark signal (b) Host image (c) watermarked image	24
4.5	Detector response (a) to 1000 randomly generated watermarks. Only watermark number 400 matches that embedding (b) on two different watermarks	28
5.1	Block diagram of watermark embedding process	30
5.2	Block diagram of watermark detection process	30
5.3	Sample cropping after rotation	34
5.4	Detector response (a) to 1000 randomly generated watermarks. Only watermark number 400 detected (b) on two different watermarks	35

List of Tables

Table No	Name of the Table	Page
4.1	Characteristics of original <i>Lena</i> and the watermarked image for different values of <i>K</i>	25
4.2	Scaling	25
4.3	JPEG Compression	26
4.4	Cropping	27
4.5	Rotation	27
5.1	Characteristics of original $Lena$ and the watermarked image for different values of K	31
5.2	Scaling Attack Detected by (a) proposed DWT method (b) the Method [6] and our proposed Methods	32
5.3	JPEG compression Attack Detected by (a) proposed DWT method (b) the Method [6] and our proposed Methods	32
5.4	Cropping Attack Detected by (a) proposed DWT method (b) the Method [6] and our proposed Methods	33
5.5	Rotation Attack Detected by (a) proposed DWT method (b) the Method [6] and our proposed Methods	33
5.6	Detector response for cropping after rotation attack.	34

Chapter I

Introduction

1.1 Introduction

The copyright of digital images i.e., the ownership and the rights of the author of those images, in the Internet, CD, DVD etc, can be easily violated by cropping and graphical modification. Some parts of an image such as the human face image can be cropped and applied to other images without permission which violates the copyright. To protect the copyright, the digital image watermarking technique is applied. In watermarking the secret information called as watermark, is invisibly embedded into the host media, while it should resist to malicious attacks. It is embedded permanently in an image and introduces invisible changes for the human vision that can be detected only by a computer program. To protect the cropping attack, the watermark should be embedded and distributed over the image. The watermarks must be robust to distortions such as those caused by image processing algorithms. Image processing does not modify only the image but may also modify the watermark as well. Thus, the watermark may become undetectable after intentional or unintentional image processing attacks. The watermark alterations should not decrease the image quality. A general watermarking framework for copyright protection has been presented in [7] and describes all these issues in detail. Watermarking techniques can be categorized into two types according to embedding and extraction processes. In the first type, the watermark is embedded in the time or spatial domain. The second type is the watermarking in the frequency domain. The advantages of embedding watermarks in the frequency domain over time domain is that the position of the watermark in time domain is sparsely spread, so that the intentional attempts to remove or destroy the watermark in time domain cannot be easily done. The disadvantage of embedding watermarks in the frequency domain is that, it does not yield better resistance in the cropping attack. The difference between the cryptosystem and digital watermarking is that, most cryptographic protocols are concerned with secured communications instead of ulterior copyright infringements.

If we hold an American \$20 bill up to the light. If we are looking at the side with the portrait of President Andrew Jackson, we will see that the portrait is echoed in a watermark on the right. This watermark is embedded directly into the paper during the papermaking process, and is

therefore very difficult to forge. It also thwarts a common method of counterfeiting in which the counterfeiter washes the ink out of \$20 bills and prints \$100 bills on the same paper. The watermark on the \$20 bill (Figure 1.1), just like most paper watermarks today, has two properties that relate to the subject of the present book. First, the watermark is hidden from view during normal use, only becoming visible as a result of a special viewing process (in this case, holding the bill up to the light). Second, the watermark carries information about the object in which it is hidden (in this case, the watermark indicates the authenticity of the bill).



Figure 1.1: American \$20 bill.

In addition to paper, watermarking can be applied to other physical objects and to electronic signals. Fabrics, garment labels, and product packaging etc. Electronic representations of music, photographs, and video are common types of signals that can be watermarked. Here we discuss only the digital image watermarking. In general, a digital image watermarking system consists of an embedder and a detector, as illustrated in Figure 1.2.

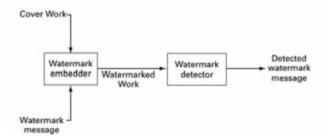


Figure 1.2: A generic watermarking system.

1.2 Motivation

The enormous popularity of the World Wide Web (WWW) in the early 1990's demonstrated the commercial potential of offering multimedia resources through the digital networks. Since commercial interests seek to use the digital networks to offer digital media for profit, they have a strong interest in protecting their ownership rights. Digital watermarking has been proposed as one way to accomplish this. As motion picture are composed of digital images and the digital videos are recently used in internet, so at present digital image watermarking is one of the most important topics in computer science. A better application for this type of

watermarking can be used by the most TV broadcast company, Music video Company, IEEE, ACM etc to protect their videos, images, research papers etc. This topic is a growing popularity which is very necessary today and in future strongly. For this reason, we were motivated to this topic and selected as our thesis topic.

1.3 Challenges in This Area

The problem is concerned with our proposed technique and comparison of the performance of different frequency domain based digital image watermarking and improvement of the performance of the existing frequency based methods. We have to show the performance comparison of the existing methods with the proposed method.

1. 4 Objectives of Our Study

We have designed a digital image watermarking technique to obtain the several objectives such as to develop frequency based digital image watermarking method, to improve the performance of the proposed method to the existing methods, to show the comparison results, etc.

1.5 Organization of the Thesis

This thesis has been organized into six chapters. Each chapter gives distinct concept.

Chapter II (*Overview of Digital Watermarking*): This chapter presents the general description about digital watermarking, the purpose of digital watermarking, visible vs. invisible watermarks, requirements, limitations, applications of digital watermarking, and different kinds of attacks on digital watermarking. This chapter also discusses about some existing image watermarking methods both in time and frequency domain and discusses the problems of those methods

Chapter III (Discrete Cosine Transform and Discrete Wavelet Transform Techniques): This chapter presents several popular techniques of digital watermarking such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT). From this description, one can easily gain the general idea about digital watermarking technique. A general watermarking

framework for copyright protection has been presented in [7] and describes all these issues in detail.

Chapter IV (An Efficient Digital Image Watermarking Technique Based on Discrete Cosine Transform): This chapter presents proposed DCT based method and it's embedding and detecting process for watermarking. We also discuss the experimental result in different image operations such as rotation, scaling, JPEG compression, cropping, and multiple watermarking by the proposed method.

Chapter V (An efficient Digital Image Watermarking Technique based on Discrete Wavelet Transform): This chapter presents proposed DWT based method and it's embedding and detecting process for watermarking. We also discuss the experimental result in different image operations such as rotation, scaling, JPEG compression, cropping, and multiple watermarking by the proposed method. The performance comparison of our proposed DCT and DWT based methods with several other methods are also described in this chapter.

Chapter VI (*Concluding Remarks*): This chapter gives the conclusion of our thesis. The limitation of our algorithms is pointed out and we have also enlightened the future recommendation here.

Chapter II

Overview of Digital Watermarking

2.1 Introduction

The ownership of an image, audio, video or any kind of digital data can be obtained by performing digital watermarking technique that means watermarking have many applications. There are two kinds of watermarks: Visible and invisible watermarks. The watermarking techniques have some limitation where this technique is not appreciable or is unable to establish the ownership robustly. There are many kinds of attacks that act as barrier in watermarking technique. The purpose of digital watermarking technique is to detect the watermark though these kinds of attack may occur.

2.2 Digital Watermarking

In the next sections, the digital watermark and different kinds of digital watermark, its purposes, requirements, techniques, limitations, and applications are described below.

2.2.1 What is Digital Watermark?

The enormous popularity of the World Wide Web (WWW) in the early 1990's demonstrated the commercial potential of offering multimedia resources through the digital networks. Since commercial interests seek to use the digital networks to offer digital media for profit, they have a strong interest in protecting their ownership rights. Digital watermarking has been proposed as one way to accomplish this. A digital watermark is a digital signal or pattern inserted into a digital image. Since this signal or pattern is present in each unaltered copy of the original image, the digital watermark may also serve as a digital signature for the copies. A given watermark may be unique to each copy (e.g., to identify the intended recipient), or be common to multiple copies (e.g., to identify the document source). In either case, the watermarking of the document involves the transformation of the original into another form. This distinguishes digital watermarking from digital fingerprinting where the original file remains intact, but another file is created that "describes" the original file's content. As a simple example, the checksum field for a disk sector would be a fingerprint of the preceding block of data.

Similarly, hash algorithms produce fingerprint files. Digital watermarking is also to be contrasted with public-key encryption, which also transform original files into another form. It is a common practice nowadays to encrypt digital documents so that they become un-viewable without the decryption key. Unlike encryption, however, digital watermarking leaves the original image or (or file) basically intact and recognizable. In addition, digital watermarks, as signatures, may not be validated without special software. Further, decrypted documents are free of any residual effects of encryption, whereas digital watermarks are designed to be persistent in viewing, printing, or subsequent re-transmission or dissemination.

2.2.2 The Purpose of Digital Watermarking

Two types of digital watermarks may be distinguished, depending upon whether the watermark appears visible or invisible to the casual viewer. Visible watermarks are used in much the same way as their bond paper ancestors, where the opacity of paper is altered by physically stamping it with an identifying pattern. This is done to mark the paper manufacturer or paper type. One might view digitally watermarked documents and images as digitally "stamped". Invisible watermarks, on the other hand, are potentially useful as a means of identifying the source, author, creator, owner, and distributor or authorized consumer of a document or image. For this purpose, the objective is to permanently and unalterably mark the image so that the credit or assignment is beyond dispute. In the event of illicit usage, the watermark would facilitate the claim of ownership, the receipt of copyright revenues, or the success of prosecution. Watermarking has also been proposed to trace images in the event of their illicit redistribution.

2.2.3 Visible vs. Invisible Digital Watermarks

Visible and invisible watermarks both serve to deter theft but they do so in very different ways. Visible watermarks are especially useful for conveying an immediate claim of ownership. The main advantage of visible watermarks, in principle at least, is that they virtually eliminate the commercial value of the document to a would-be thief without lessening the document's utility for legitimate, authorized purposes. A familiar example of a visible watermark is in the video domain where CNN and other television networks place their translucent logo at the bottom right of the screen image. Invisible watermarks, on the other hand, are more of an aid in catching the thief than discouraging the theft in the first place. Visible and invisible watermarks act as deterrence to theft in different ways. Visible watermarks diminish the commercial value of the document or image. Invisible watermarks increase the likelihood of

successful prosecution. Invisible watermarks may also act as a deterrent if perpetrator is aware of their possible use.

2.2.4 Requirements of Digital Watermarking

To be effective in the protection of the ownership of intellectual property, the invisibly watermarked document should satisfy several criteria:

- 1. the watermark must be difficult or impossible to remove, at least without visibly degrading the original image,
- 2. the watermark must survive image modifications that are common to typical imageprocessing applications (e.g., scaling, cropping, and image compression),
- 3. an invisible watermark should be imperceptible so as not to affect the experience of viewing the image, and
- 4. for some invisible watermarking applications, watermarks should be readily detectable by the proper authorities, even if imperceptible to the average observer. Such decidability without requiring the original, un-watermarked image would be necessary for efficient recovery of property and subsequent prosecution.

2.2.5 Techniques for Digital Watermarking

Watermarking techniques tend to divide into two categories, text and image, according to the type of document to be watermarked. Techniques for images: Several different methods enable watermarking in the spatial domain. The simplest is to just flip the lowest-order bit of chosen pixels in a gray scale or color image. This will work well only if the image will not be subject to any human or noisy modification. The resulting watermark may be visible or invisible depending upon the value of the watermark intensity. Watermarking can be applied in the frequency domain by first applying a transform like the Fast Fourier Transform (FFT). In a similar manner to spatial domain watermarking, the values of chosen frequencies can be altered from the original. Since high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies that contain important information of the original picture. Since watermarks applied to the frequency domain will be dispersed over the entirety of the spatial image upon inverse transformation, this method is not as susceptible to defeat by cropping as the spatial technique. However, there is more of a tradeoff here between invisibility and decidability, since the watermark is in effect applied indiscriminately across the spatial image.

Watermarking can be applied to text images as well. Three methods are commonly used: text line coding, word space coding, and character encoding.

2.2.6 Limitations of Digital Watermarking

As of this writing, a counterfeiting scheme has been demonstrated for a class of invertible, feature-based, frequency domain, invisible watermarking algorithms. This counterfeiting scheme could be used to subvert ownership claims because the recovery of the digital signature from a watermarked image requires a comparison with an original. The counterfeiting scheme works by first creating a counterfeit watermarked copy from the genuine watermarked copy by effectively inverting the genuine watermark. This inversion creates a counterfeit of the original image which satisfies two properties: (a) a comparison of the decoded versions of both the original and counterfeit original yields the owner's (authorized) signature, and (b) a comparison of decoded versions of both the original and counterfeit original yield the forged (inverted) signature. This, the technique of establishing legitimate ownership recovering the signature watermark by comparing a watermarked image with the original image breaks down. It can be shown that both the legitimate signature and counterfeiter's signature inhere in both the watermarked and counterfeit watermarked copies. Thus, while it may be demonstrated that at least one recipient has a counterfeit watermarked copy, it can not be determined which it is.

2.2.7 Applications of Digital Watermarking

In this section we discuss some of the scenarios where watermarking is being already used.

Digital Image Watermarking: In this case Digital image watermarks have been proposed as a method for discouraging illicit copying and distribution of copyrighted digital images.

Digital Audio Watermarking: In this case, time and frequency masking properties of the human ear are used to conceal the watermark and make it inaudible. The greatest difficulty lies in synchronizing the watermark and the watermarked audio file.

Digital Video Watermarking: As digital video are sequence of still images so watermarking also used in case of video watermarking.

Digital Text Watermarking: This problem, which in fact was one of the first that was studied within the information hiding area, can be solved at two levels. At the printout level, and at the semantic level

Fingerprinting: This is similar to the previous application and allows acquisition devices (such as video cameras, audio recorders, etc) to insert information about the specific device (e.g., an ID number) and date of creation. Some digital cameras already include this feature.

2.2.8 Different Kinds of Attacks in Digital Watermarking

In the following, different kinds of attacks that are generally applied to the digital watermarking are described elaborately.

JPEG Compression: In computing, JPEG (pronounced JAY-peg) is a commonly used standard method of compression for photographic images. This is generally an unintentional attack which appears very often in multimedia applications. Practically all the audio, video and images that are currently being distributed via Internet have been compressed. If the watermark is required to resist different levels of compression, it is usually advisable to perform the watermark insertion task in the same domain where the compression takes place. For instance, DCT domain image watermarking is more robust to JPEG compression than spatial-domain watermarking. Although JPEG allows for lossless compression, it is most commonly used for lossy compression of images.

Scaling: Scaling is the process of expanding or compressing the dimensions of an object. A scling constant greater than one indicates an expansion of length, and less than one, compression of length. If both scaling constants have the same value s, the scaling transformation is said to be homogeneous or uniform. Digital watermarking methods are often resilient only to uniform scaling.

Rotaion: In rotation, the object is rotated θ^0 about the origin. The convention is that the direction of rotation is counterclockwise if θ is a positive angle and clockwise if θ is a negative angle.

Cropping: 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 of frames of a video sequence. When the image is cropped, image part is lost. The larger the cropping, the most of

the image part is lost. In case of digital watermarking, the cropping must be in a reasonable rage, so that watermark can be detected.

Multiple Watermarking: An attacker may watermark an already watermarked object and later make claims of ownership. The easiest solution is to timestamp the hidden information by a certification authority.

2.3 Digital Image Watermarking

Among the applications of digital watermarking, image watermarking is an important area. In this age of internet digital image watermarking technique is a necessary subject in order preserving the ownership of the image. For this reason, several works are performed in this area. Several of these works on digital image watermarking technique and their problems are described below.

2.3.1 Several Time Domain Methods and Their Problems

There are many existing time domain methods, but these existing methods have several problems or limitations, some of them are described below.

I. Pitas [5] embedded the generated watermark by altering an original pixel with its (3 x 3) neighboring pixels and a constant value. The generated watermark is encoded with an error correction code to correct the watermark after attacking. This method is resistant to the JPEG compression and cropping attack but the watermarked image quality is suffered.

M. Ramkumar [10] proposed the watermarking in each block and used relative neighboring block for verifying the watermarks.

A. Nikolaidis and I.Pitas [12] proposed the watermarking in the important regions of an image. Although these techniques can resist the cropping attack and improve the resistance of compression, they still can not cope with the serious cropping attack, where an image is cropped with any shapes, sizes and locations.

2.3.2 Several Frequency Domain Methods and Their Problems

There are many existing frequency domain methods, but these existing methods have several problems or limitations, some of them are described below.

Piva et al. [13] suggested adding the watermark to a larger number of DCT coefficients which need not be significant. They order the DCT coefficients in a zigzag scan and the first 16000 coefficients are left out. The watermark is added to the next 25000 coefficients. Watermark detection is performed by correlating these 25000 coefficients in the test image with the original copy of the watermark.

Pereira et al. [6] describes a method for the secure and robust copyright protection of digital images. They present an approach for embedding a digital watermark into an image using the FFT. This method is robust against rotation and cropping but outperforms narrow result in JPEG compression and scaling. Again they use FFT which has both real and imaginary part that requires complex computation.

I. J. Cox et al. [11]. proposed to improve robustness of the embedded watermark by applying spread spectrum technique in DCT domain. The watermark was spread by a secure parameter called chip-rate. The redundancy of watermark can improve its robustness against several severely attacks. Unfortunately, the host media should large enough to embed the redundant version of original watermark.

Andrew B. Watson. [17]. proposed to embed watermark only in middle frequency band of DCT domain in order to retain the quality of the original images. The watermark can resist various types of attack except high-rate compression attack. The use of block based DCT was proposed by dividing an image into a block, the artifacts produced from embedding watermark process are confined with each block. Hence the quality of the watermarked image is higher than the method proposed in I. Racocevie with the same level of robustness.

X.G. Xia et al. [14]. proposed to embed watermark into middle and high frequency subbands of multiresolution version of original image. H. Inoue et al. used EZW to embed watermark in order to increase its robustness against compression attack.

Fulin et al. [16] adjusted the DCT-based technique to protect the cropping attack. They used a marking-signal in an image to specify the location of the watermark.

2.4 Conclusion

In this chapter, the basics of digital watermarking, different kinds of watermarks, their applications, requirements, techniques are described. Since our concern is with image watermark, we also describe several time and frequency domain methods and their problems for digital image watermarking. In this thesis, the frequency domain methods are of concern because frequency domain methods help to separate the image into spectral sub bands of different importance. By applying watermark to the sub band which carries least significant information help the watermark to be invisible. In our thesis we use two well known frequency domain methods DCT and DWT. Due to this reason; we describe the basic of these two methods in the next chapter.

Chapter III

Discrete Cosine Transform and Discrete Wavelet Transform Techniques

This chapter details the overview of two mathematical techniques used elaborately in digital image watermarking technique. In section 3.1 the details about Discrete Cosine Transform (DCT) technique and in section 3.2 the details about Discrete Wavelet Transform (DWT) technique are described.

3.1 Discrete Cosine Transform (DCT)

In the following subsections, the details about DCT and its comparison to DFT is described.

3.1.1 What is DCT?

The DCT is a mathematical technique for converting a signal or data in spatial (or time) domain into elementary components of frequency in the orthogonal domain, (or frequency domain). Formally, the discrete cosine transform is a linear, invertible function $F: \mathbf{R}^N \to \mathbf{R}^N$ (where **R** denotes the set of real numbers), or equivalently an $N \times N$ square matrix. There are several variants of the DCT with slightly modified definitions. The N real numbers $x_0, ..., x_{N-1}$ are transformed into the N real numbers $X_0, ..., X_{N-1}$ according to the formula. The most common variant of discrete cosine transform is the type-II DCT, which is often called simply "the DCT"; its inverse, the type-III DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT". The discreet cosine transforms converts spatial information to "frequency" or spectral information, with the X and Y axes representing frequencies of the signal in different dimensions. The pixels when transformed are arranged from the most significant pixel to the least significant pixel. The DCT functions themselves are lossless. Pixel loss occurs when the least significant pixels are quantized to 0. The discrete cosine transform (DCT) helps separate the image into spectral sub-bands of differing importance (with respect to the image's visual quality). For most images, after transformation the majority of signal energy is carried by just a few of the low order DCT coefficients. These coefficients can be more finely quantized than the higher order coefficients. Many higher order coefficients may be quantized to 0 (this allows for very efficient run-level coding). Figure 3.1(a) illustrates the arrangement of coefficients in the DCT used in the digital watermarking system and Figure.

3.1(b) illustrates the reordering of DCT coefficients in the DCT used in the digital watermarking system

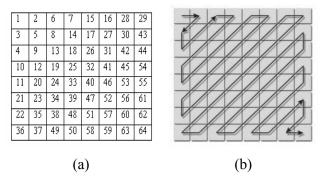


Figure 3.1: (a) Arrangement of DCT coefficients

(b) Reordering of DCT coefficients

3.1.2 The One and Two-Dimensional DCT

The one-dimensional DCT is useful in processing one-dimensional signals such as speech waveforms. For analysis of two-dimensional (2D) signals such as images, we need a 2D version of the DCT. For an N x N matrix, the 2D DCT is computed in a simple way: The 1D DCT is applied to each row and then to each column of the result. Thus, the transform is given by following equation

DCT Encoding

The equation (1) shows the equation for discrete cosine transform

$$F(u,v) = \frac{2}{N}C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right]$$
(1)

DCT Decoding

The equation (2) shows the equation for inverse discrete cosine transform

$$f(i,j) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C(u)C(v)F(u,v) \cos\left[\frac{(2x+1)u\pi}{2N}\right] \cos\left[\frac{(2y+1)v\pi}{2N}\right]$$
 (2)

In the formulas, F(u,v) is the two-dimensional NxN DCT.

$$u,v,x,y = 0,1,2,...N-1$$

x,y are spatial coordinates in the sample domain.

u,v are frequency coordinates in the transform domain.

$$C(u)$$
, $C(v) = 1/(square root(2))$ for $u, v = 0$.

C(u), C(v) = 1 otherwise.

The basic operation of the DCT is as follows:

- The input image is N x N;
- f(i,j) is the intensity of the pixel in row i and column j;
- F(u,v) is the DCT coefficient in row k1 and column k2 of the DCT matrix.
- For most images, much of the signal energy lies at low frequencies; these appear in the upper left corner of the DCT.
- Compression is achieved since the lower right values represent higher frequencies, and are often small small enough to be neglected with little visible distortion.

Since the 2D DCT can be computed by applying 1D transforms separately to the rows and columns, we say that the 2D DCT is *separable* in the two dimensions. Although the direct application of this formula would require $O(N^2)$ operations, it is possible to compute the same thing with only $O(N \log N)$ complexity by factorizing the computation similar to the fast Fourier transform (FFT). One can also compute DCTs via FFTs combined with O(N) pre- and post-processing steps. The output array of DCT coefficients contains integers; these can range from -1024 to 1023. Figure 3.2 shows the block diagram of 2D-DCT transform

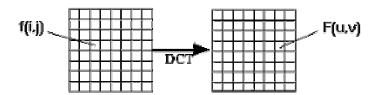


Figure 3.2: Block diagram of 2D-DCT transform

The 2-D basis functions can be generated by multiplying the horizontally oriented 1-D basis functions (shown in Figure 3.3) with vertically oriented set of the same functions. The basis functions for N = 8 are shown in figure 3.3. Again, it can be noted that the basis functions exhibit a progressive increase in frequency both in the vertical and horizontal direction.

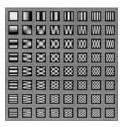


Figure 3.3: Two dimensional DCT basis functions (N = 8). Neutral gray represents zero, white represents positive amplitudes, and black represent negative amplitude

3.1.3 Comparison to DFT

The DCT is conceptually similar to the DFT, except:

- The DCT does a better job of concentrating energy into lower order coefficients than does the DFT for image data.
- The DCT is purely real, the DFT is complex (magnitude and phase). The DCT is purely real, the DFT is complex (magnitude and phase).
- A DCT operation on a block of pixels produces coefficients that are similar to the frequency domain coefficients produced by a DFT operation. An N-point DCT has the same frequency resolution as and is closely related to a 2N-point DFT. The N frequencies of a 2N point DFT correspond to N points on the upper half of the unit circle in the complex frequency plane.
- Assuming a periodic input, the magnitude of the DFT coefficients is spatially invariant (phase of the input does not matter). This is not true for the DCT.

For both transforms, there is the magnitude of the spectrum on left and the histogram on right; both spectra are cropped to 1/4, to zoom the behaviour in the lower frequencies. The DCT concentrates most of the power on the lower frequencies.

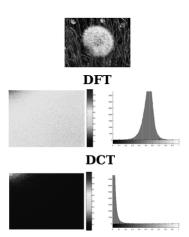


Figure 3.4: 2-D DCT compared to the DFT

Figure 3.4 shows the Histogram of 2-D DCT (Discrete Cosine transform) and DFT (Discrete cosine transform) and their comparison.

3.2 Discrete Wavelet Transform (DWT)

In the following subsections, the details about DWT and its comparison to DFT is described.

3.2.1 What is DWT?

The word *wavelet* is due to Morlet and Grossman in the early 1980s. They used the French word *ondelette* - meaning "small wave". A little later it was transformed into English by translating "onde" into "wave" - giving wavelet. Wavelets are mathematical functions that divide data into different frequency components and then study each component with a resolution matched to its scale. Each transformation of wavelets involves correlating the wavelet with the given signal (derived from image), where the coefficient values depend on how closely correlated the wavelet is with the given part of the signal. The wavelet is stretched after the entire signal is covered and the process is executed in this fashion repeatedly for all scales. The arrangement of the coefficients in the wavelet transform is shown in figure 3.5.

1	2	5	6	17	18	21	22
3	4	7	8	19	20	23	24
9	10	13	14	25	26	29	30
11	12	15	16	27	28	31	32
33	34	37	38	49	50	53	54
35	36	39	40	51	52	55	56
41	42	45	46	57	58	61	62
43	44	47	48	59	60	63	64

Figure 3.5: Arrangement of DWT coefficients

3.2.2 Details about DWT

In mathematics, wavelets, wavelet analysis, and the wavelet transform refers to the representation of a signal in terms of a finite length or fast decaying oscillating waveform (known as the mother wavelet). This waveform is scaled and translated to match the input signal. In formal terms, this representation is a wavelet series, which is the coordinate representation of a square integrable function with respect to a complete, orthonormal set of basis functions for the Hilbert space of square integrable functions. Note that the wavelets in the JPEG2000 standard are biorthogonal wavelets, that is, the coordinates in the wavelet series are computed with a different, dual set of basis functions. There are a large number of wavelet transforms each suitable for different applications. The common ones are Continuous wavelet transform (CWT), Discrete wavelet transform (DWT), Fast wavelet transform (FWT), Wavelet packet decomposition (WPD), Stationary wavelet transform (SWT).

The principal difference between continuous and discrete wavelet transform is that the continuous transform operates over every possible scale and translation whereas the discrete uses a specific subset of all scale and translation values. Wavelet theory is applicable to several other subjects. All wavelet transforms may be considered to be forms of time-frequency representation and are, therefore, related to the subject of harmonic analysis. Almost all

practically useful *discrete wavelet transforms* make use of filterbanks containing finite impulse response filters. The wavelets forming a CWT are subject to Heisenberg's uncertainty principle and, equivalently, discrete wavelet bases may be considered in the context of other forms of the uncertainty principle.

There are a number of ways of defining a wavelet (or a wavelet family). Scaling filter: The wavelet is entirely defined by the scaling filter g - a low-pass finite impulse response (FIR) filter of length 2N and sum 1. In biorthogonal wavelets, separate decomposition and reconstruction filters are defined. For analysis the high pass filter is calculated as the QMF of the low pass, and reconstruction filters the time reverse of the decomposition. Daubechies and Symlet wavelets can be defined by the scaling filter. Scaling function: Wavelets are defined by the wavelet function $\psi(t)$ (i.e. the mother wavelet) and scaling function $\phi(t)$ (also called father wavelet) in the time domain. The wavelet function is in effect a band-pass filter and scaling it for each level halves its bandwidth. This creates the problem that in order to cover the entire spectrum an infinite number of levels would be required. The scaling function filters the lowest level of the transform and ensures all the spectrum is covered. See [7] for a detailed explanation. For a wavelet with compact support, $\phi(t)$ can be considered finite in length and is equivalent to the scaling filter g. Meyer wavelets can be defined by scaling functions.

3.2.3 Comparison to DFT

The wavelet transform is often compared with the Fourier transform, in which signals are represented as a sum of sinusoids. The main difference is that wavelets are localized in both time and frequency whereas the standard Fourier transform is only localized in frequency. The Short-time Fourier transform (STFT) is also time and frequency localized but there are issues with the frequency time resolution and wavelets often give a better signal representation using Multiresolution analysis. The discrete wavelet transform is also less computationally complex, taking O(N) time as compared to $O(N \log N)$ for the fast Fourier transform (N is the data size).

3.3 Conclusion

In this chapter, we have discussed details about two methods: Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) that are of concerned in our thesis. In the next two chapters, how Discrete Cosine Transform and Discrete Wavelet Transform used in our proposed digital image watermarking techniques are described elaborately.

Chapter IV

An Efficient Digital Image Watermarking Technique Based on Discrete Cosine Transform

This chapter describes our proposed digital image watermarking technique based on discrete cosine transform (DCT). In the last section of this chapter the performance of this technique on several attacks is shown and described elaborately.

4.1 Introduction to the Technique

The desired watermark signal that we want to embed is generated as follows:

- 1) If w = watermark signal of size $M1 \times N1$
 - K_I = secret key generated by the owner
 - Then, secret watermark $w' = f(w, k_l)$
 - Where, w' is also of size of $MI \times NI$ and f is a function that converts watermark signal w to a secret form w' applying secret key k_I .
- 2) The secret watermark is then represented in binary form as $w' = w_{11}', w_{12}', ..., w_{M_1N_1}'$, where $w'_{ij} \in \{0, 1\}$, of $M_I \times N_I$ watermark signal. Here the value 0 represents black and 1 represents white color.
- 3) For higher secrecy and computational purpose, the binary form of the message w' is then transformed to obtain $w = w_{11}, w_{12}, ..., w_{M_1N_1}$, with $w_{ij} \in \{1, -1\}$. Where each -1 value is obtained from value 1 of binary watermark and 1 value is obtained from value 0 of binary watermark

The Complexity Computation for Secret Watermark Generation is described in the following: Let, the size of the watermark signal (w) is $M_I \times N_I$ and the secret key is of X decimal digits. In our method, finally the watermark signal becomes binary watermark of value $w_{ij} \in \{1, -1\}$ for i =1, 2, ..., M_I and j = 1, 2, ..., N_I . Here, the binary value 1 is obtained for those pixels of the image whose gray level value is less than a threshold T_h and the value -1 is obtained for those pixels of the image whose gray level value is greater than that threshold. In case of image of size $M_I \times N_I$, the complexity combination of fixing these two values (1 and -1)

$$= 2^{MI \times NI}$$

Now, if the key is of X decimal digits, then the complexity for finding the desired secret key $= 10^{X}$

So, total computational steps before binary watermark generation

$$=2^{MI\times NI}\times 10^{X}$$
 (a)

Now, the complexity computation for binary watermark generation with algorithm is shown in the following table.

Step	Algorithm	Complexity
1	for $i = 1$ to M_1 do	M_1+1
	for $j=1$ to N_I do	$M_1(N_1+1) = M_1 N_1 +$
	$w' = f(w, K_1)$	M_1
	$w_{ij} = f(w_{ij}, K_l)$	$M_1 N_1$
2	Input threshold T _h	1
	for $i = 1$ to M_1 do	M_1+1
	for $j=1$ to N_I do	$M_1(N_1+1) = M_1 N_1 +$
	if $w_{ij} > T_h$ then $w_{ij} = 1$	M_1
	else $w'_{ij} = 0$	$2M_1 N_1$
3	for $i = 1$ to M_1 do	M_1+1
	for $j=1$ to N_1 do	$M_1(N_1+1) = M_1 N_1 +$
	<i>if</i> $w'_{ij} = 1$ then $w'_{ij} = -1$	M_1
	else $w_{ij} = 1$	2M ₁ N ₁

 $Total = 4 + 6M_1 + 8M_1N_1$

(b)

So the complexity for the binary watermark generation = $O(M_1N_1)$

So, from (a) and (b) the total complexity for secret watermark generation

$$= 2^{MI \times NI} \times 10^{X} + O(M_1N_1)$$

For Example, if the watermark signal is of size 6 x 6 and the key is of 6 decimal digits then the total complexity for secret watermark generation,

$$= 2^{6 \times 6} \times 10^6 + O(36) = 6.87 \times 10^{16}$$

If each computation takes 1 nanosecond then the total time required

=
$$(6.87 \times 10^{16}) / (10^9 \times 3600 \times 24 \times 365) = 2.18 \text{ years}$$

So both of the secret watermark and the secret key may be determine by random computation but the time required is too large.

The proposed scheme is an image-quality guaranteed watermarking scheme as well as the conventional schemes. In our proposed technique, any extra processing such as visual masking for watermark casting and the original image or image size watermark for watermark detection

is not required whereas the existing methods require any or more of these. The amount of watermark added is adapted to the image so that less amount of watermark is added to a smooth image (e.g., *Lena*) and more to a non-smooth image (e.g., *baboon*). The human eye is fairly good at seeing small differences in brightness over a relatively large area, but not so good at distinguishing the exact strength of a high frequency brightness variation. This fact allows one to get away with greatly reducing the amount of information in the high frequency components. This is done by simply dividing each component in the frequency domain by a constant for that component, and then rounding to the nearest integer. This is the main lossy operation in the whole process. As a result of this, it is typically the case that many of the higher frequency components are rounded to zero, and many of the rest become small positive or negative numbers. That is, the human visual system is least sensitive to the range of high frequency [15]. In case of RGB color image, the blue channel has characteristic of the highest frequency range.

In out proposed method, we use the formula (1) and (2) given in chapter 2. In the formulas, F(u, v) is the two-dimensional $N \times N$ DCT; $u, v, x, y = 0, 1, 2 \dots N-1$; x, y are spatial coordinates in the sample domain; u, v are frequency coordinates in the transform domain and

$$C(u), C(v) = \frac{1}{\sqrt{2}}$$
 for $u, v = 0$;

= 1 otherwise.

f(x, y) is a two dimensional function defining an image, where x and y are spatial (plane) coordinates and f is the amplitude of that image at any pair of coordinates (x, y) which is called the intensity or gray level of the image at that point. After DCT encoding of the image f(x, y) we get a two dimensional DCT matrix F(u, v) which is used in the process of DCT decoding to get the image f(x, y) again.

The equation used for the embedding process is as follows [8] [13]:

$$\dot{F}_{i,j} = F_{i,j} + K |F_{i,j}|_{W_{i,j}} \tag{3}$$

Where i and j runs over all selected coefficients in the DCT domain and $F_{i,j}$ and $F_{i,j}$ denote the DCT coefficient of the blue channel of the watermarked image and the original image respectively, $w_{i,j}$ is the watermark signal in encoded form and K is the scaling parameter whose value is determined in section 4.3. In the case of multiple watermarking, the equation (3) can be repeated as

$$F_{i,j} = F_{i,j} + K[F_{i,j}] w_{i,j}$$
 3(a₁)

$$F_{i,j}^{"} = F_{i,j}^{"} + K |F_{i,j}^{"}| W_{i,j}^{"}$$
3(a₂)

$$F_{i,j}^{n} = F_{i,j}^{n-1} + K |F_{i,j}^{n-1}| \mathcal{W}_{i,j}^{n-1}$$
3(a_n)

Where the equations $3(a_1)$, $3(a_2)$ and $3(a_n)$ denote the watermarking in two times, three times and n times respectively. Exhaustive experiment is required to know the value of n of multiple watermarking.

In the detection process, we require a watermarked image $(N \times N)$ and watermark signal $(M_I \times N)$ N_l , $N_l \le N$, $M_l \le N$ and the detector detect whether the watermark signal is present or not in the watermarked image. At first apply DCT transform on the blue channel of the given watermarked image and determine the coefficients $F'_{i,j}$ (i, j = 1, 2 ... N). Now select $M_I \times N_I$ coefficients from the high frequency part and compute the average T as shown in (4), which we consider as a threshold.

$$T = \frac{1}{M_{i}N_{i}} \sum_{i=1}^{N} \sum_{j=1}^{N} |\vec{F}_{i,j}|$$
 (4)

Now determine the correlation C_0 (as shown in (5)) between the selected DCT coefficients $F_{i,j}$ and the provided watermark $w_{i,j}$ and compare C_0 with T.

$$C_0 = \frac{1}{M_1 N_1} \sum_{i=N-M}^{N} \sum_{j=N-N}^{N} F_{i,j}^{i} W_{i,j}$$
 (5)

If the provided watermark signal and the embedded watermark signal are similar then the value of the correlation is larger than the threshold value otherwise not, i.e. if $C_0 > T$ then we can say that the provided watermark is detected. As $F_{i,j}$ may be negative and $w_{i,j}$ has values -1 or 1, so T always greater than C_0 . As a result a scaling parameter α is required, where $\alpha = \frac{K}{2}$. The detail about K is described in section 4.3. So the adjusted threshold is as (6)

$$T = \frac{\alpha}{M_1 N_1} \sum_{i=N-M_1}^{N} \sum_{j=N-N_1}^{N} F_{i,j}^{i}$$
 (6)

4.2 Proposed DCT Based Technique

In the proposed technique DCT is considered as two frequency band (low and high as Figure 4.1). In the proposed technique for high performance the blue channel is transformed into DCT domain and watermark is embedded only from the high frequency band to the low frequency band of the blue channel of the host image. So the greater invisibility of the watermark in the watermarked image is achieved.

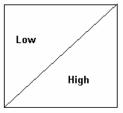


Figure 4.1: After taking DCT frequency distribution in the proposed method

4.2.1 Watermark Embedding Process

Before embedding, the watermark signal is first encoded as described before. The proposed embedding method is shown in fig.4.2.

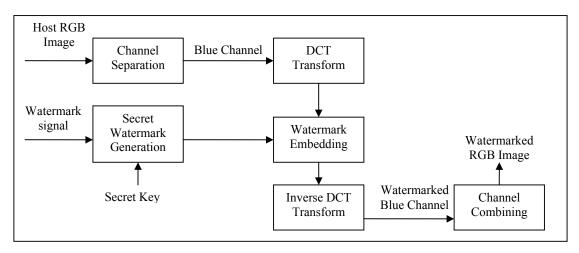


Figure 4.2: Block diagram of watermark embedding process

From the block diagram we see that, the three channels of RGB image are separated in channel separating stage and then only the blue channel is chosen to transform into DCT domain. However in case of grayscale image, it is transformed directly into DCT domain. Then the watermark is embedded from high frequency band to the low frequency band of that DCT domain and then it is transformed into inverse DCT domain. At this stage, for grayscale image we get the watermarked image but for RGB image we get the watermarked blue channel which is then combined to other two channels in channel combining stage to obtain the watermarked image.

4.2.2 Watermark Detecting Process

The proposed detection process is shown in figure 4.3.

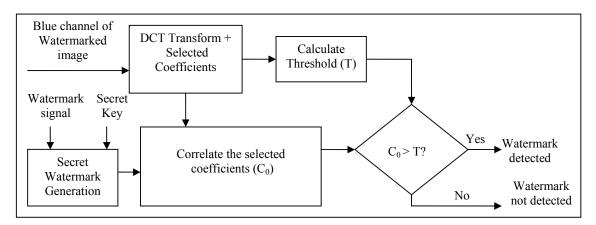


Figure 4.3: Block diagram of watermark detecting process

From the block diagram we see that the watermarked image (For RGB image, the blue channel of watermarked image) is first transformed into DCT domain. Then from the selected coefficients, the threshold is calculated. In the mean time, from the selected coefficients and the provided watermark signal the correlation is calculated. The value of threshold and correlation is used to make the decision whether the watermark is detected or not.

4.3 Experimental Results

In this Section, we illustrate and evaluate the performance of the proposed technique against rotation, scaling, cropping, JPEG compression and other attacks. Our proposed technique can be applied to both RGB and grayscale image. Here we present the experimental results using the standard image "Lena" (128 ×128 pixels, RGB) shown in Figure 4.4(b).

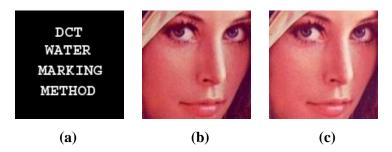


Figure 4.4: (a) Sample watermark signal (b) Host image (c) watermarked image

Figure 4.4(a) shows a sample watermark signal (128×128 pixels, Black and White) and Figure 4.4(c) shows the corresponding watermarked image after embedding.

4.3.1 Determining the Scaling Parameter *K*

In the proposed method the scaling parameter (K) is an important factor. The larger the value of K the more the image quality is degraded. But small value of K degrades the detector response. So the value of K must be in a reasonable range for successful watermark detection. Table 4.1 shows the *Mean of luminance*, *Std. Deviation of luminance*, *Median of luminance* of original *Lena* image and the watermarked image for different values of K. Luminance is a measure of the amount of energy an observer perceives from a light source. High luminance can be detected to alteration by the human eyes less than at the lower luminance pixel. From the Table 4.1 we see that, the value for K = 0.2, the image quality remains in the acceptable range. For this reason for various experiments we use this value of K.

Table 4.1: Characteristics of original Lena and the watermarked image for different values of K

	Original Lena	K=0.2	K=0.4	K=0.8
Mean of luminance	133.61	133.39	133.81	143.95
Std. Deviation of luminance	43.04	43.02	42.47	41.89
Median of luminance	137	140	136	147

4.3.2 Scaling

We scaled the watermarked image (Figure 4.4(c)) by using the scales listed in the column Scale of Table 4.2. From the table we see that the method performs well under scaling.

Table 4.2: Scaling

Scale	Threshold	Correlation
0.4	0.4688	0.4312
0.5	0.4697	0.6110
0.7	0.4700	0.8312
0.8	0.4709	0.9065
1	0.4713	0.9494
1.5	0.4810	0.9591
1.8	0.5132	0.9761
2	0.5610	0.9912

When the scaling is greater than 0.4, the correlation is always greater than the threshold. However we note that the detection becomes inaccurate when the scale changes is less than 0.5 whereas in [6] becomes inaccurate when the scale changes is 0.5 or less. So our proposed method shows a good performance in the case of scaling.

4.3.3 JPEG Compression

We compressed the watermarked image (Figure 4.4(c)) by different compression ratio, the test results are shown in Table 4.3. From the table we see that the method performs well against JPEG up to compression ratio 40%, i.e. in these cases, the correlation is always greater than threshold value. These performances are better than the method of [6]. After this level of compression most of the high frequency band is ignored, since the watermark is embedded from high frequency band to low frequency band of the DCT domain, so the watermark is more difficult to detect.

Table 4.3: JPEG Compression

Compression ratio	Threshold	Correlation
No Compression	0.4713	0.9494
10%	0.4915	0.9242
25%	0.5110	0.9007
30%	0.5321	0.8599
40%	0.6731	0.8110
50%	0.7120	0.7001

4.3.4 Cropping

We cropped the watermarked image (Figure 4.4(c)) by different range listed in the column Crop of Table 4.4. When the image is cropped by 64×64 the correlation value is less than threshold value, so the watermark cannot be detected because in this case most of the image part are lost. But if the cropping is in a reasonable range like 80×80 or more for 128×128 watermarked image, few of the image part is lost, so it can be detected by our proposed method. Our DCT based method shows narrow result than in [6].

Table 4.4: Cropping

Crop	Threshold	Correlation
128 x 128	0.4713	0.9494
120 x 120	0.5821	0.9043
100 x 100	0.6910	0.8627
80 x 80	0.7125	0.8390
64 x 64	0.9150	0.8121

4.3.5 Rotation

Rotation invariance is very useful because the digital copies coming from printing and rescanning may be rotated in comparison to the initial image. We rotated the watermarked image (Figure 4.4(c)) counter-clock wise by different angles listed in the column *Angle* of Table 4.5. The four corners of the watermarked image have been cropped, due to the rotation. From the table we see that the method performs well when the rotated angle is less than 20^{0} , in these cases the correlation is always greater than the threshold value. However, it becomes inaccurate when the rotated angle is greater than or equal to 20^{0} . This is due to the fact that when rotational degree becomes bigger, larger areas are cropped and more information is lost. However, especially in this case in [6] shows better result than our methods.

Table 4.5: Rotation

Angle	Threshold	Correlation
0_0	0.4713	0.9494
1 ⁰	0.4794	0.8121
5^{0}	0.4790	0.7819
10^{0}	0.4810	0.6714
15^{0}	0.4770	0.4815
30^{0}	0.4713	0.3590
360^{0}	0.4713	0.9494
350^{0}	0.4810	0.6714
340^{0}	0.4780	0.4110

4.3.6 Performance on Random Watermark Test

We have performed our proposed watermarking system on different watermarks (shown in Figure 4.5(a), here a watermarked image and 1000 watermark signal are used for watermark detection. Here one watermark signal is the same as the embedded watermark signal among the 1000 signals. In the figure 4.5(a), the X-axis represents 1000 randomly generated watermark signal with the embedded signal and the Y-axis shows the corresponding detector results. From

Figure 4.5(a) we see that only watermark number 400 crosses the predetermine threshold value, which was the actual watermark that was embedded.

4.3.7 Performance on Multiple Watermarks

Some applications require that more than one watermark is inserted in the image. To test the performance of our proposed technique, the original image was watermarked with two different watermarks. Figure 4.5(b) shows the detector response, which indicates the presence of all the two watermarks embedded in the image.

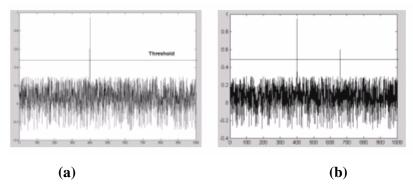


Figure 4.5: Detector response (a) to 1000 randomly generated watermarks. Only watermark number 400 matches that embedding (b) on two different watermarks

4.4 Conclusion

In this chapter, the detail of our proposed technique based on DCT is described. Section 4.3 of this chapter shows the result of this technique for several attacks applied to smooth image "Lena". From the result we see that the method performs well. We have performed the similar experiments discussed above to other test images and we obtained the similar results. Though the DCT based method performs better than existing methods in scaling, compression and Multiple Watermarking but their robustness is not so good. For this reason, we choose DWT based technique which is described in the next chapter. The performance comparison of our DCT based technique with several existing methods is also described in the next chapter.

Chapter V

An Efficient Digital Image Watermarking Technique Based on Discrete Wavelet Transform

This chapter describes our proposed digital image watermarking technique based on discrete wavelet transform (DWT). Section 5.3 of this chapter shows the performance of this technique for several attacks applied to smooth image "Lena" and also shows the performance comparison of our proposed DCT and DWT based techniques to several other techniques elaborately.

5.1 Introduction

The introduction to this technique is similar to section 4.1 of chapter 4 but the term DWT will be applied instead of DCT.

5.2 Proposed DWT Based Technique

In the proposed technique for high performance the blue channel is transformed into DWT domain and a watermark is embedded only from the high frequency band to the low frequency band of the blue channel of the host image. So the greater invisibility of the watermark in the watermarked image is achieved.

5.2.1 Watermark Embedding Process

Before embedding, the watermark signal is first generated by pseudo random bit generator as described before. The proposed embedding method is shown in figure 5.1. From the block diagram we see that, the three channels of RGB image are separated in channel separating stage and then only the blue channel is chosen to transform into DWT domain. However in case of grayscale image, it is transformed directly into DWT domain. Then the watermark is embedded from high frequency band to the low frequency band of that DWT domain and then it is transformed into inverse DWT domain. At this stage, for grayscale image we get the watermarked image but for RGB image we get the watermarked blue channel which is then combined to other two channels in channel combining stage to obtain the watermarked image.

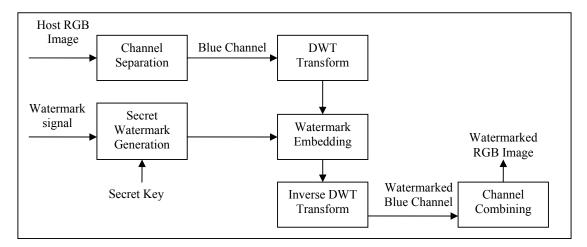


Figure 5.1: Block diagram of watermark embedding process

5.2.2 Watermark Detecting Process

The proposed detection process is shown in figure 5.2. From the block diagram we see that the watermarked image (For RGB image, the blue channel of watermarked image) is first transformed into DWT domain. Then from the selected coefficients, the threshold is calculated. In the mean time, from the selected coefficients and the provided watermark signal the correlation is calculated. The value of threshold and correlation is used to make the decision whether the watermark is detected or not.

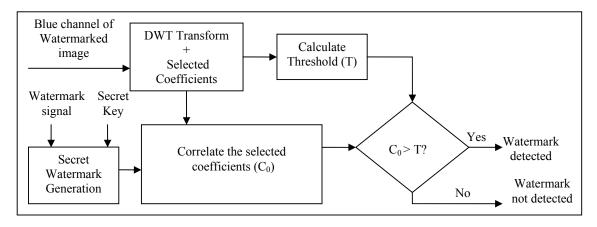


Figure 5.2: Block diagram of watermark detection process

5.3 Experimental Results

In this Section, we illustrate and evaluate the performance of the proposed technique against rotation, scaling, cropping, JPEG compression and other attacks. Our proposed technique can

be applied to both RGB and grayscale image. Here we present the experimental results using the standard image "Lena" (128×128 pixels, RGB) shown in Figure 4.4(b) of chapter 4, where figure 4.4(a) shows a sample watermark signal (128×128 pixels, Black and White) and Figure 4.4(c) shows the corresponding watermarked image after embedding.

5.3.1 Determining the Scaling Parameter *K*

In the proposed method the scaling parameter (K) is an important factor. The larger the value of K the more the image quality is degraded. But small value of K degrades the detector response. So the value of K must be in a reasonable range for successful watermark detection. Table 5.1 shows the *Mean of luminance*, *Std. Deviation of luminance*, *Median of luminance* of original *Lena* image and the watermarked image for different values of K. Luminance is a measure of the amount of energy an observer perceives from a light source. High luminance can be detected to alteration by the human eyes less than at the lower luminance pixel. From the Table 5.1 we see that, the value for K = 0.1, the image quality remains in the acceptable range. For this reason for various experiments we use this value of K.

Table 5.1: Characteristics of original Lena and the watermarked image for different values of K

	Original Lena	K=0.1	K=0.2	K=0.4
Mean of luminance	133.6	133.39	133.81	143.9
Std. Deviation of luminance	43.04	43.02	42.47	41.89
Median of luminance	137	137	136	147

5.3.2 Scaling

We scaled the watermarked image (Figure 4.4(c)) by using the scales listed in the column *Scale* of Table 5.2. From the table 5.2, we see that the detection becomes inaccurate when the scale change(s) is less than 0.5 in our DCT based technique and is less than 0.4 in our DWT based technique, whereas in [6] becomes inaccurate when the scale change(s) is 0.5 or less. So our proposed method shows a better performance in the case of scaling.

Table 5.2: Scaling Attack Detected by (a) proposed DWT method (b) the Method [6] and our proposed Methods

Scale	Threshold	Correlation
0.4	0.201	0.354
0.5	0.232	0.412
1	0.270	0.417
1.5	0.288	0.431
1.8	0.351	0.441
2	0.462	0.469

	Is Detected by							
Scale	[6]	Proposed	Proposed DWT					
Scare		DCT Method	Method					
0.4	No	No	Yes					
0.5	No	Yes	Yes					
1	Yes	Yes	Yes					
1.5	Yes	Yes	Yes					
1.8	Yes	Yes	Yes					
2	Yes	Yes	Yes					
	·		·					

(b)

5.3.3 JPEG Compression

(a)

We compressed the watermarked image (Figure 4.4(c)) by different compression ratio, the test results are shown in Table 5.3. From the table 5.3 we see that our DCT based method performs well against JPEG up to compression ratio 40% and our DWT based method performs well against JPEG compression ratio up to 50%. Both of these performances are better than the method of [6]) but show narrow result in the case of JPEG Compression than in [3] (Up to 95%).

Table 5.3: JPEG compression Attack Detected by (a) proposed DWT method (b) the Method [6] and our proposed Methods

Compression	Threshold	Correlation
ratio		
0%	0.270	0.417
25%	0.321	0.419
30%	0.361	0.425
40%	0.405	0.433
50%	0.401	0.432
60%	0.309	0.301

		Is Detected by							
	JPEG	[6]	Proposed	Proposed DWT					
	Compression		DCT Method	Method					
	25%	Yes	Yes	Yes					
	30%	Yes	Yes	Yes					
	40%	No	Yes	Yes					
	50%	No	No	Yes					
ĺ	60%	No	No	No					

(a) (b)

5.3.4 Cropping

We cropped the watermarked image (Figure 4.4(c)) by different range listed in the column *Crop* of Table 5.4. From the table 5.4 we see that, if the cropping is in a reasonable range like 80×80 or more for DCT and 64×64 for DWT of a 128×128 watermarked image, few of the

image part are lost, so it can be detected by our proposed method. So we see that our DCT based method shows narrow result but our DWT based method shows better result than [3],[6].

Table 5.4: Cropping Attack Detected by (a) proposed DWT method (b) the Method [6] and our proposed Methods

					Is Detected	by
		T	Crop	[6]	Proposed	Proposed DWT
Crop	Threshold	Correlation			DCT Method	Method
128 x 128	0.270	0.417	128 x	Yes	Yes	Yes
120 x 120	0.321	0.419	120 x	Yes	Yes	Yes
100 x 100	0.361	0.425	100 x	Yes	Yes	Yes
80 x 80	0.405	0.433	80 x	Yes	Yes	Yes
64 x 64	0.401	0.432	64 x	Yes	No	Yes
32 x 32	0.309	0.301	32 x	No	No	No
	(a)				(b)	

5.3.5 Rotation

Rotation invariance is very useful because the digital copies coming from printing and rescanning may be rotated in comparison to the initial image. We rotated the watermarked image (Figure 4.4(c)) by different angles listed in the column *Angle* of Table 5.5. From the table 5.5, we see that DCT based method performs well when the rotated angle is up to 15⁰ while it is 30⁰ for DWT based method. Method in [3] can not apply to the rotation attack. However, especially in this case [6] shows better result than our methods.

Table 5.5: Rotation Attack Detected by (a) proposed DWT method (b) the Method [6] and our proposed Methods

			Rotated Is Detected by				
			Angle	[6]	Proposed DCT	Proposed DWT	
Angle	Threshold	Correlation			Method	Method	
15 ⁰	0.441	0.459	15 ⁰	Yes	Yes	Yes	
30^{0}	0.391	0.428	30^{0}	Yes	No	Yes	
45 ⁰	0.382	0.325	45°	Yes	No	No	
315 ⁰	0.382	0.325	315^{0}	Yes	No	No	
330^{0}	0.391	0.428	330^{0}	Yes	No	Yes	
345 ⁰	0.441	0.459	345°	Yes	Yes	Yes	
•	(a)	•			(b)		

But if we crop the watermarked image from the position of significant features after rotation then we get better result than described above. Figure 5.3 and table 5.6 illustrates this.

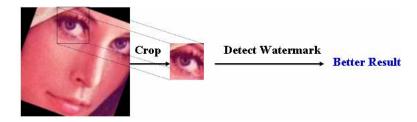


Figure 5.3: Sample cropping after rotation

Table 5.6: Detector response for cropping after rotation attack.

Rotated	Is Detected by							
Angle	[6]	Proposed DCT	Proposed DWT					
		Method	Method					
15 ⁰	Yes	Yes	Yes					
25 ⁰	Yes	Yes	Yes					
30^{0}	Yes	Yes	Yes					
35^{0}	Yes	No	Yes					
45 ⁰	Yes	No	Yes					
50^{0}	No	No	No					
315^{0}	Yes	No	Yes					
325^{0}	Yes	No	Yes					
330^{0}	Yes	Yes	Yes					
335 ⁰	Yes	Yes	Yes					
345 ⁰	Yes	Yes	Yes					

5.3.6 Performance on Random Watermark Test

We have performed our proposed watermarking system on different watermarks (shown in Figure 5.4(a)); here a watermarked image and 1000 watermark signal are used for watermark detection. Here one watermark signal is the same as the embedded watermark signal among the 1000 signals. In the figure 5.4(a), the X-axis represents 1000 randomly generated watermark signal with the embedded signal and the Y-axis shows the corresponding detector results. From Figure 5.4(a) we see that only watermark number 400 crosses the predetermine threshold value, which was the actual watermark that was embedded.

5.3.7 Performance on Multiple Watermarks

Some applications require that more than one watermark is inserted in the image. To test the performance of our proposed technique, the original image was watermarked with two different watermarks. Figure 5.4(b) shows the detector response, which indicates the presence

of all the two watermarks embedded in the image. We have performed the similar experiments discussed above to other test images and we obtained the similar results.

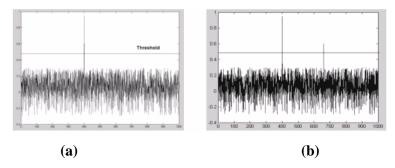


Figure 5.4: Detector response (a) to 1000 randomly generated watermarks. Only watermark number 400 detected (b) on two different watermarks

5.4 Conclusion

In this chapter, the detail of our proposed technique based on DWT is described. Section 5.3 of this chapter shows the result of this technique for several attacks applied to smooth image "Lena". Also, in this chapter the performance comparison of our DCT and DWT based techniques to several existing techniques are described. From the comparison result our DWT based method performs well than existing methods in case of scaling, compression and multiple watermarking. Our DWT based method performs well even than our proposed DCT based method. We have performed the similar experiments discussed above to other test images and we obtained the similar results.

Chapter VI

Concluding Remarks

In this discussion, the Digital image watermarking method based on DCT, and DWT applied to the blue channel of the *RGB* image are described. The main goal of the proposed method is to improve the performance of the digital image watermarking process. To improve the performance of watermarking technique based on DCT, and DWT, a scaling parameter is used which is very important for invisibility and detection of the watermark signal. From the experimental results, we see that the proposed approach shows robust result than some existing methods in scaling, cropping and competitive in JPEG compression.

From the result of proposed method we see for several attacks such as scaling, JPEG compression, Cropping, and multiple watermarking, shows better result when the attack is in a reasonable range. However especially in the case of Rotation, our proposed method shows narrow result in comparison to existing methods.

We give attention to detect the watermarking signal by varying the scaling parameter. But if the scaling parameter is varied a lot, the quality of the watermarked image may be damaged. So the possible value of the scaling parameter will be such that both the image quality is guaranteed and more robustly the watermarking signal is detected for robust attacking.

Bibliography

- [1] S. Ratanasanya and T. Amornraksa, "Digital watermarking using cascading transform," *ISCIT, On Acoustics, Speech and Signal Processing, Munich, Germany, Sapporo, Japan, October, 2004*
- [2] T. Tachibana, M. Fujiyoshi and H. Kiya, "An image-quality guaranteed watermarking scheme with spreading spectrum of watermark," *ISCIT*, Sapporo, Japan, October, 2004.
- [3] Rakesh Dugad, Krishna Ratakonda and Narendra Ahuja, "A New Wavelet-Based Scheme for Watermarking Images", *International Conference on Image Processing*, Chicago, October, 2004.
- [4] D. Zheng and J. Zhao, "RST invariant digital image watermarking: importance of phase information," *IEEE canadian Conference on Electrical and Computer Enginnering (CCECE)*, 2003
- [5] I. Pitas, "A method for signature casting of digital image", in International Conference on Image Processing, pp. 215-218, 2003
- [6] S. Pereira, J.K. Ruanaidh and F. Deguillaume, "Template based recovery of Fourier-based watermarks using log-polar and log-log maps", *IEEE Int. Conf. on Multimedia computing an Systems*, Florence, Italy, June, 1999.
- [7] G. Voyatzis and I. Pitas, "Protecting digital-image copyrights: a framework," *IEEE Comput. Graph. Applicat.*, vol. 19, pp. 18–24, February 1999.
- [8] H. Inoue, A. Miyazaki, A. Yamamoto and T. Katsura, "A digital watermarking based on the wavelet transform and its robustness on image compression and transformation," *IEICE Trans. Fundamentals*, Vol. E82-A, No.1. pp. 1-9, January 1999.
- [9] G. Strang, "The Discrete Cosine Transform," *SIAM Review*, Volume 41, Number 1, pp. 135-147, 1999.
- [10] M. Ramkumar. *Data hiding in multimedia: Theory and applications*. PhD thesis, New Jersey Institute of Technology, 1999.
- [11] I. J. Cox, J. Kilian, F.T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. on Image Processing*, Vol. 6, pp. 1673-1687, December 1997.
- [12] N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures", *Proc. IEEE Con\$ on Acoustics, Speech and Signal Processing*, May 1996, vol. 4, pp. 2168-2171.
- [13] A. Piva, M.Barni, F. Bartolini and V. Cappellini, "DCT-based watermark recovering without restoring to the uncorrupted original image," *International Conference on Image Processing*, vol. III, pp. 520-523, 1997.

- [14] X.-G. Xia, C. G. Boncelet, and G.R. Arce, "A multiresolution watermark for digital images," *in International Conference on Image Processing*, vol. III, pp. 548-551,1997.
- [15] R.C. Gonzalez and R.E. Woods, "Digital image processing," *Wesley*, pp. 21-25, 191-195, 1993.
- [16] F. Lin and R. D. Brandt, "Toward absolute invariants of images under translation, rotation, and dilation," *Pattern Recognit. Lett.*, vol. 14, no. 5, pp. 369–379, 1993.
- [17] Andrew B. Watson. DCT quantization matrices optimized for individual images. *Human Vision, Visual Processing, and Digital Display IV*, SPIE-1913:202–216, 1993.
- [18] N. Ahmed, T. Natarajan and K. R. Rao, "Discrete cosine transform," *IEEE Transactions on Computers*, vol. C-32, pp. 90-93, Jan. 1974.

Appendix A

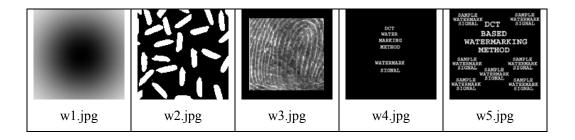
List of the Accepted Papers Related to This Thesis

- [1] S.K. Alamgir Hossain, S.M. Mohidul Islam, Rameswar Debnath, "Improvement of the Performance of DCT Based Digital Image Watermarking Technique", *International conference on computer and information technology (ICCIT)*, Dhaka, Bangladesh, December, 2006.
- [2] S.K. Alamgir Hossain, S.M. Mohidul Islam, Rameswar Debnath, "DWT Based digital Watermarking Technique and its Robustness on Image Rotation, Scaling, JPEG compression, Cropping and Multiple watermarking", *International conference on information and communication technology (ICICT)*, Dhaka, Bangladesh, January, 2007.

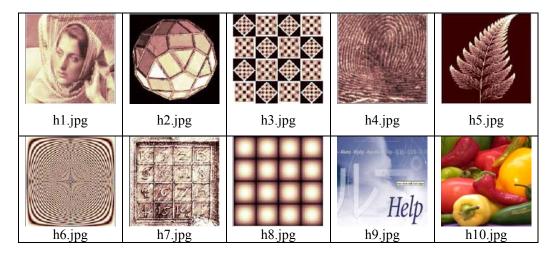
Appendix B

Sample Experimental Results

Sample Watermark Signals



Sample Host or Original Images



Experimental Results for Our DCT Based Method

The Experimental results of our DCT based method for scaling, JPEG Compression, Cropping and Rotation attacks for the above 10 host images are shown below. Here the host images are watermarked by 5 different watermark signals.

Scaling

Image	Watermark		Scaled by						
		0.4	0.5	0.7	0.8	1	1.5	1.8	2
h1.jpg	w1.jpg	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
h2.jpg	w1.jpg	No	No	No	Yes	Yes	Yes	Yes	Yes
h3.jpg	w2.jpg	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
h4.jpg	w2.jpg	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
h5.jpg	w3.jpg	No	No	Yes	Yes	Yes	Yes	Yes	Yes
h6.jpg	w3.jpg	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
h7.jpg	w4.jpg	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
h8.jpg	w4.jpg	No	No	No	No	Yes	Yes	Yes	Yes
h9.jpg	w5.jpg	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
h10.jpg	w5.jpg	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

JPEG Compression

Image	Watermark	JPEG Compression Ratio					
		0%	10%	25%	30%	40%	50%
h1.jpg	w1.jpg	Yes	Yes	Yes	Yes	Yes	No
h2.jpg	w1.jpg	Yes	Yes	Yes	Yes	No	No
h3.jpg	w2.jpg	Yes	Yes	Yes	Yes	No	No
h4.jpg	w2.jpg	Yes	Yes	Yes	Yes	Yes	No
h5.jpg	w3.jpg	Yes	Yes	Yes	No	No	No
h6.jpg	w3.jpg	Yes	Yes	Yes	Yes	No	No
h7.jpg	w4.jpg	Yes	Yes	Yes	Yes	Yes	No
h8.jpg	w4.jpg	Yes	Yes	Yes	Yes	No	No
h9.jpg	w5.jpg	Yes	Yes	Yes	Yes	Yes	No
h10.jpg	w5.jpg	Yes	Yes	Yes	Yes	No	No

Cropping

Image	Watermark	Cropped by								
		128 x 128	120 x 120	100 x 100	80 x 80	64 x 64				
h1.jpg	w1.jpg	Yes	Yes	Yes	Yes	No				
h2.jpg	w1.jpg	Yes	Yes	Yes	Yes	No				
h3.jpg	w2.jpg	Yes	Yes	Yes	Yes	No				
h4.jpg	w2.jpg	Yes	Yes	Yes	Yes	No				
h5.jpg	w3.jpg	Yes	Yes	Yes	Yes	Yes				
h6.jpg	w3.jpg	Yes	Yes	Yes	No	No				
h7.jpg	w4.jpg	Yes	Yes	Yes	Yes	No				
h8.jpg	w4.jpg	Yes	Yes	Yes	Yes	Yes				
h9.jpg	w5.jpg	Yes	Yes	Yes	Yes	No				
h10.jpg	w5.jpg	Yes	Yes	Yes	Yes	No				

Rotation

Image	Watermark	Rotated by								
		0_0	10	5 ⁰	10^{0}	15^{0}	30^{0}	350^{0}	340^{0}	
h1.jpg	w1.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	No	
h2.jpg	w1.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	
h3.jpg	w2.jpg	Yes	Yes	Yes	Yes	No	No	Yes	No	
h4.jpg	w2.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	No	
h5.jpg	w3.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	
h6.jpg	w3.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	No	
h7.jpg	w4.jpg	Yes	Yes	Yes	Yes	No	No	Yes	No	
h8.jpg	w4.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	No	
h9.jpg	w5.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	
h10.jpg	w5.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	

Experimental Results for Our DWT Based Method

The Experimental results of our DCT based method for scaling; JPEG Compression, Cropping and Rotation attacks for the above 10 host images are shown below. Here the host images are watermarked by 5 different watermark signals.

Scaling

Image	Watermark	Scaled by								
		0.4	0.5	0.7	0.8	1	1.5	1.8	2	
h1.jpg	w1.jpg	No	Yes							
h2.jpg	w1.jpg	No	Yes							
h3.jpg	w2.jpg	No	Yes							
h4.jpg	w2.jpg	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
h5.jpg	w3.jpg	No	Yes							
h6.jpg	w3.jpg	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
h7.jpg	w4.jpg	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
h8.jpg	w4.jpg	No	Yes							
h9.jpg	w5.jpg	No	Yes							
h10.jpg	w5.jpg	No	Yes							

JPEG Compression

Image	Watermark	JPEG Compression Ratio								
		0%	10%	25%	30%	40%	50%			
h1.jpg	w1.jpg	Yes	Yes	Yes	Yes	Yes	No			
h2.jpg	w1.jpg	Yes	Yes	Yes	Yes	Yes	No			
h3.jpg	w2.jpg	Yes	Yes	Yes	Yes	Yes	No			
h4.jpg	w2.jpg	Yes	Yes	Yes	Yes	Yes	Yes			
h5.jpg	w3.jpg	Yes	Yes	Yes	Yes	Yes	No			
h6.jpg	w3.jpg	Yes	Yes	Yes	Yes	No	No			
h7.jpg	w4.jpg	Yes	Yes	Yes	Yes	Yes	No			
h8.jpg	w4.jpg	Yes	Yes	Yes	Yes	Yes	No			
h9.jpg	w5.jpg	Yes	Yes	Yes	Yes	Yes	No			
h10.jpg	w5.jpg	Yes	Yes	Yes	Yes	No	No			

Cropping

Image	Watermark	Cropped by									
		128 x 128	120 x 120	100 x 100	80 x 80	64 x 64					
h1.jpg	w1.jpg	Yes	Yes	Yes	Yes	No					
h2.jpg	w1.jpg	Yes	Yes	Yes	Yes	No					
h3.jpg	w2.jpg	Yes	Yes	Yes	Yes	Yes					
h4.jpg	w2.jpg	Yes	Yes	Yes	Yes	No					
h5.jpg	w3.jpg	Yes	Yes	Yes	Yes	Yes					
h6.jpg	w3.jpg	Yes	Yes	Yes	Yes	No					
h7.jpg	w4.jpg	Yes	Yes	Yes	Yes	Yes					
h8.jpg	w4.jpg	Yes	Yes	Yes	Yes	Yes					
h9.jpg	w5.jpg	Yes	Yes	Yes	Yes	Yes					
h10.jpg	w5.jpg	Yes	Yes	Yes	Yes	No					

Rotation

Image	Watermark	Rotated by									
		0_0	1 ⁰	5 ⁰	10^{0}	15 ⁰	30^{0}	350^{0}	340^{0}		
h1.jpg	w1.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	No		
h2.jpg	w1.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes		
h3.jpg	w2.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes		
h4.jpg	w2.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	No		
h5.jpg	w3.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes		
h6.jpg	w3.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes		
h7.jpg	w4.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	No		
h8.jpg	w4.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes		
h9.jpg	w5.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes		
h10.jpg	w5.jpg	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes		