A COMPARISON OF DISCRETE COSINE TRANSFORM AND DISCRETE WAVELET TRANSFORM ALGORITHM IN WATERMARKING AGAINST COMMON ATTACKS

MOHAMED ABDISALAN SAID

A dissertation submitted in partial
fulfillment of the requirement for the award of the
Degree of Master of Computer Science (Information Security)

Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia

FEBRUARY 2015

ABSTRACT

Digital watermarking is a technique to embed additional data to digital images, audios and videos without affecting the quality of the original image. Watermark can be extracted for ownership verification or authentication. Currently, there is no comparison documented done between Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). In this report, the DCT watermarking algorithms and DWT watermarking algorithms were compared based on robustness and imperceptibility criteria. With DCT, the watermark bits were embedded into the mid-band coefficients of the DCT in the cover image where the DWT algorithm was embedded the watermark bits into the horizontal and vertical sub-bands of DWT in the cover image. Experimental results had shown that the watermark is robust to geometric attacks and removal attacks. DCT and DWT are compared with regard to peak signal to noise ratio (PSNR), Mean Square Error (MSE) and Normalized Correlation (NC). The PSNR value of the watermarked Lena image in DWT is 47, higher than the DCT which is 44. The Normalized Correlation (NC) also had clarified that the extracted watermark in DWT 0.9964 is greater than the extracted watermark in DCT 0.2057. Thus, the results had indicated that the DWT gives better image quality than DCT.

ABSTRAK

Tera air digital adalah satu teknik untuk membenamkan data tambahan kepada imej digital, audio dan video tanpa menjejaskan kualiti imej asal. Tera air boleh diekstrak keluar bagi tujuan pengesahan hakmilik atau kesahihan kandungan. Pada masa ini, tiada perbandingan telah dibuat di antara Jelmaan Kosinus Diskret (DCT) dan Jelmaan Gelombang Kecil Diskret (DWT). Dalam kajian ini, algoritma tera air DCT dan algoritma tera air DWT dibandingkan berdasarkan kriteria kelasakan dan kehalusan. Dengan menggunakan DCT, bit tera air dibenam ke dalam pekali pertengahan band pada imej asal. Manakala bagi algoritma DWT pula, bit tera air terbenam pada kedudukan sub-band mendatar dan menegak pada imej asal. Hasil kajian mendapati tera air adalah lasak dalam menghadapi serangan geometri dan serangan penyingkiran. DCT dan DWT dibandingkan dengan mengambil kira Nisbah Isyarat Puncak kepada Hingar (PSNR), Min Ralat Kuasa Dua (MSE) dan Korelasi Ternormal (NC). Nilai PSNR tera air bagi imej Lena dalam DWT adalah 47, lebih tinggi berbanding dengan DCT iaitu pada nilai 44. Korelasi Ternormal (NC) juga telah menjelaskan bahawa tera air yang diekstrak dalam DWT dengan nilai 0.9964 adalah lebih besar daripada tera air yang diekstrak dalam DCT iaitu 0.2057. Oleh itu, keputusan kajian menyarankan bahawa DWT memberikan kualiti imej yang lebih baik berbanding DCT.

CONTENTS

TITLE		**i**
DECLARATION		**ii**
DEDICATION		**iii**
ACKNOWLEDGEMENT		**iv**
ABSTRACT		**v**
CONTENTS		**vii**
LIST OF TABLES		**xi**
LIST OF FIGURES		**xiii**
LIST OF SYMBOLS AND ABBREVIATIONS		**xv**
CHAPTER 1 INTRODUCTION		**1**
1.1	Overview	1
1.2	Problem Statement	3
1.3	Motivation	4
1.4	Objectives	5
1.5	Scope	5
1.6	Significant of Study	5

CHAPTER 2 LITERATURE REVIEW 6

2.1 Introduction 6

2.2. History of Digital Watermarking 6

2.3. Basic Watermarking Principles 9

2.3.1 Peak Signal to Noise Ratio 10

2.3.2 Mean Square Error 11

2.3.3 Normalized Correlation 11

2.4 Classification of Digital Watermarks 12

2.4.1 Host Signals 12

2.4.1.1 Image Watermarking 12

2.4.1.1.1 Image Compression 12

2.4.1.2 Video Watermarking 13

2.2.4.3 Audio Watermarking 13

2.4.2 Human Perceptivity 14

2.4.2.1 Visible Watermarking 14

2.4.2.2 Invisible Watermarking 15

2.4.3 Robustness of Watermarks 15

2.4.3.1 Fragile Watermark 16

2.4.3.2 Semi-Fragile Watermark 16

2.4.3.3 Robust Watermark 17

2.4.4 Division Based Extraction Process 17

2.4.4.1 Non-Blind Watermarks 17

2.4.4.2 Semi-Blind Watermarks 18

2.4.4.3 Blind Watermarks 18

2.4.5 Domain Watermarks 18

2.4.5.1 Spatial Domain 18

2.4.5.2 Frequency Domain 19

2.4.6 Classification by Application 19

2.4.6.1 Copyright Protection 19

2.4.6.2 Data Authentication 20

2.4.6.3 Broadcast Monitoring 20
2.4.6.4 Copy Protection 21
2.4.6.5 Fingerprinting 21
2.5 Techniques of Digital Watermarking 21
2.5.1 Spatial Domain Techniques 22
2.5.2 Frequency Domain Techniques 22
2.5.2.1 Discrete Cosine Transform 23
2.5.2.2 Discrete Wavelet Transform 25
2.6 Watermarking Attacks 26
2.6.1 Salt and Pepper Noise Attack 27
2.6.2 Image Compression Attack 27
2.6.3 Gaussian Noise Attack 28
2.6.4 Speckle Noise Attack 28
2.6.5 Cropping Attack 28
2.6.6 Resizing Attack 29
2.6.7 Image Contrast Attack 29
2.7 Summary 30

CHAPTER 3 METHODOLOGY 31
3.1 Introduction 31
3.2 The Research Framework 31
3.2.1 Discrete Cosine Transform 33
3.2.2 Discrete Wavelet Transform 35
3.3 Summary 39

CHAPTER 4 IMPLEMENTATION 40
4.1 Introduction 40
4.2 Discrete Cosine Transform 40
4.2.1 Discrete Cosine Transform Embedding Algorithm 40
4.2.2 Discrete Cosine Transform Extracting Algorithm 44
4.3 Discrete Wavelet Transform 46
4.3.1 Discrete Wavelet Transform Embedding Algorithm 46

4.3.2 Discrete Wavelet Transform Extracting Algorithm 49
4.4 Performance Evaluation 51
4.5 Summary 52

CHAPTER 5 RESULT AND DISCUSSIONS 53
5.1 Introduction 53
5.2 Discrete Cosine Transform 54
5.2.1 Discrete Cosine Transform Embedded Result 54
5.2.2 Discrete Cosine Transform Extraction Result 55
5.3 Discrete Wavelet Transform 55
5.3.1 Discrete Wavelet Transform Embedded Result 56
5.3.2 Discrete Wavelet Transform Extraction Result 56
5.4 Comparison and Performance Evaluation 57
5.5 Analysis of Test Results for DCT and DWT 60
5.6 Attacks on the Watermarked Image 62
5.6.1 Salt and Pepper Noise Attacks 62
5.6.2 Image Compression Attacks 65
5.6.3 Gaussian Attacks 68
5.6.4 Speckle Attacks 71
5.6.5 Resizing Attacks 74
5.6.6 Cropping Attacks 76
5.6.7 Image Contrast Attack 78
5.7 Summary 81

CHAPTER 6 CONCLUSION AND FUTURE WORK 82
6.1 Conclusion 82
6.2 Contribution 83
6.3 Future Work 84

REFERENCES 85

VITA 88

LIST OF TABLES

2.1	Comparison between watermarking techniques	23
5.1	Cover images for Discrete Cosine Transform	58
5.2	Cover images for Discrete Wavelet Transform	59
5.3	Discrete Cosine Transform watermarked image result	60
5.4	Discrete Wavelet Transform watermarked image result	60
5.5	Comparison of SSIM of the recovered watermark images in DCT and DWT	61
5.6	DCT analysis based the robustness of the Lena against Salt and Pepper attacks	64
5.7	DWT analysis based the robustness of the Lena against Salt and Pepper attacks	64
5.8	Difference between the extracted watermark from the attack watermarked image and original watermark in DCT	65
5.9	Difference between the extracted watermark from the attack watermarked image and original watermark in DWT	65
5.10	DCT analysis based the robustness of the Lena against Compression attacks	67
5.11	DWT analysis based the robustness of the Lena against Compression attacks	67
5.12	Difference between the extracted watermark from the attack watermarked image and original watermark in DCT	68
5.13	Difference between the extracted watermark from the attack watermarked image and original watermark in DWT	68
5.14	DCT analysis based the robustness of the Lena against Gaussian attacks	70
5.15	DWT analysis based the robustness of the Lena against Gaussian attacks	70

LIST OF FIGURES

2.1	Representation of the oldest known watermark	7
2.2	Watermarking embedding process	9
2.3	Watermarking extraction process	10
2.4	NC Formula	11
2.5	Visible watermarked image	14
2.6	Invisible watermarked image	15
2.7	Fragile watermarked images	16
2.8	Elements of an 8 x 8 DCT matrix	24
2.9	Two-level decomposition of image	26
3.1	Research framework	32
3.2	DCT based embedded scheme	34
3.3	DCT based extraction scheme	35
3.4	DWT based embedded scheme	37
3.5	DWT based extraction scheme	38
4.1	DCT based embedded implementation code in Matlab	43
4.2	DCT based extracted implementation code in Matlab	45
4.3	DWT based embedded code in Matlab	48
4.4	DWT based extracted code in Matlab	50
4.5	Matlab code for PSNR and MSE in DCT	51
4.6	Matlab code for PSNR and MSE in DWT	51
5.1	Discrete Cosine Transform embedded result	54
5.2	Discrete Cosine Transform extraction result	55
5.3	Discrete Wavelet Transform embedded result	56
5.4	Discrete Wavelet Transform extraction result	57
5.5	PSNR comparison of watermarked images for DCT and DWT	61
5.6	Lena image of DCT with Salt and Pepper attacks	63

LIST OF SYMBOLS AND ABBREVIATIONS

2D	-	Two Dimensions
BMP	-	Bitmap
DCT	-	Discrete Cosine Transform
DFT	-	Discrete Fourier Transform
DWT	-	Discrete Wavelet Transform
HVS	-	Human Visibility System
IDCT	-	Inverse of Discrete Cosine Transform
IDWT	-	Inverse of Discrete Wavelet Transform
IEEE	-	Institute of Electrical and Electronics Engineers
JPEG	-	Joint Photographic Experts Group
LSB	-	Least Significant Bit
MSE	-	Mean Square Error
NC	-	Normalized Correlation
PSNR	-	Peak Signal to Noise Ratio
QF	-	Quality Factor
SSIM	-	Structural Similarity
UTHM	-	Universiti Tun Hussein Onn Malaysia

CHAPTER 1

INTRODUCTION

1.1 Overview

With the rapid development of the modern multimedia technologies and computer networking, security and legal issues have become the most important aspects. Owners of digital content seek effective techniques on how to protect their digital information from unauthorized access, use, disclosure, modification and destruction. Consequently, the acceptance of new services depends on whether suitable techniques for the protection of the work providers' interests are available (Delaigle and Christophe, 1996). Usually, problems with digital media are related to intellectual property rights and the trustworthiness of the content. Digital media such as text, audio, video and image are susceptible to privacy attack, and they can be copied, edited, modified and widely distributed without any significant loss of quality. However, the risk of illegal copying or unauthorized reproduction of digital documents has increased for many years, especially with respect to their authorship claims (Kim and Sungeon, 2009). Thus, many people have looked for data embedding methods which can be used to identify digital data owners in order to protect copyright (Kim and Sungeon, 2009). As a protected method of intellectual property or copyrights for information security is to embed digital watermark inside the information so that ownership of the information cannot be claimed by third parties. The data embedding and information hiding is known as watermarking, and the media being protected is called as host or cover media.

The watermark has been introduced as a complementary protection of multimedia technology. Watermarking is a pattern of bits inserted into a digital content, including audio, video or image data to protect the copyright of information such as author, rights, etc.) which could be the owner's logo, serial number or control information (Bamatraf, 2012). Recently, many watermarking schemes have been proposed in the area of images and watermarking research has received a very significant attention from many researchers since the early 1990s.

There are three main requirements of digital watermarking; robust, imperceptibility and capacity (Hussein and Mohamed, 2012). Robustness is one of the most important attributes of a digital watermark. The system is considered robust if the watermark is still detectable or recoverable under several kinds of attack on the watermarked host, such as cropping and compression. Imperceptibility is a measure of the quality of the watermarked image. It means that the human visual senses are unable to detect the difference between the watermarked image and the cover image. Capacity refers to the maximum amount of information that can be embedded in the cover image.

According to a digital watermarking classification, watermarking researchers can be divided into different categories based on: host signal, human perceptivity, robustness, necessary data for extraction process, features and by applications (Hussein and Mohamed, 2012).

Watermarking scheme can be implemented either in spatial domain or transform domain. Spatial domain technique is the most straightforward way to hide the information. The data are embedded directly by modifying the pixel values of the original image (Khalid et al., 2013). On the other hand, in transform domain techniques, the original image is to be transformed into the frequency domain by using several transforms like Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). After that, the watermark can be hidden into coefficients.

1.2 Problem Statement

Ownership protection of digital information has become a pressing issue in many organizations and companies in the world wide, many of copyright owners are worried about protecting of an illegal duplication or reproduction of their data or work. Digital watermarking is one of the popular techniques used to protect the contents of an intellectual copyright. If copyright has some problems, anyone can claim the ownership rights of any digital media, such as audio (speech and music), images (photography and graphics), and video (movies), but digital watermark can provide evidence of the ownership authentication and rights of the multimedia objects. Therefore, Digital Watermarking is a technology of embedding watermark with intellectual property rights into images, audios and video files. Watermarks should not be removable and imperceptible by unauthorized persons and should be robust to incidental against intentional and unintentional attacks.

A watermarking scheme can be implemented either in spatial domain or transform domain. Each scheme has its own strength. Spatial domain watermarking produces a very good watermarked image and high capacity watermark, but it is less robust against certain attacks such as compression. However, the frequency domain watermarking outputs a watermarked image that is more robust, but with small capacity (Rao et al., 2012).

In this project, a comparison of DCT and DWT watermarking against common attacks was conducted. It implements two domains with respect of relevant parameters of each. Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Normalized Correlation (NC) are used to compare their performances.

1.3 Motivation

In the last decade, the revolution of usage information hiding techniques in the digital multimedia has received more popularity. These information hiding can be mainly divided into three processes- steganography, cryptography and digital watermark. Usually the properties such as images need more protection, and keeping ownership authentication has become an important issue in this world. Nowadays digital images can be easily copied, distributed and forged by unauthorized criminals. Therefore, organizations and companies are using different watermarked methods to protect their own data from any attack trying to copy or manipulate this information. Digital watermarking is one of the popular approaches used to prevent copying and ownership authentication simultaneously. Many researchers have proposed watermarking techniques in the early 1990s, but mostly they are looking forward to find the best algorithm that can produce a watermarked image with lower distortion and has top performance (Bamatraf, 2012).

Day after day the number of copying images is increasing. The attackers are trying to break the watermark protection methods to see the embedded information. If the attacker can change the contents of an image, it is considers that the watermark method is weak. A powerful watermarked should be difficult to remove the mark without damaging the content of the object.

1.4 Objectives

The goals of this research are:

i. To implement an image watermarks system based on DCT and DWT.

ii. To compare the performances of DCT and DWT against common attacks using the standard datasets and measurements, including Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Normalized Correlation (NC).

1.5 Scope

The scope of this research is limited to a comparison of DCT and DWT based on image watermarking. In this research, a Matlab environment tool is used to implement the performance of our system or work. Likewise, the host images used in this research are bmp format, but the output images that have been watermarked are saved as JPG format.

1.6 Significance of the Study

This research concentrates on the comparison of DCT and DWT techniques on image watermarking. The watermark should be robust and able to protect the copyright of image owners. The signal of watermark should be stored in the cover images without affecting the quality of the image and able to extract that watermark from the original images at the same time.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

In this section of the study, all the related items in the review of digital watermarks used for pictures are discussed. It describes in detail how previous research works have been conducted by other researchers using different techniques.

2.2 History of Digital Watermarking

The usage of watermark in the art of handmade papermaking appeared nearly 700 years ago. The earliest watermark was produced in Europe, specifically a town called Fabriano in Italy and considered as the birthplace of watermarking (Hartung and Kutter, 1999).

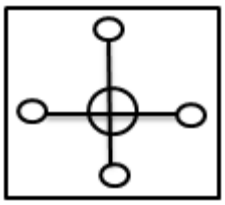

Figure 2.1: Representation of the oldest known watermark (Smith, 2003)

The history of watermark shows the existence of many various names in many languages. For instance, the Dutch called watermark as the 'Papermarken', from which the name paper mark comes. Similarly, the French used another name for watermark named 'Filigrane', which basically refers to the shape of the bent wire. On the other hand, in the beginning of the eighteenth century, the English started to use the name watermark, while the Germans began to use the word 'Wasserzeichen', which was their version of the English word. To the present day, some paper makers still use the name paper mark, for the shaped piece of wire, while the image left by it in the paper has become known as the watermark (Smith, 2003).

During the end of the thirteenth century, around 40 paper mills shared in Fabriano and produced paper with different shape, quality and price. They produced raw, rough paper which was smooth and post processed by artisans and sold by traders ((Hartung and Kutter, 1999).

A lawyer named Bartola de Sassoferrato was the first man who used the terminology. In his papers dating between 1340 and 1350, he proposed that a papermaker could be prohibited from using the mark of different papermakers (Smith, 2003). At first, they utilized watermark to differentiate the product of individual papermakers within each single paper mill since there was no other way to do so. This would support them to solve disputes in the event that one papermaker would accuse another of theft. Throughout the date of watermarks, the most common watermarks were those devised by paper makers to indicate their own product. These marks, known as counter marks, were commonly small and easy designs, in many cases simply the paper maker's initials, placed in an area of the paper reverse in the actual watermark design. There were many different countries which didn’t have papermaking guilds.

Therefore, they began to import much desired watermarked paper from other countries like Italy. History also shows that there was a wealth of Greek manuscript dated back to the thirteenth century written on watermarked paper imported from Italy.

Smith, on the other hand, mentioned that the art and craft of papermaking started from the Middle East and southern Europe and further spread to other places. The earliest paper mill was found in northern European region in Germany. It was the first country to have the first paper mill built and established in 1390 in Nurnberg. The mill company was using a watermark that consisted of the letter 'S' and the Nurnberg's heraldic arms. In the early 1405, a mill company was established in Netherland by Jean L'Espagnol and imported the papermaking from Spain. Later in 1495, introduced by John Tate in Hertfordshire, England joined the race of establishment of the paper making company. After that, other countries started to adopt the idea of establishing paper mill companies, and Russia happened to be one of them which established the company in 1576 in Moscow. In 1591, Mungo Russel and his son Gideon decided to uplift their country in terms of development by establishing the paper making company in their country which was the first of its kind in Scotland. In the mid-1400s, watermarks had received more attention in many areas in the world, and smaller papers were produced without watermark. Although there were some probabilities for applying watermarks into software programmes, this idea did not start till 1995, when they realized that there was a possibility to use watermark into software programmes to identify copyright violators.

On the other side, watermarks on paper in Europe and America had become clearer and useful, when they started to use it as an anti-counterfeiting in the eighteenth century. The idea of using trademarks in watermarking was to know the date of manufacturing the paper, and to point the size, brand, quality and strength of the original sheets. The watermarks were used as security features in banknotes, passports, postage stamps and other documents to protect them against forgery or counterfeit (Wang, 2011).

2.3 Basic Watermarking Principles

Generally, any watermarking algorithm consists of three parts; watermark embedding algorithm, watermark extraction algorithm and watermark detection algorithm (Zhang, 2009).

In an embedding process, the algorithm allows adding a watermark signal into the original image to be watermarked image, that mark could be unique to the owners of digital contents to protect their products from unauthorized copying. Usually the watermarked signals transmit from a person to another person. If this person does not make any modification, the watermark is still present and it can be retrieved. Likewise, if the signal is copied, then the information is also carried in the copy (Syed, 2011). However, the private or public key is used to enforce security during the embedding and the retrieving process in order to prevent forgery or illegal access to the watermark.

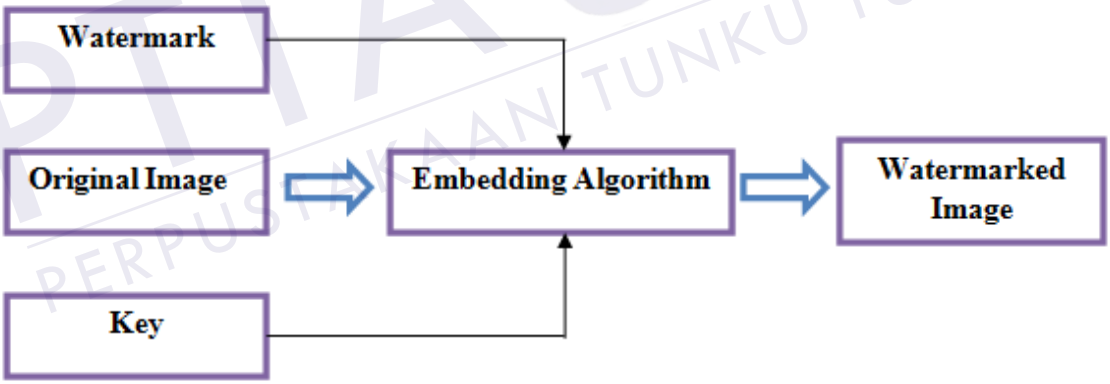

Figure 2.2: Watermarking embedding process (Sharma and Gupta, 2012)

However, Figure 2.3 shows the watermarking extraction process. This operation is usually reversed of embedding system. The goal of this stage is to retrieve the original watermark.

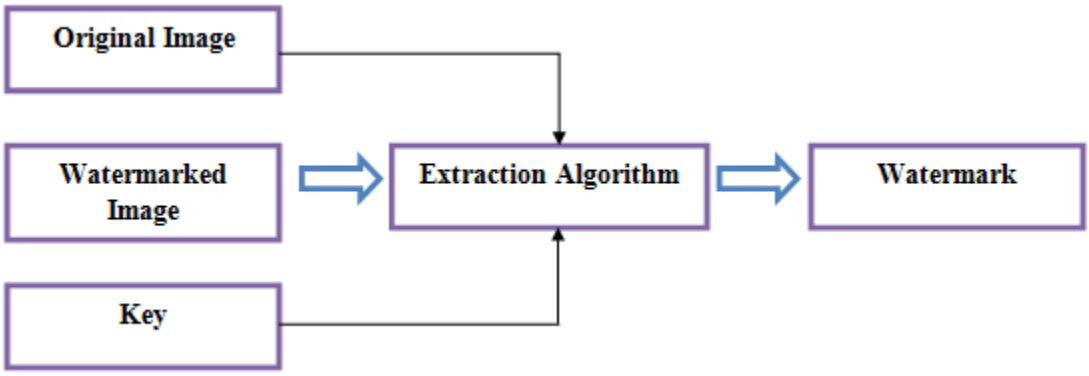

Figure 2.3: Watermarking extraction process (Hussein and Mohamed, 2012)

2.3.1 Peak Signal to Noise Ratio (PSNR)

In order to evaluate the performance of the watermarked images, there are some types of measurements to determine the quality of image including, PSNR and MSE. However, the PSNR is most commonly used as a measure of quality of reconstruction in image compression (Lee et al., 2008). Where the peak signal noise ratio (PSNR) formula is:

$$PSNR = 10.\log \frac{(MAXi^2)}{MSE} \quad (2.1)$$

PSNR formula (Bamatraf, 2012)

Where *MAXI* is the maximum possible pixel value of the image and MSE is Mean Square Error. The high PSNR value indicates high security because it indicates the minimum difference between the original and watermarked data. So no one can suspect the hidden information.

2.3.2 Mean Square Error (MSE)

The MSE represents the cumulative squared error between the compressed and the original image. The mathematical formula for the mean square error is:

$$MSE = \frac{1}{m*n} \sum_{i=0}^{m-1} \sum_{i=0}^{n-1} [I(i.j) - K(i,j)]^2 \quad (2.2)$$

MSE Formula (Bamatraf, 2012)

Where m and n are the number of rows and columns in the input images, respectively and I (i, j) is the original image, K (i, j) is the watermarked image.

2.3.3 Normalized Correlation (NC)

The watermarking system should be robust against data distortions introduced through standard data processing and attacks. Normalized Correlation is a measurement used to estimate the quality of extracted watermark.

$$NC = \frac{\sum_{m=1}\sum_{n=1} W * W'}{\sqrt{\sum_{m=1}\sum_{n=1} W^2} \times \sqrt{\sum_{m=1}\sum_{n=1} W'^2}} \quad (2.3)$$

Figure 2.4: NC Formula (Jadhav and Bhalchandra, 2010)

Where **W** is original watermark and **W'** is recovered watermark.

2.4 Classifications of Digital Watermarks

There are many ways which the digital watermarking schemes have been classified by researchers. These classifications are based on different categories according to several criteria. The following section describes the different types of watermarking.

2.4.1 Host Signals

The host signal is the object that carries the watermark inside it. The cover signals are used to transmit information from the sender to the recipient. According to Ensaf Hussein (2012), the common types of host signals are as the following:-

2.4.1.1 Image Watermarking

Nowadays, most of the digital watermarking researchers concentrate on the images. The cause might be back the availability of unlimited images on the World Wide Web without cost and also without any copyright protection.

2.4.1.1.1 Image Compression

In order to minimize the size in bytes of the original image file without degrading the quality of the image it may need to compress the image. Digital images with greater bit depth usually require larger space and more bandwidth for transmitting photographs on the World Wide Web. The reduction in image 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. Image compression is divided into two types: lossy and lossless compression (Morkel et al., 2005).

Lossy compression is a data embedding method that compresses data by losing some of it. The goal of this procedure is to reduce the amount of data that needs to be handled or transmitted by a computer. This method is more harmful as compared to lossless compression methods. JPEG images are the most common use this technique.

A lossless compression method is considered as a data compression algorithm, which allows the original data to be perfectly reconstructed from the compressed data. It reduces a file's size with no loss of quality of the images. This technique can be applied with either GIF or Bmp image formats.

2.4.1.2 Video Watermarking

A video sequence is an extension of the image. Consequently, all the watermarking methods used in image can also be applied to video. This method requires real time extraction and robustness for compression. Video watermarking should be robust against all kinds of attacks including frame averaging, frame dropping and frame swapping.

2.4.1.3 Audio Watermarking

The term 'watermark' can be defined as robust and inaudible transmission of additional data along with audio signals ((Bamatraf, 2012). This host signal has become a hot area in the last previous years. The reason might be back to the rapidly increasing of the internet music such as MP3 and MP4. There are other host signal types including

hologram, software, database, and text watermarking. In this research, the discussion is only focused on the digital image.

2.4.2 Human Perceptivity Watermarks

Digital watermarking can be divided into two basic types which are visible and invisible watermarking.

2.4.2.1 Visible Watermarking

The visible watermark is a semi-transparent in which text or logo can be overlapped on the original image. Mostly it is used to identify the ownership and copyrights of digital contents. Viewers can clearly see the original image, but it protected by copyright. Usually, visible watermarking techniques change the original signal because the watermarked signal is different from the original signal. However, visible watermark embedding algorithms are low computationally complex. The watermarked image cannot withstand the signal processing attacks. For example, the watermark can be cropped from the watermarked image (Chawla et al., 2012).

Figure 2.5: Visible watermarked image (Chawla et al., 2012)

2.4.2.2 Invisible Watermarking

Invisible watermark is embedded in an image or text in such a way that it cannot be perceived by the human eyes. Only electronic devices can retrieve the hidden information to identify the copyright owner. The Invisible watermarks are used as evidence of image authentication and preventing it from being copied. This watermark cannot be seen by the viewer. Similarly, the watermarked signal is almost similar to the original signal because the output signal does not change much when compared to the original signal. The invisible watermarking is more robust to signal processing attacks when compared to visible watermarking. Likewise, the quality of the image does not suffer much, it can be used in almost all the applications (Chawla et al., 2012).

Figure 2.6: Invisible watermarked image (Chawla et al., 2012)

2.4.3 Robustness of Watermarks

Watermarks should be designed a better way, resisting any manipulation from malicious attacks to protect the ownership. The security of all applications are mostly depending on how the watermark is robust. The following three types are the classifications of robustness of a watermarking.

2.4.3.1 Fragile Watermark

This watermark is designed with very low robustness. Fragile watermark is very sensitive and it can be easily destroyed with slight modifications in the watermarked signal (Chawla et al., 2012). Usually they used this kind of watermark to check the integrity of original contents.

Figure 2.7: Fragile watermarked images (Chawla et al., 2012)

2.4.3.2 Semi-Fragile Watermark

If the watermark is able to resist benign transformation, but fails detection after malignant transformations, this is called as digital semi-fragile watermark (Bamatraf, 2012). It is suitable of tolerating some degree of change to a watermarked image such as

the addition of quantization noise from lossy compression. This method can be used to verify data integrity and authentication as well.

2.4.3.3 Robust Watermark

One of the most important demands of watermark is that the embedded watermark should be strong against intentional attacks such as cropping and compression and non-intentional malicious which are aimed to destroy the watermark. Robust digital watermark is a watermark that resists a designated class of transformations (Bamatraf, 2012). Any attempts to remove or destroy the watermark may affect or degrade the quality of the image (Chawla et al., 2012). Nowadays robust watermark is used widely to protect the owner's legal application rights.

2.4.4 Division Based Extraction Process

The extraction process of digital watermarking consists of three different categories such as Non-blind, Semi-blind and Blind respectively.

2.4.4.1 Non-Blind Watermarks

The detection of this process depends on the availability of an original image. In the watermark embedding system the watermark is extracted from the distorted data and the original data is used as a source to find where the watermark is present in the distorted data (Singh et al., 2012). Non-blind watermarks are more robust to any attacks on the signal when compared to blind watermarks (Chawla et al., 2012).

2.4.4.2 Semi-Blind Watermarks

The semi-blind watermark requires secret key and watermark bit sequence for an extraction. Also, it needs some special information to detect the embedded data in the watermarked signal. It does not demand an original image for detection. Some applications of this watermark are fingerprinting and copy control (Singh et al., 2012).

2.4.4.3 Blind Watermarks

If the Digital watermark does not require an original image, it is called blind watermarking. This type of watermarks does not require either the original image or the embedded watermark. It is also referred to as public watermarking. Blind watermarks are less robust to any attacks on the signal (Singh et al., 2012).

2.4.5 Domain Watermarks

Most researchers have mentioned that the domain watermark consisted of two major domain types, which are spatial and frequency domains.

2.4.5.1 Spatial Domain

Spatial domain watermarking technologies are embedded by directly editing pixel values of cover image. These modifications may include flipping the low-order bit of each pixel. Spatial watermarking is simple and with less computing complexity as no

frequency transform is required. It has high capacity, more perceptual quality, but less robust and mainly capable for authentication applications. However, this approach is not reliable when subjected to normal media operations such as filtering or lossy compression (Syed, 2011).

2.4.5.2 Frequency Domain

The frequency domain is inserted into transformed coefficients of the host image, giving more information hiding capacity and more robustness against various watermarking attacks because information can spread out to the entire image (Gunjal and Manthalkar, 2010). Embedding is done by frequency domain techniques after taking an image transforms. Generally, frequency domain has more robust compared with spatial domain, less control of perceptual quality and it is suitable for copyright application.

2.4.6 Classification by Applications

Digital watermarking has been widely and successfully applied in billions of media applications objects across a wide range of applications such as copyright protection, data authentication, broadcast monitoring, copy protection and fingerprinting (Hussein and Mohamed, 2012).

2.4.6.1 Copyright Protection

With a large amount of images being exchanged over insecure networks daily, copyright protection has become a very important matter. Digital contents are easily transferred

from one person to another since the start of the internet revolution. Using digital embed watermarks is an efficient method which can ensure our ownership of media content. This watermark may contain imperceptible digital data that can include ownership information, contact details and usage rights. Copyright protection should be a high level of robustness. Therefore, the embedded image makes it difficult for the watermark to be removed without data distortion (Singh, 2011).

2.4.6.2 Data Authentication

A watermark is an evidence of ownership. The slight modification may remove or lose the authenticity of the digital contents where anyone can claim the ownership of these objects. For that reason, it needs to verify the ownership of the objects. Like this application, it detects the modification of data. To verify the authenticity of the received data, watermark is embedded in the host image (Singh, 2011).

2.4.6.3 Broadcast Monitoring

A watermark is embedded in trade advertisements. Its automated monitoring system is used to verify the programs broadcasted on television or radio. The prime reason of using broadcast monitoring is to protect the valuable TV products such as news items from illegal transmission (Singh, 2011). It particularly helps the advertising organizations and companies to see if their advertisements appeared for the right duration or not.

2.4.6.4 Copy Protection

Copy protection is a prevention of making, unofficial and unauthorized copies of copyrighted objects. Only those with permission can access or copy the contents of these media.

2.4.6.5 Fingerprinting

This method is used to detect the owner of the content. Each owner has only one unique fingerprint. The technique is like giving a serial number to every product. Each distributed multimedia copy is embedded with a different watermark. The objective is to transfer the information about the legal recipients. A robust watermarking algorithm is required for this application (Singh, 2011).

2.5 Techniques of Digital Watermarking

There are many digital watermarking techniques. Most of the researchers said it can be divided into two general categories including spatial domain and frequency domain techniques. Any of these domains consists of several image watermarking sub techniques. This work focuses on frequency domain which is related to our research area.

2.5.1 Spatial Domain Techniques

Spatial domain refers to embedding watermarks by directly modifying pixel values of an original image. Tirkel et al. implemented one of the earliest techniques used for image watermarking in 1993. They used two techniques to hide data in the spatial domain of watermarking images (Bamatraf, 2012). Least Significant Bit (LSB), mainly used to hide the information, is the most well-known image watermarking technique in spatial domain. A pixel in images is stored as binary integers. Usually, LSB indicates to right most bits which represent smaller values compared to the left side bits. Modifying the LSB of digital image does not cause changes in the visual quality of the original image (Chen and Lu, 2012). To implement this technique is very simple. In general, spatial domain methods are difficult to survive under malicious attacks compared with the frequency domain. In 1995, Laterin et al. proposed an algorithm relied on the pixel region classification. Pixels are divided into homogeneous luminance zones. Then, the pixels have their gray levels changed following a rule that takes into account the location where the pixel is inserted and the value of the byte to be embedded. However, extracting the least significant bits of the watermarked image can give a distortion estimation of the watermark image (Bamatraf, 2012).

2.5.2 Frequency Domain Techniques

In 1997, Cox et al. had presented a spread spectrum and the first frequency transform domain in watermarking scheme. Most frequency domains use spread spectrum communication techniques in watermarking to embed a one bit in the image. Later in 1998 O'Ruanaidh and Pun introduced a spread spectrum as a watermarking approach. The watermark is embedded in the form of a pseudo-random sequence, in order to embed the watermark or to detect it. It is important to have access to the key, which is simply the seed used to generate the pseudo-random sequences. After that, a lot of

watermarking algorithms in frequency domain have been developed (Bamatraf, 2012). The watermark has been embedded and extracted using different frequency domain techniques. The most well-known transform operating in the frequency transform are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). However, compared to spatial domain, watermark in frequency transform is more robust and suitable to popular image compression standards. Therefore, this research area has received more attention since the application of digital watermarking on an image in 1993.

Table 2.1: Comparison between watermarking techniques (Hussein and Mohamed, 2012)

Characteristics	**Spatial Domain**	**Frequency Domain**
Computation Cost	Low	High
Robustness	Fragile	More Robust
Perceptual Quality	High Control	Low Control
Capacity	High (depending on the size of the image)	Low
Applications	Mainly Authentication	Copy Rights

2.5.2.1 Discrete Cosine Transform

The Discrete Cosine Transform is closely related to Discrete Fourier Transform. It is a mathematical conversion that takes a signal or image and transforms it from the spatial domain into the frequency domain. Lower frequency is clearer in an image than higher frequency. So, if an image is transformed into frequency component and thrown away a lot of higher frequency coefficients, it can reduce the amount of data needed to describe the image without sacrificing too much image quality. Many digital image or video compression schemes can be applied by either globally DCT watermarking or block-based DCT watermarking. When used as globally, the conversion is applied in all parts of the image, separating the spectral regions according to their ability. When applied in blocks, the process is analogous, only the transform is applied to every block separately

(Nivedita et al., 2012), (Fung et al., 2011). Watermarking based on DCT has two facts. The first fact is that much of the signal energy lies at low-frequencies sub-band which contains the most important visual parts of the image. The second fact is that the high frequency components of the image are usually removed during compression and noise attacks. Therefore, the watermark is embedded by modifying the coefficients of the middle frequency sub-band so that the visibility of the image is not affected and the watermark is not removed by compression (Amirgholipour and Nilchi, 2009). There are many variants of the Discrete Cosine Transform, but DCT that have 2-dimensional is the most commonly used for digital images. The formula of 2D (N by M) DCT is defined as the following:

$$F(u, v) = \left(\frac{2}{N}\right)^{½}\left(\frac{2}{M}\right)^{½}\sum_{i=0}^{N-1}\sum_{i=0}^{M-1} \wedge(I).\wedge(j).\cos\left[\frac{\pi.u}{2.N}(2i+1)\right]\mathrm{Cos}\left[\frac{\pi.v}{2.M}(2j+1)\right].f(i, j) \quad (2.4)$$

However, the corresponding inverse 2D-DCT transform F^{-1} (u, v) formula is:

$$\wedge(\boldsymbol{\xi}) = f(x) = \begin{cases} \frac{1}{\sqrt{2}} & \text{For } \boldsymbol{\xi}=0 \\ 1 & \text{Otherwise} \end{cases} \quad (2.5)$$

The equation (2.4) given by:

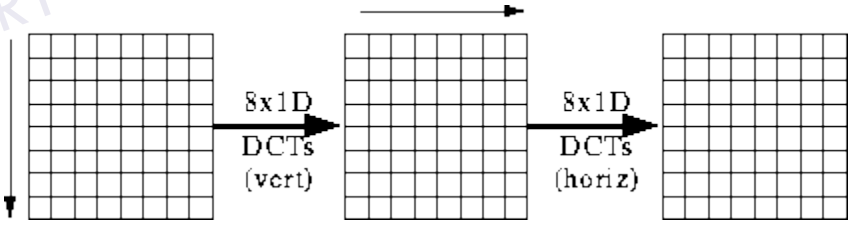

Figure 2.8: Elements of an 8x8 DCT matrix (Marshall, 2001)

The 1D DCT is applied to each row of *F* and then to each column of the result. Since the 2D DCT can be computed by applying 1D transforms separately to the rows and columns, it may say that the 2D DCT is separable in the two dimensions. However, the process of Discrete Cosine Transforms algorithm steps are the following:-

REFERENCES

Amirgholipour, S. & Nilchi, A. (2009). Robust Digital Watermarking Based on Joint DWT-DCT. *International Journal of Digital Content Technology and its Applications (JDCTA), 3(2),* pp. 42 - 54.

Bamatraf, A. O. (2012). *An Improved Digital Watermarking Algorithm using Combination of Least Significant Bit (LSB) and Inverse Bit*. Universiti Tun Hussein Onn Malaysia: Master's Thesis.

Chawla, C. & Saini, R. & Yadav, R. (2012). Classification of Watermarking Based upon Various Parameters. *International Journal of Computer Applications & Information Technology, 1(2)*.

Chen, C. & Lu, H. (2012). Robust Spatial LSB Watermarking of Color Images against JPEG Compression. *Fifth International Conference on Advanced Computational Intelligence (ICACI)*. Jiangus. China. IEEE. pp. 872-875.

Delaigle, J. & Christophe, D. (1996). Digital Watermarking. *Proceedings-Spie The International Society for Optical Engineering.* pp. 99-110.

Fung, C. & Gortan, A. & Junior, W. (2011). A Review Study on Image Digital Watermarking. *The Tenth International Conference on Networks (ICN)*. CAPES. Brazil. pp. 24-28.

Gunjal, B. & Manthalkar, R. (2010). Discrete Wavelet Transform based Strongly Robust Watermarking Scheme for Information Hiding in Digital Images. *Third International Conference on Emerging Trends in Engineering and Technology (ICETET)*. Geo. IEEE. pp. 124-129.

Hartung, F. & Kutter, M. (1999). Multimedia Watermarking Techniques. *Proceedings of the IEEE*. pp. 1079-1107.

Hussein, E. & Mohamed, A. (2012). Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey. *International Journal of Engineering, 1(7)*.

Jadhav, S., & Bhalchandra, A. (2010). Robust Digital Image-Adaptive Watermarking using BSS Based Extraction Technique. *International Journal of Image Processing (IJIP), 4(1),* pp. 77.

Khalid, S. & Deris, M. & Mohamad, K. (2013). Anti–Cropping Digital Image Watermarking using Sudoku. *International Journal of Grid and Utility Computing, 4(2),* pp. 169 - 177.

Kim, J. & Sungeon, H. (2009). Development of Digital Watermarking Technology to Protect Cadastral Map Information. *Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human*. pp. 923-929.

Lee, G. & Yoon, E. & Yoo, K. (2008). A New LSB based Digital Watermarking Scheme with Random Mapping Function. *International Symposiun on Ubiquitous Multimedia Computing.* Hobart. Australia. IEEE. pp. 130-134.

Mansoori, S. & Kunhu, A. (2012). Robust Watermarking Technique based on DCT to Protect the Ownership of DubaiSat-1 Images against Attacks. *International Journal of Computer Science and Network Security (IJCSNS), 12(6),* pp. 1.

Marshall, D. (2001). *Discrete Cosine Transform*. Retrieved on May 2, 2014, from http://www.cs.cf.ac.uk/Dave/Multimedia/node231.html#

Morkel, T. & Eloff, J. & Olivier, M. (2005). An Overview of Image Steganography. *Information and Computer Security Architecture (ICSA).* pp. 1-11.

Nivedita. & Singh, P. & Jindal, S. (2012). A Comparative Study of DCT and DWT-SPIHT. *International Journal of Computational Engineering and Management (IJCEM), 15(2),* pp. 26 – 32.

Rao, S. & Shekhawat, R. & Srivastava, V. (2012). A DWT-DCT-SVD based Digital Image Watermarking Scheme using Particle Swarm Optimization. *IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS).* pp. 1-4.

Rohith, S. & Bhat, K. (2012). A Simple Robust Digital Image Watermarking against Salt and Pepper Noise using Repetition Codes. *Aceee International Journal on Signal & Image processing, 3(1).*

Saini, L. & Shrivastava, V. (2014). Analysis of Attacks on Hybrid DWT-DCT Algorithm for Digital Image Watermarking With MATLAB. *International Journal of Computer Science Trends and Technology (IJCST), 2(3)*.

Sharma, M. & Gupta, P. (2012). A Comparative Study of Steganography and Watermarking. *International Journal of Research in IT & Management (IJRIM), 2 (2)*, pp. 2231 - 4334.

Singh, V. (2011). Digital Watermarking: A Tutorial. *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), January Edition.*

Singh, A. & Dave, M. & Mohan, A. (2012). A Novel Technique for Digital Image Watermarking in Frequency Domain. *2nd International Conference on Parallel Distributed and Grid Computing (PDGC).* Solan. India. IEEE. pp. 424-429.

Smith, L. (2003). *Watermarking Blossoms through the Renaissance.* Retrieved on April 15, 2014, from http://www.motherbedford.com/Watermark1B3.htm

Song, C. & Sudirman, S. & Merabti, M. (2009) Recent Advances and Classification of Watermarking Techniques in Digital Images. *International Conference*. October. Liverpool. UK.

Song, C. & Sudirman, S. & Merabti, M. & Jones, D. (2010). Analysis of Digital Image Watermark Attacks. 7th International Conference on *Consumer Communications and Networking Conference (CCNC).* Las Vegas. USA. IEEE. pp. 1-5.

Syed, A. (2011). *Digital Watermarking.* The University of Texas: Master's Thesis.

Wang, J. (2011). *New Digital Audio Watermarking Algorithms for Copyright Protection*. National University of Ireland Maynooth: Ph.D. Thesis.

Zhang, Y. Digital Watermarking Technology: A Review. (2009). *ETP International Conference on Future Computer and Communication*. Wuhan. China. IEEE. pp. 250-252.

Zong, T. & Xiang, Y. & Elbadry, S. & Nahavandi, S. (2013). A modified moment-based Image Watermarking Method Robust to Cropping Attack. *8th IEEE Conference on Industrial Electronics and Applications (ICIEA)*. Melbourne. Australia. IEEE. pp. 881-885.