# A ROBUST DIGITAL IMAGE WATERMARKING USING REPETITION CODES AGAINST COMMON ATTACKS

ABDULLAHI MOHAMUD HASSAN

A thesis report submitted in partially
fulfillment of the requirement for the award of the
Degree of Master ofComputer Science (Information Security)

Faculty of Computer Science and Information Tecnology
UniversitiTun Hussein Onn Malaysia

FEBRUARY 2015

# ABSTRAK

Tera air digital adalahkaedahmenyembunyikanmaklumat media digital bertujuanmenghalangperbuatanmengubahkandunganatauhakciptadokumentersebut. Padamasaini, kajianberkaitankeupayaankaedahulangankodbagimenghalangpelbagaiseranganmasih belumdibuatsepenuhnya. Dalamprojekini, satu skim domain tera air yang lasakmenggunakanJelmaanKosinusDiskret (DCT) telahdilaksanakan. Idea skim iniadalahuntukmembenamkankodtera air yang menggunakanulangankod (3,1) kedalampikselimejasalberdasarkanteknikpembenamanJelmaanKosinusDiskret (DCT).

Beberapaujianserangansimulasiuntukmenyemakdanmembandingkankelasakanmerek aterhadappelbagaiseranganiaituserangangaramdanlada, bintik, pemampatan, Gaussian, kontrasimej, perubahansaizdankeratanimejtelahdijalankan.Kelasakan skim tera air telahdihitungmenggunakankaedahNisbahIsyaratPuncakkepadaHingar (PSNR), Min RalatKuasaDua (MSE) danKorelasiTernormal (NC). Keputusankajianmendapatikelasakantera air dengankodpengulanganadalahjauhlebihbaikberbandingtera air tanpakodpengulangan

# ABSTRACT

Digital watermarking is hiding the information inside a digital media to protect for such documents against malicious intentions to change such documents or even claim the rights of such documents. Currently the capability of repetition codes on various attacks in not sufficiently studied. In this project, a robust frequency domain watermarking scheme has been implemented using Discrete Cosine Transform (DCT). The idea of this scheme is to embed an encoded watermark using repetition code (3, 1) inside the cover image pixels based on Discrete Cosine Transform (DCT) embedding technique. The proposed methods have undergone several simulation attacks tests in order to check up and compare their robustness against various attacks, like salt and pepper, speckle, compress, Gaussian, image contrast, resizing and cropping attack. The robustness of the watermarking scheme has been calculated using Peak Signal-To-Noise Ratio (PSNR), Mean Squared Error (MSE) and Normalized Correlations (NC). In our experiments, the results show that the robustness of a watermark with repetition codes is much better than without repetition codes.

# CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | | |
|---|---|---|
| LSB | - | Least Significant Bit |
| DWT | - | Discrete Wavelet Transform |
| DCT | - | Discrete Cosine Transform |
| DFT | - | Discrete Fourier Transform |
| PSNR | - | Peak Signal-to-Noise Ratio |
| MSE | - | Mean Squared Error |
| NC | - | Normalized Correlations |
| JPEG | - | Joint Photographic Experts Group |
| BMP | - | Bitmap |
| IDCT | - | Inverse Discrete Cosine Transform |

# CHAPTER 1

# INTRODUCTION

## 1.1 Background and History

The growth of powerful World Wide Web and multimedia system hasresulted a lot of people to use this high speed internet. Whole millions of people use the internet to transmit their digital media application such as images, audio, and video, others areworried with the growth of illegal copiesof their intellectual works. Therefore, there is a great need to protect this content against unauthorized copying. There are a lot of solutions to protect these properties like watermarking, steganography, and cryptography. Thefocused area of research is watermarkingasit has beenwidely used for ownership protection against unauthorized copying (Rohith et al., 2012). Watermarking is a branch of information hiding technique which hides information ownership information inside the cover image. Watermarking makes itvery difficult forthe attacker to remove the secret. The origin of watermarking as an information hiding technique can be traced to ancient Greece as steganography (Songet al., 2010).

Copyright protection and ownership identification for digital images are important applications of digital watermarking technology. To achieve this goal, robust watermarking has been quickly developed in the past decade. Robust watermarking is designed to survive various types of attacks such as JPEG compression, additive noise, filtering and geometric distortions. Digital watermarking is a technique that allows you

to add hidden copyright notices or other verification messages to digital audio, video, or image signals and documents (El-Ghoneimy, 2008).

Watermarking was first used for copyright protection but applications of watermarking have recently been expanded to content verification, authentication, secret communications and information retrieval (Duan et al., 2008). An image watermarking scheme should at least meet the following requirements: transparency and robustness. Transparency means that the embedded watermark should be perceptual invisible and robustness means that the embedded watermark should not be erased by any attack that maintains the acceptable host image quality. Tradeoff between transparency and robustness is one of the most important issues in image watermarking (Liu, 2005).

Watermark robustness is one of the major characteristics that influences the performance and applications of digital image watermarks. Robustness in this context means the ability of a watermark to resist malicious distortion and discover common image processing. Robust watermarking is designed to endure different manipulations such as JPEG compression, additive noise, filtering and geometric distortions (Duan,et al., 2008).

Watermarks can be divided into three major groups according to their robustness: robust, fragile, and semi fragile watermarks. Robust watermarks should be detected successfully in images that have been through manipulative distortions and it is very difficult to attack and remove. Fragile watermarks are very sensitive and easily destroyed or corrupted by image processing transformation or image modifications, while semi fragile are designed to become corrupt when subjected to any change that exceeds a user-specified threshold. But the one and only watermark that can resist legitimate changes is robust watermark, while being sensitive to severe tampering (Chaw, 2007).

## 1.2 Problem statement

The growth of the Internet and multimedia systems has created the need of the copyright protection for various digital contentssuch as images, audio and video from illegal access and unauthorized modifications. An important approach in watermarking is to use repetition codes. There are already a few but very limited works done in this area. However, the capabilities of repetition codes under various attacks are not sufficiently explored. In this project, a robustness of watermarking scheme with repetition codes will be investigated under common attacks.

## 1.3 Motivation

The success of the Internet and digital consumer devices has become an important issue and has extremely changed the world and daily lives throughexchanging ofinformation viathe internet. Besides that, there are a lot of malicious parties that take the advantage of these information by copying or attackssuch as filtering, scaling, cropping, blurring, sharpening, rotating and collusion of the image the properties without permission of the content owners. Hence, there is a big concern in how to protect these data and preventing from unauthorized users. This issue has become challenging in many areas (Tsui, 2008). For example, there are many studies showing that the music and video industry loses billions of dollars per year due to illegal copying and downloading of copyrighted materials from the Internet. Some researchers have invented digital watermarking method and algorithms to address this issue. The basic idea is to embed some secret data in digital content to be protected, and “seal” it within the content (Salama et al., 2011).

## 1.4 Objectives

The main objectives of this research are:

i) To implement a watermarking scheme using repetition codes (3, 1) in Discrete Cosine Transform (DCT).
ii) To test the watermarked scheme againstcommonattacks likesalt and pepper, speckle, compress, Gaussian, image contrast, resizing and cropping attacks.
iii) To analyzethe robustness of the schemeusing common metrics like Mean Squared Error (MSE), Peak Signal-To-Noise Ratio (PSNR) and Normalized Correlations (NC).

## 1.5 Scope

This research investigates the effect of repetition codes on increasing its robustness using DCT approach. It does not concern with the spatial domain and other parts of frequency domain approaches like DWT. The advantage of using frequency domain especially DCT is because it is more robust than other frequency and spatial domains.

## 1.6 Significance of the Study

The previous researchers have applied limited attacks on watermarking scheme based on repetition codes. However, this current research applies more elaborate attacks to determine its robustness against common attacks onmultiple copies of watermark in the cover images.

# CHAPTER 2

# LITERATURE REVIEW

## 2.1 Introduction

This chapter presents an overview of digital watermarking technology. It provides essential material that is needed in understanding various components in digital watermarking. Furthermore, it discusses the limitations in current works and highlights some of the challenges in which this thesis aims to address.

## 2.2 Overview of Watermarking

The history of watermark dated back to the 13th century. Watermarks were used to indicate the paper brand and the mill that produced it was in Italy. By the 18th century, watermarks began to be used as anti- counterfeiting measures on money and other documents and in 1995, the interest in digital watermarking began to mushroom. Intense research has been carried out in this field for the past few years which has led to the discovery of various algorithms (Katariya et al., 2012).

Throughout this thesis some of these techniques are discussed and one such technique is implemented. As many advances are made in the field of communication, it became rather simple to decrypt a ciphered text. Hence, more sophisticated methods

are designed to offer better security than what cryptography can offer. The term watermarking is often related to information hiding and steganography. This has led to the discovery of stenography and watermarking. Stenography is the process of hiding information over a cover object sothat the hidden information cannot be perceived by the user. Watermarking is closely related to steganography, but in watermarking the hidden information is usually related to the cover object. Hence, it is mainly used for copyright protection and owner authentication.

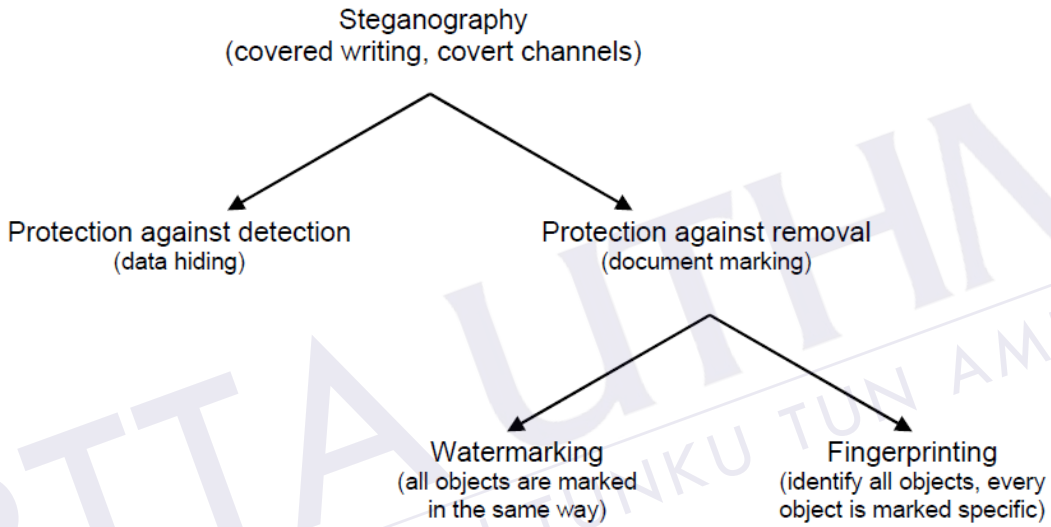


Figure 2.1: Types of Steganography (Potdar et al., 2005)

### 2.2.1 Definition of Watermarking

Embedding a digital signal such as audio, video or image with information which cannot be easily removed is called digital watermarking. Watermark is also a digital signal, pattern, image or text inserted into a multimedia object to protect the ownership right. The multimedia object may be an image, audio, video, software or hardware (Sharma et al., 2013).

### 2.2.2 Key Terms of Watermarking

This section provides an overview of digital watermarking and it covers some basic terms. The list below contains the meaning of standard terms used throughout this proposal (Samuel, 2007).

i) **Cover image**: the original image used in watermarking.
ii) **Stego image**: the cover image following watermark embedding
iii) **Test image**: the possibly modified stego image from which the watermark is to be extracted
iv) **Reference image**: the image used to assist watermark detection, and also it could be a cover image, stego image, or a test image.
v) **Watermark**: can be a simple signal consists of pseudo-random binary sequence, or a multi-bit message encoded in a transform domain.
vi) **Watermark embedding**: the process of encoding a watermark signal (i.e. the watermark into an image).

## 2.3 Requirements (Properties) of Digital Watermarking

Watermarking systems can be characterized by a number of properties to get the activeness of watermark. In this section, the most common properties of a digital watermarking scheme are highlighted such astransparency, robustness, capacity and security (Potdar et al., 2005).

### 2.3.1 Transparency or Fidelity

Transparency or Fidelity of the watermark can be considered as a measure of perceptual transparency or fidelity of watermark. Itis also not visible and does not affect the overall visual quality of the watermarked content. In other words, the watermark is neither visible by human eyes nor affects the carrier fidelity. This is why transparency is assumed as one of the basic requirements of digital watermarking (Duan et al., 2008).

### 2.3.2 Robustness

Robustness is one of the most commonly tested properties in digital watermarking systems, and the watermarks should not be removed intentionally or unintentionally by simple image processing operations. Hence, watermarks should be robust against variety of such attacks. Robust watermarks are designed to resist normal processing. On the other hand, fragile watermarks are designed to convey any attempt to change digital content (Chen et al, 2012).

### 2.3.3 Capacity or Data Load

Capacity or payload of the watermarking system refers to the size of the watermark that the watermarking algorithm can embed within the digital content. . It is the maximum amount of information that can be hidden without degrading the image quality. Unfortunately, higher capacity is usually obtained at the expense of either robustness, or imperceptibility, or both. This requirement, payload, is highly dependent on three factors; the host medium, the intended application, and the aimed resulted quality. Therefore this property describes how much data should be embedded as a watermark so that it can be successfully detected during extraction (Katariya et al., 2012).

### 2.3.4 Security

Security is one of basic requirements of a digital watermarking system. The security in a digital watermark system is defined as the ability to resist any intentional process or attack intended to destroy the watermark's purpose. It is also used to protect digital content from illegal use and distribution. However, secret key has to be used for embedding and detection process in case where security is a major concern.

Therefore, there are three types of keys used in watermark systems; private-key, detection-key and public-key, and the attackers areunable to remove watermark. The protection is diminished if the attackers can estimate, remove, or insert a watermark. Different applications have different levels of security. Some watermarks provide enhanced functionalities such as separating commercials from programs in TV broadcasting, in which security is less of a concern. On the other hand, security is a key for watermarks that are used for photo forensics (Katariya et al., 2012).

## 2.4 Watermark Applications

The requirements that a watermarking system needs to comply with depends upon the specific type of application. Digital watermarking can be used for a wide range of applications, such as: copy protection, broadcast monitoring, digital fingerprinting, tamper detection and data authentication (Potdar et al., 2005).

### 2.4.1 Copy Protection

Watermarking can be used to protect the copyrighted material from being copied redistributedan unauthorized person. A watermark can be introduced in the data with a copy protect bit. When the copying device reads the data, the watermark detecting circuitry should detect the watermark and stop recording. This would need all the copying machines to have the watermark circuitry to identify the watermark and act for that reason (Katariya et al., 2012).

### 2.4.2 Broadcast Monitoring

Jabade et al. (2011) define the Broadcast Monitoring as an application used to monitor unauthorized broadcast situation. It can verify whether the content is really broadcasted or not. Italso refers to the technique of cross-verifying whether the content that was supposed to be broadcasted (on TV or Radio) has really been broadcasted or not. Watermarking can also be used for broadcast monitoring. Itsmajor application is commercial advertisement broadcasting where the entity who is advertising wants to monitor whether their advertisement was actually broadcasted at the right time and for the right duration.

### 2.4.3 Digital Fingerprinting

Digital Fingerprinting is a technique used to detect the owner of the digital content and used to inform when an illegal copy appeared. Fingerprints are unique to the owner of the digital content. Therefore, a single digital object can have different fingerprints because they belong to different users (Potdar et al., 2005).

### 2.4.4 Tamper Detection

Fragile watermarks are used for tamper detection. If the watermark is destroyed or degraded, it indicates presence of tampering and hence digital content cannot be trusted. Digital content can be detected for tampering by embedding fragile watermarks. If the fragile watermark is destroyed, then, it will be able to indicate the presence of tampering and thus the digital content cannot be trusted. Tamper detection is very important for some applications that involve highly sensitive data like satellite imagery or medical imagery. Tamper detection is also useful in court of law where digital images could be used as a forensic tool to prove whether the image is tampered or not (Jabade et al., 2012).

### 2.4.5 Data Authentication

Content authentication is able to detect any change in digital content. This can be achieved through the use of fragile or semi-fragile watermark which has low robustness to modification in an image. Thus, the images can be labeled with its content and can be used in search engines (Jabade et al., 2012).

## 2.5 Attacks on Digital Watermarking

According to (Song et al., 2010) watermarking attacks are divided into four classes of attacks; removal attacks, geometric attacks, cryptographic attacks, and protocol attacks. These four attack types are describedbriefly here.

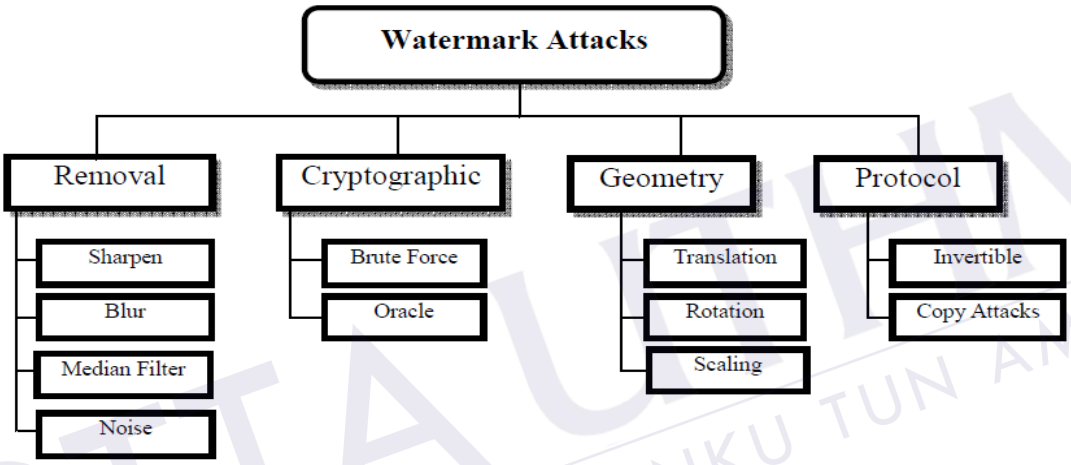


Figure2.2: Classification of watermark attacks (Song et al., 2010)

### 2.5.1 Removal Attacks

Removal attacks are watermarking attacks that try at removing the watermark signal from the watermarked image without attempting to break the security of the watermarking algorithm or without cracking the security of the watermarking algorithm, e.g., without the key used for watermark embedding. This type of watermark attack does not attempt to find out the encryption techniques used or how the watermark has been embedded. As theresult will bea damaged watermarked image, no simple post processing can recover the watermark signal from the attacked data. Included in this category are noising, histogram equalization, blur, sharpen and Gaussian noise attacks.

#### 2.5.1.1Salt and Pepper Attack

Salt and pepper noise is an example of statistical noise although it contaminates the image with a very different probability density function (PDF).However, it presents itself as randomly occurring white and black pixels in an image. Its PDF takes the form of two impulse functions at two discrete locations. In this attack, it could happen intentionally by an attacker who is trying to destroy the watermark (or make it undetectable) by adding noise to the watermarked cover. In MATLAB, command function AI = imnoise(image,'salt&pepper',den); is used to generate salt and pepper noise of various densities. (Song et al., 2010).

#### 2.5.1.2Speckle NoiseAttack

Speckle is a Multiplicative noise attack that inherently exists in and degrades the quality of the image, distributed random noise with mean 0 and different number of variance. In MATLAB, command function AI = imnoise(image,'speckle',variance); is used to generate speckle noise of various variances.

#### 2.5.1.3Gaussian NoiseAttack

Gaussian noising attack is a statistical noise that adds a noise signal to an image with different variances in order to intentionally corrupt the image. It is also known as Gaussian distribution;wherebythe visual quality isreduced. In MATLAB, command function AI = imnoise( image,'gaussian',mean_value, variance); is used to generate Gaussian noise of various variances (Song et al., 2010).

#### 2.5.1.4Image CompressionAttack

Image compression is used to compress and reduce the size or reduce the cost of bandwidth before we transmit still images for storage and transmission. However, image compression can be considered as an unintentional attack. In MATLAB, the quality setting is defined as a number between 0 and 100 with higher numbers mean higher quality in different quality factors (Song and Merabati, 2010).

### 2.5.2Geometric Attacks

Geometry attacks are rather different from removal attacks. Instead of removing the watermark, the watermark is distorted using spatial or temporal alteration of stego data. This type of attack intends to distort the watermark signal. It is still theoretically possible for the detector to recover the original watermark if the detail of the geometry attack can be established and a counter-measure is applied. The process of correcting this type of attack is often referred to as synchronization. However, the complexity of the required synchronization process might be too prohibitively expensive and slow. Included in this category of watermark attacks are image rotation, scaling, and translation (Chaw, 2007).

### 2.5.3Cryptographic Attacks

Cryptographic attacks aim to crack the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed ambiguous watermarks. One of the techniques in this category is the brute-force search for the embedded secret information. Another attack in this category is called Oracle

attack, which can be used to create a non-watermarked signal when a watermark detector device is available. Practically, application of these attacks is restricted due to their high computational complexity. If the image is watermarked, it requiresa key to decipher.Brute force attacks are used for exhaustive search to find the key to decipher. These are called cryptographic attacks (Samuel, 2007).

#### 2.5.3.1Cropping Attack

Cropping attack is a very common attack that involves the attacker in the small apportion of located watermark if imperceptible and then removing the mark by cropping this area. This kind of attack is also called as the target image. In MATLAB command “imcrop” is used to crop operation or adjust different intensity (Ram, 2013).

#### 2.5.3.2Image Contrast Attack

Image contrast attack is a method in image processing in contrast and mostly it can be performed with the help of histogram to specify the image type. In MATLAB, command function AI = histeq (image); is used to specify the value of the image.

#### 2.5.3.3Resizing Attack

Resizing attack is one of the famous attacks in geometric attack used to reduce or enlarge an image for display and to change the dimension of an image to fit a specific resolution or display while retaining as much information in the image as possibleby removing data from the image that has minimal contact on the image content.

However,the function of this process is to select different size. In MATLAB, command "imresize" is used to perform the resize operation (Ram, 2013).

### 2.5.4 Protocol Attacks

The goal of Protocol attacks is to attack the entire concept of the watermarking application and also to destroy or extract watermark signal. One category of protocol attack is invertible watermarks. The idea behind inversion is that the attacker subtracts his own watermark from the watermarked data and claims to be the owner of the watermarked data. In this attack, there is no respect to the right ownership of the data. It has been shown that for copyright protection applications, watermarks need to be non-invertible. The requirement of non-invertibility of the watermarking technology implies that it should not be possible to extract a watermark from a non-watermarked document. Another protocol attack inthis category is called copy attack. In this case, the goal is not to destroy the watermark or damage its detection but to estimate a watermark from watermarked data and copy it to some other data, called target data. The copy attack is applicable when a valid watermark in the target data can be produced with neither algorithmic knowledge of the watermarking technology nor the knowledge of the watermarking key. Again, signal-dependent watermarks might be resistant against the copy attack (Perwej et al., 2012).

## 2.6 Classification for Digital Image Watermarking

Classification of digital watermarking can be made according to the ability of the watermark to resist attacks, visibility of the watermark, how the watermark is extracted, the domain in which the watermark is embedded, or according to the ability of recovering the original image.

### 2.6.1 Division Based on Characteristics

Digital watermarking can be divided into robust watermarking and fragile watermarking depending on its characteristics. Robust watermarking is mainly used to sign copyright information of the digital works. The embedded watermark can resist the common edit processing, image processing and lossy compression, and these watermarks cannot be broken easily. Robust watermark should remain intact permanently in the embedded signal as such that attempts to remove or destroy the robust watermark will degrade or may even destroy the quality of the image (Katariya et al., 2012).Fragile watermarking is mainly used for integrity protection which must be very sensitive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking. These watermarks are very sensitive. They can be destroyed easily with slight modifications in the watermarked signal (Katariya et al., 2012).

### 2.6.2 Division Based on Human Perception

Digital watermarking can be divided into visible watermarking and invisible watermarking according to the detection process. Visible watermarkis the watermark

that is visible in the digital data like stamping a watermark on papersuch as television channels, whose logo is visible atthe corner of the TV picture and needs the original data in testing course, but they are transparent. Such watermarks cannot be removed by cropping the center part of the image (Perwej et al., 2012)

Invisible watermarkalso called blind watermarking as it does not need original data.Although ithas wide application field, blind watermarking requires a higher watermark technology. For this, there is technology available whereinformation can be inserted into an image thatcannot be seen by the human eyes and requiresome type of extraction algorithm to be able to read the watermark. Invisible watermarking is more robust to signal processing attacks when compared to visible watermarking as the quality of the image does not suffer much (Singh and Chadha, 2013).

### 2.6.3 Division Based on Media/Host Signal

Digital watermarking can be divided into image watermarking, video watermarking, audio watermarking, and text watermarking and graphic watermarking based on the attached media (Singh and Chada, 2013)

i) **Image watermarking:** refers to adding watermark in still image. and also used to hide the special information into the image and later to detect and extract that special information for the author‘s ownership.
ii) **Video watermarking:** adds digital watermark in the video stream to control video applications. It is the extension of image watermarking; this method requires real time extraction and robustness for compression.
iii) **Audio watermarking*:*** This application area is one of the most popular and hot issue due to internet music, MP3.
iv) **Text watermarking:** This adds watermark to the PDF, DOC and other text file to prevent the changes made to text. The watermark is inserted in the font shape and the space between characters and line spaces.

v) **Graphic watermarking:** It embeds the watermark to 2D or 3D computer generated graphics to indicate the copyright.

## 2.7 Techniques for Digital Image Watermarking

Digital image watermarking techniques can be grouped into two major classes: Spatial Domain Watermarking and Frequency Domain Watermarking. Each one has its advantages. Here we are focusing in frequency domain area and will be discussed later.

### 2.7.1 Spatial Domain

Spatial domain technique is whenthe data are embeddedby directly modifying the pixel values of the original image (Sharma et al., 2013). This technique can also be applied using color separation as such that the watermark appears in only one of the color bands.

#### 2.7.1.1 Least Significant Bit (LSB)

LSB is one of the most common popular techniques used in spatial domain and is also one of the earliest works of digital image watermarking schemes that embeds watermarks of the pixels (Pithiya et al., 2013).

Chan et al. (2013) implemented one of the first used techniques for image watermarking. These two techniques hide data in the spatial domain of images. These methods were based on the pixel value's Least Significant Bit (LSB) modifications. The algorithm proposed by Chan et al. (2013) to hide a data scheme is by applying a simple LSB substitution. To apply an optimal pixel adjustment process to the stego-image

obtained by the simple LSB substitution method, the image quality of the stego-image can be greatly improved with low extra computational complexity. The worst case mean-square-error between the stego-image and the cover-image is derived.

Bamatraf et al. (2013) introduced a new digital image watermarking using least significant bit (LSB) because of its little effect on the image. In this algorithm,theyused LSB by inversing the binary values of the watermark text and shifting the watermark according to the odd or even number of pixel coordinates of image before embedding the watermark. This algorithm is flexible depending on the length of the watermark text. Bamatrafet al. (2013) had used algorithm that could improve the quality of the watermarked image and also attacked the watermarked image by using cropping and adding noise.

### 2.7.2 Frequency Domain

The transform domain image is represented in terms of its frequencieswherethe image is segmented into multiple frequency bands. Generally, this technique has been found to have the greatest robustness against common signal processing operations. The most commonly used methods of data transformation in frequency domain are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT) (Kaur et al., 2011) In this thesis, we are only interested in Discrete Cosine Transform.

#### 2.7.2.1 Discrete Wavelet Transform (DWT)

Wavelet Transform is a modern technique commonly used in digital image processing, compression, watermarking and others. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. DWT also separates an image into a

lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. Nowadays, DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image (Salama et al., 2011).

**2.7.2.2Discrete Cosine Transform (DCT).**

DCT represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. DCT based watermarking techniques are robust compared to spatial domain techniques. The reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustmentand blurring. However, they are difficult to implement and are computationally more expensive. At the same time, they are weak against geometric attacks like rotation, scalingand cropping. DCT domain watermarking can be classified into Global DCT watermarking and Block based DCT watermarking. The DCT transforms a signal from an image representation into a frequency representation by grouping the pixels into 8 × 8 pixel blocks and transforming the pixel blocks into 64 DCT coefficients.A modification of a single DCT coefficient will affect all 64 image pixels in that block. The next step is the quantization phase of the compression (Singh and Chada, 2013).

Kaurt et al (2011) proposed a DCT based watermarking scheme which provides higher resistance to image processing attacks such as JPEG compression, noise, rotation and translation. In this approach, the watermark is embedded in the mid frequency band of the DCT blocks carrying low frequency components. Watermark is inserted by adjusting the DCT coefficients of the image and by using the private key. Watermark then can be extracted using the same private key. Performance analysis shows that the

watermark is robust.DCT plays a very important role in image compressing; coding and other applications. The watermarking algorithms based on DCT domain are compatible with the existing international compression standards like JPEG and MPEG. Italso states that DCT is the most widely used transform technique in image compression.
DCT block consists of three frequency bands-Low frequency band (FL), High frequency band (FH), mid frequency band (FM) as shownin Figure 2.3

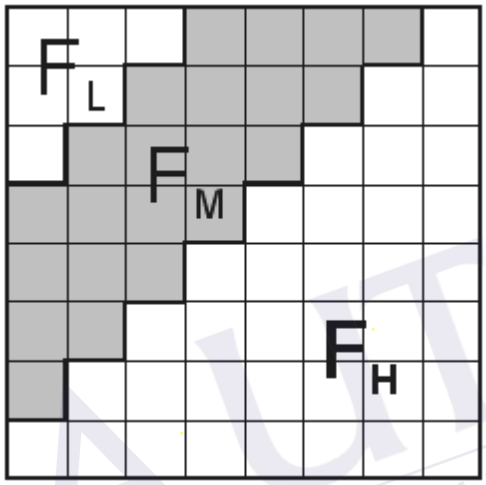


Figure 2.3 Definition of DCT regions

DCT plays a very important role in image compressing; coding and other applications. The watermarking algorithms based on DCT domain are compatible with the existing international compression standards like JPEG and MPEG. Italso states that DCT is the most widely used transform technique in image compression.

### 2.7.2.2 .1 Advantages of DCT

DCT has a lot of advantages then other frequency domain like DWTand DFT.some of the advantages are discussed here:

DCT coefficients are smaller in compression then others, so it provides good amount of same data to 0's to transfer in communication. DCT also has semantically meaningful watermark pattern and good perceptual invisibility.However, DCT is acceptably robust than others and various user-selected options and reasonable complexity/execution time in operation. Another benefit of DCT is it is fast and suitable for robustness against JPEG compression and it is a real transform with better computational efficiency than DFT which by definition is a complex transform (Ram, 2013).

**2.7.2.2.2Disadvantages of DCT**

One of the main problems and the criticism of the DCT is the blocking effect. In DCT, images are broken into blocksof 8x8 or 16x16 or bigger. The problem with these blocks is that when the image is reduced to higher compression ratios, these blocks become visible. This has been termed as the blocking. Another disadvantage of DCT is the effect of picture cropping after adjusting the crop area. Thus, it can be concluded that certain higher frequency components tend to be suppressed during the quantization step (Ram, 2013).

**2.8 Digital watermarking Based on Repetition Codes.**

Repetition code is one of the most basic error correcting codes. In order to transmit a message over a noisy channel that may corrupt the transmission in a few places, the idea of the repetition code is to just repeat the message several times andthey try to reduce the error rate. It ishopedthat the channel corrupts only a minority of these repetitions. This way, the receiver will notice that a transmission error occurred since the received data stream is not the repetition of a single message, and moreover, the receiver can recover the original message by looking at the received message in the data stream that

occurs most often. There are two parts to the repetition code: the encoder and decoder (MacKay, 2003).

**Example of Error Correction: A Repetition Code**

Let's say we have a repeated message of 3 bits that is sent 3 times. When it is received, each message is different:

- 101
- 001
- 100

Because we didn't receive exactly the same message all 3 times, we have detected that some errors occurred.

We can see that the middle bit is almost certainly a 0, because it is the same in all messages. We can also see that the first and the last digit are likely to be a 1 because 2 out of 3 of the messages say that these values are 1. The transmitted message then was most likely 101.

Table 2.1: Example of repetition codes (MacKay, 2003)

| Received codeword | Decoded |
|---|---|
| 000 | O(No error) |
| 001 | 0 |
| 010 | 0 |
| 100 | 0 |
| 111 | 1(No error) |
| 110 | 1 |
| 101 | 1 |
| 011 | 1 |

**Repetition Encoder:** For example, suppose we have a (3, 1) repetition code, then encoding the signal **m** =101001 yields a code then **c** = 111000111000000111.

# REFERENCES


Bamatraf, A., Ibrahim, R., Salleh, M., & Mohd, N. (2011). A new digital watermarking algorithm using combination of least significant bit (LSB) and inverse bit. *Journal of computing,3(4).*

Chaw-Seng, W. O. O. (2007). Digital image watermarking methods for copyright protection and authentication. Queensland University of Technology: Doctoral dissertation.

Chan, C. K., & Cheng, L. M. (2013). Hiding data in images by simple LSB substitution. *pattern recognition*, *37*(3), pp.469-474.

Chen, Y. H., & Chen, J. C. (2012). Digital Image Watermarking Based on Mixed Error Correcting Code. *Journal of Information Security*, *3*(2), p. 156-161.

David MacKay (2003), Basics of Error Control Codes Retrieved May 16, 2014 from http://courses.cs.washington.edu/courses/cse466/11au/calendar/11ErrorControlCodes-posted3.pdf.

Deepthi, K., & Ramprakash, R. (2013). Design and Implementation of JPEG Image Compression and Decompression. . *International Journal of Innovations in Engineering and Technology (IJIET)*, 2(1), pp. 90-98.

Duan, G., Ho, A. T., & Zhao, X. (2008). A novel non-redundant contourlet transform for robust image watermarking against non-geometrical and geometrical attacks. *Proc. of 5th International Conference in Visual Information Engineering (VIE), pp.124-129.*

El-Ghoneimy, M. M. (2008). Comparison between two watermarking algorithms using DCT coefficient and LSB replacement. *Journal of Theoretical & Applied Information Technology*, *4*(2), pp. 132-139.

Jabade, V. S., & Gengaje, S. R. (2011). Literature Review of Wavelet Based Digital Image Watermarking Techniques. *International Journal of Computer Applications*, *31*(1), pp. 28-35.

Katariya, S. S. (2012). Digital Watermarking: Review. *International Journal of Engineering & Innovative Technology*, *1*(2), pp.143-153.

Kaur, B., Kaur, A., & Singh, J. (2011). Steganographic approach for hiding image in DCT domain. *International Journal of Advances in Engineering & Technology*, *1*(3), pp. 72-78.

Perwej, Y., Parwej, F., & Perwej, A. (2012). An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection. *International Journal of Multimedia & Its Applications*, *4*(2), pp. 21-38.

Pithiya, P. M., & Desai, H. L. (2013). DCT Based Digital Image Watermarking, De-watermarking & Authentication. *International Journal of Latest Trends in Engineering and Technology (IJLTET), 2(3),* pp. 213-219.

Potdar, V. M., Han, S., & Chang, E. (2005). A survey of digital image watermarking techniques. *Proc* of *3rd IEEE International Conference* In *Industrial Informatics (INDIN),* pp. 709-716.

Ram, B. (2013). Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform. *International Journal of Advancement in Research & Technology,* 2(4), pp. 19-27.

Rohith, S., & Bhat, K. N. (2012). A Simple Robust Digital Image Watermarking against Salt and Pepper Noise using Repetition Codes. *International Journal on Signal & Image Processing*, *3*(1), pp. 47-54.

Salama, A., Atta, R., Rizk, R., & Wanes, F. (2011). A robust digital image watermarking technique based on wavelet transform. *Proc IEEE International Conference In System Engineering and Technology (ICSET),* pp. 100-105.

Samuel, S. (2007). *Digital rights management (DRM)-watermark encoding scheme for JPEG images.* University of Pretoria: Doctoral dissertation.

Sharma, P., & Swami, S. (2013). Digital Image Watermarking Using 3 level Discrete Wavelet Transform. In *Proceedings of the Conference on Advances in Communication and Control Systems(*CAC2S). Atlantis Press, pp. 129-133.

Singh, P., & Chadha, R. S. (2013). A Survey of Digital Watermarking Techniques, Applications and Attacks. *International Journal of Engineering and Innovative Technology (IJEIT)*, *2*(9), pp. 709-716.

Song, C., Sudirman, S., & Merabti, M. (2010). A Spatial and Frequency Domain Analysis of the Effect of Removal Attacks on Digital Image Watermarks. *Proc of 11th conf of Post Graduate Network Symposium*, pp. 119-124.

Song, C., Sudirman, S., Merabti, M., & Llewellyn-Jones, D. (2010). Analysis of digital image watermark attacks. *Proceedings of the 7th IEEE in conference on Consumer communications and networking conference*. IEEE Press, pp. 941-945.

Tsui, T. K., Zhang, X. P., & Androutsos, D. (2008). Color image watermarking using multidimensional Fourier transforms. *Information Forensics and Security, IEEE Transactions*, 3(1), pp.16-28.