

**2011-2012**

Prepared by: Amal Haj Ali Maleka Hanhan Submitted To: Dr. Allam Mousa

AN-Najah National University

Faculty of Engineering

Electrical Engineering Department

Graduation Project

Digital Image Watermarking



Table of Contents

[Table of Figures 4](#_Toc312013121)

[ACKNOWLEDGEMENT 5](#_Toc312013122)

[List of Acronyms 6](#_Toc312013123)

[List of Symbols 6](#_Toc312013124)

[Chapter1: Introduction 8](#_Toc312013125)

[History of watermarking 11](#_Toc312013126)

[Requirements for watermarking algorithms: 12](#_Toc312013127)

[Importance of Digital Watermarking 13](#_Toc312013128)

[Aims 14](#_Toc312013129)

[Classification of digital watermark 14](#_Toc312013130)

[Visible watermarks 14](#_Toc312013131)

[Invisible watermark 14](#_Toc312013132)

[Applications of digital watermarking 15](#_Toc312013133)

[Digital watermarking technology for rights management 15](#_Toc312013134)

[Digital watermarking technology for authentication and tamper proofing 15](#_Toc312013135)

[Visible reversible watermarking for electronic distribution 16](#_Toc312013136)

[Watermarking as Communication System 16](#_Toc312013137)

[DISTORIONS AND ATTACKS 17](#_Toc312013138)

[Removal attacks 17](#_Toc312013139)

[Geometrical attacks 18](#_Toc312013140)

[Cryptographic attacks 19](#_Toc312013141)

[Protocol attacks 19](#_Toc312013142)

[Quality Measurements 20](#_Toc312013143)

[Chapter2: DWT Image watermarking 21](#_Toc312013144)

[DWT Domain Watermarking 22](#_Toc312013145)

[Simulation results 23](#_Toc312013146)

[First Level Decomposition 24](#_Toc312013147)

[Chapter3: DCT Image watermarking 29](#_Toc312013148)

[Introduction 30](#_Toc312013149)

[INSERTION OF WATERMARK 30](#_Toc312013150)

[Simulation result 31](#_Toc312013151)

[Chapter4: FFT Image watermarking 34](#_Toc312013152)

[INSERTION OF WATERMARK 35](#_Toc312013153)

[Extracted of watermark 35](#_Toc312013154)

[Simulation result 36](#_Toc312013155)

[Comparison between DCT and FFT 39](#_Toc312013156)

Conclusions………………………………………..…………………………………………………………………………………….42

Appindex………………………………………….……………………………………………………………………………………….43

Referances……………………………………….……………………………………………………………………………………….45

# Table of Figures

[Figure 1: Image showing an INR 100 note having watermark at its left side which is considerably visible when note hold under light 9](#_Toc312010423)

[Figure 2: watermarking system 10](#_Toc312010424)

[Figure 3: Watermark system in DWT 21](#_Toc312010425)

[Figure 4: DWT decomposition with two levels 21](#_Toc312010426)

[Figure 5: a) Cover Image b) Watermark Image 23](#_Toc312010427)

[Figure 6: Watermarking image in LL, LH, HL and HH bands 24](#_Toc312010428)

[Figure 7: watermark extracted from the LL, LH, HL and HH bands 25](#_Toc312010429)

[Figure 8: Attacks on the watermarked image on LL band 26](#_Toc312010430)

[Figure 9: Watermarks recovered from the LL band after attacks 27](#_Toc312010431)

[Figure 10: Watermark insertion Process 30](#_Toc312010432)

[Figure 11: a) Host Image b) Watermark Image 30](#_Toc312010433)

[Figure 12: Watermarked image without attacks and with different type of attacks 31](#_Toc312010434)

[Figure 13: Extracted watermark after each attack 32](#_Toc312010435)

[Figure 14: Watermark embedding using FFT 35](#_Toc312010436)

[Figure 15: a) Cover Image b) Watermark Image 35](#_Toc312010437)

[Figure 16: Watermarking Images after different types of attacks 36](#_Toc312010438)

[Figure 17: Extracted watermark after different types of attacks 37](#_Toc312010439)

[Figure 18: insertion and retrieval of watermark 39](file:///C:\Users\StarNet\Desktop\finally\ANn%20(Repaired).docx#_Toc312010440)

# ACKNOWLEDGEMENT

Our heart pulsates with the thrill for tendering gratitude to those persons who helped us in completion of the project.

The most pleasant point of presenting a thesis is the opportunity to thank those who have contributed to it. Unfortunately, the list of expressions of thank no matter how extensive is always incomplete and inadequate. Indeed this page of acknowledgment shall never be able to touch the horizon of generosity of those who tendered their help to us.

First and foremost, we would like to express our gratitude and indebtedness to Dr.Allam Mousa, for his kindness in allowing us for introducing the present topic and for his inspiring guidance, constructive criticism and valuable suggestion throughout this project work. We are sincerely thankful to him for his able guidance and pain taking effort in improving our understanding of this project. We are also grateful to everyone taught us in the Department of Electrical Engineering.

An assemblage of this nature could never have been attempted without reference to and inspiration from the works of others whose details are mentioned in reference section. we acknowledge our indebtedness to all of them.

Last but not least, our sincere thanks to all our friends and our family who have patiently extended all sorts of help for accomplishing this undertaking.

# List of Acronyms

Acronym Description

DCT Discrete Cosine Transformation

DWT Discrete Wavelet Transformation

FFT Fast Fourier Transformation

JPEG Joint Photographic Expert Group

SNR Signal-to-noise Ratio

IDCT Inverse Discrete Cosine Transform

IFFT Inverse Fast Fourier Transformation

IDWT Inverse Discrete Wavelet Transformation

SR Similarity Ratio

QF Quality Factor

# List of Symbols

Symbol Description

Embedding factor or scaling factor

Cover image (host image)

Watermark image

Watermarked image

Abstract

Today’s world is digital world. Nowadays, in every field there is enormous use of digital contents. Information handled on internet and multimedia network system is in digital form. The copying of digital content without quality loss is not so difficult. Due to this, there are more chances of copying of such digital information. So, there is great need of prohibiting such illegal copyright of digital media. Digital watermarking (DWM) is the powerful solution to this problem. Digital watermarking is nothing but the technology in which there is embedding of various information in digital content which we have to protect from illegal copying. This embedded information to protect the data is embedded as watermark. Beyond the copyright protection, Digital watermarking is having some other applications as fingerprinting, owner identification etc. Digital water-marks are of different types as robust, fragile, visible and invisible .Application is depending upon these watermarks classifications. There are some requirements of digital watermarks as integrity, robustness and complexity.

In digital watermarking, a watermark is embedded into a cover image in such a way that the resulting watermarked signal is robust to certain distortion caused by either standard data processing in a friendly environment or malicious attacks in an unfriendly environment. This project presents a digital image watermarking based on two dimensional discrete wavelet transform (DWT2), two dimensional discrete cosines transform (DCT2) and two dimensional fast Fourier transform (FFT2). Signal to noise ratio (SNR) and similarity ratio (SR) are computed to measure image quality for each transform.

Chapter 1

Introduction

Introduction

We are living in the era of information where billions of bits of data is created in every fraction of a second and with the advent of internet, creation and delivery of digital data (images, video and audio files, digital repositories and libraries, web publishing) has grown many fold. Since copying a digital data is very easy and fast too so, issues like, protection of rights of the content and proving ownership, arises. Digital watermarking came as a technique and a tool to overcome shortcomings of current copyright laws for digital data. The specialty of watermark is that it remains intact to the cover work even if it is copied. So to prove ownership or copyrights of data watermark is extracted and tested. It is very difficult for counterfeiters to remove or alter watermark. As such the real owner can always have his data safe and secure. Our aim was to study different watermarking techniques and implement the one which is most resistant to all types of attack, scalar or geometric. Counterfeiters try to degrade the quality of watermarked image by attacking an image (generally attacks are median and Gaussian filter, scaling, compression and rotation of watermarked image).By attacking watermarked image it become very difficult to recover watermark back from the watermarked image and even if it extracted one may no longer use it to prove the ownership and copyrights. So our main idea was to find such regions, also known as patches, in an image which are very stable and resistant to attacks. The report is divided mainly in 4 chapters Wavelet Image Watermarking (chapter2), DCT Image watermarking (chapter3), FFT Image watermarking (chapter4), and conclusions.

This chapter gives full insight of digital watermarking, its history, requirements, application and possible attacks. The first subheading tells how, with information revolution, the need to have some technique to prevent piracy and illegal copying of data arises. This need give rise to a new technique, known as Digital Watermarking. While proposing any algorithm some parameters are needed to keep in mind on which the proposed algorithm must be consistent. These parameters are discussed in following section. Following sections are dedicated to watermarking application and attacks. A lot of work is going on for making watermarking techniques immune towards attack to retain the originality of watermark and assuring successful extraction of watermark with low error probabilities so to sort out disputes, if any, over copyrights or ownership.

Overview

Hold an Rs100 note up or your offer letter up to light. What you will see is a picture of Mahatma Gandhi or company’s logo respectively. This is what is known as a watermark mainly used to prove the ownership (in case of offer letter, watermark prove that the document is of facial document of company meant for official work) or authenticity (in case of Rs 100, watermark rule out the forgery and authenticate the piece of paper of its worth).The watermark on the Rs100 (Figure1), just like most paper watermarks today, has two properties. 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) [1].



Figure 1: Image showing an INR 100 note having watermark at its left side which is considerably visible when note hold under light

Thus, watermarking is defined as, *“*the *process of possibly irreversibly embedding information into a digital signal. The signal may be audio, pictures or video”.*

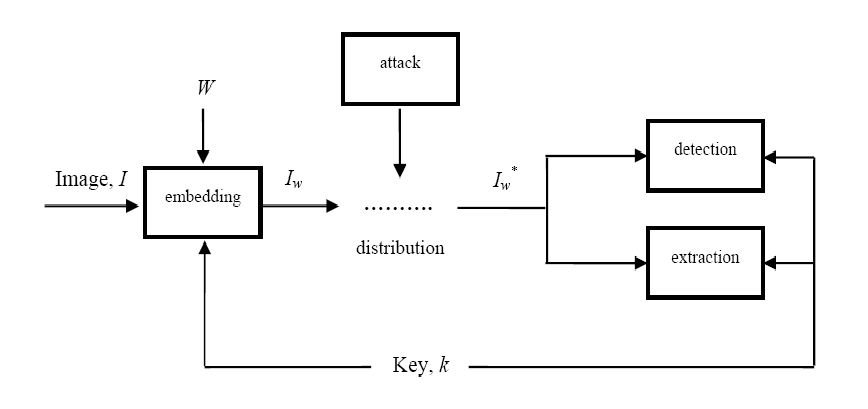


Figure 2: watermarking system

The components of a watermark embedding/detection/extraction system are shown in Figure 2.The embedded data can be detected in, or extracted from, a multimedia element in an application.

## History of watermarking

Although the art of papermaking was invented in China over one thousand years earlier, paper watermarks did not appear until about 1282, in Italy. The marks were made by adding thin wire patterns to the paper molds. The paper would be slightly thinner where the wire was and hence more transparent. The meaning and purpose of the earliest watermarks are uncertain. They may have been used for practical functions such as identifying the molds on which sheets of papers were made, or as trademarks to identify the paper maker. On the other hand, they may have represented mystical signs, or might simply have served asdecoration. By the eighteenth century, watermarks on paper made in Europe andAmerica had become more clearly utilitarian. They were used as trademarks,

To record the date the paper was manufactured, and to indicate the sizes of original sheets. It was alsoabout this time that watermarks began to be used as anticounterfeiting measures on moneyand other documents. The term watermark seems to have been coined near the end of the eighteenth century and may have been derived from the German term was sermarke (though it could also be that the German word is derived from the English). The term is actually a misnomer, in that water is not especially important in the creation of the mark. It was probably given because the marks resemble the effects of water on paper. About the time the term watermark was coined, counterfeiters began developing methods of forging watermarks used to protect paper money. Counterfeiting prompted advances in watermarking technology. William Congreve, an Englishman, invented a technique for making color watermarks by inserting dyed material into the middle of the paper during papermaking. The resulting marks must have been extremely difficult to forge, because the Bank of England itself declined to use them on the grounds that they were too difficult to make. A more practical technology was invented by anotherEnglishman,WilliamHenrySmith.Thisreplacedthe fine wire patterns used to make earlier marks with a sort of shallow relief sculpture, pressed into the paper mold. The resulting variation on the surface of the mold produced beautiful watermarks with varying shades of gray. This is the basic technique used today for the face of President Jackson on the $20 bill. Four hundred years later, in 1954, Emil Hembrooke of the Muzak Corporation filed a patent for “watermarking” musical Works. An identification code was inserted in music by intermittently applying a narrow notch filter centered at 1 kHz. The absence of energy at this frequency indicated that the notch filter had been applied and the duration of the absence used to code either a dot or a dash. The identification signal used Morse code. It is difficult to determine when digital watermarking was first discussed. In 1979, Szepanski described a machine-detectable pattern that could be placed on documents for anti-counterfeiting purposes. Nine years later, Holt described a method for embedding an identification code in an audio signal. However, it was Komatsu and to minaga, in 1988, which appear to have first used the term digital watermark. Still, it was probably not until the early1990s that the term digital watermarking really came into vogue. About 1995, interest in digital watermarking began to mushroom. In addition, about this time, several organizations began considering watermarking technology for inclusion in various standards. The Copy Protection Technical Working Group (CPTWG) tested watermarking systems for protection of video on DVD disks. The Secure Digital Music Initiative (SDMI) made watermarking a central component of their system for protecting music. Two projects sponsored by the European Union, VIVA and Talisman, tested watermarking for broadcast monitoring. The International Organization for Standardization (ISO) took an interest in the technology in the context of designing advanced MPEG standards. In the late 1990s several companies were established to market watermarking products. More recently, a number of companies have used watermarking technologies for a variety of applications [1].

## Requirements for watermarking algorithms:

A watermarking algorithm should be consistent over following properties and parameters:

* Transparency: The most fundamental requirement for any Watermarking method shall be such that it is transparent to the end user. The watermarked content should be consumable at the intended user device without giving annoyance to the user. Watermark only shows up at the watermark-detector device.
* Security: Watermark information shall only be accessible to the authorized parties. Only authorized parties shall be able to alter the Watermark content. Encryption can be used to prevent unauthorized access of the watermarked data
* Ease of embedding and retrieval: Ideally, Watermarking on digital media should be possible to be performed “on the fly”. The computation need for the selected algorithm should be minimum.
* Robustness: Watermarking must be robust enough to withstand all kinds for signal processing operations, “attacks” or unauthorized access. Any attempt, whether intentional or not, that has a potential to alter the data content is considered as an attack. Robustness against attack is a key requirement for Watermarking and the success of this technology for copyright protection depends on this.
* Effect on bandwidth: Watermarking should be done in such a way that it doesn’t increase the bandwidth required for transmission. If Watermarking becomes a burden for the available bandwidth, the method will be rejected.
* Interoperability: Digitally watermarked content shall still be interoperable so that it can be seamlessly accessed through heterogeneous networks and can be played on various plays out devices that may be watermark aware or unaware.

## Importance of Digital Watermarking

The sudden increase in watermarking interest is most likely due to the increase in concern over copyright protection of content. The Internet had become user friendly with the introduction of Marc Andreessen’s Mosaic web browser in November 1993, and it quickly became clear that people wanted to download pictures, music, and videos. The Internet is an excellent distribution system for digital media because it is inexpensive, eliminates warehousing and stock, and delivery is almost instantaneous. However, content owners (especially large Hollywood studios and music labels) also see a high risk of piracy. This risk of piracy is exacerbated by the proliferation of high-capacity digital recording devices. When the only way the averagecustomer could record a song or a movie was on analog tape, pirated copies were usually of a lower quality than the originals, and the quality of second-generation pirated copies (i.e., copies of a copy) was generally very poor. However, with digital recording devices, songs and movies can be recorded with little, if any, degradation in quality. Using these recording devices and using the Internet for distribution, would-be pirates can easily record and distribute copyright protected material without appropriate compensation being paid to the actual copyright owners. Thus, content owners are eagerly seeking technologies that promise to protect their rights. The first technology content owners turn to is cryptography. Cryptography is probably the most common method of protecting digital content. It is certainly one of the best developed as a science. The content is encrypted prior to delivery, and a decryption key is provided only to those who have purchased legitimate copies of the content. The encrypted file can then be made available via the Internet, but would be useless to a pirate without an appropriate key. Unfortunately, encryption cannot help the seller monitor how a legitimate customer handles the content after decryption. A pirate can actually purchase theproduct, use the decryption key to obtain an unprotected copy of the content, and thenproceed to distribute illegal copies. In other words, cryptography can protect content intransit, but once decrypted, the content has no further protection. Thus, there is a strong needfor an alternative or complement to cryptography: a technology that can protect content even after it is decrypted. Watermarking has the potential to fulfill this need because it places information within the content where it is never removed during normal usage. Decryption, re encryption, compression, digital-to-analog conversion, and file format changes a watermark can be designed to survive all of these processes. Watermarking has been considered for many copy prevention and copyright protection applications. In copy prevention, the watermark maybe used to inform software or hardware devices that copying should be restricted. In copyright protection applications, the watermark may be used to identify the copyright holder and ensure proper payment of royalties. Although copy prevention and copyright protection have been major driving forces behind research in the watermarking field, there is a number of other applications for which watermarking has been used or suggested. These include broadcast monitoring, transaction tracking, authentication (with direct analogy to our Rs100 example), copy control, and device control [1].

# Aims

An effective authentication scheme should have the following desirable features:

1. To be able to determine whether an image has been altered or not.
2. To be able to locate any alteration made on the image.
3. To be able to integrate authentication data with host image rather than as a separate data file.
4. The embedded authentication data be invisible under normal viewing conditions.
5. To allow the watermarked image be stored in lossy- compression format [3].

# Classification of digital watermark

Some of the important types of watermarking based on different watermarks are given below:

## Visible watermarks

Visible watermarks are an extension of the concept of logos. Such watermarks are applicable to images only. These logos are inlaid into the image but they are transparent. Such watermarks cannot be removed by cropping the center part of the image. Further, such watermarks are protected against such as statistical analysis.

The drawbacks of visible watermarks are degrading the quality of image and detection by visual means only. Thus, it is not possible to detect them by dedicated programs or devices. Such watermarks have applications in maps, graphics and software user interface.

Invisible watermark

invisible watermark is hidden in the content. It can be detected by an authorized agency only. Such watermarks are used for content and /or author authentication and for detecting unauthorized copier.

* **Robust Watermark**
  + Embedded invisible watermarks.
  + Resist to image processing or attacks.
  + Used for copyright protection or to verify the ownership.
* **Fragile Watermark**

Fragile watermarks are those watermarks which can be easily destroyed by any attempt to tamper with them. Fragile watermarks are destroyed by data manipulation. In the following figure an example of fragile watermarking the first one represent the original image, the second is the modified image and the third the detected modification.

* **Semi Fragile Watermark**
  + Sensitive to signal modification.
  + Feature of both robust & Fragile watermark.
  + Provides data authentication.

Besides watermark robustness, watermark can also categorized into visible and invisible types, visible watermarks are perceptible to a viewer. On the other hand, invisible watermarks are imperceptible and don’t change the visual of the images. In our project, we are interested in invisible watermarks because they have a wider range of applications compared to visible watermarks[4].

# Applications of digital watermarking

## Digital watermarking technology for rights management

One of the traditional applications of the watermark is copyright protection. The primary reason for using watermarks is to identify the owner of the content by an invisible hidden “mark” that is imprinted into the image. In many cases, the watermark is used in addition to the content encryption, where the encryption provides the secure distribution method from digital watermarking. the content owners to the receivers, and the watermark offers the content owners the opportunity to trace the contents and detect the unauthorized use or duplications. Without watermarking, there is no way to extend the control of the content owner once the content leaves the protected digital domain and is released to the user. Digital watermark is used to extend the protection and provide the opportunities for the content owners to protect the rights and properties of the electronic distributed contents. The signature of the owner, content ID and usage limitation can be imprinted into the contents, and stay with the contents as far as it travels. This mechanism extends the opportunity of protecting the contents after the release of the contents to the open environment. The major technical requirements for this application are as follows:

* The watermark does not incur visible (or audible) artifacts to the ordinary users.
* The watermark is independent of the data format.
* The information carried by the watermark is robust to content manipulations, compression, and so on.
* The watermark can be detected without the un watermarked original content.
* The watermark can be identified by some kind of “keys” that are used to identify large number of individual contents uniquely.

## Digital watermarking technology for authentication and tamper proofing

Another application of digital watermark is contents authentication and tamper proofing. The objective is not to protect the contents from being copied or stolen, but is to provide a method to authenticate the image and assure the integrity of the image. Since low-end digital camera arrived to the consumer market, it rapidly expanded to a number of industrial applications as well, because the use of a digital image is far more cost effective and can also save time and cost for the Developing/ Printing/Exposing (DPE) compared to the traditional chemical photos. However, there are some critical issues for some particular applications, where the photos are used as evidence or the material for some kind of business judgment. For instance, automobile insurance companies sometimes use photos of the damaged car sent by the repair shop to estimate the repair cost. A shift to digital photos will save a great amount of time and money for these kinds of processes. However, the digital photos might be altered to exaggerate damage, or even made up from nothing, since the modification of the digital image is getting much easier with some advanced photo-retouching tools be available. This could result in large amounts of extra payment for the insurance company, or more seriously, undermine the credibility of the insurance company itself. A type of digital watermark, called tamper-detect watermark, might resolve this problem, and provide a secure environment for the evidence photos. The way to realize this feature is to embed a layer of the authentication signature into the subject digital image using a digital watermark. This additional layer of watermark is used as a “sensor” to detect the alteration. Our recent implementation can even detect the location of the alteration from the altered image itself. Through a joint study with a major Japanese insurance company, we confirmed the technical feasibility of the technology for the above-mentioned industrial applications. The technical requirements for this application are as follows:

* Invisible to the ordinary users.
* Applicable to compressed image format (most digital cameras use JPEG compatible format).
* Sensitive to content manipulations, compression, and so on.

## Visible reversible watermarking for electronic distribution

Unlike other digital watermarking technologies described above, the visible reversible watermark is visible. It is available as a commercial product . This unique form of watermarking technology by IBM allows the content owners to embed a visible shape or logo mark such as company’s logo on top of the image. The mark is removed (the watermark is reversed) only with the application of an appropriate “decryption” key and watermark remover software. This mark is applied by modifying the Discrete Cosine Transformation (DCT) coefficients of the JPEG compressed image following certain pre-defined rule and visual effect analysis result to make it half transparent, but not totally destructive. The key, with the mark removal program, will be used to remove the mark from the image. The removal of the visible mark may be tied up with the embedding of another invisible mark for the tracking purpose. With this visible watermark on the image, the content becomes self-protective, and content owners can distribute the entire image as a sample to various open media or to the Internet. When a user wants to use a clean copy of the image, all he/she needs to be is to request a “decryption” key and pay some fee for it. This will reduce the security risk and the amount of the data transmission per each buy/sell transaction[5].

# Watermarking as Communication System

Watermarking system can be viewed as some form of communication. The payload message *P*, encoded as a watermark *W*, is modulated and transmitted across a communication channel to the watermark detector. In this model, the cover work represents a communication channel and therefore it can be viewed as one source of noise. The other source of noise is a distortion caused by normal signal processing and attacks. Modeling watermarking as communication is important because it makes it possible to apply various communication system techniques, such as modulation, error correction, coding, spread spectrum communication, matched filtering, and communication with side information, to watermarking. Those techniques could be used to help design key building blocks of a watermarking system which deal with the following:

How to embed and detect one bit.

What processing/embedding domain to use.

How to use side information to ensure imperceptibility.

How to use modulation and multiplexing techniques to embed multiple bits.

How to enhance robustness and security, where robustness can be defined as a watermark resistance to normal signal processing, and security can be defined as a watermark resistance to intentional attacks [6].

# DISTORIONS AND ATTACKS

First of all, we have to distinguish two “reasons” or “purposes” for an attack against a watermark image:

• Hostile or malicious attacks, which are an attempt to weaken, remove or alter the watermark, and

• Coincidental attacks, which can occur during common image processing and are not aimed at tampering with the watermark. Lossy image compression is considered the most common form of attack a watermarking scheme has to withstand. The harsh term “attack” can be easily justified: an efficient image compression has to suppress or discard perceptually irrelevant information the invisible watermark. A wide range of attacks has been described in the literature . The following four large categories of attacks can be invoked to penetrate a watermarking system:

• Removal attacks

• Geometrical attacks

• Cryptographic attacks

• Protocol attacks

## Removal attacks

**Removal (simple) attacks** attempt to separate and remove the watermark. If somebody tries to remove the watermark from the data, this is called a removal attack. The means employed most frequently are filter models taken from statistical signal theory. Denoising the marked image through median or high-pass filtering as well as nonlinear truncation or spatial watermark prediction are methods considered very likely to succeed. The goal is to add distortion to the host image in order to render the watermark undetectable or unreadable [4]. The attack is successful if the watermark cannot be detected anymore, but the image is still intelligible and can be used for a particular determined purpose. Many such attack operations have been proposed:

• Lossy image compression (JPEG, JPEG 2000)

• Addition of Gaussian noise

• Denoising

• Filtering

• Median filtering and blurring

• Signal enhancement (sharpening, contrast enhancement)

**Compression**: this is generally an unintentional attack, which appears very often in multimedia applications. Practically all images currently being distributed via Internet have been compressed. the watermark is required to resist different levels of compression, it is usually advisable to perform the watermark embedding in the same domain where the compression takes place. For instance, the Discrete Cosine Transform (DCT) domain image watermarking is more robust to Joint Photograph Expert Group (JPEG) compression than the spatial-domain watermarking. Also, the Discrete Wavelet Domain (DWT) domain watermarking is robust to JPEG 2000 compression.

**Additive noise**: a random signal with a given distribution (e.g. Gaussian, uniform, Poisson, Bernoulli) is added to the image unintentionally. In certain applications the additive noise may originate from Digital-to-Analog (D/A) and A/D converters, or as a consequence of transmission errors. However, an attacker may introduce perceptually shaped noise (image-dependent mask) with the maximum unnoticeable power. This will typically force to increase the threshold at which the correlation detector operates.

**Denoising explores** the idea that a watermark is an additive noise (which can be modeled statistically) relative to the original image. These attacks include: local median, midpoint, trimmed mean filtering, Wiener filtering, as well as hard and soft thresholding.

**Filtering attacks** are linear filtering: high-pass, low pass, Gaussian and sharpening filtering, etc. Low-pass filtering, for instance doesn’t introduce considerable degradation in watermarked images, but can dramatically affect the performance since spread-spectrum-like watermarks have non negligible high-frequency spectral contents. To design a watermark robust to a known group of filters that might be applied to the watermarked image, the watermark message should be designed in such a way to have most of its energy in the frequencies which filters change the least.

**Statistical averaging**: the aim of these attacks is retrieving the host image and/or watermark by statistical analysis of multiple marked data sets. An attacker may try to estimate the watermark and then to “unwatermark” the object by subtracting the estimation. This is dangerous if the watermark doesn’t depend substantially on data. This is a good reason for using perceptual masks to create a watermark. In this group of attacks belong the averaging and collusion attacks. Averaging attack consists of averaging many instances of a given data set each time marked with a different watermark. In this way an estimate of the host data is computed and each of the watermarks is weakened. Collusion attack consists of averaging different host data containing the same watermark. The resulting signal may serve as a good estimate of the watermark, which can be used to remove it from the watermarked data.

## Geometrical attacks

These attacks are not aimed at removing the watermark, but try to either destroy it or disable its detection. They attempt to break the correlation detection between the extracted and the original watermark sequence, where the image is subjected to translation, rotation, scaling and/or cropping. This can be accomplished by “shuffing” the pixels. The values of corresponding pixels in the attacked and the original image are the same. However, their location has changed. These attacks can be subdivided into attacks applying general affine transformations and attacks based on projective transformation. Cropping 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 or frames of video sequence. With this in mind, in order to survive, the watermark needs to be spread over the dimensions where this attack takes place.

**Mosaic attack.** This point is emphasized by a “presentation” attack, which is of quite general applicability and which possesses the initially remarkable property that a marked image can be unmarked and yet still rendered pixel for pixel in exactly the same way as the marked image by a standard browser. The attack was motivated by a fielded automatic system for copyright piracy detection, consisting of a watermarking scheme plus a web crawler that downloads pictures from the net and checks whether they contain a watermark. It consists of chopping an image up into a number of smaller sub images, which are embedded in a suitable sequence in a web page. Common web browsers render juxtaposed sub images stuck together, so they appear identical to the original image, which is shown in Fig. 3. This attack appears to be quite general; all marking schemes require the marked image to have some minimal size (one cannot hide a meaningful mark in just one pixel). Thus by splitting an image into sufficiently small pieces, the mark detector will be confused. The best that one can hope for is that the minimal size could be quite small and the method might therefore not be very practical.

## Cryptographic attacks

Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks. One such technique is brute-force search for the embedded secret information. Practically, application of these attacks is restricted due to their high computational complexity. They cover, for example, direct attacks to find the secret key or attacks called collusion attacks. Cryptographic attacks are very similar to the attacks used in cryptography. There are the brute force attacks, which aim at finding secret information through an exhaustive search. Since many watermarking schemes use a secret key, it is very important to use keys with a secure length. Another attack in this category is so-called Oracle attack which can be used to create a non-watermarked image when a watermark detector device is available.

## Protocol attacks

Protocol attacks neither aim at destroying the embedded information nor at disabling the detection of the embedded information (deactivation of the watermark). Rather, they take advantage of semantic deficits of the watermark’s implementation. The protocol attacks aim at attracting the concept of the watermarking application. The first protocol attack was proposed by Craveret al. They introduced the framework of invertible watermark and showed that for copyright protection applications watermarks need to be non-invertible. The idea of inversion consists of the fact that an attacker who has a copy of the stego-data can claim that the data contains also the attacker’s watermark by subtracting his own watermark. This can create a situation of ambiguity with respect to the real ownership of the data. The requirement of non-invertability on the watermarking technology implies that it should not be possible to extract a watermark from non-watermarked image. As a solution to this problem, the authors proposed to make watermarks signal-dependent by using a one-way function. Consequently, a watermark must not be invertible or to be copied. A copy attack, for example, would aim at copying a watermark from one image into another without knowledge of the secret key. It also belongs to the group of the protocol attacks. In this case, the goal is not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data [7].

In our work we use removal attacks to compare between the different techniques, we compress the watermarking image using JPEG compression; also we add Gaussian noise and salt and peppers noise to the watermarking image and then we filtering it using median filter.

# Quality Measurements

In order to evaluate the quality of watermarked image, the following signal-to-noise ratio (SNR) equation is used:

OR,

The number of mismatched data between the embedded watermark and the extracted watermark is used to represent the similarity of watermarks. The similarity factor of extracted watermark and original watermark is computed by the following:

Where and represent the original watermark image and the extracted watermark image, respectively, M and N represent the image size. The magnitude range of SF is [0, 1]. SF is near or equals to 1, the extracted watermark is more effective extraction. In general, it is considered acceptable that SF is 0.75 or above.

Chapter 2

DWT Image watermarking

# DWT Domain Watermarking

Wavelet transform is a time domain localized analysis method with the window’s size fixed and forms convertible. There is quite good time differentiated rate in high frequency part of signals DWT transformed. Also there is quite good frequency differentiated rate in its low frequency part. It can distill the information from signal effectively. The basic idea of discrete wavelet transform (DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district .Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low frequency district(LL) and three high-frequency districts(LH,HL,HH). If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. The following figure represents the watermarking system in DWT [8]:

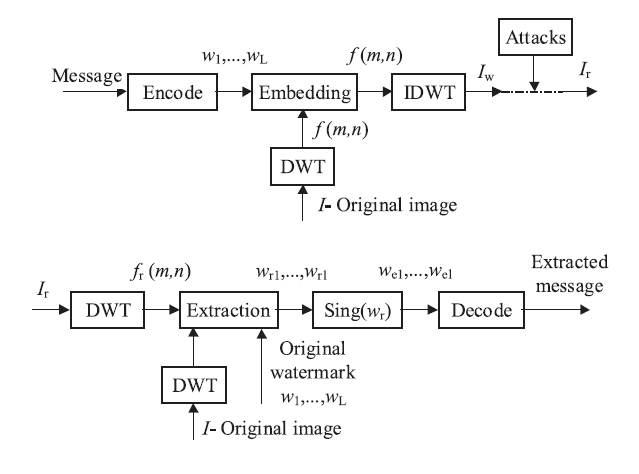


Figure 3: Watermark system in DWT

In two-dimensional separable dyadic DWT, each level of decomposition produces four bands of data, one corresponding to the low pass band (LL), and three other corresponding to horizontal (HL), vertical (LH), and diagonal (HH) high pass bands. The decomposed image shows a coarse approximation image in the lowest resolution low pass band, and three detail images in higher bands. The low pass band can further be decomposed to obtain another level of decomposition. This process is continued until the desired number of levels determined by the application is reached [2].

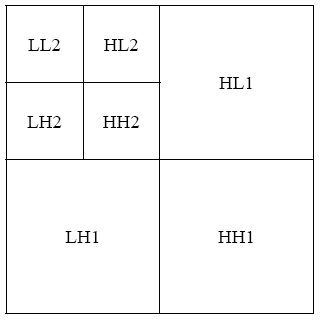


Figure 4: DWT decomposition with two levels

The proposed watermarking system is given in the following process:

**Embedding watermarking**

**Input:** Cover image, watermark image.

**Process:**

1. using two-dimensional separable dyadic DWT, obtain the first level decomposition of the cover image *I*.

2. Modify the DWT coefficientsin the LL band:

3. Apply inverse DWT to obtain the watermarked cover Image, *Iw.*

**Output:** Watermarked image.

**Extracting watermarking**

**Input:** Watermarked cover image.

**Process:**

1. using two-dimensional separable dyadic DWT, obtain the first level decomposition of the watermarked (and possibly attacked) cover image .

2. Extract the binary visual watermark from the LL band:

**Output:** watermark image.

# Simulation results

Since the magnitudes of DWT coefficients are larger in the lowest band at each level of decomposition, it is possible to use a larger scaling factor for watermark embedding. For the other 3 bands, the DWT coefficients are smaller, allowing a smaller scaling factor to be used. The resulting watermarked image does not have any degradation leading to a loss in its commercial value. In the below experiments, we measured the visual quality of watermarked and attacked images using the Signal To-Noise Ratio (SNR), SNR measures are estimates of the quality of the reconstructed image compared with an original image. The fundamental idea is to compute the value which reflects the quality of the reconstructed image. Reconstructed image with higher metric are judged as having better quality.

The visual quality of extracted visual watermarks is measured by the Similarity Factor (SF). The DWT was performed using Matlab with the wavelet filter. The chosen attacks were JPEG compression (with 3 quality factors), also we measured a compression ratio (CR) it defined by compression Ratio=image bytes/compressed bytes.

For first levels of decomposition, the proposed watermarking scheme was tested using six types of attacks. The DWT was performed using Matlab. The chosen attacks were JPEG compression (with 3 quality factors), blurring, adding Gaussian noise, filtering, histogram equalization, intensity adjustment and rotation. The scaling factor we use it with three different values 0.09, 0.5 and 0.8.

The following data calculated from run matlab code for DWT watermarking for different value of quality factor and alpha (gain).

## First Level Decomposition

Figure 5 shows the 256x256 gray scale cover image Cameraman and 128x128 visual watermark copyright.

Figure 5: a) Cover Image b) Watermark Image

The watermarked image in LL, LH, HL and HH bands are presented respectively in Figure 6 for different value of scaling factors and different quality factors, and the number below each image denotes the SNR value.

Figure 7 contains the watermarks extracted from the four bands for each value of alpha and QF. The numbers below the images are the SF values. According to Figure 7 we can note that watermark embedding in the LL band is most resistant to JPEG compression than other bands.

The attacked images are presented in Figure 8 together with the tools and parameters used for the attacks. The number next to the label below each image denotes the SNR value. Figure 9 contains the watermarks extracted from the LL band for each of the attacks. The numbers next to the images are the SF values. According to Figure 8 and Figure 9, it is possible to note the resistance of watermarked image for each attack using either subjective human evaluation or objective SF.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | |  |  | | SNR=21.2103 | SNR=21.7414 | |  |  | | SNR=19.9011 | SNR= 21.2960 | | |  |  | | --- | --- | |  |  | | SNR= 21.7846 | SNR=20.9185 | |  |  | | SNR= 21.5097 | SNR= 20.2804 | | |  |  | | --- | --- | |  |  | | SNR= 22.3557 | SNR=21.7990 | |  |  | | SNR= 21.7980 | SNR= 21.7985 | |
| JPEG 60 , alpha=0.09 | JPEG 80 , alpha=0.09 | JPEG 100 , alpha=0.09 |
| |  |  | | --- | --- | |  |  | | SNR=9.5809 | SNR=7.7289 | |  |  | | SNR=7.8155 | SNR=7.8995 | | |  |  | | --- | --- | |  |  | | SNR=9.5944 | SNR=7.7605 | |  |  | | SNR=7.8104 | SNR= 7.7374 | | |  |  | | --- | --- | |  |  | | SNR=9.6126 | SNR=7.7757 | |  |  | | SNR=7.7747 | SNR= 7.7772 | |
| JPEG 60 , alpha=0.5 | JPEG 80 , alpha=0.5 | JPEG 100 , alpha=0.5 |
| |  |  | | --- | --- | |  |  | | SNR=7.2860 | SNR=4.7894 | |  |  | | SNR=4.7978 | SNR= 4.7805 | | |  |  | | --- | --- | |  |  | | SNR=7.2937 | SNR=4.8100 | |  |  | | SNR=4.8029 | SNR= 4.8017 | | |  |  | | --- | --- | |  |  | | SNR=7.2941 | SNR=4.8041 | |  |  | | SNR=4.8062 | SNR= 4.8085 | |
| JPEG 60 , alpha=0.8 | JPEG 80 , alpha=0.8 | JPEG 100 , alpha=0.8 |

Figure 6: Watermarking image in LL, LH, HL and HH bands

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | |  |  | | SF= 0.8521 | SF=0.4917 | |  |  | | SF=0.8788 | SF= 0.3811 | | |  |  | | --- | --- | |  |  | | SF=0.8728 | SF=0.8886 | |  |  | | SF=0.7940 | SF=0.9052 | | |  |  | | --- | --- | |  |  | | SF=0.999 | SF=1 | |  |  | | SF=1 | SF=1 | |
| JPEG 60 , alpha=0.09 | JPEG 80 , alpha=0.09 | JPEG 100 , alpha=0.09 |
| |  |  | | --- | --- | |  |  | | SF=0.9937 | SF=0.7698 | |  |  | | SF=0.7770 | SF=0.7808 | | |  |  | | --- | --- | |  |  | | SF=0.9941 | SF=0.7785 | |  |  | | SF=0.7798 | SF=0.7797 | | |  |  | | --- | --- | |  |  | | SF=0.9941 | SF=0.7841 | |  |  | | SF=0.7809 | SF=0.7836 | |
| JPEG 60 , alpha=0.5 | JPEG 80 , alpha=0.5 | JPEG 100 , alpha=0.5 |
| |  |  | | --- | --- | |  |  | | SF=0.8016 | SF=0.7502 | |  |  | | SF=0.7544 | SF=0.7444 | | |  |  | | --- | --- | |  |  | | SF=0.8030 | SF=0.7569 | |  |  | | SF=0.7586 | SF=0.7570 | | |  |  | | --- | --- | |  |  | | SF=0.7996 | SF=0.7580 | |  |  | | SF=0.7602 | SF=0.7618 | |
| JPEG 60 , alpha=0.8 | JPEG 80 , alpha=0.8 | JPEG 100 , alpha=0.8 |

Figure 7: watermark extracted from the LL, LH, HL and HH bands with SF

|  |  |  |
| --- | --- | --- |
|  |  |  |
| JPEG 60: 21.2103 | Intensity Adj.: 14.7251 | Bluring: 12.4582 |
|  |  |  |
| Salt& peppers noise(0.02): 16.1830 | Salt& peppers noise(0.5): 4.2115 | median filter: 19.3196 |
|  |  |  |
| Gaussian noise : 11.3945 | Rotating °35 : 0.4775 | Histogram Equalization: 14.2974 |

Figure 8: Attacks on the watermarked image on LL band

|  |  |  |
| --- | --- | --- |
|  |  |  |
| JPEG 60 : 0.8521 | Intensity Adj. :0.7669 | Bluring: 0.7537 |
|  |  |  |
| Salt& peppers noise(0.02): 0.9623 | Salt& peppers noise(0.5): 0.5215 | median filter: 0.9123 |
|  |  |  |
| Gaussian noise : 0.6419 | Rotating °35 : 0.2802 | Histogram Equalization: 0.5118 |

Figure 9: Watermarks recovered from the LL band after attacks showing SF

Chapter 3

DCT Image watermarking

# Introduction

The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies. The DCT has special property that most of the visually significant information of the image is concentrated in just a few coefficients of the DCT. It’s referred as ‘Energy compaction Property’.

As DCT is having good energy compaction property, many DCT based Digital image watermarking algorithms are developed. Common problem with DCT watermarking is block based scaling of watermark image changes scaling factors block by block and results in visual discontinuity [9]. In this chapter, we propose a visible watermarking technique that modifies the DCT coefficients of the host image using eqn. (1). We call an embedding factor we try different values for it to achieve visible watermarking we find α =10 a good value and we also use α =0.09 for invisible watermarking. We have also proposed a modification to make the watermark more robust.

# INSERTION OF WATERMARK

Figure 5 gives the schematic representation of the insertion process. The steps for watermark insertion are discussed below:

* The original image I (to be watermarked) and the watermark image W are reading. (Both the images may be not of equal size).
* The watermark image resize if necessary to make it size the same of host image.
* The DCT coefficients for host image and watermark image are found out.
* The value of embedding factor defined to be suitable for visible watermarking.
* The DCT coefficient of the host image and watermark image is modified using the following equation. The IDCT of modified coefficients give the watermarked image.

To extract the watermark applying the following equation:

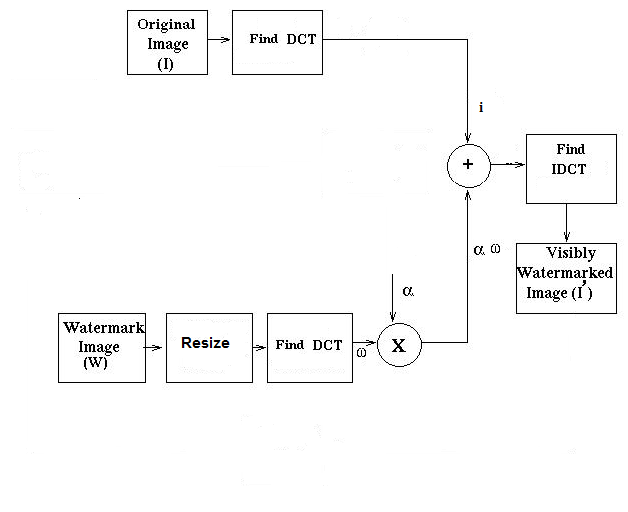


Figure 10: Watermark insertion Process

# Simulation result

Figure 11 shows the 512x512 gray scale cover image Lena and 512x512 watermark copyright.

Figure 11: a) Host Image b) Watermark Image

After running code and achieve desired result five types of attacks applied to the watermarked image. The attacked images are presented in Figure 12 together with the tools and parameters used for the attacks. The number next to the label below each image denotes the SNR value. Figure 13 contains the watermarks extracted from the watermarked for each of the attacks. The numbers next to the images are the SF values. According to Figure 12 and Figure 13, it is possible to note the resistance of watermarked image for each attack using either subjective human evaluation or objective SF.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| JPEG 75: 88.1841 | Salt& peppers noise(0.02): 31.7002 | Salt& peppers noise(0.02): 44.4603  With alpha=0.09 |
|  |  |  |
| Bluring: 16.1210 | Rotating °35 : 0.8822 | Gaussian noise(0.025): 11.1045 |

Figure 12: Watermarked image with different types of attack

|  |  |  |
| --- | --- | --- |
|  |  |  |
| JPEG 75: 0.9998 | Salt& peppers noise(0.02): 0.5511  With alpha=10 | Salt& peppers noise(0.02): 0.1190  With alpha=0.09 |
|  |  |  |
| Bluring: 0.6195 | Rotating °35 : 0.0925 | Gaussian noise(0.025): 0.2859 |

Figure 13: Extracted watermark after each attack

Chapter 4

FFT Image watermarking

http://homepages.inf.ed.ac.uk/rbf/HIPR2/mote.gifFourier Transform

The Fourier Transform is an important image processing tool which is used to decompose an image into its sine and cosine components. The output of the transformation represents the image in the Fourier or [frequency domain](http://homepages.inf.ed.ac.uk/rbf/HIPR2/freqdom.htm), while the input image is the [spatial domain](http://homepages.inf.ed.ac.uk/rbf/HIPR2/spatdom.htm) equivalent. In the Fourier domain image, each point represents a particular frequency contained in the spatial domain image [10].

The Fourier Transform is used in a wide range of applications, such as image analysis, image filtering, image reconstruction, image compression and image watermarking.

# INSERTION OF WATERMARK

Figure 14 gives the schematic representation of the insertion process. The steps for watermark insertion are discussed below:

* The original image I (to be watermarked) and the watermark image W are reading. (Both the images may be not of equal size).
* The watermark image resize if necessary to make it size the same of host image.
* The FFT coefficients for host image and watermark image are found out.
* The value of embedding factor defined to be suitable for visible watermarking.
* The FFT coefficient of the host image and watermark image is modified using the following equation. The IFFT of modified coefficients give the watermarked image.

# Extracted of watermark

To extract the watermark applying the following equation:

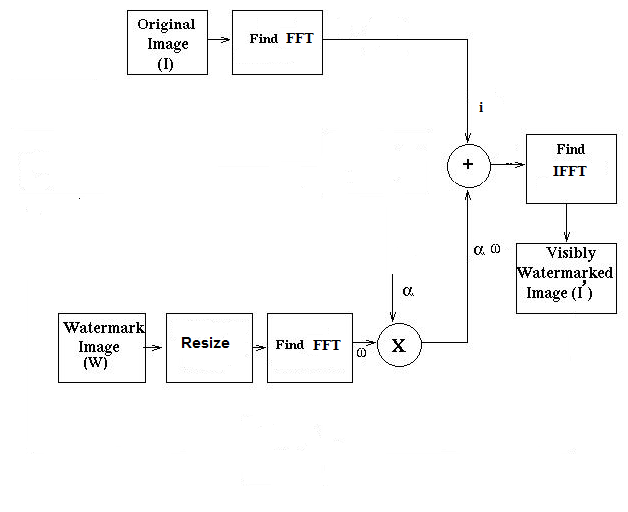


Figure 14: Watermark embedding using FFT

# Simulation result

Figure 15 shows the 512x512 gray scale cover image Lena and 512x512 watermark copyright.

Figure 15: a) Cover Image b) Watermark Image

After running code and achieve desired result five types of attacks applied to the watermarked image. The attacked images are presented in Figure 16 together with the tools and parameters used for the attacks. The number next to the label below each image denotes the SNR value. Figure 17 contains the watermarks extracted from the watermarked for each of the attacks. The numbers next to the images are the SF values. According to Figure 16 and Figure 17, it is possible to note the resistance of watermarked image for each attack using either subjective human evaluation or objective SF.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| JPEG 75: 88.5531 | Salt& peppers noise(0.02): 31.4703 | Without attacks: 42.1499 |
|  |  |  |
| Bluring: 30.4845 | Rotating °35 : 0.8801 | Gaussian noise(0.025): 11.162 |

Figure 16: Watermarking Images after different types of attacks

|  |  |  |
| --- | --- | --- |
|  |  |  |
| JPEG 75: 0.9996 | Salt& peppers noise(0.02): 0.5546 | Without attacks: 1 |
|  |  |  |
| Bluring: 0.6195 | Rotating °35 : 0.0925 | Gaussian noise(0.025): 0.2881 |

Figure 17: Extracted watermark after different types of attacks

In the Figure above we have extracted watermarks after different type of attacks applying on the watermarking image, we can note that this method robust against JPEG compression.

# Comparison between DCT and FFT

As discussed in two previous chapters we can note that the DCT and FFT algorithm are the same. The process doesn’t change; Figure 18 show the summary of insertion and retrieval of watermark process we can easily change the type of the transformer. The different between the two types will appear in the results, Table 5 show the results.

|  |  |  |
| --- | --- | --- |
| Type of attack | DCT scheme | FFT scheme |
| JPEG 75 | 88.1841 | 88.5531 |
| Salt & peppers noise | 31.7002 | 31.4703 |
| Gaussian noise | 11.1045 | 11.162 |
| Rotating °35 | 0.8822 | 0.8801 |
| Blurring | 16.1210 | 30.4845 |

Table 1: Comparison between DCT &FFT for different types of attack

From the table above we can note that the two methods have approximately, the same result. The value of SNR in the table indicates that FFT robust to blurring attack more than DCT but for other attacks are the same. For retrieval watermark image we can also compare between the two techniques. In Table 2 we compare between them for different types of attacks using SF as visual quality.

|  |  |  |
| --- | --- | --- |
| Type of attack | DCT scheme | FFT scheme |
| JPEG 75 | 0.9998 | 0.9996 |
| Salt & peppers noise | 0.5511 | 0.5546 |
| Gaussian noise | 0.2859 | 0.2881 |
| Rotating °35 | 0.0925 | 0.0925 |
| Blurring | 0.6195 | 0.6195 |

Table 2: comparison between extracted watermarks using SF.

DCT / FFT

DCT / FFT

IDCT / IFFT







α

Watermark image

Host image

Retrieval

Salt & peppers noise





Watermarking

Image

Watermarking image with noise

Extracted Watermark

Conclusions

Figure 18: insertion and retrieval of watermark

In chapter one we have general definition of digital image watermarking, our own work in watermarking start on chapter two using DWT first we decompose the host image into four bands LL, LH, HL and HH and we embedding the watermark in each band and with different values of QF and embedding factor we note that at QF=100 and alpha=0.09 we can retrieval the watermark image with SF=1 , Figure 6 show watermarking image in different bands and we use SNR to compare between them, Figure 7 show extracted watermark from each band also we use SF to compare between them. Applying different type of attacks on watermarking image embedding on the LL band we record the result in Figure 8 and note the effect of each type, LL band more robust to JPEG compression and intensity adjustment.

In chapter three and four we discuss watermarking process in two frequency domain DCT and FFT we notice that the process is the same but we apply different transformation, also we can note that the two method have the same robust for all types of attack except blurring we can note that FFT more robust than DCT.

Appendix

In this section we will show our codes for digital image watermarking using different techniques

DWT code

*% loading cover image*

X=imread('cameraman.tif');

X=im2double(X);

[F1,F2]= wfilters('db1', 'd');

[LL,LH,HL,HH] = dwt2(X,'db1','d');

%Watermark image

b=imread('message\_copyright.bmp');

level=graythresh(b);

w=im2bw(b,level);

w=double(w);

alpha=0.09;

k=w\*alpha;

LL\_1=LL+k;

Y = idwt2(LL\_1,LH,HL,HH,'db1','d');

% Storing the image to lossy file formats.jpeg

q=input('Quality Factor q = ');

imwrite(Y,'xyz.jpg','jpg','quality',q);

Y=imread('xyz.jpg');

imshow((Y)); % Stego image

title ('watermarked Image');

w1= (HL1-HL)./alpha ; % extracted the watermark

level1=graythresh(w1);

w2=im2bw(w1,level1);

w2=im2double(w2);

imshow((w2));

title ('Extrected Watermark');

%SNR measurement

z1=double(Y);

snr\_num=0;

snr\_den=0;

for i=1:256

for j=1:256

snr\_num=snr\_num+(z1(i,j)\*z1(i,j));

snr\_den=snr\_den+((X(i,j)-z1(i,j))\*(X(i,j)-z1(i,j)));

end

end

snr=10\*log10(snr\_num/snr\_den)

%Similarity Factor (SF) Measurement

sf\_num=0; sf\_den=0;a=0; b=0;

for i=1:512

for j=1:512

sf\_num=sf\_num+(w1(i,j)\*o(i,j));

a=a+(o(i,j)\*o(i,j));

b=b+(w1(i,j)\*w1(i,j));

sf\_den=sqrt(sf\_den+a\*b);

end

end

sf=(sf\_num/sf\_den)

sf=(sf\_num/sf\_den)

DCT Code

FFT Code

*I = im2double(imread(*'bb.bmp'));

alpha=10;

X = dct2(I);

o=im2double(imread('ba.bmp'));

imshow (o),

r=dct2(o);

K2=r\*alpha;

X=X+K2;

a = idct2(X);

w1=(a-I)./alpha;

%Storing the image to lossy file formats.jpeg

q=input('Quality Factor q = ');

imwrite(a,'xyz.jpg','jpg','quality',q);

a=imread('xyz.jpg');

imshow((a));

title ('Watermarking Image');

imshow((w1));

title('detected Embedded Watermark');

% %SNR measurement

z1=double(a);

snr\_num=0;

snr\_den=0;

for i=1:512

for j=1:512

snr\_num=snr\_num+(z1(i,j)\*z1(i,j));

snr\_den=snr\_den+((I(i,j)-z1(i,j))\*(I(i,j)-z1(i,j)));

end

end

snr=10\*(log10(snr\_num/snr\_den))

%Similarity Factor (SF) Measurement

sf\_num=0;

sf\_den=0;

a=0;

b=0;

for i=1:512

for j=1:512

sf\_num=sf\_num+(w1(i,j)\*o(i,j));

a=a+(o(i,j)\*o(i,j));

b=b+(w1(i,j)\*w1(i,j));

sf\_den=sqrt(sf\_den+a\*b);

end

end

sf=(sf\_num/sf\_den)

*close* all; clc;

I = im2double(imread('bb.bmp'));

imshow(I);

X=fft(I);

alpha=10;

o=im2double(imread('ba.bmp'));

r=fft(o);

K=r.\*alpha;

X=X+K;

T=ifft(X);

w1= (a-I)./alpha;

%Storing the image to lossy file formats.jpeg

q=input('Quality Factor q = ');

imwrite(a,'xyz.jpg','jpg','quality',q);

a=imread('xyz.jpg');

a=im2double(a);

imshow((a));

title ('Watermarking Image');

imshow((w1));

title('detected Embedded Watermark');

%SNR measurement

z1=double(a);

snr\_num=0;

snr\_den=0;

for i=1:512

for j=1:512

snr\_num=snr\_num+(z1(i,j)\*z1(i,j));

snr\_den=snr\_den+((I(i,j)-z1(i,j))\*(I(i,j)-z1(i,j)));

end

end

snr=10\*log10(snr\_num/snr\_den)

%Similarity Factor (SF) Measurement

sf\_num=0;

sf\_den=0;

a=0;

b=0;

for i=1:512

for j=1:512

sf\_num=sf\_num+(w1(i,j)\*o(i,j));

a=a+(o(i,j)\*o(i,j));

b=b+(w1(i,j)\*w1(i,j));

sf\_den=sqrt(sf\_den+a\*b);

end

end

sf=(sf\_num/sf\_den)

References

[1]. <http://www.scribd.com/doc/37021026/Project-Report-on-Digital-Watermarking>.

[2]. Min Wu Bede Liu, “WATERMARKING FOR IMAGE AUTHENTICATION”, Department of Electrical Engineering, Princeton University, Princeton.

[3]. <http://homepages.vub.ac.be/~andooms/research.html>

[4]. http://www.alpvision.com/watermarking.html

[5].Edin Muharemagic and Borko Furht, “Survey Of Watermarking Techniques And Applications”, Department of Computer Science and Engineering, Florida Atlantic University.

[6]. Andreja Samˇcovi´c, J´an Tur´an, “ATTACKS ON DIGITALWAVELET IMAGEWATERMARKS”, Journal of ELECTRICAL ENGINEERING.

[7]. Peining Taoa and Ahmet M. Eskicioglub, “A robust multiple watermarking scheme in the Discrete Wavelet Transform domain ”, The Graduate Center, The City University of New York.

[8]. Baisa L. Gunjal, “AN OVERVIEW OF TRANSFORM DOMAIN ROBUST DIGITAL IMAGE WATERMARKING ALGORITHMS”, Department of Computer Engineering, Amrutvahini College of Engineering.

[9]. R. Gonzales, R. Woods  “Digital Image Processing”, Addison-Wesley Publishing Company.

Contents