Implementation & Performance Analysis of Various Digital Watermarking Techniques

A thesis submitted in partial fulfillment of the

requirements for the award of the Degree of

MASTER of ENGINEERING

in

ELECTRONICS AND COMMUNICATION ENGINEERING

Submitted by:

GAURAV KUMAR

Roll No. 800861005

Under the guidance of:

Dr. KULBIR SINGH

Assistant Professor, ECED

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

THAPAR UNIVERSITY

PATIALA-147004, Punjab, INDIA.

June 2010

CERTIFICATE

I, Gaurav Kumar, hereby certified that the work which is being presented in this thesis entitled **"Implementation & Performance Analysis of various Digital Watermarking Techniques"** in partial fulfillment of requirements for the award of degree of Master of Engineering in Electronics and Communication from Thapar University, Patiala, is an authentic record of my own work carried under the supervision of Dr. Kulbir Singh.

The matter presented in this thesis has not been submitted in any other University / Institute for the award of Master of Engineering.

(Gaurav Kumar)
Signature of the student

This is certified that the above statement made by the candidate is correct to the best of my knowledge

(Dr.Kulbir Singh)
Supervisor

(Dr. A.K. Chatterjee) 9.7.10.
Head of Department
ECED, T.U. Patiala

(Dr. R.K. Sharma) 13.7.10
Dean of Academic Affairs
T.U. Patiala

ACKNOWLEDGEMENT

Words are often to less to revels one's deep regards. An understanding of the work like this is never the outcome of the efforts of a single person. I take this opportunity to express my profound sense of gratitude and respect to all those who helped me through the duration of this thesis.

First, I would like to thank the Supreme Power, one who has always guided me to work on the right path of the life. Without his grace, this would never come to be today's realty.

This work would not have been possible without the encouragement and able guidance of my supervisor **Dr.Kulbir Singh,** his enthusiasm and optimism made this experience both rewarding and enjoyable. Most of the novel ideas and solutions found in this thesis are the result of our numerous stimulating discussions. His feedback and editorial comments were also invaluable for the writing of this thesis. I am grateful to Head of the Department **Dr. A. K. Chaterjee** for providing the facilities for the completion of thesis.

I take pride of my self being son of ideal great parents whose everlasting desire, sacrifice, affectionate blessing and help without which it would have not been possible for me to complete my studies.

At last, I would like to thank to all the members of Electronics and Communication Department whose love and affection made my stay at T.U. campus a memorable.

Place: T.U. Patiala, India (GAURAV KUMAR)

ABSTRACT

The digitization of the information has revolutionized the daily lives of the peoples in this world. The many advantages of digital information have also generated new challenges and new opportunities for innovation. This thesis discusses the issues regarding data hiding and its application to multimedia security and communication, addressing both theoretical and practical aspects, and tackling both design and attack problems. In the fundamental part, it has been identified a few key elements of data hiding through a layered structure. Data hiding is modeled as a communication problem where the embedded data is the signal to be transmitted. Various embedding mechanisms target different robustness-capacity tradeoffs. The tradeoff for different major categories of embedding mechanisms has been done. In addition, it has been found that the unevenly distributed embedding capacity brings difficulty in data hiding. A comprehensive study has been done to solve this problem, addressing the considerations for choosing constant or variable embedding rate and enhancing the performance for each case i.e. using smaller watermark or increasing processing gain at the cost of degradation in the image quality. Various, data hiding algorithms in spatial domain, frequency domain, fractal domain and wavelet domain for binary images, grayscale images has been implemented. These algorithms are covering applications such as annotation, tamper detection, copy/access control, fingerprinting, and ownership protection.

Data hiding can also be used in video communication to convey side information for additional functionalities or better performance. In the attack part, discussion on a number of attacks like cropping, addition of noise, JPEG compression and other geometrical attacks and countermeasures for data hiding systems has been done. The investigation begins with four specific types of watermarking schemes, in which full knowledge of the watermarking algorithms is available. The attack problems have been studied for digital images under a unique competitive environment, using blind and non blind watermarking algorithms of digital watermarking. On basis of overall discussion it can be concluded that watermarking in dual domain is considered the best among the discussed algorithms.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

BER	Bit Error Rate
CD	Compact Disk
CDMA	Code Division Multiple Access
CR	Compression Ratio
DCT	Discrete Cosine Transform
DVD	Digital Versatile Disk
DWT	Discrete Wavelet Transform
FFT	Fast Fourier Transform
FT	Fourier Transform
FRFT	Fractional Fourier Transform
FRDCT	Fractional Discrete Cosine Transform
HDTV	High Definition Television
HVS	Human Visual System
LSB	Least Significant Bit
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio
RMSE	Root Mean Square Error

CHAPTER 1

Introduction

1.1 Preamble

Digital watermarking includes a number of techniques that are used to imperceptibly convey information by embedding it into the cover data. There has always been a problem in establishing the identity of the owner of an object in this digital world where the unlimited number of copies of the digital data can be produced with zero to no error. In case of a dispute, identity was established by either printing the name or logo on the objects. But in the modern era where things have been patented or the rights are reserved i.e. copyrighted, more modern techniques to establish the identity and leave it unhampered have come into picture. Unlike printed watermarks, digital watermarking is a technique where bits of information are embedded in such a way that they are completely invisible. Actually, digital watermarking exploits the limitation the human visual system (HVS). The problem with the traditional way of printing logos or names is that they may be easily tampered or duplicated. In digital watermarking, the actual bits are scattered in the image in such a way that they cannot be identified and show resilience against attempts to remove the hidden data [1].

Digital Watermarking can be defined as a technology of embedding watermark with intellectual property rights into images, videos, audios and other multimedia data by a certain algorithm. This kind of watermark contains the author and the user's information, which could be the owner’s logo, serial number or control information. In fact, it’s making use of the ubiquitous redundancy and randomness in data, and adding to the data information which is difficult to be detected but can be distinguished to protect product copyright and data integrity. The difference between digital watermarking and other technology is of three important aspects: First of all, unlike encryption, watermarking is imperceptible so that the image will not be detract from the aesthetic sense. Second, the watermarks and the cover data they in which they are embedded should be inseparable. Even if the data were displayed or converted into other file formats, the watermarks will not be eliminated. This is different from the first section. Finally, the watermarks will have exactly the same transformation experience as the data that means you can get the information of transformation by looking at the watermarks.

1.2 History of Data hiding techniques:

The core principles of watermarking and data hiding can be traced back approximately 4,000 years to Egypt and Greece. At this time, hidden packets of information had been transferred by special character adjustments or mutations (Hanjalic et al., 2000). Herodotus, the great Greek storyteller, often refers to the hidden information methodology transferred on wax tablets or smuggling secret messages tattooed on the skull of human messengers (Cox et al., 2002).

In Roman times a slave would have his head shaved, then tattooed with an important message, and as the hair began growing, he made his way as instructed through enemy lines and indifferent countries, across water and inhospitable terrain, sleet and snow, mountain ranges, etc. finally reaching the reader who immediately had the head shaved, and eagerly scanned the message.

The United States Constitution states that "The Congress shall have Power to promote the progress of Science and useful Arts, by securing for limited times to Authors and Inventors the exclusive right to their respective writings and discoveries." The origin of this concept, but not of the noble sentiment of promoting progress in the arts and sciences, in the Anglo-American legal system (similar restrictions also existed in France) stems from a royal charter granted by Mary Tudor, Queen of England, to the Stationer's Company [2] in 1557. This charter limited the right to print books to the members of the company. The intent behind this privilege was primarily to exert censorship, the commercial interests of the publishers were of secondary interest only. Even after the repealing of the 1662 Licensing Act in 1681, the Stationer's Company retained control over the printing trade through the use of a bylaw establishing rights of ownership for books registered to its members. This common law mechanism was supplanted in 1710 by the Statute of Anne enacted in 1709. The Act of Parliament granted authors copyright over their work initially for 14 years and was the first copyright legislation in the current sense, in most European states the rights of the authors were recognized only partially until the French Revolution [3]. Cryptography and steganography have been used throughout history as means to add secrecy to communications especially during the times of war and peace [4].

Some of the early methods to hide information include text written on wax-covered tablets, invisible writing using invisible ink .In World War II null ciphers were used in which the secret was camouflaged in an innocent sounding message as in the example below [5]

Apparently neutral's protest is thoroughly discounted and ignored**.** Islam hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suet and vegetable oils.
Taking the second letter in each word the following message emerges:

Pershing sails from NY June 1

As technology developed and detection methods improved, more effective methods of hiding information were developed. The Germans invented microdot technology for covert communication in 1941. In microdots, the messages were neither hidden nor encrypted but their size was too small to be seen by the naked eye [5]. Advances in microdot technology still continue to this day, the latest development being the embedding of a message in a strand of DNA by the use of the technique of genomic steganography.

With the advent of the internet, steganography has found new applications. But, at the same time it is also vulnerable to more powerful attacks since the medium is relatively insecure. To overcome this limitation, watermarking comes into picture. The main difference between the two techniques is the superior robustness capability of watermarking schemes. This will be clearer in the following sections which explain the basic concepts of cryptography, steganography and watermarking. It also lists some of the most common applications of watermarking in today's world [6]

1.3 Relationship of Watermarking with Information Hiding

In addition to Digital watermarking, the general idea of hiding some information in digital content has a wider class of applications that go beyond mere copyright protection and authentication. The techniques involved in such applications are collectively referred to as *information hiding*. For example, an image printed on a document could be annotated by information that could lead an user to its high resolution version. Metadata provides additional information about an image. Although metadata can also be stored in the file header of a digital image, this approach has many limitations. Usually, when a file is transformed to another format (e.g., from TIFF to JPEG or to bmp), the metadata is lost. Similarly, cropping or any other form of image manipulation destroys the metadata. Finally, the metadata can only be attached to an image as long as the image exists in the digital form and is lost once the image is printed. Information hiding allows the metadata to travel with the image regardless of the file format and image state (digital or analog). Metadata information embedded in an image can serve many purposes.

For example, a businessman can embed the website URL for a specific product in a picture that shows an advertisement for that product. The user holds the magazine photo in front of a low-cost CMOS camera that is integrated into a personal computer, cell phone, or a palm pilot. The data is extracted from the low-quality picture and is used to take the browser to the designated website. Further, Before Understanding the watermarking it is very essential to understand the subtle difference between the most popular forms of data hiding techniques. Therefore, an attempt has been made to differentiate cryptography, Stegnography and Watermarking as following.

1.3.1 Cryptography:

Cryptography as the study of secret (*crypto*) writing (*graphy*) can be defined as the science of using mathematics to encrypt and decrypt data back [2]. It allows two people, commonly known as Alice and Bob, to communicate with each other securely. This means that an eavesdropper known as Eve will not be able to listen in on their communication.

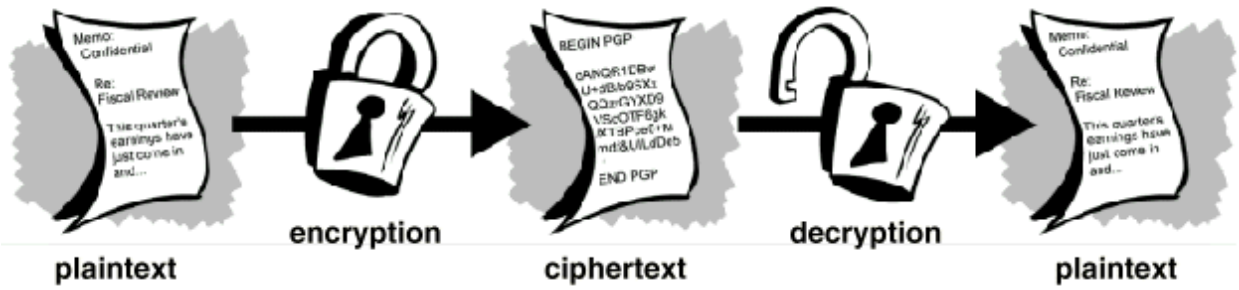


Figure 1.1: Cryptography for secure communication [4].

Cryptography also enables Bob to check that the message sent by Alice was not modified by Eve and that the message he receives was really sent by Alice [3]. A message is known as a plaintext or clear text. The method of disguising the plaintext in such a way as to hide its information is encryption and the encrypted text is also known as a ciphertext. The process of reverting ciphertext back to its original text is decryption, shown in figure 1.1.

1.3.2 Steganography:

While cryptography is about protecting the content of the messages, steganography is about concealing their very existence. Steganography comes from a Greek word that means covered writing (*stego* = covered + *graphy* = writing) [5]. Examples can be thought as messages exchanged between drug dealers via emails in encrypted forms, or messages exchanged by spies in covert communication. Steganography hides the fact that the communication ever occurred as shown in Figure 1.2.

Let us consider that Alice, who wants to share a secret message *m* with Bob, selects randomly a harmless message or a *cover* object *C*. The message to be shared is then embedded into *C*, by using key *K* (called *stego-key*), and the cover object *C* is transformed to *stego* object *S*.

This *stego* object can be transmitted to Bob without raising any suspicion. This should be done in such a way that a third party knowing only the apparently harmless message *S* cannot detect the existence of the secret. The cover object could be any data such as image files, written text or digital sound. In a perfect system, a normal cover object should not be distinguishable from the stego object, neither by a human nor by a computer looking for statistical patterns [2].

Alice transmits the stego object *S* to Bob over an insecure channel. Bob can reconstruct the message *m* by using the same key *K* as used by Alice during embedding the message in the cover object. The extraction process should not need any knowledge of the cover object. Any person watching the communication should not be able to decide whether the sender is sending covers with messages embedded into them.

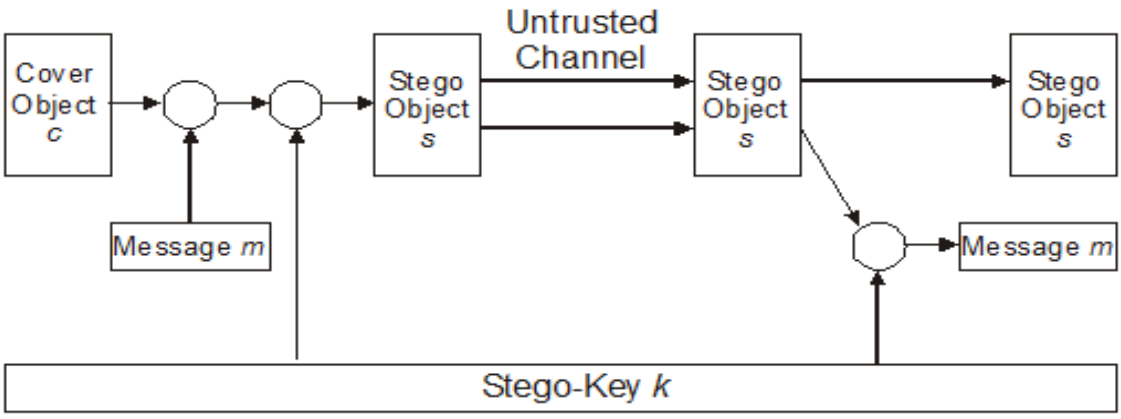


Figure 1.2: General Stegnographic process [6]

In other words, a person with a number of cover objects C_1, C_2, ……, C_n should not be able to tell which cover object C_i has the message embedded in it, and the security of invisible communication lies in the inability to distinguish cover objects from the stego objects [5]. However, not all the cover objects can be used to hide the data for covert communication, since the modifications done after the data is hidden should not be visible to anyone not involved in the communication. The cover object needs to have sufficient redundant data, which can be replaced by secret information.

Some applications for steganography include the automatic monitoring of radio advertisements, where it would be convenient to have an automated system to verify that adverts are played as contracted, indexing of video mail. In medical safety, where current image formats such as DICOM separate image data from the text (such as the patient's name, date and physician), with the result that the link between image and patient occasionally.

1.3.3 Watermarking:

Although steganography and watermarking both describe the techniques used for covert communication, steganography typically relates only to covert point to point communication between two parties [7]. Steganographic methods are not robust against attacks or modification of data that might occur during transmission, storage or format conversion [1]. Watermarking, as opposed to steganography, has an additional requirement of robustness against possible attacks. An ideal steganographic system would embed a large amount of information perfectly securely, with no visible degradation to the cover object.

For the embedding process the inputs are the watermark, cover object and the secret or the public key. The watermark used can be text, numbers or an image. The resulting final data received is the watermarked data W*'*. The inputs during the decoding process are the watermark or the original data, the watermarked data and the secret or the public key. The output is the recovered watermark W.

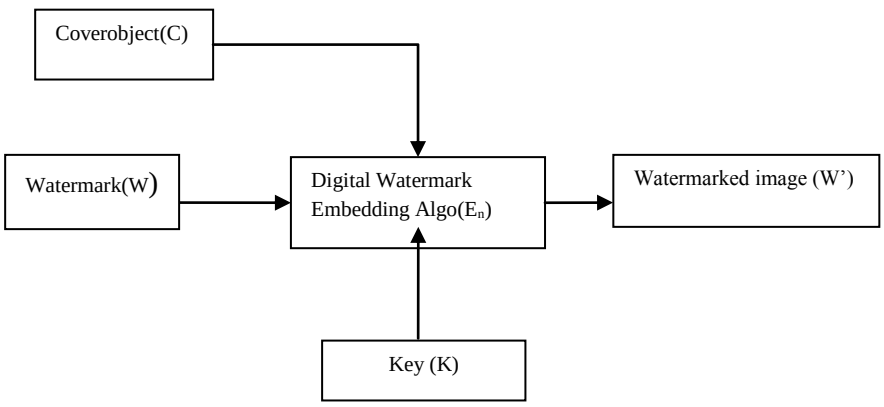


Figure1.3: General embedding process

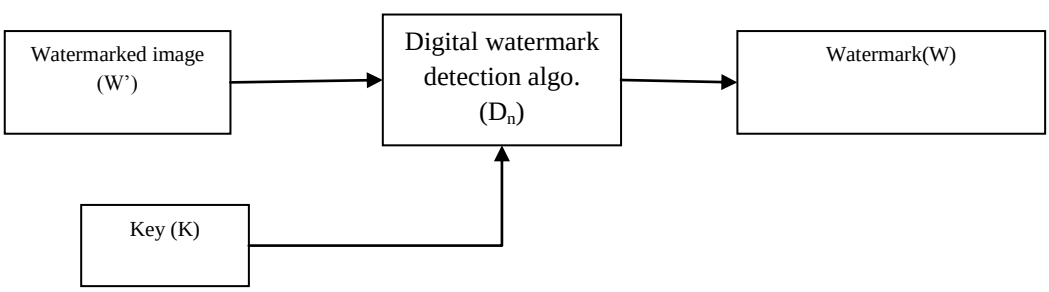


Figure 1.4: Watermark extraction process

1.4 Resemblance between Watermarking System and Communication system:

Watermarking can be considered as communication of the watermark over a channel consisting of the original work to be watermarked. Therefore, a natural approach in development of conceptual models for watermarking is to study the similarities between communication models and corresponding watermarking algorithms. Both models transmit data from an information source (the watermark) to a destination (the user or another system). The typical model of communication consists of several blocks as shown in figure 1.5.This model was introduced by Shannon in his landmark 1948 paper [4]. In order to transmit the discrete symbols over a physical channel, a *modulator* transforms each symbol of the encoded sequence into a form suitable for transmission. During transmission over the channel, the transformed sequence is distorted by noise. The different forms of noise that can disturb the transmission are driven by the channel characteristics.

On the receiver side, the *demodulator* processes the transmitted sequence and produces an output consisting of the counterpart of the encoded sequence. Corresponding to the encoder, the *channel decoder* transforms the output of the demodulator into a binary sequence, which is an estimation of the true sequence being transmitted. Besides the channel characteristics, the transmission can be further classified according to the security it provides against active attacks trying to disable communication and against passive attacks trying to monitor the communication. The defense against the attacks is based on-

- Spread-spectrum techniques trying to prevent active attacks;
- Cryptography encrypting the messages in order to ensure privacy.

Digital watermarking and spread-spectrum techniques try to fulfill similar security requirements in preventing active attacks like jamming the communication between different communicating parties. Spread-spectrum technologies establish secrecy of communication by performing modulation according to a secret key in the channel encoder and decoder as shown Figure 1.5.

A watermarking model based on same communication system patterns consists of the same basic blocks as the communication model but with different interpretations. There is a direct resemblance between the watermark embedder/detector and the channel encoder/decoder including the modulation/demodulation blocks respectively.

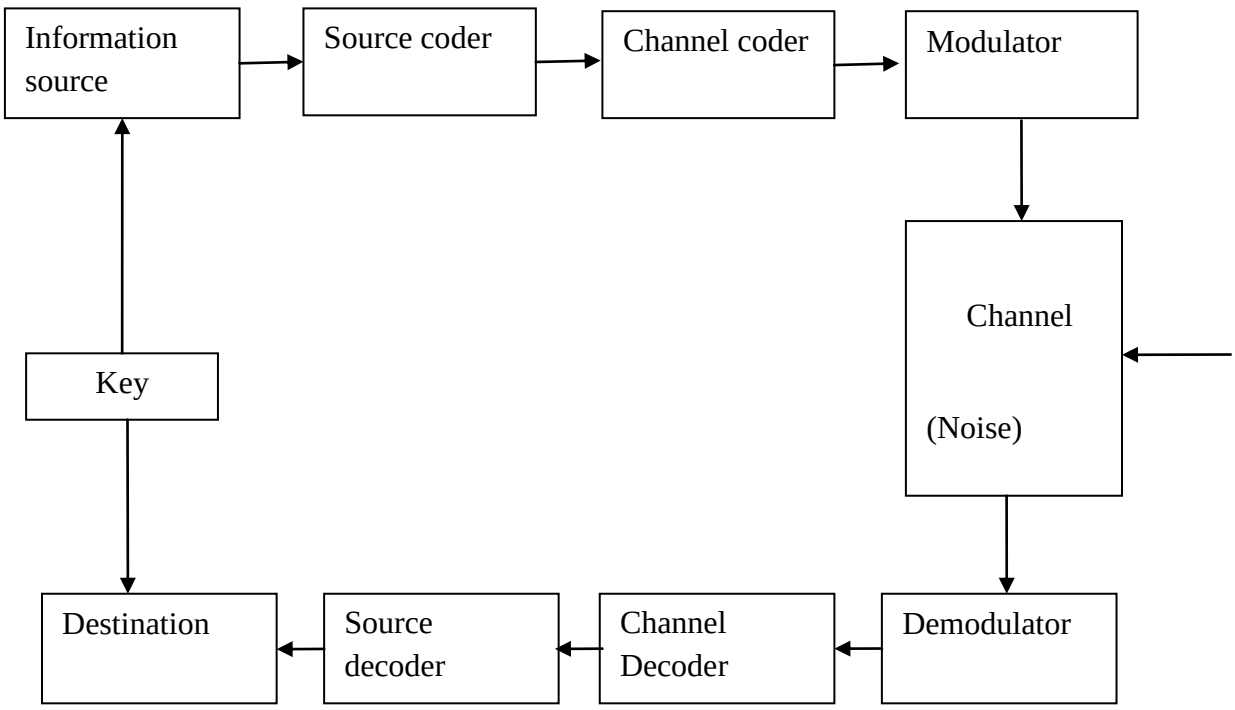


Figure 1.5: Basic Communication systems [4]

The message to be transmitted is the watermark itself. The additional requirement of secure transmission of the signal over the channel requires the usage of a secret key in the encoding and decoding procedure the channel characteristics can be modeled by:

- The cover object representing the channel carrying the watermark.
- The kind of noise introduced by the different processing that can happen during transmission of the watermarked object.

This additional processing may be anticipated manipulations or intentional attacks. The encoding block of the watermark embedder encodes the watermark message into a coded sequence. During the modulation, the sequence is transformed into a physical signal, the watermark signal that can be transmitted over the channel [8]. The difference between the marked and original cover object which actually forms the added watermark will essentially have the same digital representation as the original data set. For example, in the case of an audio file, the added watermark will be a signal with the same sample rate and bit resolution as the cover track. At the watermark detector site, the possible distorted marked object is demodulated into , which is a distorted version of the coded sequence. The watermark message is obtained by means of the watermark message detector. Analogous with the basic communication system; the embedder has to perform three steps-

- Encode the message into a coded sequence using a secret key.

- Modulate the coded sequence into a physical representation according to the channel respectively the cover object.
- Add the modulated sequence to the cover object to produce the watermarked object

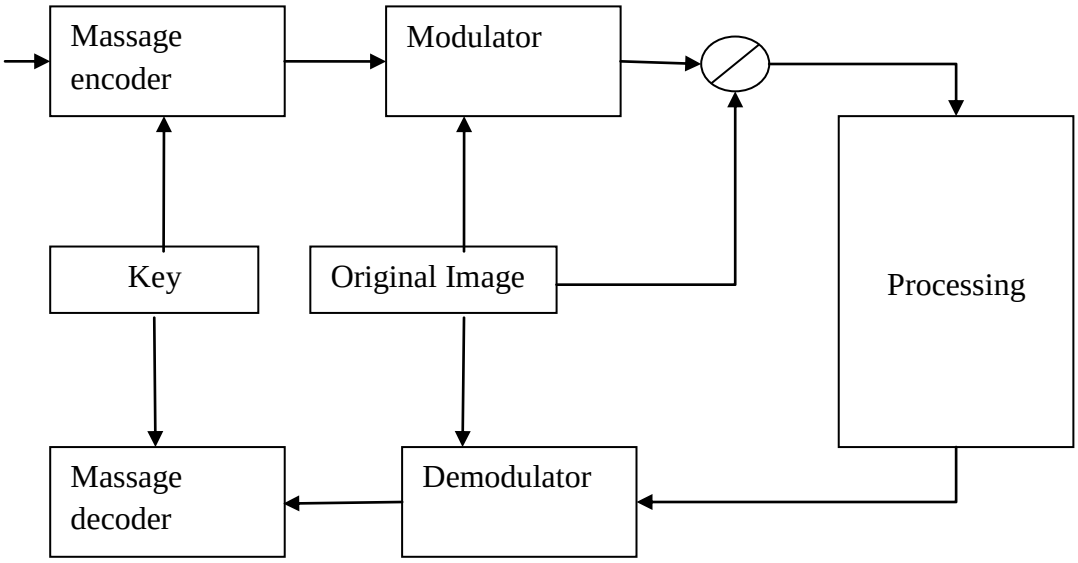


Figure1.6: Basic watermark communication models [7].

1.5 Objectives of the Thesis:

The objectives of thesis are:

- To achieve digital watermarking using different techniques i.e. spatial domain, transform domain and hybrid domain(i.e. DCT-DWT-SVD)
- To obtain the optimum parameter i.e. PSNR, MSE and BER for different watermarking techniques under cropping and Gaussian noise.
- To discuss and implement different watermarking algorithms (i.e. digital watermarking using Discrete Cosine Transform, Discrete Wavelet transform and Singular value decomposition method) and study their limitations and attributes.

1.6 Outline of the Thesis:

- In chapter 2 the Basic building Blocks of digital watermarking system i.e. Blind and non blind Watermarking, requirements of digital watermarking and various applications of Watermarking etc. are discussed. This chapter also includes type of watermark and their requirements.

- In chapter 3 the different watermarking techniques i.e. Watermarking in spatial domain, Watermarking in frequency domain, Watermarking in fractional domain , Watermarking in wavelet domain and watermarking using DCT-DWT-SVD are discussed.
- Chapter 4 describes the possible attack on watermarking system such as JPEG compression, addition of AWGN noise, Geometric Transformations, Enhancement technique etc.
- Chapter 5 provides the simulation results for reference image of Lena, for different techniques under different kind of attacks.
- In Chapter 6 enlists the important conclusion of the thesis.

1.7 Specification of the system:

PC configuration:	Intel(R) Core(TM) 2 Duo CPU E8200, 2.66 GHz, 2 GB of RAM.
Operating System:	Microsoft Window XP Professional Version 2002 Service Pack2.
Software:	MATLAB 7.5**.**

CHAPTER 2

2.1 Basic principles of watermarking:

Since this research field is still relatively young and has contributors from several disciplines with varying traditions, the terminology used is still quite diverse. This section provides a formal introduction to watermarking systems and the terms used in this context for their presentation.

The basic principle of current watermarking systems is comparable to symmetric encryption as to the use of the same key for encoding and decoding of the watermark. Each watermarking system consists of two subsystems: a watermarking encoder and a respective decoder. Formally, a watermarking system can be described by a tuple (O,W, K, E_K , D_K , C_τ) where O is the set of all original data the set of all watermarks, and K the set of all keys. The two functions describe

$$E_K : O \times W \times K = O \quad (2.1)$$

$$D_K : O \times K = W \quad (2.2)$$

the embedding and detection process, respectively. The comparator function

$$C_\tau : W^2 \longrightarrow \{0,1\} \quad (2.3)$$

Compares the extracted with the really embedded watermark using the threshold τ for comparison. The input parameters of the embedding process are the carrier object (or original c_o), the watermark **w** to be embedded, as well as a secret or public key K:

$$E_K(c_o, \mathrm{w}) = \mathrm{c_o} \quad (2.4)$$

The output of the encoder forms the marked data set

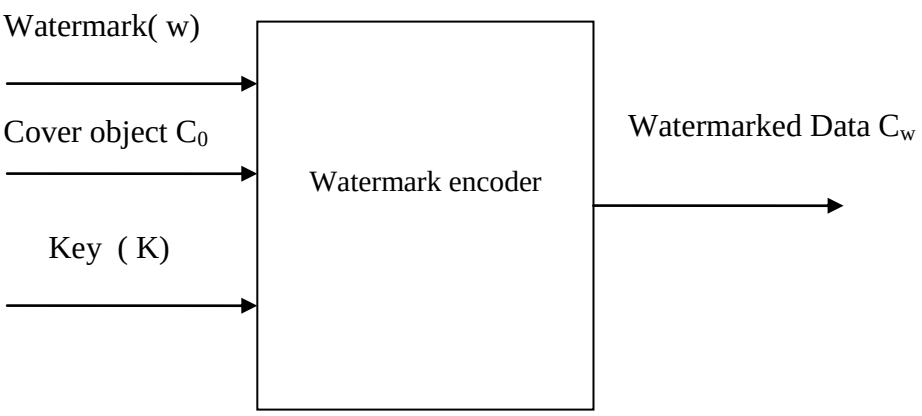


Figure 2.3: Generic watermark encoder

In the detection process, the marked and possibly manipulated data set$\hat{c}_w$, the original **co**, the watermarkc_w, and the key *K* used during the embedding process form the maximal set of input parameters. The various types of watermarking systems differ in the number of input parameters in the reading process. The extracted watermark $\hat{w}$ differs in general from the embedded watermark *w* due to possible manipulations. In order to judge the correspondence of both watermarks, the comparator function *Cτ* compares the suspected watermark with the retrieved one against a threshold *τ:*

$$C_\tau(\hat{w}, w) = \begin{cases} 1, & c \geq \tau \\ 0, & c < \tau \end{cases} \qquad (2.5)$$

The threshold τ depends on the chosen algorithm and should in a perfect system be able to clearly identify the watermarks. This formal analysis of the watermarking systems can also be used to develop a geometric interpretation of the watermarking algorithms as shown in [9].

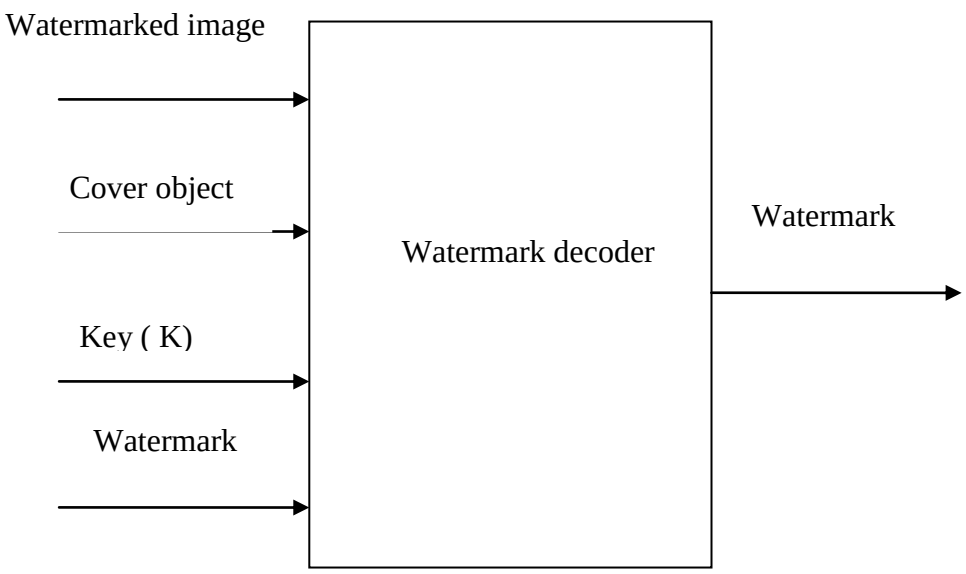


Figure 2.4: Generic watermark decoder

Using more information at the detector site increases the reliability of the whole watermarking system but limits the practicability of the watermarking approach on the

embedder side. The side information in the detection process can be the original C_o and the watermark *w* itself.

2.2 Basic Requirements of a Good Watermarking System:

Good watermarking depends on the few things like watermark being used, size of watermark and method being used. Since watermarking is a application dependent technology ,Here we shall discuss the bare minimum requirement of good watermarking system.

2.2.1 Perceptibility: The first requirement would clearly be that of perceptibility. A watermarking system is of no use to anyone if it distorts the cover image to the point of being useless, or even highly distracting. Ideally the watermarked imaged should look indistinguishable from the original even on the highest quality equipment [10].

2.2.2 Robustness: The ideal watermark must also be highly robust, entirely resistant to distortion introduced during either normal use (unintentional attack), or a deliberate attempt to disable or remove the watermark present (intentional, or malicious attack). Unintentional attacks involve transforms that are commonly applied to images during normal use, such as cropping, resizing, contrast enhancement…etc. A particularly interesting form of unintentional attack is that of image *compression* [11]. Lossy compression and watermarking are inherently at odds watermarking seeks to encode information in extra bits that compression hopes to remove. Thus, ideal watermarking and compression systems are most likely inherently exclusive.

In *malicious* attacks, an attacker deliberately tries to disable the watermark, often through a geometric distortion or the addition of noise. A final note is that robustness can include either resilience to attack, or complete fragility. It may be the case that some watermarking systems may require the watermark to totally destroy the cover object if any tapering is present [12].

2.2.3 Security: Another property of an ideal watermarking system is that it implement the use of *keys* to ensure that the approach is not rendered useless the moment that the algorithm becomes known [10]. It may also be a goal that the system utilizes an asymmetric key system such as in public / private key cryptographic systems. Although private key systems are fairly easy to implement in watermarking, asymmetric key pairs are generally not. The risk here is that embedded watermarking systems might have their private key discovered, ruining security of the entire system. This was exactly the case when a single DVD decoder

implementation left it's secret key unencrypted, breaching the entire DVD copy protection mechanism.

2.2.4 Capacity: Slightly less important requirements of an ideal watermarking system might be *capacity***,** and speed. A watermarking system must allow for a useful amount of information to be embedded into the image. This can range from a single bit all the way up to multiple paragraphs of text. Furthermore, in watermarking systems destined for embedded applications, the watermark detection (or embedding) may not be overly computationally intensive as to preclude its use on low cost micro-controllers.

2.2.5 Statistical imperceptibility: The last possible requirement of an ideal watermarking system is that of *statistical imperceptibility* [13]. The watermarking algorithm must modify the bits of the cover in such a way that the statistics of the image are not modified in any telltale fashion that may betray the presence of a watermark. This requirement is not quite as important here as it is in steganography, but some applications may require it.

How then do we provide metrics for the evaluation of watermarking techniques? Capacity and speed can be easily evaluated using the number of bits per cover size, and computational complexity, respectfully. The systems use of keys is more or less by definition, and the statistical imperceptibility by correlation between the original images and watermarked counterpart.

The more difficult task is providing metrics for perceptibility and robustness. Criterions suggested for the evaluation of perceptibility as shown in Table 1.

Table 2.1 - Summery of Possible Perceptibility Assurance Levels [13]

Level of Assurance	**Criteria**
Low	- Peak Signal-to-Noise Ratio (PSNR) - Slightly perceptible but not annoying
Moderate	- Metric Based on perceptual model - Not perceptible using mass market equipment
Moderate High	- Not perceptible in comparison with original under studio conditions
High	- Survives evaluation by large panel of persons under the strictest of conditions.

2.3 Types of Digital Watermarking Systems

There are several types of robust copyright marking systems. They are defined by their inputs and outputs:

2.3.1. Private watermarking:

Private watermarking systems are also called non-blind watermarking. In this watermarking system, the original image is required during detection. There are two types of systems i.e. Type I and Type II. In type I systems the mark M is extracted from the possibly distorted image $\tilde{I}'$ and use the original image as a hint to find where the mark could be in $\tilde{I}'$ ($\tilde{I}' \times I \times k \to W$). Type II systems also require a copy of the embedded mark for extraction and just yield a `yes' or `no' answer to the question: does $\tilde{I}'$ contain the mark M? ($\tilde{I}' \times I \times k \times W \to \{0,1\}$). It is expected that this kind of scheme will be more robust than the others since it conveys very little information and requires access to secret material.

2.3.2 Semi-private watermarking: In semi-private watermarking does not use the original image for detection ($\tilde{I}' \times K \times W \to \{0,1\}$) but answers the same question. The main uses of private and semi-private marking seem to be evidence in court to prove ownership and copy control in applications such as DVD where the reader needs to know whether it is allowed to play the content or not. Many of the currently proposed schemes fall in this category [7][8].

2.3.3 Public watermarking: This scheme is also known as blind watermarking. In this case, the detection process (and in particular the detection key) is fully known to anyone as opposed to private watermarking where a secret key is required. So here, only a public key is needed for verification and a private key (secret) is required for embedding. The knowledge of the public key does not help to compute the private key (at least in reasonable time), it does not either allow removal of the mark nor it allows an attacker to forge a mark.Indeed such systems really extract n bits of information (the mark) from the marked image: $\tilde{I}' \times K \to W$ [7].

2.3.4 Asymmetric & symmetric watermarking: Asymmetric watermarking (also called asymmetric key watermarking) is a technique where different keys are used for embedding and detecting the watermark. It should have the property that any user can read the mark, without being able to remove it. In symmetric watermarking (or symmetric key watermarking), the same keys are used for embedding and detecting watermarks.

2.3.5 Blind watermarking: Blind watermarking techniques can perform verification of the mark without use of the original image. Other techniques rely on the original to detect the watermark. Many applications require blind schemes; these techniques are often less robust than non blind algorithms.

2.3.6 Steganographic & non-steganographic watermarking: Steganographic watermarking is a technique where content users are unaware that a watermark is present. In non-steganographic watermarking, the users are aware of the presence of a images are required but one also wants to protect these images after they are resampled and used watermark. Steganographic watermarking is used in fingerprinting applications while non-steganographic watermarking techniques can be used to deter piracy.

2.3.7 Parameters and variables used in Digital Watermarking: There are different parameters, which are used for performance evaluation of the watermarking techniques. Some of them are discussed as:

2.3.8 Amount of embedded information: This is an important parameter since it directly influences the watermark robustness. The more information one wants to embed the lower is the watermark robustness. The information to be hidden depends on the application. In order to avoid small scale proprietary solutions, it seems reasonable to assume that one wants to embed a number similar to the one used by the International Standard Book Numbering i.e. ISBN (roughly 10 digits) or better International Standard Recording Code i.e. ISRC (roughly 12 alphanumeric characters) on top of this one should also add the year of copyright, the permission granted on the work and rating for it. This means that roughly 70 bits of information should be embedded in an image. This does not include extra bits added for error correction codes.

2.3.9 Watermark embedding strength: Watermarking embedding strength can be defined as the measure of watermark robustness. For a good watermarking system there is a tradeoff between the watermark embedding strength (hence the watermark robustness) and quality.

Increased robustness requires a stronger embedding, which in turn increases the visual degradation of the images

2.3.10 Size and nature of the picture: Although very small pictures do not have much commercial value, watermarking software needs to be able to recover a watermark from them. This avoids a "Mosaic" attack [9] on them and allows tiling, used very often in Web applications. For printing applications, high resolution on the Web. Photographers and stock photo companies have great concerns about having their work stolen and most of them still rely on small images, visible watermarks and even "roller java script" to reduce infringement. These scripts are used to display images in such a way that they are replaced by another image (typically a copyright sign) when the users moves the cursor on it to save it, but contrary to popular belief that this does not provide any security. Furthermore the nature of image has also an important impact on the watermark robustness. Very often methods featuring a high robustness for scanned natural images have a surprisingly reduced robustness for synthetic images (e.g. computer generated images). A fair benchmark should use a wide range of picture sizes, from few hundred to several thousands pixels, and different kind of images.

2.3.11 Fidelity: A watermark is said to have high fidelity if the degradation it causes is very difficult for a viewer to perceive. However, it only needs to be imperceptible at the time that the media is viewed. If it can be certain that, the media will be seriously degraded before it is viewed, one can rely on that degradation to help mask the watermark. Such a case occurs when one watermarks the video which will be transmitted over NTSC, or audio that will be transmitted over AM radio. The quality of these broadcast technologies is so low that our initial fidelity need not be very good. Conversely, in HDTV and DVD video and audio, the signals are very high quality, and require much higher fidelity watermarks (though, of course, the quality of the content remains the same, a bad movie is a bad movie whether on VHS or DVD).

In some applications, one can accept mildly perceptible watermarks in exchange for higher robustness or lower cost. For example, Hollywood dailies are not finished products. They are usually the results of poor transfers from film to video. Their only purpose is to show those involved in a film production the raw material that has been shot so far. A small visible distortion caused by a watermark will not diminish their value [14].

2.3.12 Secret information: Although the amount of secret information i.e. key has no direct impact on the visual fidelity of the image or the robustness of the watermark, it plays an

important role in the security of the system. The key space, that is the range of all possible values of the secret information, must be large enough to make exhaustive search attacks possible.

2.4 Parameters for Watermarking:

2.4.1 Mean Square Error: This parameter is defined as the root mean square of difference of corresponding pixel values in the original image and watermarked image. Similarly root mean square can be defined as the root mean square of difference of corresponding pixel values in the original image and watermarked image. For a good watermarking system, MSE should be minimum. Further, the root mean square can be calculated by taking square root of the MSE. The mean square error can be expressed as in equation 2.1,

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[\hat{f}(i,j) - f(i,j)\right]^2 \tag{2.1}$$

2.4.2 Peak Signal to Noise Ratio (PSNR):

The PSNR is the only rigorously defined metric. The main reason for this is that no good rigorously defined metrics have been proposed that take the effect of the Human Visual System (HVS) into account. PSNR is provided only to give us a rough approximation of the quality of the watermark. The PSNR in mathematical form can be define as in below equation 2.2

$$PSNR = 10\log_{10}\left[\frac{512\times 512}{MSE}\right] \tag{2.2}$$

2.4.3 Bit Error Rate (BER):

The bit error rate is defined as the ratio of wrong extracted bits to the total number of embedded bits. It is one of the important parameters to be calculated for performance analysis. Thus by calculating the BER of a watermarked image for different conditions such as different block size, different values of robustness coefficient or gain factor, different values of fractional order (a) , one can find out the optimal domain for better watermarking.

2.5 Choice of Watermark-Object:

The first question we need to ask with any watermarking or stenographic system, is what form will the embedded message take? The most straight-forward approach would be to embed text strings into an image, allowing an image to directly carry information such as author, title, date…and so forth. The drawback however to this approach is that ASCII text in a way can be considered to be a form of LZW compression, which each letter being represented with a certain pattern of bits. By compressing the watermark-object before insertion, robustness suffers.

Due to the nature of ASCII codes, a single bit error due to an attack can entirely change the meaning of that character, and thus the message. It would be quite easy for even a simple task such as JPEG compression to reduce a copyright string to a random collection of characters. Rather then characters, why not embed the information in an already highly redundant form, such as a raster image? Not only do images lend themselves to image watermarking applications, but the properties of the HVS can easily be exploited in recognition of a degraded watermark. Consider Figure 3 below:

Figure 2.5: Ideal Watermark-Object vs. Object with Additive Gaussian Noise [12]

2.5. Types of watermarks: The different authors use different meanings for the word 'watermark', it is mostly agreed that the watermark is one, which is imperceptibly added to the cover-object in order to convey the hidden data. The process of embedding information into another object is called watermarking. There are different types of watermarks such as:

2.5.1 Visible watermarks: Visible watermarks are designed to be easily perceived by the viewer, and clearly identify the owner. The watermark must not detract from the image content itself, however.

2.5.2 Invisible watermarks: Invisible watermarks are designed to be imperceptible. This type of watermark is not visible in the watermark image without degradation of image or data. Invisible watermark may be any logo or any signature**.** Most research currently focuses on invisible watermarks, which are imperceptible under normal viewing conditions.

2.5.3 Fragile watermarks: Fragile watermarks are designed to be distorted, or to be broken, under the slightest changes to the image. Semi-fragile watermarks are designed to break under all changes that exceed a user-specified threshold

2.5.4 Robust watermarks: These are the watermarks, which survive any reasonable processing inflicted on the original object. These watermarks are embedded in such a way that any signal transformation of reasonable strength cannot remove the watermark. Hence, a pirate willing to remove the watermark will not succeed unless they debase the document too much to be of commercial interest.

2.5.5 Image-adaptive watermarks: These are usually transform-based and very robust. They locally adapt the strength of the watermark to the image content through perceptual models for human vision. These models were originally developed for image compression.

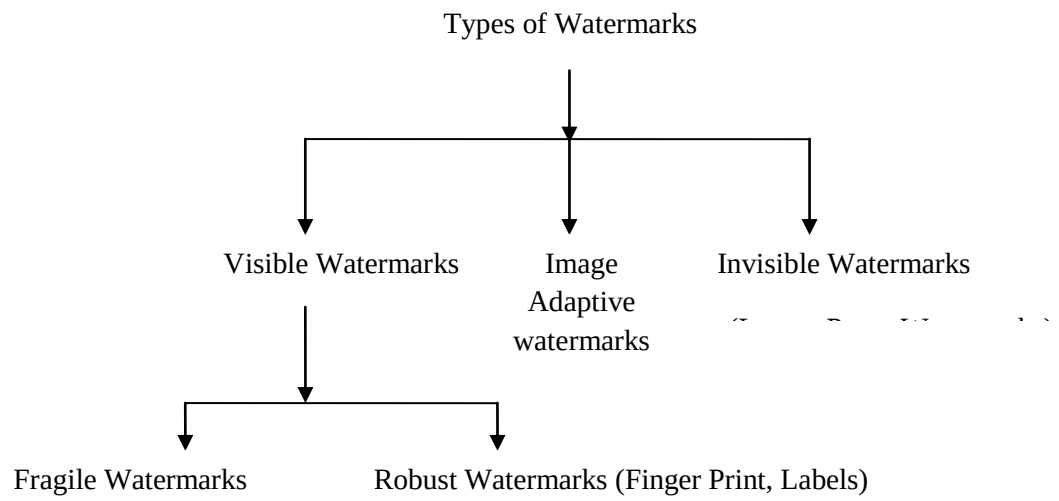


Figure 2.6 Types of Watermarks

2.6 Characteristics of Watermark: A watermark is designed to permanently reside in the host data. When the ownership of data is in question, the information can be extracted to completely characterize the owner. To achieve maximum protection of intellectual property with watermarked media, several requirements must be satisfied such as [10]:

- **Imperceptible:**
  The watermark should be imperceptible so as not to affect the viewing experience of the image or the quality of the audio signal.

- **Undeletable:**
  The watermark must be difficult or even impossible to remove by a malicious cracker, at least without obviously degrading the host signal

  .

- **Statistically undetectable:**
  A pirate should not be able to detect the watermark by comparing several watermarked signals belonging to the same author.

- **Lossless:**
  It should imply no loss of relevant information while an attack is taking place.
- **Robustness:**
  The watermark should be able to survive lossy compression techniques like JPEG, which is commonly used for transmission and storage. The watermark should be retrievable even if common signal processing operations are applied, such as signal enhancement, geometric image operations and noise filtering.

- **Unambiguous:**
  Retrieval of the watermark should unambiguously identify the owner, and the accuracy of identification should degrade gradually in the face of attacks.

2.7 Application of Digital Watermarking:

Although digital data has many advantages over analog data, service providers are reluctant to offer services in digital form because they fear unrestricted duplication and dissemination of copyrighted material. Because of possible copyright issues, the intellectual property of digitally recorded material must be protected. The lack of such adequate protection systems for copyrighted content was the reason for the delayed introduction of the digital versatile disk (DVD) . Several media companies initially refused to provide DVD material until the copy protection problem had been addressed [15].

Representatives of the consumer electronics industry and the motion picture industry have agreed to seek legislation concerning digital video recording devices. Recommendations describing ways that would protect both intellectual property and consumers' rights have been submitted to the U.S. Congress and resulted in the Digital Millennium Copyright Act, which was signed by President Clinton on October 28, 1998. The European Union is also

preparing such intellectual property rights protection for digital multimedia products including CDs or DVDs [16]. To provide copy protection and copyright protection for digital audio and video data, two complementary techniques are being developed encryption and watermarking. Encryption techniques can be used to protect digital data during the transmission from the sender to the receiver.After the receiver has received and decrypted the data, however, the data is identical to the original data and no longer protected. Watermarking techniques can compliment encryption by embedding a secret imperceptible signal, a watermark, directly into the original data in such a way that it always remains present. Such a watermark, for instance, can be used for the following purposes:

- **Owner Identification**: The owner identification can be printed on the covers or mentioned somewhere on the item. Examples are the identification mark of an audio company on the CD case or the mark of the paper manufacturer on top corner of the paper. These types of watermarks can be easily removed by cropping the image or by tearing the part that has the identification. Digital watermarking helps to overcome this problem by embedding the watermark in the form of bits and forming an integral part of the content. The device reads the CD and identifies the watermark. For having further access to the CD the owner should have a license or he should have paid a fee to access the copyrighted work [16].

- **Copy Protection:** To prevent the data from being copied 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 accordingly [14].For the protection of intellectual property, the data owner can embed a watermark representing copyright information in his data. This watermark can prove his ownership in court when someone has infringed on his copyrights.

- **Broadcast Monitoring**: A commercial advertisement may be watermarked by putting a unique watermark in each video or sound clip prior to broadcast. Automated monitoring systems can then receive broadcasts and check for these watermarks, identifying when and where each clip appears. This proves very helpful for the advertisers as they actually pay for only the number of times the advertisement was actually relayed [10]. By embedding watermarks in commercial advertisements, an

automated monitoring system can verify whether advertisements are broadcasted as contracted [3]. Not only commercials but also valuable TV products can be protected by broadcast monitoring [16]. News items can have a value of over US$100,000 per hour, which make them very vulnerable to intellectual property rights violation. A broadcast surveillance system can check all broadcast channels and charge the TV stations according to their findings.

- **Medical applications:** Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster.
- **Fingerprinting:** A fingerprinting technique can be used to trace the source of illegal copy. Every copy available can be watermarked with a unique bit sequence. Now, if a copy is made illegally the source can be easily tracked since each original copy had a unique bit sequence embedded into it [8]. To trace the source of illegal copies, the owner can use a fingerprinting technique. In this case, the owner can embed different watermarks in the copies of the data that are supplied to different customers. Fingerprinting can be compared to embedding a serial number that is related to the customer's identity in the data. It enables the intellectual property owner to identify customers who have broken their license agreement by supplying the data to third parties.
- **Data Authentication:** A given set of data (images) can be easily tampered without even being detected. To avoid this and maintain the originality of the image a watermark like signature, a set of words, may be embedded into the image. If the image is now being tampered it can be easily detected as the pixel values of the embedded data would change and not match the original pixel values. If the image is being copied it would lose its authentication as the embedded data would not be copied along with the image. In this section we discuss some of the scenarios where watermarking is being already used as well as other potential applications. The list given here is by no means complete and intends to give a perspective of the broad range of business possibilities that digital watermarking opens. Fragile watermarks [16] can be used to check the authenticity of the data. A fragile watermark indicates whether the data has been altered and supplies localization information as to where the data was altered. Watermarking techniques are not only used for protection purposes.

- **Authentication:** This is a variant of the previous application, in an area where cryptographic techniques have already made their way. However, there are two significant benefits that arise from using watermarking: first, as in the previous case, the signature becomes embedded in the message; second, it is possible to create 'soft authentication' algorithms that offer a multi valued [15].
- **Hardware/Software Watermarking:** This is a good paradigm that allows us to understand how almost every kind of data can be copyright protected. If one is able to find two different ways of expressing the same information, then one bit of information can be concealed, something that can be easily generalized to any number of bits. This is why it is generally said that a perfect compression scheme does not leave room for watermarking. In the hardware context, Boolean equivalences can be exploited to yield instances that use different types of gates and that can be addressed by the hidden information bits. Software can be also protected not only by finding equivalences between instructions, variable names, or memory addresses, but also by altering the order of non-critical instructions. All this can be accomplished at compiler level.
- **Executable Watermarks:** Once the hidden channel has been created it is possible to include even executable contents, provided that the corresponding applet is running on the end user side.
- **Text Watermarking:** This problem, which in fact was one of the first that was studied within the information hiding area can be solved at two levels. At the printout level, information can be encoded in the way the text lines or words are separated (this facilitates the survival of the watermark even to photocopying). At the semantic level (necessary when raw text files are provided), equivalences between words or expressions can be used, although special care has to be taken not to destruct the possible intention of the author[14].
- **Labeling:** The hidden message could also contain labels that allow for example to annotate images or audio. Of course, the annotation may also been included in a separate file, but with watermarking it results more difficult to destroy or loose this label, since it becomes closely tied to the object that annotates. This is especially useful in medical applications since it prevents dangerous errors.
- **Fingerprinting:** This is similar to the previous application and allows acquisition devices (such as video cameras, audio recorders, etc) to insert information about the specific device (e.g.,an ID number) and date of creation. This can also be done with conventional digital signature techniques but with watermarking it becomes

considerably more difficult to excise or alter the signature. Some digital cameras already include this feature.

- **Copy and Playback Control:** The message carried by the watermark may also contain information regarding copy and display permissions. hence, a secure module can be added in copy or playback equipment to automatically extract this permission information and block further processing if required. In order to be effective, this protection approach requires agreements between content providers and consumer electronics manufacturers to introduce compliant watermark detectors in their video players and recorders. This approach is being taken in Digital Video Disc (DVD). The information stored in a watermark can directly control digital recording devices for copy protection purposes [16]. In this case, the watermark represents a copy-prohibit bit and watermark detectors in the recorder determine whether the data offered to the recorder may be stored or not.
- **Signalling:** The imperceptibility constraint is helpful when transmitting signalling information in the hidden channel. The advantage of using this channel is that no bandwidth increase is required. An interesting application in broadcasting consists in watermarking commercials with signaling information that permits an automatic counting device to assess the number of times that the commercial has been broadcast during a certain period. An alternative to this would require complex recognition software.
- **Indexing:** Indexing of video mail, where comments can be embedded in the video content; indexing of movies and news items, where markers and comments can be inserted that can be used by search engines.
- **Data Hiding:** Watermarking techniques can be used for the transmission of secret private messages. Since various governments restrict the use of encryption services, people may hide their messages in other data. Some authors, for example in [11], refer to watermarking technique only when the application embeds a few bits (as few as one bit) of data for copyright notice/ protection applications. Other applications are considered to fall into the category of data article. In our opinion, watermarking hanowadays been used for applications beyond the limits of copy protection/authentication, an example of which is Digimarc's Smart Images [1]
- **Video Watermarking**: In this case, most considerations made in previous sections hold. However, now the temporal axis can be exploited to increase the redundancy of the watermark. As in the still images case, watermarks can be created either in the spatial or in the DCT domains. In the latter, the results can be directly extrapolated to

MPEG-2 sequences, although different actions must be taken for I, P and B frames. Note that perhaps the set of attacks that can be performed intentionally is not smaller but definitely more expensive than for still images.

- **Audio Watermarking**: Again, previous considerations are valid. In this case, time and frequency masking properties of the human ear are used to conceal the watermark and make it inaudible. The greatest difficulty lies in synchronizing the watermark and the watermarked audio file, but techniques that overcome this problem have been proposed.

CHAPTER 3

Digital Watermarking Techniques

3.1 General

The digital watermarking is technique of embedding the hidden information into original data. There may be different way of embedding the watermark (hidden information) into host data such as embedding in spatial domain, transform domain and fractional domain. The concept of digital watermarking consists of inserting information into the host signal under the condition that the modifications are not perceptible. In addition, it is desirable to put maximum energy into the watermark in order to achieve high robustness. This is a well known concept from communication theory: to decrease the error rate, the signal energy must be maximized. In mathematical formulation, the watermark embedding process can be considered as a constrained maximization problem i.e. to maximize the watermark energy under the visibility constraint. Although the problem is straightforward to formulate, it is extremely difficult to implement because of the visibility constraint, which is usually based on a non-linear model of the human visual system.

A perfect vision system is defined as one that has the capability to distinguish even the slightest changes in visual stimuli. For the human visual system this is, however, not the case. Digital watermarking is only possible because our vision system is not perfect. The deficiencies in detecting certain stimuli or changes in stimuli have been extensively investigated in the past. Models to describe some of the visual effects, such as contrast sensitivity and masking, have been proposed, but for the moment no accurate mathematical description has been found that would allow simulating the full functional range of the human visual system.

Watermark embedding can be performed in a variety of ways as shown in figure 3.1. There are two main groups of watermark embedding technologies: coefficient-based and system-based. Coefficient-based approaches are the most obvious approaches since the embedding process is performed by a direct modification of pixel values or transform coefficient values. Examples of this group are approaches based on pixel modifications in the spatial domain, such as least significant bit watermarking where the least significant bit of the pixel values are replaced by the binary watermark values. Extensions of this basic idea are based on spread spectrum communications and can be applied to a variety of domains a

variety of domains, such as the frequency domain and wavelet domain. Recently, watermarking in the space/spatial-frequency domain has been defined.

The main objective of thesis is to analyze the watermarking in spatial domain, frequency domain fractional domain and wavelet domain. So, these techniques such as least significant bit substitution, correlation based, DCT based, FRDCT, DWT and DWT-SVD based techniques are discussed.

3.2 Spatial Domain Watermarking:

In the spatial domain, watermarking the watermark is embedded by directly modifying the pixel values of the original image. Two techniques under this category are discussed as:

3.2.1 Least Significant Bit Substitution:

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. *Least significant bit (LSB) insertion* is a common, simple approach to embedding information in a cover file. Unfortunately, it is vulnerable to even a slight image manipulation. Converting an image from a format like GIF or BMP, which reconstructs the original message exactly (*lossless compression*) to a JPEG, which does not (*lossy compression*), and then back could destroy the information hidden in the LSBs The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. It can be understand by the following example when using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte.

In other words, one can store 3 bits in each pixel.
An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [17]. For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [19]. Since there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference. In the above example, consecutive bytes of the image data – from the first byte to the end of the message are used to embed the information. This approach is very easy to detect [10]. A slightly more secure system is for the sender and receiver to share a secret key that specifies only certain pixels to be changed. Should an adversary suspect that LSB steganography has been used, he has no way of knowing which pixels to target without the secret key [20]. .The results are shown here. It can be analyzed that LSB method exploits the limitations of HVS.

An improvement on basic LSB substitution would be to use a pseudo-random number generator to determine the pixels to be used for embedding based on a given "seed" or key [21]. Security of the watermark would be improved, as the watermark could no longer be easily viewed by intermediate parties. The algorithm however would still be vulnerable to replacing the LSB's with a constant. Even in locations that were not used for watermarking bits, the impact of the substitution on the cover image would be negligible. LSB modification proves to be a simple and powerful tool for stenography, however lacks the basic robustness that watermarking applications require.

3.2.2 Correlation-Based Techniques:

Another technique for watermark embedding is to exploit the correlation properties of additive pseudo-random noise patterns as applied to an image [22]. A pseudo-random noise (PN) pattern $W(x, y)$ is added to the cover image $I(x, y)$, according to the equation 3.1.

$$I_w(x, y) = I(x, y) + k * W(x, y) \tag{3.1}$$

In equation 3.1, k denotes a gain factor, and $I_w(x, y)$ the resulting watermarked image. Increasing *k* increases the robustness of the watermark at the expense of the quality of the watermarked image [22].

To retrieve the watermark, the same pseudo-random noise generator algorithm is seeded with the same key, and the correlation between the noise pattern and possibly watermarked image compute. If the correlation exceeds a certain threshold T, the watermark is detected, and a single bit is set. This method can easily be extended to a multiple-bit watermark by dividing the image up into blocks, and performing the above procedure independently on each block.

3.2.2.1 Threshold Based Correlation in Spatial Domain:

In this algorithm, a threshold level is used for determining a logical "1" or "0" and it can be eliminated by using two separate pseudo-random noise patterns. One pattern is designated a logical "1" and the other a "0". The above procedure is then performed once for each pattern, and the pattern with the higher resulting correlation is used. This increases the probability of a correct detection, even after the image has been subject to attack. The method can be further modified by pre-filtering the image before applying the watermark. If one can reduce the correlation between the cover image and the PN sequence, one can increase the immunity of the watermark to additional noise. By applying the edge enhancement filter shown below in figure 3.2, the robustness of the watermark can be improved with no loss of capacity and very little reduction of image quality.

$$F_{edge} = \frac{1}{2}\begin{bmatrix} -1 & -1 & -1 \\ -1 & 10 & -1 \\ -1 & -1 & -1 \end{bmatrix}$$

Figure 3.2: FIR Edge Enhancement Pre-Filter [22]

3.2.2.3 CDMA spread spectrum watermarking:

In this technique rather than determining the values of the watermark from "blocks" in the spatial domain, one can employ CDMA spread-spectrum techniques to scatter each of the bits randomly throughout the cover image, increasing capacity and improving resistance to cropping. The watermark is first formatted as a long string rather then a 2D image. For each value of the watermark, a PN sequence is generated using an independent seed. These seeds could either be stored, or themselves generated through PN methods. The summation of all of these PN sequences represents the watermark, which is then scaled and added to the cover image. To detect the watermark, each seed is used to generate its PN sequence, which is then correlated with the entire image. If the correlation is high, that bit in the watermark is set to

“1”, otherwise a “0”. The process is then repeated for all the values of the watermark. CDMA improves on the robustness of the watermark significantly, but requires several orders more of calculation [22].

3.3 Frequency Domain Techniques:

In frequency domain watermarking the cover object is first transformed in frequency domain and then the watermark is added into the frequency domain. Spatial domain watermarking has the advantage that they can be easily applied to any image; regardless of subsequent processing (whether they survive this processing however is a different matter entirely). A possible disadvantage of spatial techniques is they do not allow for the exploitation of this subsequent processing in order to increase the robustness of the watermark.

In addition to this, adaptive watermarking techniques are a bit more difficult in the spatial domain. Both the robustness and quality of the watermark could be improved if the properties of the cover image could similarly be exploited. For instance, it is generally preferable to hide watermarking information in noisy regions and edges of images, rather then in smoother regions. The benefit is two-fold; Degradation in smoother regions of an image is more noticeable to the HVS, and becomes a prime target for lossy compression schemes. Considering these aspects, working in a frequency domain of some sort becomes very attractive. The classic and still most popular domain for image processing is that of the Discrete Cosine Transform (DCT).

3.3.1 Discrete Cosine Transform (DCT):

The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain as shown in figure 3.3(a).

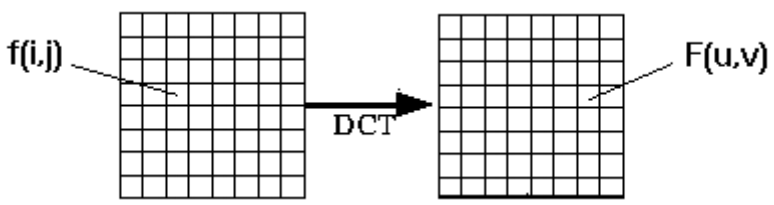


Figure 3.3(a): Spatial to Frequency Domain transformation

3.3.1.1 DCT Encoding:

The general equation for a 1D (*N* data items) DCT is defined by the following equation:

$$C(u) = \alpha(u)\sum_{x=0}^{N-1} f(x)\cos\left[\frac{(2x+1)u\pi}{2N}\right] \qquad (3.2)$$

where u=0,1,2,……, N-1

The corresponding ***inverse*** 1D DCT transform is defined as

$$f(x) = \sum_{x=0}^{N-1}\alpha(u)C(u)\,f(x)\cos\left[\frac{(2x+1)u\pi}{2N}\right] \qquad (3.3)$$

where

$$\alpha(u) = \begin{cases}\sqrt{\frac{1}{N}} & for \quad u = 0\\ \sqrt{\frac{2}{N}} & for \quad u = 1,2,3.....,N-1\end{cases}$$

If one interpret the N-size sequences as column vectors $f = f(x) = \left[f_0, f_{1.....,}f_{N-1}\right]^t$ and $C = C(u) = \left[C_0, C_{1.....,}C_{N-1}\right]^t$ denote the $N \times N$ matrix by

$$D = \left\| \frac{1}{\sqrt{N}}\alpha(u)\cos\left(2\pi\frac{(2x+1)u}{4N}\right)\right\| \qquad (3.4)$$

The general equation for a 2D (*N* by *N* image) DCT is defined by the following equation:

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{u(2x+1)\pi}{2N}\right]\cos\left[\frac{v(2y+1)\pi}{2N}\right] \qquad (3.5)$$

where u, v = 0,1,2,……..,N-1

and the corresponding ***inverse*** 2D DCT transform is defined as

$$f(x,y) = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} C(u,v)\alpha(u)\alpha(v)\cos\left[\frac{u(2x+1)\pi}{2N}\right]\cos\left[\frac{v(2y+1)\pi}{2N}\right] \qquad (3.6)$$

where x, y = 0,1,2,…….N-1

The basic operation of the DCT is as follows:

- The input image is N by M
- $f(x,y)$ is the intensity of the pixel in row x and column y
- $C(u,v)$ is the DCT coefficient in row $u1$ and column $u2$ of the DCT matrix.
- For most images, much of the signal energy lies at low frequencies; these appear in the upper left corner of the DCT.
- Compression is achieved since the lower right values represent higher frequencies, and are often small - small enough to be neglected with little visible distortion.
- The DCT input is an 8 by 8 array of integers. This array contains each pixel's gray scale level.
- 8-bit pixels have levels from 0 to 255.

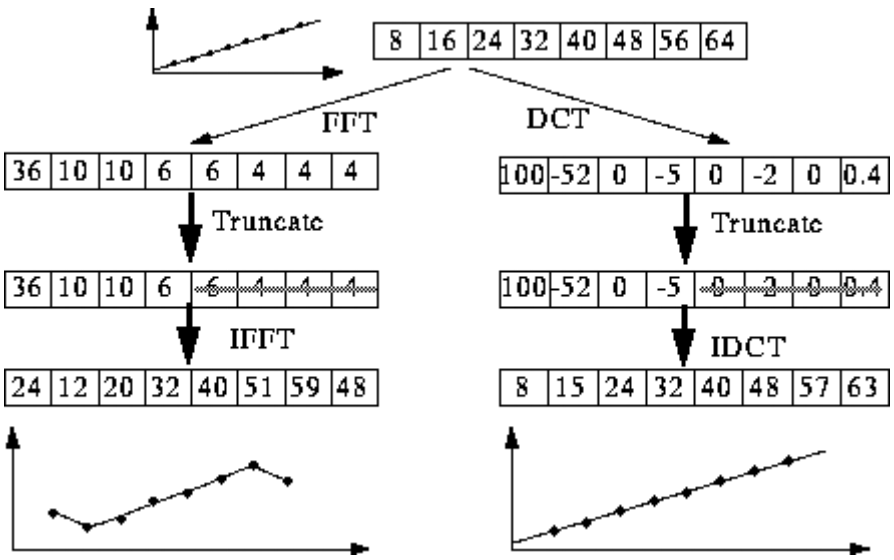


Figure3.3 (b): Computation of DCT vs. FFT

- The output array of DCT coefficients contains integers; these can range from -1024 to 1023.

DCT is similar to the Fast Fourier Transform (FFT), but can approximate lines well with fewer coefficients as shown in figure 3.3(b).

3.3.1.2 Computing the 2D DCT

- Apply 1D DCT (Vertically) to Columns
- Apply 1D DCT (Horizontally) to resultant Vertical DCT above or alternatively Horizontal to Vertical. The equations are given by:

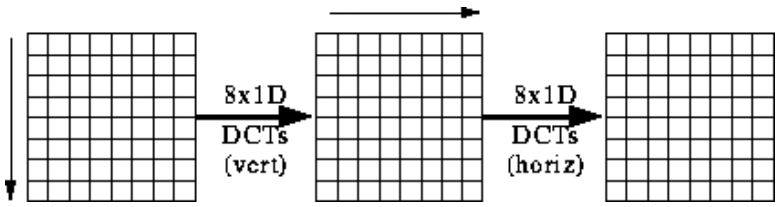


Figure 3.3(c): Computation of 2D DCT

The output array of DCT coefficients contains integers; these can range from -1024 to 1023.

3.3.1.3 Comparison between DCT and FFT: DCT is actually a ***cut-down*** version of the FFT:

- Only the real part of FFT
- Computationally simpler than FFT
- DCT - Effective for Multimedia Compression
- DCT much more commonly used.

3.3.2 Digital watermarking using DCT: Considering these aspects, working in a frequency domain of some sort becomes very attractive. The classic and still most popular domain for image processing is that of the Discrete Cosine Transform (DCT). The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies) [11].

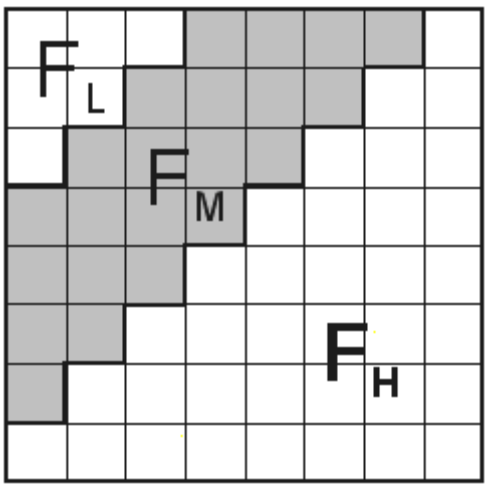


Figure 3.4: Definition of DCT Regions [22]

One such technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. To begin, one define the middle-band frequencies (F_M) of an 8x8 DCT block as shown below in figure 3.4.

F_L is used to denote the lowest frequency components of the block, while F_H is used to denote the higher frequency components. F_M is chosen as the embedding region as to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image [23].

Next two locations $B_i(u1,v1)$ and $B_i(u2,v2)$ are chosen from the F_M region for comparison. Rather then arbitrarily choosing these locations, extra robustness to compression can be achieved if one bases the choice of coefficients on the recommended JPEG quantization table shown below in table 3.1. If two locations are chosen such that they have identical quantization values, it can be felt confident that any scaling of one coefficient will scale the other by the same factor, preserving their relative size.

Table 3.1 Quantization values used in JPEG compression scheme [19]

16	11	10	26	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56

14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Based on the table, it can be observed that coefficients (4, 1) and (3, 2) or (1, 2) and (3, 0) would make suitable candidates for comparison, as their quantization values are equal. The DCT block will encode a "1" if $B_i(u1,v1) > B_i(u2,v2)$; otherwise it will encode a "0". The coefficients are then swapped if the relative size of each coefficient does not agree with the bit that is to be encoded [19]. The swapping of such coefficients should not alter the watermarked image significantly, as it is generally believed that DCT coefficients of middle frequencies have similar magnitudes. The robustness of the watermark can be improved by introducing a watermark "strength" constant *k*, such that $B_i(u1,v1) - B_i(u2,v2) > k$. Coefficients that do not meet these criteria are modified though the use of random noise as to then satisfy the relation. Increasing *k* thus reduces the chance of detection errors at the expense of additional image degradation.

3.3.2.1 Comparison-Based Correlation in DCT mid-band:

Another possible technique is to embed a PN sequence *W* into the middle frequencies of the DCT block. Uses two PN sequences; one for a "0" and another for a "1". If message bit contains zero then embed PN sequence generated for zero into the mid-band components of the DCT transformed block otherwise, embed PN sequence generated for one into the mid-band components of DCT transformed block. After embedding PN sequence the resultant data is transformed back into spatial domain.

DCT block x, y can be modulated by using the equation 3.7 shown below [9]:

$$I_{W_{x,y}}(u,v) = \begin{cases} I_{x,y}(u,v) + k * W_{x,y}(u,v) & u,v \in F_M \\ I_{x,y}(u,v) & u,v \notin F_M \end{cases} \qquad (3.7)$$

For each 8×8 block x, y of the image, the DCT for the block is first calculated. In that block, the middle frequency components F_M are added to the PN sequence *W*, multiplied by a gain factor *k*. Coefficients in the low and middle frequencies are copied over to the transformed image unaffected. Each block is then inverse-transformed to give the final watermarked image.

3.3.2.2 Threshold-Based Correlation in DCT mid-band:

The watermarking procedure can be made somewhat more adaptive by slightly altering the embedding process to the method shown in equation 3.7 [22] as:

$$I_{W_{x,y}}(u,v) = \begin{cases} I_{x,y}(u,v) * (1 + k * W_{x,y}(u,v)) & u,v \in F_M \\ I_{x,y}(u,v) & u,v \notin F_M \end{cases} \quad (3.8)$$

This slight modification scales the strength of the watermarking based on the size of the particular coefficients being used. Larger value of *k* can thus be used for coefficients of higher magnitude, in effect strengthening the watermark in regions that can afford it, weakening it in those that cannot [22].

For detection, the image is broken up into those same 8×8 blocks, and a DCT is performed. The same PN sequence is then compared to the middle frequency values of the transformed block. If the correlation between the sequences exceeds some threshold T, a "1" is detected for that block; otherwise a "0" is detected. The threshold limits is calculated by storing the correlation of each PN sequence and then use the mean of all the correlation of each PN sequence and then use the mean of all the correlations as the threshold T. Here, k denotes the strength of the watermarking, where increasing k increases the robustness of the watermark at the expense of quality.

3.4 Fractional Domain Watermarking:

Watermarking in the fractional domain is the modern technique. This approach uses combination of the space/spatial and frequency domains, without introducing the multidimensional Radon-Wigner distribution [23]. This technique offers many advantages over spatial and transform domain. Watermarking in fractional domain can be obtained by either using Fractional Fourier Transform or Fractional Discrete Cosine Transform (FRDCT). In this thesis, the watermarking in fractional domain is obtained by using FRDCT. Since the

FRDCT has the same property as DCT and DCT has many advantages over FFT. So obviously the FRDCT will give better result as compared to Fractional Fourier Transform (FRFT) but FRFT and FRDCT are discussed here in considerable detail.

3.4.1 Watermarking Using FRFT:

Many techniques are DCT based. Only one specific technique has been discussed here proposed by I. Djurovic et al [23] which adds a watermark in the fractional Fourier transform domain. Not many papers deal with watermarking based on the fractional Fourier technique. See for example [23, 27] for other methods which are more DCT-like since the basic idea is to subdivide the image in smaller (e.g., 8×8 blocks) and hide some bits of the watermark in the transform of each block. We discuss here another technique which computes the fractional Fourier transform (FRFT) of the whole image, then adds a random watermark with certain statistical and deterministic properties and back-transform. The watermark can be detected when the statistical properties are recovered in the appropriate transform.

The fractional Fourier transform (FRFT) over an angle $\propto= \frac{\pi}{2}$ corresponds to the classical Fourier transform, which is denoted as$F^1 = F$. Setting $\propto= \frac{a\pi}{2}$ then F^a is a FRFT over an angle $\propto$ and the notation suggests that it can be interpreted as the a_{th}power of the Fourier operator. Its meaning is that a signal whose energy is concentrated in some domain D of the time-frequency plane, will after the transform F^ahave its energy concentrated in a domain that is obtained by rotating D over an angle $\propto$ from time axis towards frequency axis. The FRFT F^a of order $a \in R$ is a linear integral operator that maps a given function (signal) $f(x), \quad x \in R$ onto $fa(\xi), \xi \in R$ by

$$fa(\xi) = (F^a f)(\xi) = \int K_a(\xi, x) f(x) dx \tag{3.9}$$

where the kernel is defined as follows. Set $\propto= \frac{a\pi}{2}$ then

$$Ka(\xi, x) = c_\alpha \, exp\left\{-i\pi\left(2\frac{x\xi}{sin\alpha} - (x^2 + \xi^2)\, cot\alpha\right)\right\} \tag{3.10}$$

With

$$C_\alpha = \sqrt{1 - cot\,\alpha} = \frac{expf\left\{-i\left[\frac{\pi sgn(sin\,\alpha)}{4} - \frac{\alpha}{2}\right]\right\}}{\sqrt{sin\alpha}} \tag{3.11}$$

For $k \in 2Z$, limiting values are taken which means that

$$K4n(\xi, x) = \delta(\xi, -x) and\ K2 + 4n(\xi, x) = \delta(\xi + x);\ n \in Z \qquad (3.12)$$

The inverse of F^a is given by F^{-a} just change the sign of angles. The discrete FRFT (DFRFT) is for the FRFT like what the DFT is for the Fourier transform. There is not a unique definition, but there is some general agreement on the definition given by Candan and co-workers. It is based on a fractional power of the DFT matrix. For the DFRFT of an image, we consider subsequently the DFRFT of the rows to give a row transformed matrix, and then apply the DFRFT on the columns of the resulting matrix. Note that the transformation angle for rows and columns can be different[28].

3.4.1.1 Watermark Embedding:

The general idea of watermarking in a transform domain is to first compute the transform, then modify the coefficients of the transform and transform back. The method proposed in [4] goes along this idea.

First compute the DRFFT of the image. The watermark should not be embedded in the smallest coefficients because that would make it very sensitive to e.g., noise removing or compressing operations, but it should neither be embedded in the largest coefficients because that would disturb the image too much while we want the watermark to be hidden for normal visual inspection.

Let us sort the DFRFT coefficients according to their magnitude and denote the sorted array as $$\{Si = Vi + jWj : |S_i| \leq |S_{i+1}|, i = 1, 2, 3 \ldots.\} \qquad (3.13)$$

Then we embed the watermark into the coefficients

$$Si, i = L + 1; L + 2, \ldots\ldots, L + M. \qquad (3.14)$$

The watermark itself is a sequence of M complex numbers. The real and imaginary parts are drawn from a normal distribution with mean zero and variance

$$\sigma^2 = 2 \qquad (3.15)$$

Let us denote the watermark as

$$\{s_i = v_i + jw_i : i = L + 1, \ldots\ldots\ldots, L + M\}. \qquad (3.16)$$

The sorted vector s_i is then modified to embed the watermark by setting

$$S_i^w = S_i + v_i|Vi| + jw_i|Wi|;\ i = L + 1, \ldots\ldots\ldots\ldots, L + M \qquad (3.17)$$

After the modified array S_i^w has been rearranged in the original two-dimensional array where the original S_i come from, the watermarked image is then obtained by computing the inverse DFRFT [24].

3.4.1.2 Detection of the watermark:

The image that is submitted to see if it contains the watermark is first transformed with the same DFRFT angles and the result is put in the same order as was used for the embedding.

Because the image may have undergone modifications that may have been deliberate or accidental attacks to the image, we do not get the coefficients S_i^w but we get some coefficients S_i^a instead.

Next the detection value d is computed as:

$$d = \sum_{i=L+1}^{L+M} [v_i - jw_i S_i^a] \quad (3.18)$$

The expected value of d (assuming that the watermark and the image are uncorrelated and assuming that $S_i^a = S_i^w$) is given by

$$E[d] = \frac{1}{2}\sigma^2 (\sum_{i=L+1}^{L+M} |V_i| + |W_i|) \quad (3.19)$$

In [4], it is decided that a watermark has been detected if the computed value of d is larger than a threshold, which is set to $\frac{E[d]}{2}$. This seems reasonable since an image without a watermark has $E[d] = 0$. However, when attacks have modified the image, then the expected value may change drastically.

For example, noise may have been added which increases the total energy, or after cropping several of the watermarked DFRFT coefficients may have been set to zero, which may give a much lower value for the computed d which produces the false conclusion that there is no watermark, while it may still be perfectly detectable.

Therefore the following method is proposed. After the modified image has been DFRFT transformed with the correct angles, then the value of d is computed as suggested above. Next the detection value dt for a sufficiently large number of random watermarks s^t and t = 1, 2……n is computed. The average (sayμ) and the standard deviation (say σ)of these d^tgive for the manipulated image (which may be cropped, noise corrupted. . .) an estimate for the average value of d when the correct watermark is not embedded. The value d for the correct watermark should stand out above this average. Here \stand out" can be defined as being larger than

$$\tau = \mu + p\sigma \quad (3.19)$$

Where p is a suitable number (say 4). The value of p can be used to avoid wrong conclusions. If p is too large, then the real watermark may not be detected and if p is too small, some random watermarks may be identified as the right one, while they are different form the correct one. It is illustrated in Figure 1 that the threshold may vary depending upon the modification that has been induced on the image[24].

So to do a correct detection one has to know

- The correct angles for the DFRFT
- The correct place and length of the watermark (i.e., L and M and the ordering of the DFRFT coefficients).

- The correct watermark, i.e., the sequence $\{s_i : i = L+1, \ldots\ldots, L+M\}$ or a way to generate it.

These data have to be stored during the embedding stage and have to be passed on to the detection algorithm.

3.4.2. Fractional Discrete Cosine Transform (FRDCT):

Fractional Discrete Cosine Transform is a generalized form of Discrete Cosine Transform and it provides a tool to compute the mix time and frequency components of a signal. FRDCT share many useful properties of the regular DCT and it has a free parameter, its fraction. When the fraction is zero, we get the cosine modulated version of the input signal. When it is unity, the conventional DCT is obtained. As the fraction changes from 0 to 1 one get the different forms of the signal which interpolate between the cosine modulated form of the signal and its DCT representation.

Let D_a be a linear operator that for any given fraction $a \in R$ maps an N size vector f into another N size vector $C_a = D_a[f]$. D_a will be an FRDCT operator if one have the following.

(1). D_a verifies the DCT condition $D_1 = D$

(2). D_a has the additive property $D_{a+b} = D_a D_b$ for every choice of real a and b.

(3). D_a is real in the sense that $f \in R^N \Rightarrow C_a \in R^N$ for every $a \in R$ which implies that matrix D_a must be real.

The FRDCT operator can be expressed as

$$D_a : C_a = D_a f \tag{3.20}$$

for a suitable $N \times N$ matrix D_a.The DCT condition (1,2) is then given by $D_1 = D$, where D is the DCT matrix defined by (3).The additive property becomes $D_{a+b} = D_a D_b$, which implies the properties $D_{a+b} = D_b D_a$ and $D_0 = I$. The class of possible definitions is generalized by matrices D_a that satisfy conditions (1, 2, 3). When possible, i.e. when permitted by the eigenstructure, a further constraint is added.

It becomes evident that the formulation of the FRDCT operator requires a rigorous definition of a real power $D_a = D^a$ of the DCT matrix D . To define, D^a one cannot use the theory of "functions of a matrix" since the corresponding scalar function $f(Z) = z^a$ is not analytic.

3.4.2.1 Mathematical analysis in the domain of "Fraction"

The real valued expression for the DCT matrix can be written as

$$D = \sum_{n=1}^{N/2} \left(A_n \cos \varphi_n + B_n Sin \varphi_n \right) \tag{3.21}$$

where φ_n is real and lie in between 0 and π

Similarly the FRDCT matrix D_a can be expressed as

$$D_a = \sum_{n=1}^{N/2} \left(A_n \cos \omega_n a + B_n Sin \omega_n a \right) \tag{3.21}$$

Considering the trigonometric expression of D_a given by equation (3.21), it is easy to write an interpolation formula that allows constructing the whole function D_a, which is continuous in *a,* from *N* of its sample in *a*. Let $a_0, a_1, \ldots\ldots\ldots a_{N-1}$ be *N* distinct fractions and write the system of *N* equations as

$$D_{a_r} = \sum_{n=1}^{N/2} (A_n Cos \omega_n a_r + B_n Sin \omega_n a_r) \tag{3.22}$$

Where r = 0, 1,2……., *N*-1

It can also be written in terms of interpolation sequence as shown in equation (3.23).

$$D_a = \sum_{r=0}^{N-1} D_{a_r} p_r(a) \tag{3.23}$$

Where

$$p_r(a) = \sum_{n=1}^{N/2} (k_{2n-1,r} Cos \omega_n a + k_{2n,r} Sin \omega_n a) \tag{3.24}$$

This is the interpolation formula that gives the FRDCT matrix as a weighted combination of its values at the *N* fractions a_r. From equation (3.23) one can find that the FRDCT C_a of a given sequence f is obtained as

$$C_a = \sum_{r=0}^{N-1} S_{a_r}\, p_r(a) \tag{3.25}$$

Thus to calculate C_a, for all fractions $a \in R$, it is sufficient to evaluate the FRDCTs S_{a_r} of the given sequence f for *N*fraction a_r .To calculate the inverse FRDCT, $f = D_a^{-1}[C_a] = D_a^{-1} C_a$, one can use i.e.

$$f = D_{-a} C_a = \sum_{r=0}^{N-1} D_{a_r} C_a\, p_r(-a) \tag{3.26}$$

Where $C_{a_r} S_a$ the forward FRDCT of is C_a evaluated[24, 27]at the fraction a_r

3.4.2.2 Real Power of FRDCT matrix:

To get a real power of the DCT matrix, one consider the expansion (3) of D and replace the eigen values $\lambda_n = e^{j\phi_n}$ by their a^{th} powers λ_n^a, that is, the matrix Λ by it's a^{th} power Λ^a . Then D_a can be written in the compact form

$$D_a = U \Lambda^a U^* \tag{3.27}$$

where U is a unitary matrix with columns u_n, Λ is the diagonal matrix, with diagonal entries λ_n and $U_n \equiv u_n u_n^*$ are unitary matrices having the properties

$$U_m U_n = \delta_{mn} U_m \ , \ \sum_n U_n = I \tag{3.28}$$

The equation (3.28) satisfies both the DCT condition and the additive property.

As D_a has been defined for any given sequence f , the corresponding FRDCT D_a , with fraction *a*, can be calculated by (3.19). Using the additive property, one have $D_{-a} D_a = D_0 = I$ so that the inverse FRDCT is obtained by using the matrix D_{-a} namely

$$C_a = D_a f \ , \quad f = D_{-a} C_a \tag{3.29}$$

The matrix D_a, which is given by equation (3.27), can be written in alternative forms such as

$$D_a = 2R\left[\sum_{n=1}^{k} U_n \lambda_n^a\right] + V_1(1)^a = V_{-1}(-1)^a \tag{3.30}$$

The latter shows that for $N \neq 4N_0$, the presence of the eigenvalues ± 1 leads to a complex-valued FRDCT matrix since for *'a'* non-natural, $(\pm 1)^a = e^{\pm j2\pi a}$ is a complex number. On the other hand, when $N = 4N_0$, the absence of $(\pm 1)^a$ guarantees that D_a becomes a real-valued matrix. Since the case $N = 4N_0$ is the more attractive for applications. However, an extension of the theory to merely complicate the formulas, but the basic idea still holds.

3.4.2.3 Properties of FRDCT:

The FRDCT [16] has been defined by modifying the DCT and, more specifically, by preserving the orthonormal basis of eigenvectors $u_{\pm n}$ and changing the corresponding eigenvalues $\lambda_{\pm n}^a = e^{\pm j w_n a}$. Since these new eigenvalues have modulus 1 and are distinct (for $a \neq 0$), for every fraction $a \neq 0$ and every generating sequence, the FRDCT operator D_a has exactly the same properties as the original DCT operator D, namely, it is unitary, real orthogonal, and has a unique orthonormal basis (i.e. $u_{\pm n}$). In particular, the unitary property assures the Parseval's relationship $C_a^{'} C_a == f^{'} f = C^{'} C$ for every 'a' and every generating sequence.

The orthogonality property $D_a^{'} D = I$, compared with the additive property $D_{-a} D_a = D_0 = I$, gives

$$D_a^{-1} = D_{-a} = D_a^{'} \tag{3.31}$$

So the matrix D_{-a} is the inverse FRDCT is simply given by transpose of D_a .

3.4.2.4 Computing the 2D FRDCT:

- Apply 1D FRDCT (Vertically) to Columns
- Apply 1D FRDCT (Horizontally) to resultant Vertical DCT above or alternatively Horizontal to Vertical.

In the case of two dimensional FRDCT the two angles of rotation $\alpha = a\pi/2$ and $\beta = b\pi/2$ are to be considered. If one of these angles is zero, the 2D transformation kernel reduces to the 1D transformation kernel. In this paper the angle $\alpha = \beta \neq 0$ is assumed.

The algorithm used for watermarking is same as that used in DCT domain except transformation used. In this type of watermarking, the 2D FRDCT is used for transformation in fractional domain and inverse 2D FRDCT for transformation back into spatial domain[25]. The whole algorithm is same for watermarking process as discussed in section 3.3.

3.5 Wavelet Domain Watermarking:

The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well [9]. We use the DWT to implement a simple watermarking scheme. The 2-D discrete wavelet transform (DWT) decomposes the image into sub-images, 3 details and 1 approximation. The approximation looks just like the original, only on 1/4 the scale.

The 2-D DWT is an application of the 1-D DWT in both the horizontal and the vertical directions. The DWT separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The low-pass and high-pass filters of the wavelet transform naturally break a signal into similar (low pass) and discontinuous/rapidly-changing (high-pass) sub-signals. The slow changing aspects of a signal are preserved in the channel with the low-pass filter and the quickly changing parts are kept in the high-pass filter's channel. Therefore we can embed high energy watermarks in the regions that human vision is less sensitive to, such as the high resolution detail bands (LH, HL, and

HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality [10]. The fact that the DWT is a multi-scale analysis can be used to the watermarking algorithm's benefit. Multi-resolution is the process of taking a filter's output and putting through another pair of analysis filters. The first approximation will be used as a "seed" image and recursively apply the DWT a second and third time.

If watermarking techniques can exploit the characteristics of the HVS, it is possible to hide watermarks with more energy in an image, which makes watermarks more robust. From this point of view the discrete wavelet transform (DWT) is a very attractive transform, because it can be used as a computationally efficient version of the frequency models for the HVS [7]. For instance, it appears that the human eye is less sensitive to noise in high resolution DWT bands and in the DWT bands having an orientation of 45° (i.e.,*HH* bands). Furthermore, DWT image and video coding, such as embedded zero-tree wavelet (EZW) coding, will be included in the upcoming image and video compression standards, such as JPEG2000. By embedding a watermark in the same domain (DWT domain) we can anticipate lossy EZW compression because we can anticipate which DWT bands is going to be affected by the compression scheme. Furthermore, we can exploit the DWT decomposition to make real-time watermark applications. Many approaches apply the basic techniques described at the beginning of this section to the high resolution DWT bands, *LH*1 , *HH*1 , and *HL*1.

an example has been given of an image in which a 2-D CDMA watermark *W* is embedded in the *LH*1 *HH*1 , and *HL*1 DWT bands using a large gain factor *k.*

The DWT coefficients in each of the three DWT bands are modulated as follows:

$$I_w(u,v) = I(u,v) + k \cdot W(u,v) \tag{3.32}$$

TheDWTwatermark can be made image dependent by modulating the DWT coefficients in each of the three DWT bands as follows:

$$I_w(u,v) = I(u,v) * (1 + k.W_{u,v}) \tag{3.33}$$

3.6 DWT –DCT- SVD Watermarking:

This method utilizes the wavelet coefficients of the cover image to embed the watermark. Any of the four sets of wavelet coefficients can be used to watermark the image. The DCT coefficients of the wavelet coefficients are calculated and singular values decomposed. The same procedure is applied to the watermark also. The singular values of the cover image and watermark are added to form the modified singular values of the watermarked image. The modified DCT coefficients form the singular value decompositions triangular matrices. Then the inverse DCT transform is applied followed by the inverse DWT. This is the algorithm that

clubs the properties of SVD, DCT and DWT. This is a technique that has never been used before. Watermark embedded using this algorithm is highly imperceptible. This scheme is robust against all sorts of attacks. It has very high data hiding capacity[32].

First of all we need to understand what singular value Decomposition (SVD) is. Here I have tried to explain as following.

3.6.1 Singular Value Decomposition:

In linear algebra, the singular value decomposition (SVD) is an important factorization of a rectangular real or complex matrix, with several applications in signal processing and statistics. The spectral theorem says that normal matrices can be unitarily diagonalized using a basis of eigen vectors. The SVD can be seen as a generalization of the spectral theorem to arbitrary, not necessarily square, matrices.

Suppose *M* is an *m*-by-*n* matrix. Then there exists a factorization for *M* of the form where, *U* is an *m*-by-*m* unitary matrix, the matrix Σ is *m*-by-*n* with nonnegative numbers on the diagonal and zeros on the off diagonal, and $M = U\Sigma V^T$ denotes the conjugate transpose of *V*, an n-by-n unitary matrix. Such a factorization is called a singular-value decomposition of *M*.

- The matrix *V* thus contains a set of orthonormal 'input' vector directions for the matrix *M*.
- The matrix *U* contains a set of orthonormal 'output' basis vector directions for the matrix *M*
- The matrix Σ contains the singular values, which can be thought of as scalar 'gain controls' by which each corresponding input is multiplied to give a corresponding output.

3.6.2 Watermark Embedding Algorithm:

Lets take a cover image. Apply DWT to decompose the image into four sub-bands LL, HL, LH and HH. Take any of these four sub-bands. Apply DCT to the chosen sub-band. Let '*B*' denote the matrix obtained after applying DCT. Now *B* acts as the host image. Apply SVD so that '*B*' can then be written as

$$B = U_B \Sigma_B {V_B}^T \qquad 3{\cdot}34$$

Where U_B and ${V_B}^T$ are the orthonormal unitary matrices of *B*. The term Σ_B constitutes the singular values of the matrix of *B*.

Let '*W*' represent the watermark. Apply DWT and take any of the four sub-bands. Apply DCT to the chosen sub-band. Let '*S*' denote the matrix obtained after applying DCT. Now *B* acts as the host image. Apply SVD so that '*S*' can then be written as

$$S = U_S \Sigma_S {V_S}^T \qquad 3{\cdot}35$$

where $U_{S \text{ and }} {V_S}^T$ are the orthonormal unitary matrices of *S* . The term Σ_S constitute the singular values of the matrix *S*. Modify the singular values of *B* using singular values of *S*.

Then perform IDCT followed by IDWT to obtain the watermarked image. The four sets of DWT coefficients can be used to embed four different visual watermarks or the same watermark[33].

3.6.3 Watermark Recovery Algorithm:

Let '*A*' be the cover image. Apply DWT and take any of the four sub-bands. Apply DCT to the chosen sub-band. Let '*B*' denote the matrix obtained after applying DCT. Now *B* acts as the host image. Apply SVD so that '*B*' can then be written as

$$B = U_B \Sigma_B V_B{}^T \qquad 3{\cdot}36$$

Where U_B and V_B^T are the orthonormal unitary matrices of *B*. Term Σ_B constitutes the singular values of the matrix of *B*.

Let 'w*' be the watermarked image. Apply DWT and take any of the four sub-bands. Apply DCT to the chosen sub-band. Let '*A**' denote the matrix obtained after applying DCT. Now *A** acts as the host image. Apply SVD so that '*B*' can then be written as

$$B = U_{A^*} \Sigma_{A^*} V_{A^*}^T \qquad 3{\cdot}37$$

Where U_{A^*} and $V_{A^*}^T$ are the orthonormal unitary matrices of A^*. Term Σ_{A^*} constitutes the singular values of the matrix of A^*. Watermark is extracted by subtracting the singular values obtained above.

CHAPTER 4

ATTACKS ON WATERMARKING

The purpose of watermarking is to survive the authenticity of the original data against threats or attacks. Attacks can be of different types such as: removal attacks, geometrical attacks, cryptographic attacks, and protocol attacks [17]. The aim of removal attacks, as the word indicates, is to remove the embedded watermark. This type of attack is based on, for example, denoising or watermark prediction and removal. The effect of removal attacks is, in general, a decrease in the effective channel capacity. Geometrical attacks do not intend to remove the embedded watermark, but to distort it so that detection is impaired. In terms of communication theory, it may be considered as a process with the aim of desynchronizing the signals. Depending on the underlying watermarking technology, geometrical attacks either reduce the channel capacity or fully impair watermark detection. Cryptographic attacks describe attacks very similar to those used in cryptography. Cryptographic attacks [18] aim to remove or destroy the embedded watermark. They are based on concepts such as brute force search of the key space, statistical averaging of several watermarked images, or the collusion of several watermarked images. The last group, protocol attacks, takes a more global approach by identifying weaknesses on a system level and then showing that a given watermarking method is not secure. An example of a protocol attack is the copy attack, which is very efficient in cases where the watermark is used to authenticate the image on an identification document, that is, when the watermarking technology is used to embed information about the owner of the passport into the image. If someone swaps the images it can be easily detected since the new image does not contain a valid watermark. However, if the watermarking technology is not resilient to the copy attack, then it is possible to copy the watermark from the original image to the counterfeit image. From the above discussion, it is found that for an effective technology development, it is of the most importance to consider attacks during the design process. The result will be better system performance and higher security due to an optimized design of the watermark extractor. Thus the possible attacks on watermarks can be defined as:

4.2 JPEG Compression

JPEG stands for Joint Photographic Experts Group. JPEG is a standardized image compression mechanism [19-20]. JPEG is designed for compressing either full-color (24 bit/pixel) or gray-scale images of natural, real-world scenes. It works well on photographs, naturalistic artwork and similar material; not so well on lettering, simple cartoons or line drawings. JPEG handles only still images, but there is a related standard called MPEG for motion pictures A useful property of JPEG is that the degree of lossiness can be varied by adjusting compression parameters. This means that the image maker can trade off file size against output image quality. One can make extremely small files at the cost of image quality. This is useful for applications such as indexing image archives. Conversely, if compressed image quality is not satisfactory at the default compression setting, one can jack up the quality until satisfactory result is found and accept lesser compression.For full-color images, the uncompressed data is normally 24 bits/pixel. The best known lossless compression methods can compress such data about 2:1 on average. JPEG can typically achieve 10:1 to 20:1 compression without visible loss, bringing the effective storage requirement down to 1 to 2 bits/pixel. 30:1 to 50:1 compression is possible with small to moderate defects, while for very-low-quality purposes such as previews or archive indexes, 100:1 compression is quite feasible. An image compressed 100:1 with JPEG takes up the same space as a full-color one-tenth-scale thumbnail image, yet it retains much more detail than such a thumbnail. The second fundamental advantage of JPEG is that it stores full color information: 24 bits/pixel (16 million colors). GIF, the other image format widely used on the net, can only store 8 bits/pixel (256 or fewer colors). GIF is reasonably well matched to inexpensive computer displays. Most run-of-the-mill PCs can't display more than 256 distinct colors at once. But full-color hardware is getting cheaper all the time and JPEG photos look much better than GIFs on such hardware. Furthermore, JPEG is far more useful than GIF for exchanging images among people with widely varying display hardware, because it avoids prejudging how many colors to use. If JPEG is compared with GIF, the size ratio is usually less like 1:4. Hence JPEG is considerably used for compression instead of other technique. So any watermarking system designed for watermarking should be resilient to some degree of compression.

4.3 Geometric Transformations

In geometric transformation [21] the position and value of pixels are changed by using the different transformation such as

4.3.1 Horizontal Transformation

Many images can be flipped without loosing any value. Although resilience to flipping is usually straightforward to implement only very few systems do survive it.

4.3.2 Rotation

Small angle rotation, often in combination with cropping, does not usually change the commercial value of the image but can make the watermark undetectable. Rotations are used to realign horizontal features of an image after it has been scanned. For benchmarking rotated image is proposed to be cropped so that there is no need to add a fixed border to it.

4.3.3 Cropping

In some cases, infringers are just interested by the "central" part of the copyrighted material moreover more and more Web sites use image segmentation, which is the basis of the "Mosaic" attack. This is of course an extreme case of cropping.

4.3.4 Scaling

This happens when a printed image is scanned or when a high resolution digital image is used for electronic application such as Web publishing. Scaling can be divided into two groups, uniform and non-uniform scaling. Very often digital watermarking methods are resilient only to uniform scaling.

4.3.5 Deletion of Lines or Columns

This was the first attack on copyright marking systems and is very efficient against any straightforward implementation of spread spectrum techniques in the spatial domain. Removing *k* samples at regular intervals in a pseudo random sequence (-1, 1) (hence shifting the next ones) typically divides by *k* the amplitude of the cross correlation peak with the original sequence.

4.3.6 Generalized geometrical transformations

A generalized geometrical transformation is a combination of non-uniform scaling, rotation and shearing.

4.3.7 Geometric distortions with JPEG

Rotation and scaling alone are not enough they should be tested in combination with JPEG compression. Since most artists will first apply the geometric transformation and then save the image in a compressed format it makes sense to test robustness of watermarking system to geometric transformation followed by compression**.** However an exhaustive test should also include the contrary since it might be tried by willful infringers. It is difficult to choose a minimal "quality factors" for JPEG as artifact quickly appear. However experience from professionals show that "quality factors" down to 70% are reasonable. Artists seem to use JPEG extensively as well as resizing.

4.4 Enhancement Techniques

Image enhancement refers to accentuation or sharpening of image feature such as edge boundaries or contrast to make a graphic more useful for display and analysis. Enhancement process increases dynamic range of the chosen features so that they can be detected easily. Image enhancement includes following process [22].

4.4.1 Smoothing Filters

Smoothing filters are used for blurring and noise reduction. Blurring is used in preprocessing steps, such as removal of small details from an image prior to object extraction and bridging of small gaps in lines or curves. This includes linear and non-linear filters. Frequently used filters include median, Gaussian and standard average filters. In median filter the gray level of each pixel is replaced by the median of the gray levels in a neighborhood of that pixel, instead of by the average.

4.4.2 Sharpening

The principle operation of sharpening is to highlight fine detail in an image or to enhance detail that has been blurred, either in error or as a natural effect of a particular method of image acquisition. The sharpening filters [23] can be used an effective attack on some watermarking schemes because they are very effective at detecting high frequency noise introduced by some digital watermarking software.

CHAPTER 5

Results & Discussions

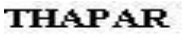
5.1 Results and Discussion:

The algorithms are tested on the reference Lena image figure 5.1 (a) for a small range of gain (*k*) and correlation coefficient (*k*) and two types of attacks i.e. addition of Gaussian noise and JPEG compression. Evaluating each of the algorithms against all attacks across a full range of gain values is well beyond the scope of this report. Therefore, first, robustness evaluations were limited to testing against JPEG compression and the addition of random noise. However, watermarking in DWT domain has been tested for robustness using different kind of attacks like motion blur and sharpening etc.

Two different watermarks shown in figure 5.1(b) and 5.1(c) of different size are used for embedding the original image. The graph for robustness coefficient (*k*) vs. different parameters are taken for each watermarked image and discussed in this chapter, however these figures are only to be taken lightly. PSNR does not take aspects of the HVS into effect so images with higher PSNR's may not necessarily look better than those with a low PSNR. This will prove particularly true in all the cases.

The algorithms are implemented in the most straightforward way, not the most computationally optimal. Furthermore, MATLAB may handle certain programming constructs differently from other languages, thus the best performing algorithm may vary for each language and implementation.

(a)



(b) **(c)**

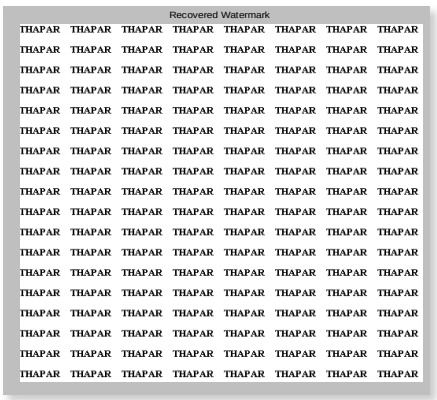
Figure 5.1: (a) Original Lena Image (b) Large watermark (65× 24)

(c) Small Watermark (12× 9)

5.2 Spatial Domain Watermarking

5.2.1 Digital Watermarking using Least Significant Bit Substitution:

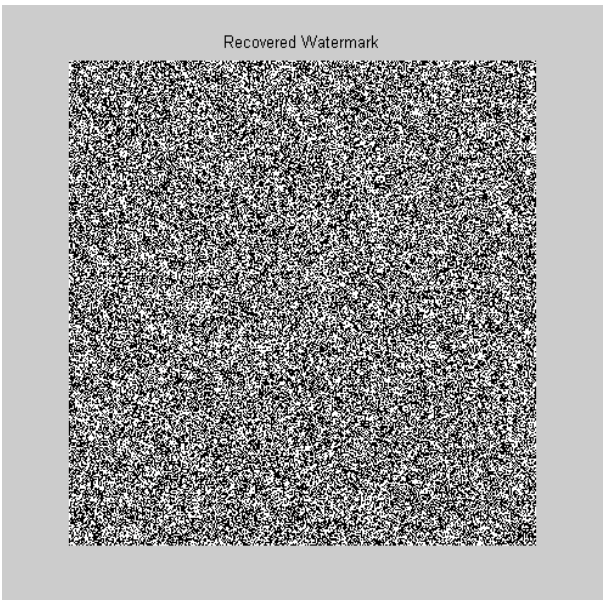
Results from LSB substitution are shown in figure 5.2(a)-(f). The watermarked image shows little but not noticeable degradation, while the large watermark is recovered perfectly as shown in figure 5.2 (b).Although the watermark is recovered perfectly in the ideal case, the addition of any amount of noise or compression of the image using JPEG fully destroys the embedded watermark, leaving nothing but noise as shown in figures 5.2(e) and (f). Even worse, the watermark can be removed with no perceivable change to the watermarked image. The message capacity of LSB embedding however is quite good, a 1:1 correlation with the size of the image. The addition of noise or JPEG compression up to a limit does not cause the noticeable visual degradation in watermarked image as shown in figures 5.2 (c) and (d). If some attack takes place then watermark is not recognizable. After addition of Gaussian noise to the image the recovered watermark can be seen in figure 5.2 (e) and after compression the recovered watermark is shown in figure 5.2(f).



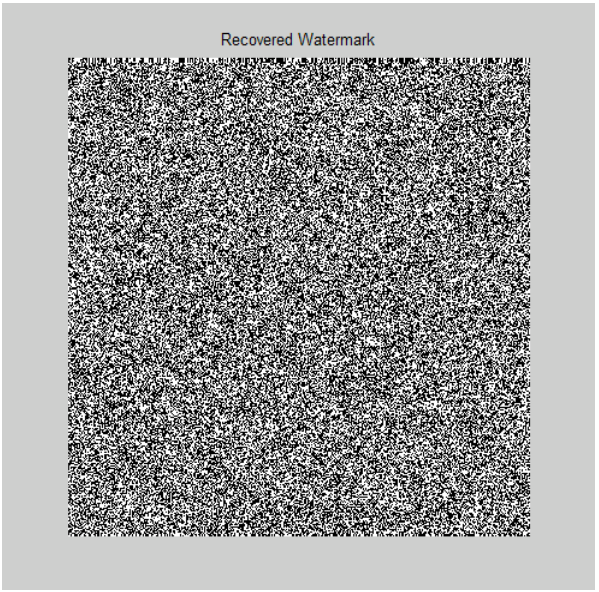
(a) Watermarked Image **(b) Recovered Watermark**

(c) Watermarked Image after addition of 7% Gaussian

(d) Watermarked Image after 50% compression



(e) Recovered Watermarked after addition of 7% Gaussian noise



(f) Recovered Watermarked after 50% compression

Figure 5.2: Watermarking using LSB method

5.2.2 Digital Watermarking using Threshold-Based Correlation:

The results of threshold-based correlation are shown in figure 5.3(a)-(f) several parameters however have been discussed before moving on to results of this technique. An optimum gain factor is chosen experimentally by calculating PSNR, MSE and BER for different gain factor. However, larger factors might be used for increased robustness at the expense of visual quality.

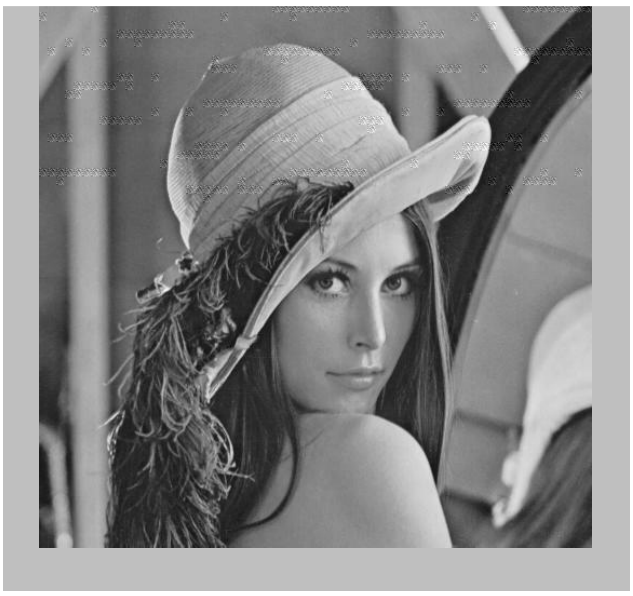
A final consideration is the size of the watermark being embedded. Use of a smaller watermark will allow larger blocks to be used, increasing the strength of correlation and thus system robustness. Using the normal sized watermark, the largest possible block size {8, 16, 32…} is determined by: $1000 \leq \frac{512 * 512}{16^2}$ for a maximum block size of 16 [22].

Thus, the size of watermark does not much effect the visual quality of the watermarked image a normal watermark of size. Although with a gain of 5 the watermark can still be recognized, the results are not spectacular. Increasing the gain does improve watermark recovery, however beyond a *k* of 5, the blocky regions of noise become visible in the watermarked image, as shown in figure 5.3(c) and (d). Also, note the severe drop in PSNR between the two watermarked images. Although the watermark is not perfectly recovered as shown in figure 5.3(e), threshold-based correlation fares much better then LSB in the presence of noise and compression. Using a gain of 5, the watermark is still slightly distinguishable after light levels of noise and compression as shown in figure 5.3(a) and 5.3(b). As expected, increasing the gain to 50, improves the watermark's robustness significantly as shown in figure 5.3(c) and 5.3(d). But increasing the processing gain reduces the imperceptibility of the technique used as the blocky regions appear in the watermarked image. The watermark is recovered with better visibility with increase in the processing gain. Figure 5.3(i) and (h) are the recovered watermark for small watermark.

The water mark recovered in figure 5.3(h) is using a pre filter having *k*=30. The use of pre filter helpful for watermark extraction process.

(a)Watermarked image without using pre filter, *k*=5

(b) Watermarked image using pre filter *k*=5



(c) Watermarked image with *k*=30

(d) Watermarked image with *k*=50

(e) Watermark recovered, *k*=5

(f) Watermark recovered, *k*=30

(g) Watermark recovered *k*=50

(h) Watermark recovered using pre filter *k*=30

(i) Small watermark recovered after 5% Gaussian noise *k*=20

(j) Small watermark recovered after JPEG compression 50% *k*=20

Figure 5.3: Watermarked image and Recovered watermark under different attacks with varying value of *k*.

5.2.3 Digital Watermarking using Comparison-Based Correlation

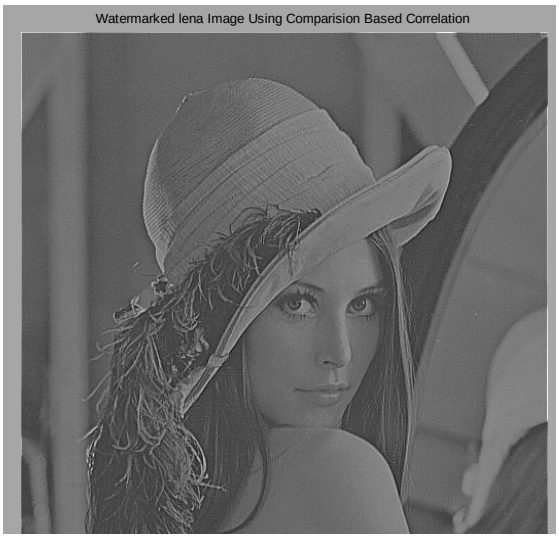
In this technique, two separate PN sequences are used for embedding; one to encode a "1" and another "0". This approach has the advantage of not requiring a "blind" choice of threshold, as the pattern with the higher correlation is chosen. Furthermore, by careful choice of these two patterns to be as un-correlated as possible, we can reduce the change of false detection significantly.

A more subtle advantage is that the approach makes better use of the HVS in spreading its noise throughout the image. The eye is more sensitive to abrupt changes in quality, hence blocky regions of noise will tend to disturb viewers more than a constant level of noise would.

As shown in figure 5.34 the PSNR has decreased by nearly 10 dB and even after that the image remains nearly identical to the reference image. The bit error rate is also lesser as compared to threshold based embedding as shown in figure 5.36.

From the figure 5.4(a)-(d) it can be noted that the comparison-based watermark with gain 20 performed marginally better then even the threshold-based with gain 40; with less impact on the cover image. This method also performs better under the attack as shown in figure 5.4(g) and 5.4(h). Hence robustness is improved as well in the comparison-based watermark.

A disadvantage of these block-based techniques in relation to LSB embedding is that they are highly fragile to flips, crops and rotations i.e. geometric attacks. These transformations alter the coordinate systems of the image, making the task of matching up blocks in embedding and recovery quite difficult. The technique however should prove fairly resistant to contrast, brightness and any other sort of per-pixel transform. Keeping Block size =8 the results are obtained by varying processing gain *k.*

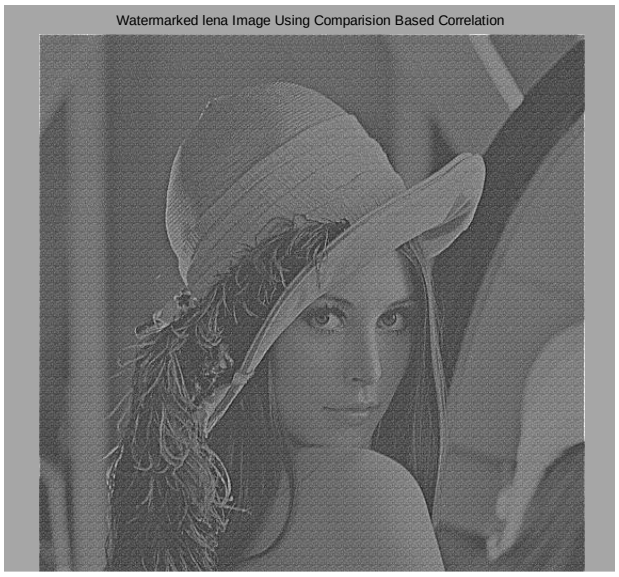


(a) Watermarked image using small watermark with *k*=20

(b) Recovered Watermark, *k*=20

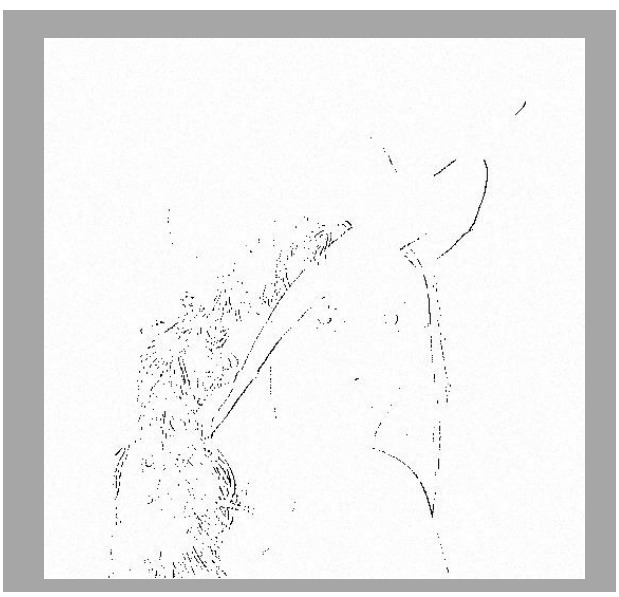
(c) Watermarked image using small watermark with *k*=50

(d) Recovered watermark, *k*=50

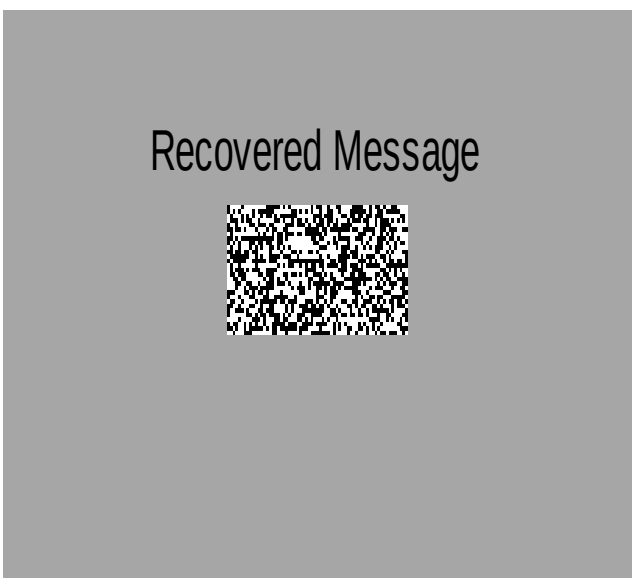


(e) Watermarked image using normal watermark with *k*=50

(f) Recovered watermark, *k*=50



(e) Watermarked image with 5% Gaussian noise with k=20



(f) Recovered watermark, *k*=20

Figure 5.4: Watermarked image and recovered watermark for varying *k*

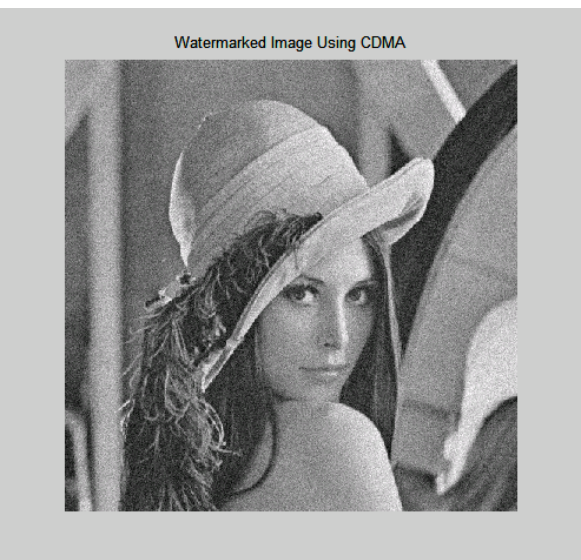
5.2.4 Digital Watermarking using CDMA Spread-Spectrum

As shown in figure 5.5(a)- (d) CDMA performed wonderfully using the smaller message under the attacks. The watermark is recovered perfectly even after addition of 5% Gaussian noise and JPEG compression with compression ratio (CR) of 50% with smaller gain factor i.e. *k*=5, thus increasing the robustness. This technique survives up to 50% addition of noise

and JPEG with CR of 85%. Through experimentation, the gain factor k=5 is arrived at as a good balance between visual quality and watermark robustness.

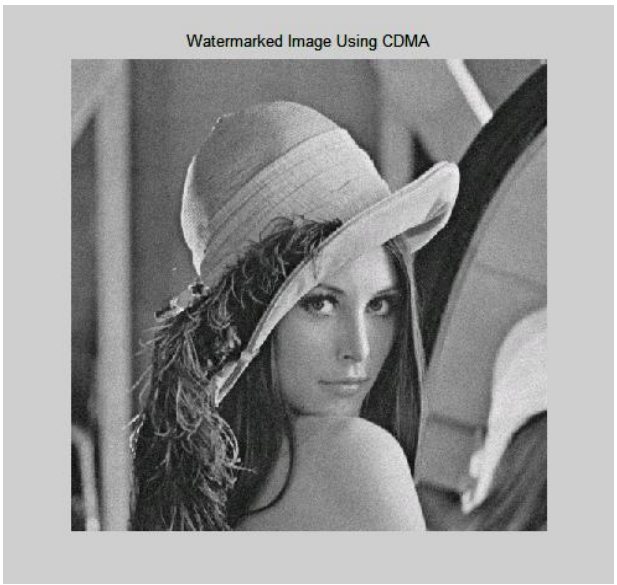
Based on the results of figure 5.5(e) and 5.5(f), it can be concluded that CDMA in the spatial domain easily meets the requirements for "moderate" robustness, provided that the encoding messages are relatively small. The watermarked image is entirely unrecognizable after the addition of 50% Gaussian noise or after compression with CR of 85%. Even after such heavy attacks, the watermark survives in the watermarked image and can be recovered as shown in figure 5.5(e) and 5.5(f).

The main limitations of CDMA in the spatial domain however remain its limited capacity and high processing requirements. Processing time for spatial-domain CDMA watermarking increases exponentially with increasing message sizes. The embedding of large watermarks using CDMA requires the embedding gain to be lowered to preserve the visual quality of the image. As more PN sequences are added to the cover image however, larger gains are required to preserve correlation between like sequences. This underlying conflict is the reason that CDMA in the spatial domain will remain more limited in capacity then other techniques.

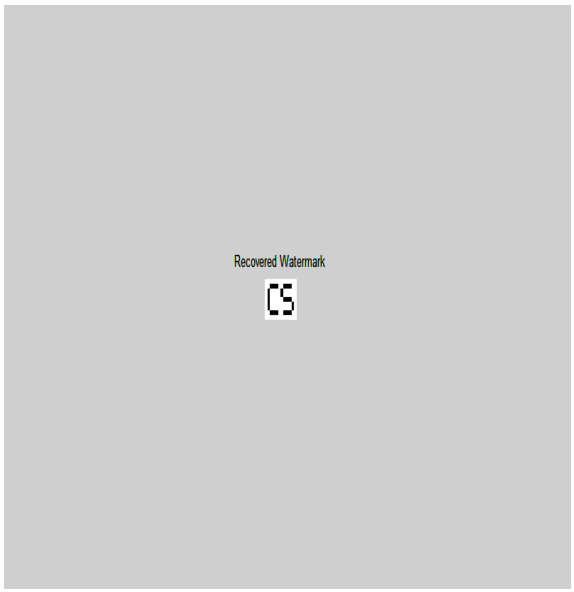


(a) Watermarked image with Normal watermark when k=5

(b) Recovered watermark



(c) Watermarked image with small watermark k=5



(d) Recovered watermark

(e) Recovered watermark after addition of 5% Gaussian noise

(f) Recovered smaller watermark

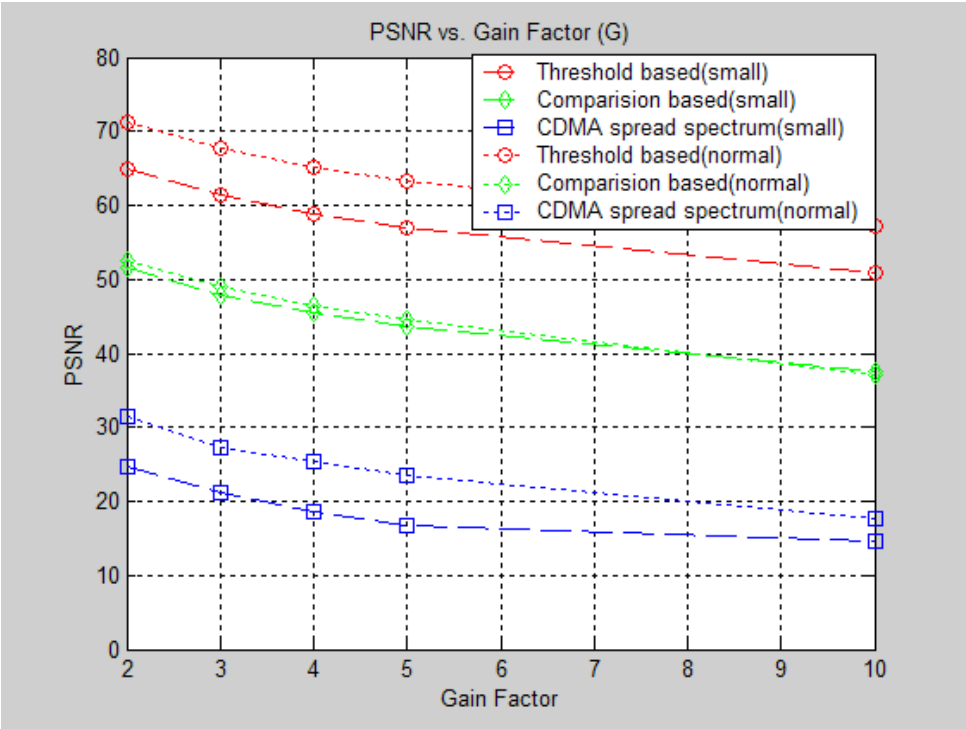
Figure 5.5: Watermarked image and recovered watermark for varying k using CDMA

5.2.5 Effects of varying Gain Factor:

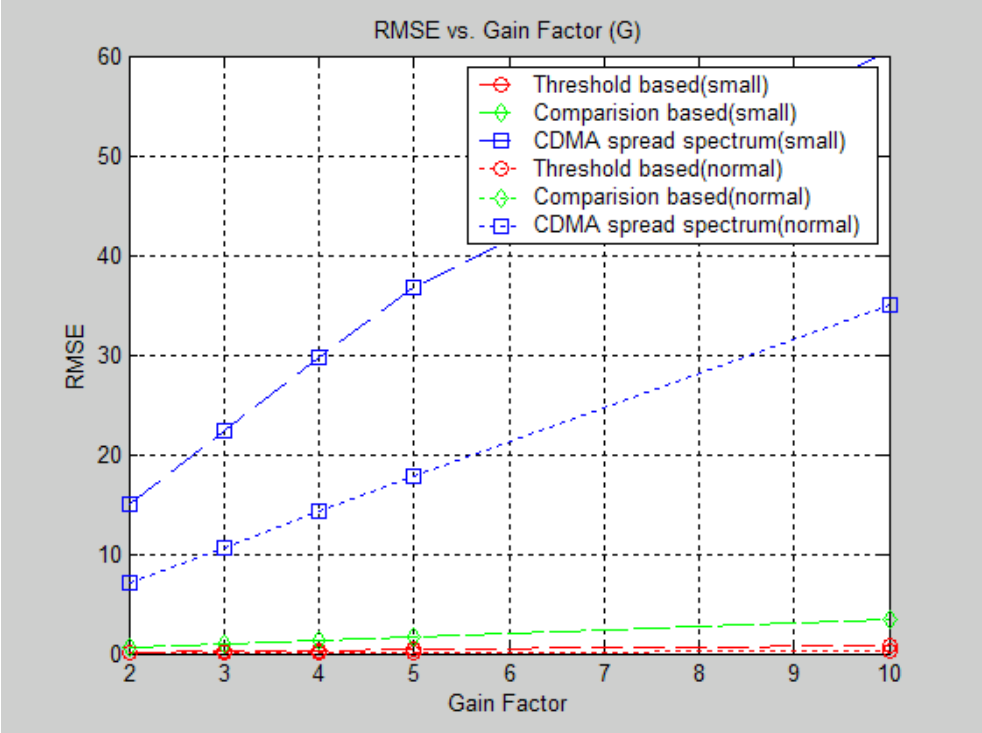
Figure 5.6(a) and 5.6(b) show the effect of variation of gain factor (*k*) on the PSNR and MSE. As the gain factor is increased the PSNR reduces hence reducing the image quality. This is true for all the techniques discussed above. However, higher the gains factor more the robustness. Thus, a gain factor is chosen, which maintain the robustness as well as quality of image.

5.2.6 Effect of Watermark Size:

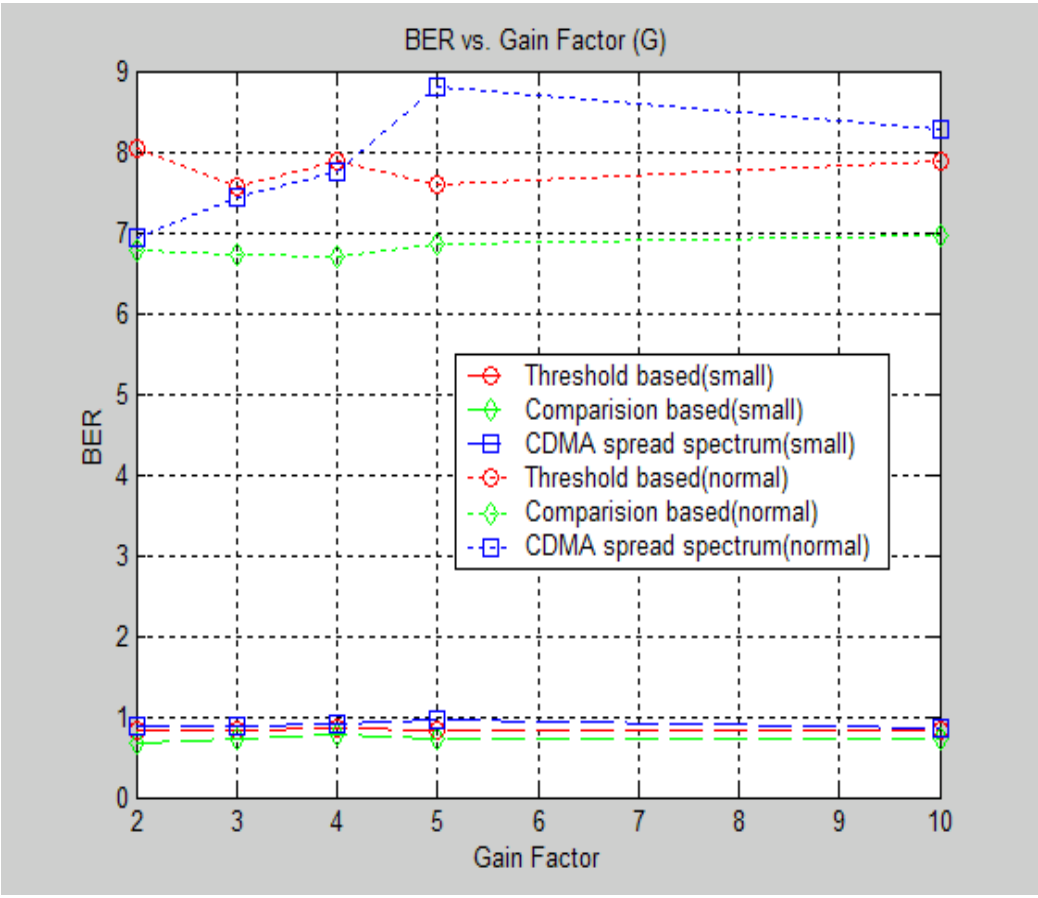
From the figure 5.6(a) and5.6 (b) it is observed that as the size of watermark is decreased, the PSNR increases and MSE decreases. However, bit error rate decrease as the size of watermark is reduced as shown in figure 5.6(c).



(a) Different processing Gain factor (k) v_s. PSNR for different size watermark



(b) Different processing Gain factor (*k*) v_s. RMSE for different size watermark



(c) Different processing gain factor (*k*) v_s. BER for different size watermark

Figure 5.6: (a) Processing gain(*k*) v_s PSNR (b) Processing gain(*k*) v_s RMSE

(c) Processing gain(*k*) v_s BER

5.3 Transform Domain Watermarking

5.3.1 Comparison of mid-band DCT Coefficients:

In this case, a correlation coefficient (*k*) is taken to increase the robustness instead taking a gain factor such as correlation-based techniques. When the two differences in magnitude between the two coefficients being compared do not exceed (*k*), those coefficients are scaled such that they meet this requirement. As in previous techniques, *k* is chosen experimentally however larger *k*'s may be used for increased robustness at the expense of quality.

As shown in figure 5.7(a)-(d) one can observe that the technique works perfectly for un-altered images, with good visual quality of the watermarked image. The results are taken for correlation coefficient of 35. The block size for each of the DCT-based techniques is kept constant i.e. 8×8, in anticipation of JPEG compression. Better results could be obtained using larger block sizes at the expense of message capacity.

The comparison of mid-band based DCT-coefficients proved to be both moderately robust against Gaussian noise, and extremely robust against JPEG compression as shown in figure 5.7(c) and 5.7(d).Good recovery results are still possible with heavy attack as shown in figure 5.7(b) and5.7(d). As shown in figure 5.7(d) the recovered watermark is still recognizable after compression with CR of 85%. The watermarked image at this point is showing heavy JPEG artifacts, reducing quality of the attacked image beyond usability. Figure 5.7(e) and 5.7(f) show that the smaller watermark has been extracted completely.

The best comparison can be made with CDMA in the spatial domain. Although CDMA was more resistant to Gaussian noise, comparison of DCT coefficients proved far more resistant to JPEG compression. This would tend to indicate that embedding the watermark in the same domain as expected transformations is clearly advantageous. By predicting which DCT coefficients would be altered using JPEG, an extremely high level of JPEG robustness was achieved.

(a) Watermarked image using comparison of mid band coefficient

(b) Recovered watermark

(c) Watermarked image after CR=50%

(d) Recovered watermark after Compression

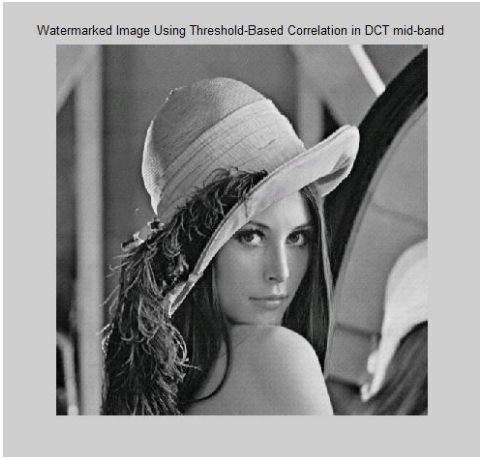
(e) Watermarked image with small watermark

(f) Recovered Watermark

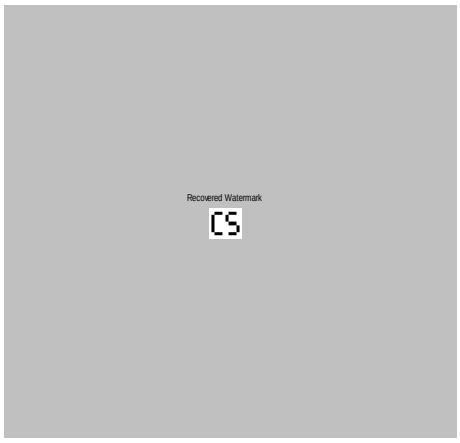
Figure 5.7 Watermarked image and recovered watermarks for correlation coeff. *k* =30

5.3.2 Threshold - based correlation in the DCT mid-band:

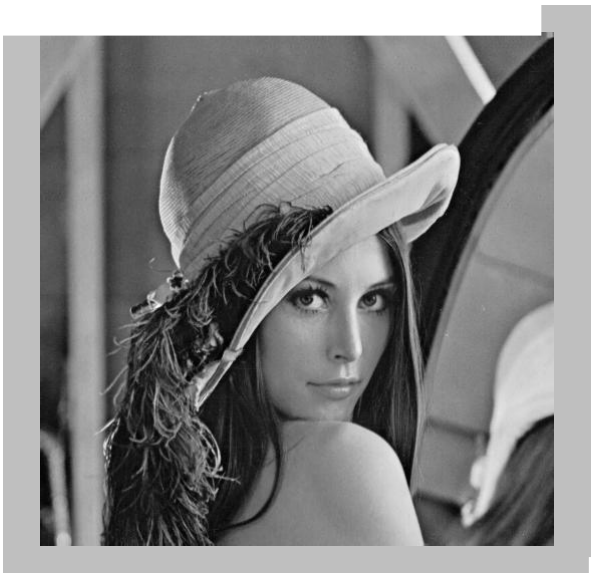
This technique gives the better result as compare to comparison of DCT mid band coefficient technique as shown in figure 5.8(a)-(d).The PSNR for this technique is reduced by 2 dB, still it gives higher robustness with gain factor (k=5) under the attacks as shown in figure 5.8(e)-(h) and 5.47.Although the watermark was not perfectly recovered, threshold-based correlation fares better then the mid band comparison of DCT coefficient in the presence of noise an compression.



(a) Watermarked image using small watermark, *k*=5



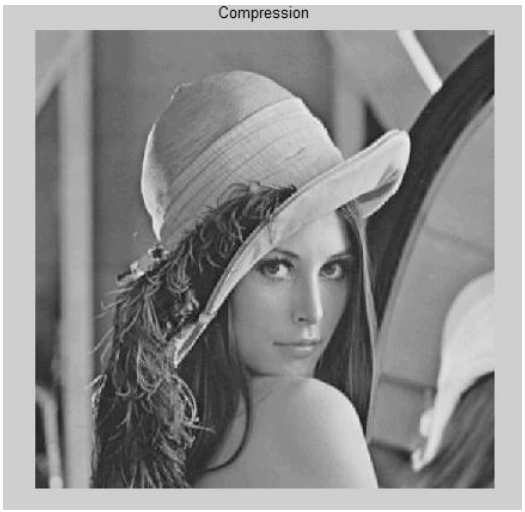
(b) Recovered Watermark



(c) Watermarked image using *k*=5

(e) Watermarked image after 50% Gaussian noise

(f) Recovered Watermark



(g) Watermarked image after 50% JPEG compression

(h) Recovered watermark

Figure 5.8: Threshold Based watermarking and performance under different attacks

5.3.3 Comparison-based correlation in the DCT mid-band:

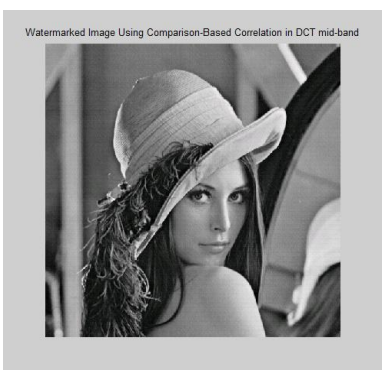
The comparison based correlation in the DCT mid-band give the better result for smaller gain factor as compared to threshold-based correlation as shown in figure 5.9(a)-(b). The results are taken for the gain factor of 10. If compression has been done using 50% CR than the recovered watermark has been shown in figure 5.9(c)-(d). Correlation-based DCT appeared to be slightly weaker for lower levels of distortion, yet stronger for the higher levels as shown in figure 5.9(c)-(d). From these results, it can be concluded that the results obtained from threshold-based correlation in the DCT mid-band are worse than the comparison-based approach. However, better results can be achieved using smaller watermark. The results can be seen in figure 5.9(e)-(f). The smaller Watermark recovered in figure 5.9(f) is almost recovered perfectly using k=5.The watermarked image and recovered watermark has been shown in figure5.9 (g)-(h) under heavy compression ratio 85%.

(a) Watermarked image using comparison Based Corr. in DCT mid-band

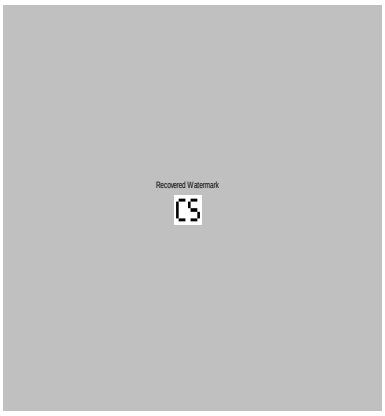
(b) Recovered Watermark

(c) Watermarked Comparison-Based corr in DCT Mid band with CR 50%

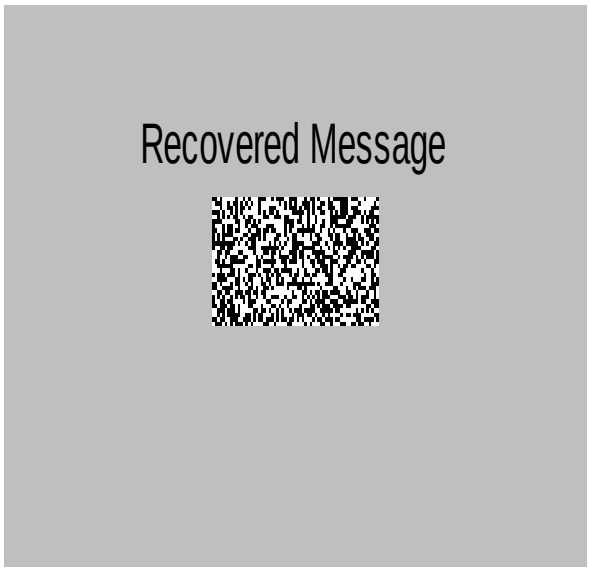
(d) Recovered Watermark



(e) Watermarked Comparison-Based Correlation in DCT Mid band, *k*=5



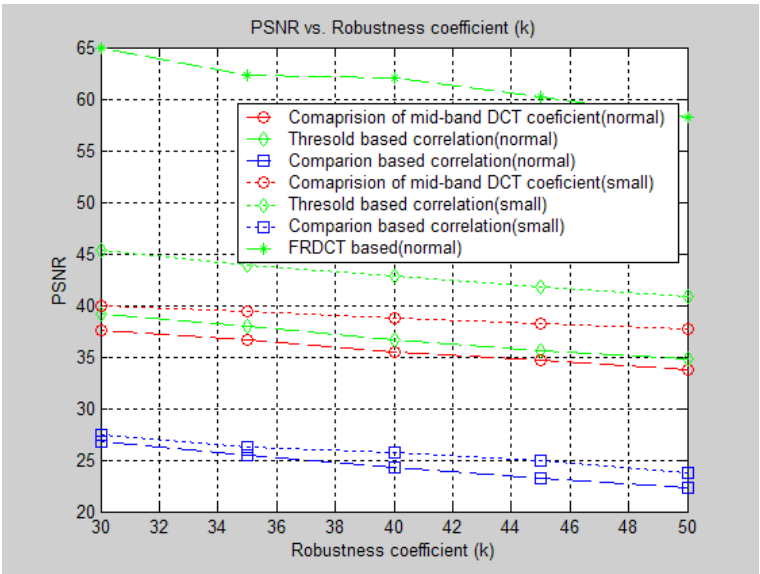
(f) Recovered Watermark



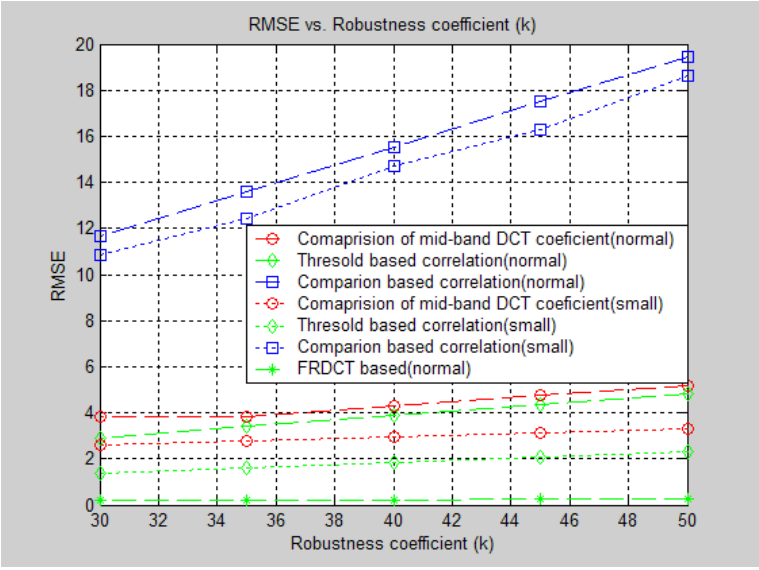
(g) Watermarked image after 80% Gaussian noise

(h) Recovered Watermark

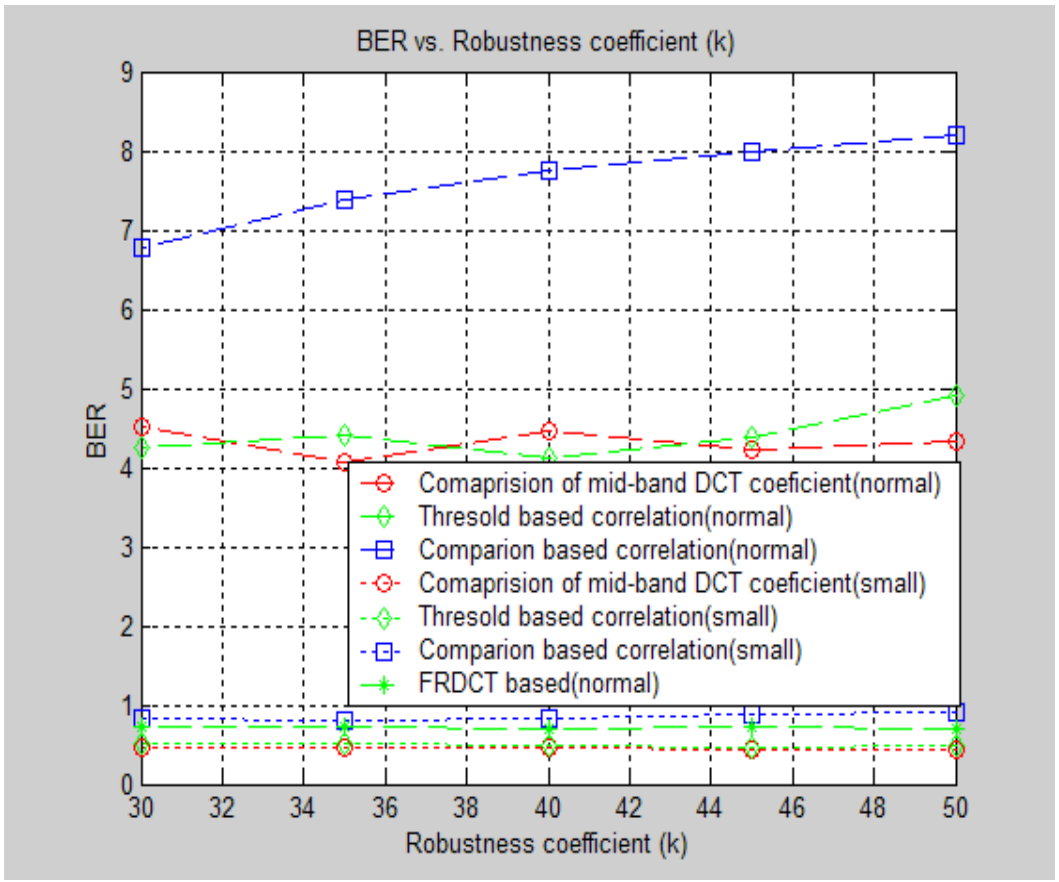
Figure 5.9: Watermarked image and recovered watermarks Comparison-based correlation in the DCT mid-band and performance under attacks



(a) Different robustness coefficient (*k*) v$_s$. PSNR for different size watermark



(b) Different robustness coefficient (*k*) v$_s$. RMSE for different size watermark



(c) Different robustness coefficient (*k*) v$_s$. BER for different size watermark

Figure 5.10: (a) Processing gain(*k*) v$_s$ PSNR (b) Processing gain(*k*) v$_s$ RMSE

(c) Processing gain(*k*) v$_s$ BER

5.4 Digital watermarking in Fractional Domain

5.4.1 Digital Watermarking using Fractional Fourier Transform

The reference image is of Lena has been taken for DFRFT analysis. The image is transformed by the DFRFT with powers 0.8 and 0.4 in the x and y direction respectively. Then three watermarks are embedded using the method described above with parameters L,M and σ^2given by the table shown below

Table 5.1: The specifications of the Three Watermarks:

Watermark	First	Second	Third
L	96000	90000	100000
M	800	800	300
σ^2	50	100	25

(a) Original Image

(b) Watermarked Image

(b), terma

noise and recovered watermark have been shown in figure5.11(c)-(d).After cropping the result has been shown in figure 5.11(e)- (f). The mean and standard deviation of the detection value is computed using 1000 random watermarks with the same parameters as the correct one. The threshold is fixed at the mean plus 4 times the standard deviation. These values and

the PSNR can be found on row (1) of the table 5.2. The valuesμ_i, $\sigma_{i,}$ τ_i, d_i refer to the mean, the standard deviation, the threshold and the detection value of watermark i. The corresponding plots are given on the first row of Figure 5.12. In this way, it can be seen that the three embedded watermarks are detected. The next attack is adding noise to the watermarked image. To the watermarked and compressed image, a zero mean Gaussian noise with standard deviation 60 is added. The result is again jpeg compressed and given again to the detection algorithm. The resulting image can be seen in Figure 5.11(c) and figure 5.11(d). The mean and standard deviation of the randomly selected watermarks is definitely different from what was found in the previous case. These are given, together with the PSNR of the image in row (2) of the table 5.2. The 1000 values of d and the correct one on position 501 for the three embedded watermarks is what is shown in the middle plot of Figure 5.77. Again the three watermarks were detected.

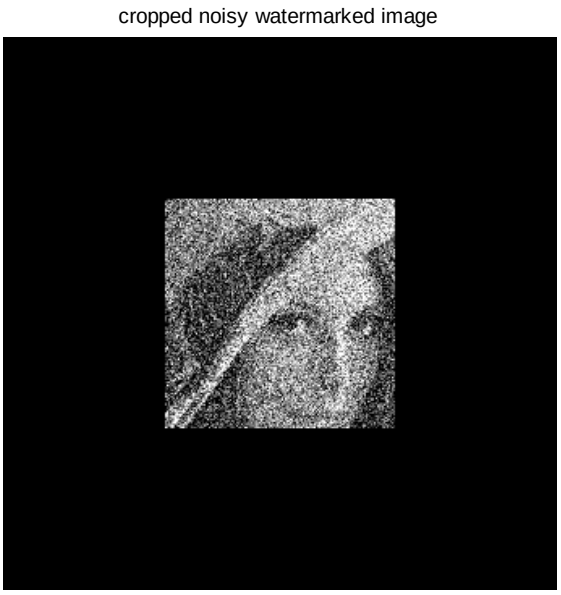
Finally we crop the previous noisy image by taking only the First 100 rows out of the 512 rows in the image. See table 5.2. The result is again submitted to the detection algorithm and the mean and standard deviation for 1000 random watermarks is computed. The result is shown on row (3) of Figure 5.12. The values of the PSNR, the mean and the threshold are given on row (3) of the table 5.2. Now the first two watermarks are detected, but the third is not. Indeed the effect of the watermark is spread out over the whole image and can be recovered from any part of the image. Looking at the plots of Figure 5.12, it is also seen that there are sometimes `false alarms'. Some of the randomly generated watermarks also give a detection value above the threshold. It is clear from these plots that a threshold $\tau = \mu + p\sigma$ with p = 4 is not a bad choice. If we take p larger, we require the detection value of the correct watermark to be a more pronounced outlier. If we decrease p, we are at a higher risk that we detect a watermark that is not the correct one. It could of course accidentally happen that the falsely detected watermark is strongly correlated with the correct one, in which case of course its detection value should be in the neighborhood of the detection value of the correct watermark. The number of false alarms for the three different watermarks on the three different corrupted situations is mentioned in Figure 5.78 (the “false=n” text). Obviously, in these particular situations the chance of having a false alarm when the image is not too much corrupted is very small.

Table 5.2: The values obtained for the compressed and watermarked image (1), additive noise (2), and cropped (3)

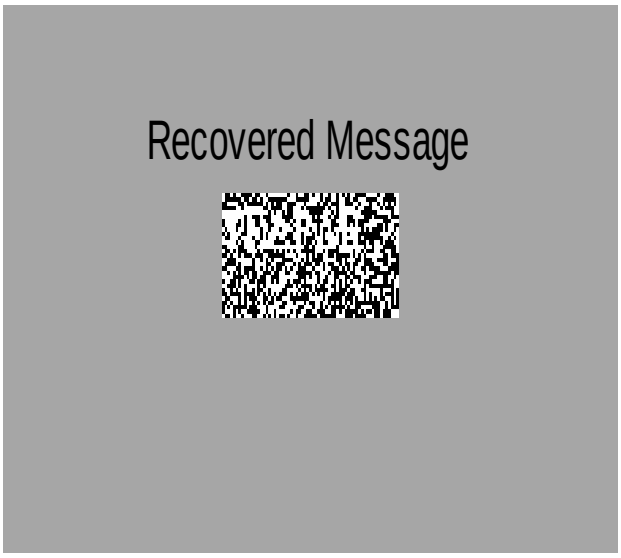
S.no.	PSNR(dB)	μ_1	$\sigma_{1,}$	τ_1	d_1	μ_2	$\sigma_{2,}$	τ_2	d_2	μ_3	$\sigma_{3,}$	τ_3	d_3
1.	39.51	1236	664	3892	17772	1847	905	5334	27999	633	342	2001	4433
2.	28.55	1781	915	5443	19412	2527	1328	7839	27838	943	496	2927	4590
3.	0.97	681	345	2061	1847	952	503	2966	4149	387	204	1204	969

(c) Watermarked Image after addition of 60% Gaussian Noise

(d) Recovered Watermark after addition of 60% Gaussian Noise

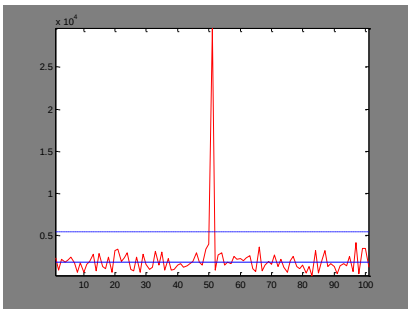


(e) Watermarked Image after addition of 60% Noise and cropping

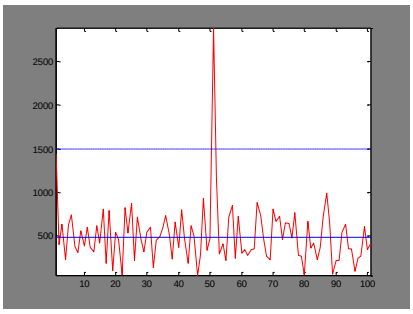


(f) Watermarked Image after addition of 60% Noise and cropping

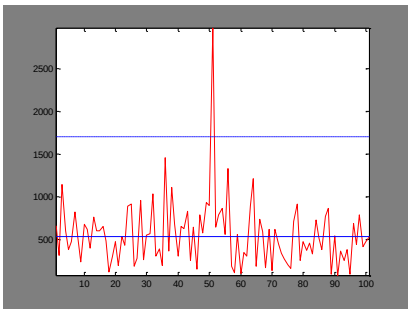
Figure 5.11: Watermarking In FRFT domain and performance under attacks



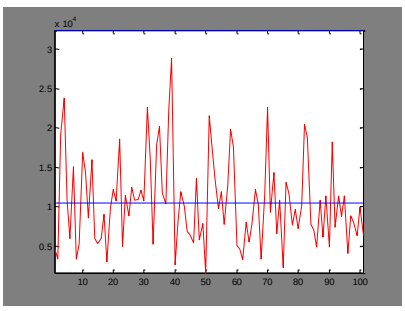
(a) Detected,false=1



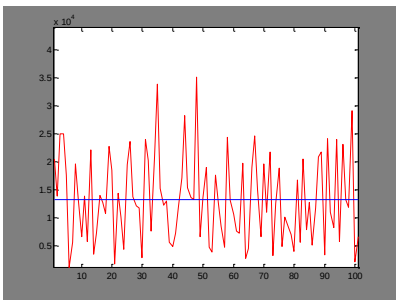
(b) Detected, false=2



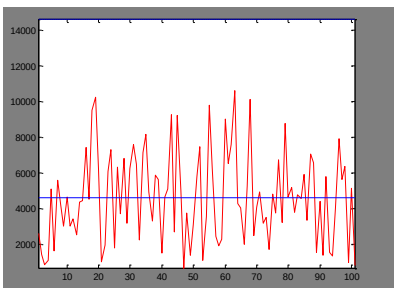
(c) Detected, false=0



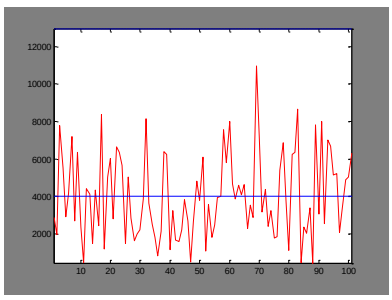
(d) Detected, false=2



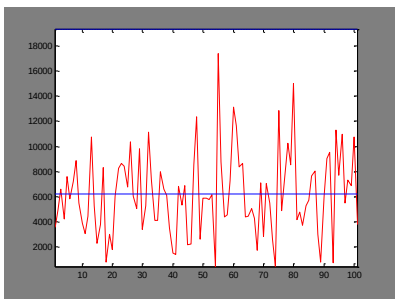
(e) Detected, false=0



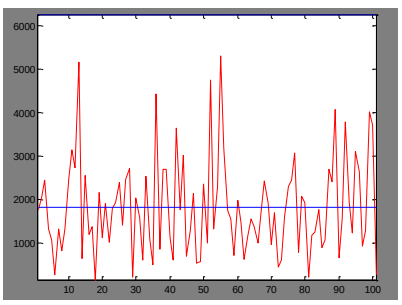
(f) Detected, false=1



(g)Detected, false=0



(h) Detected, false=0



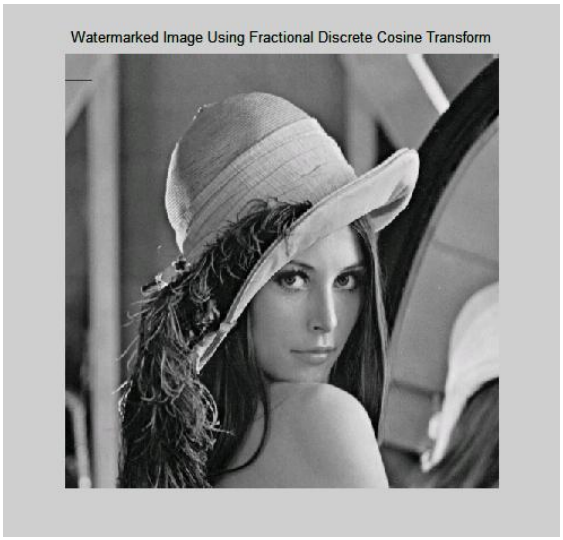
(i) Detected, false=2

Figure 5.12: A 1000 samples for three watermarks (columns) for the compressed image (top), the noisy compressed image (middle), and the noisy cropped and compressed

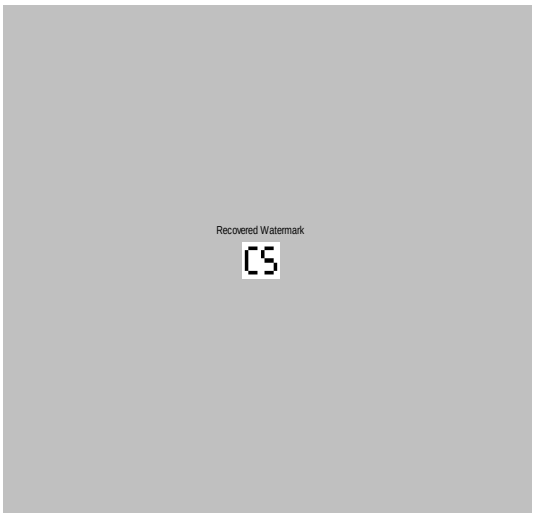
5.4.2 Digital watermarking using Fractional Discrete Cosine Transform:

Digital watermarking in fractional domain is the new approach in the field of digital watermarking. The results for watermarking using 2D Fractional Discrete Cosine Transform (FRDCT) for smaller correlation coefficient are better than other watermarking techniques discussed above. As shown in figure 5.13(a) one can find the optimum domain for watermarking after choosing the appropriate value of fractional order (*a*).

Here for '*a*'=0.98 it gives the highest PSNR, least MSE and lower BER. So this will be the optimum domain for watermarking for '*k*'=35 and block size of 8×8 . Other domain can be found out for different values of '*k*' and block size. This technique gives extra robustness due to fractional domain. For a pirate it becomes necessary to have the knowledge of exact value of '*a*', otherwise he will not be able to recover the watermark from the watermarked image. The watermarked images shown in figure 5.13(a)-(b) are watermarked for value of '*a*'=0.98. When the watermark is recovered for values other than '*a*'=0.98 the watermark is not perfectly recovered, thus increasing the robustness. Thus using this technique the watermark can be recovered perfectly under small attacks as well as heavy attack. The results for different values of 'a' has been shown from figure 5.13(c) – 5.13(h).

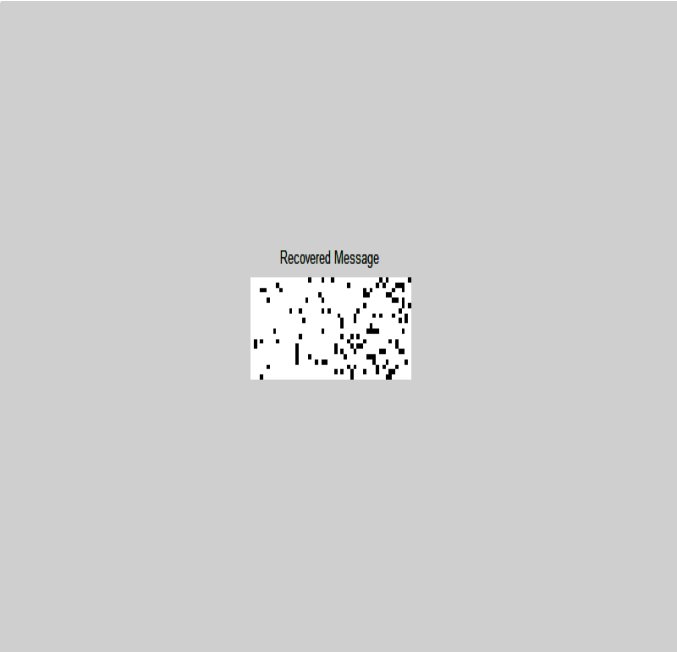


(a) Watermarked Image using FRDCT, *k*=35, 'a=0.98'



(b) Recovered watermark

(c) Watermarked Image using FRDCT, *k*=35, 'a=0.9'



(d) Recovered watermark a=0

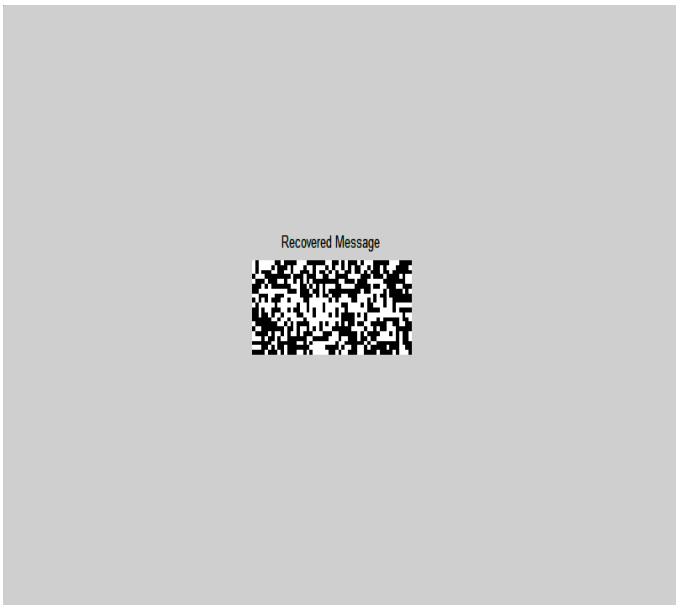


Figure5.70: Recovered watermark 'a=0.1'

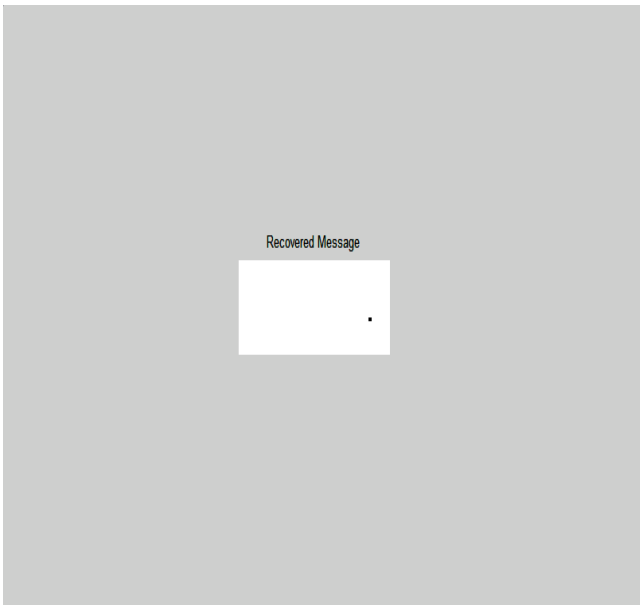
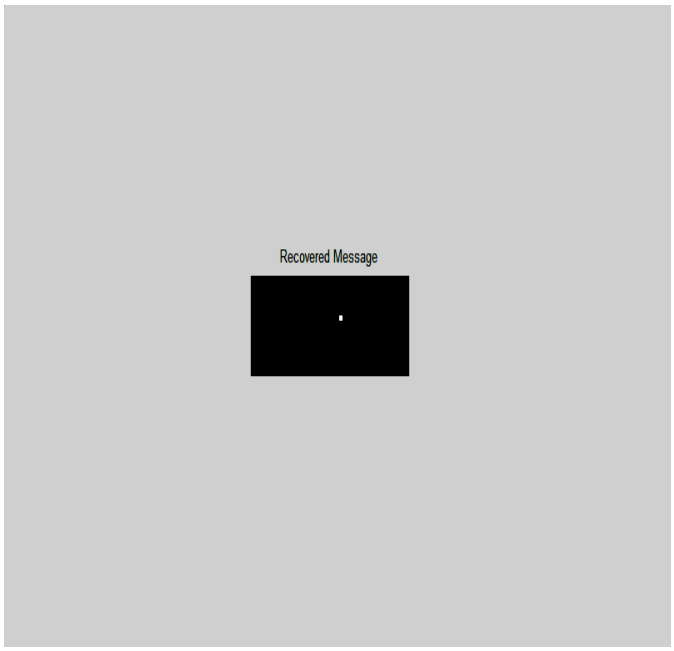
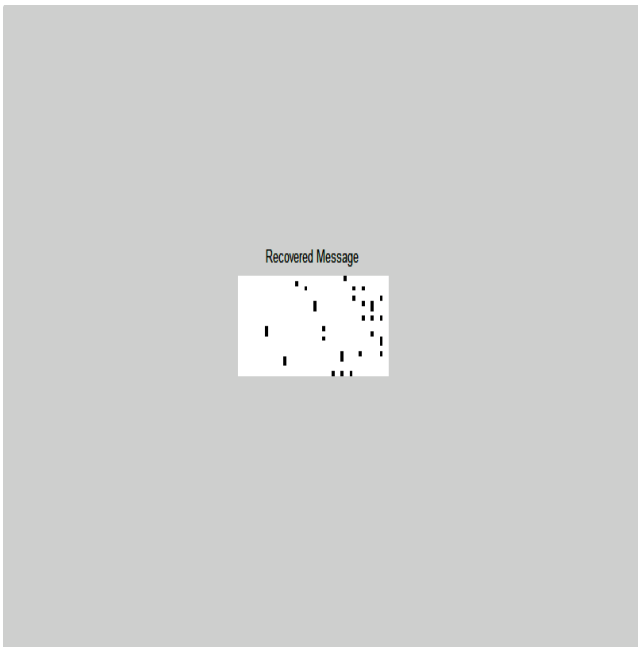


Figure 5.71: Recovered watermark 'a=0.2'



(f) Recovered watermark ‘a=0.5’



(g) Recovered watermark ‘a=0.7’

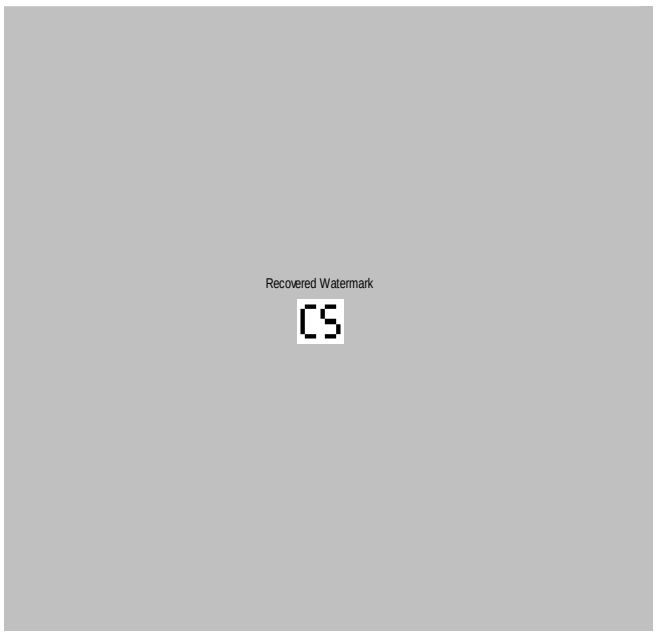


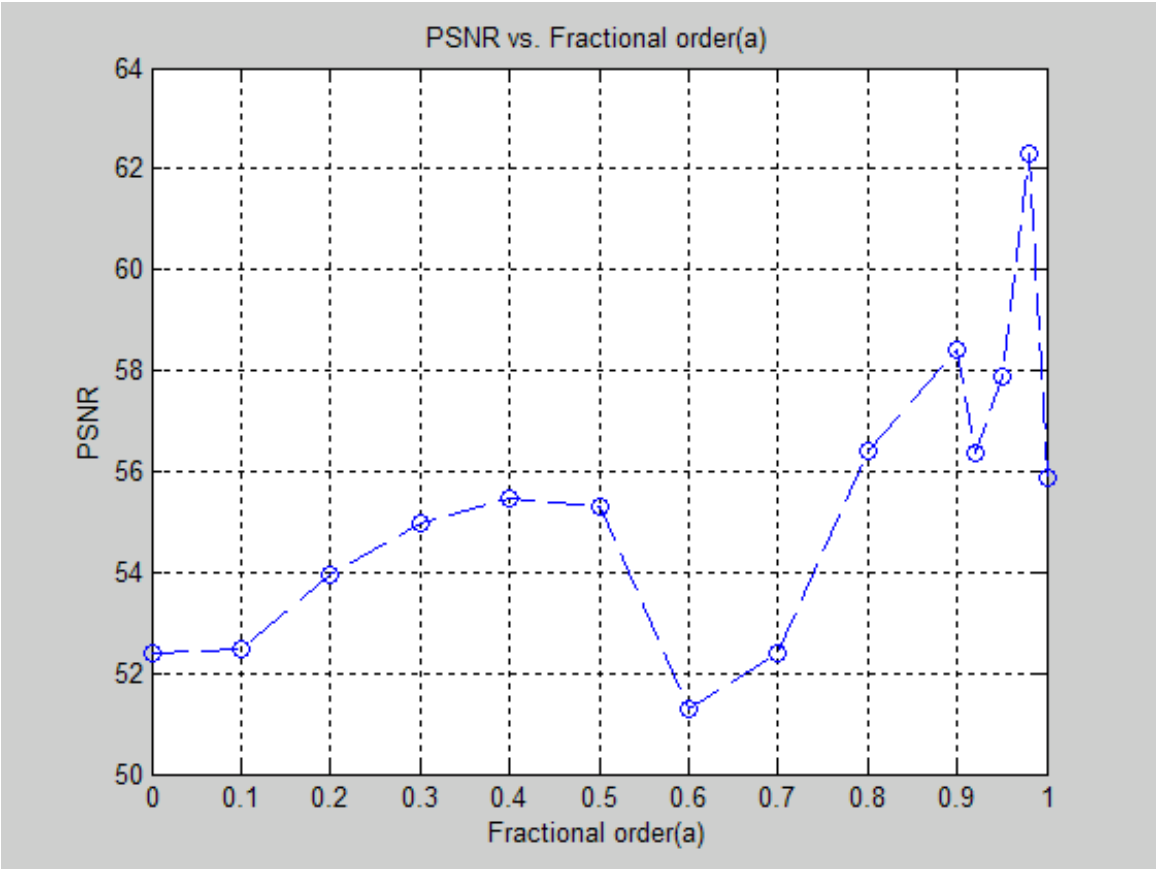
Figure 5.13: Recovered watermark for varying ‘*a*’

5.5 Effects of varying robustness coefficient:

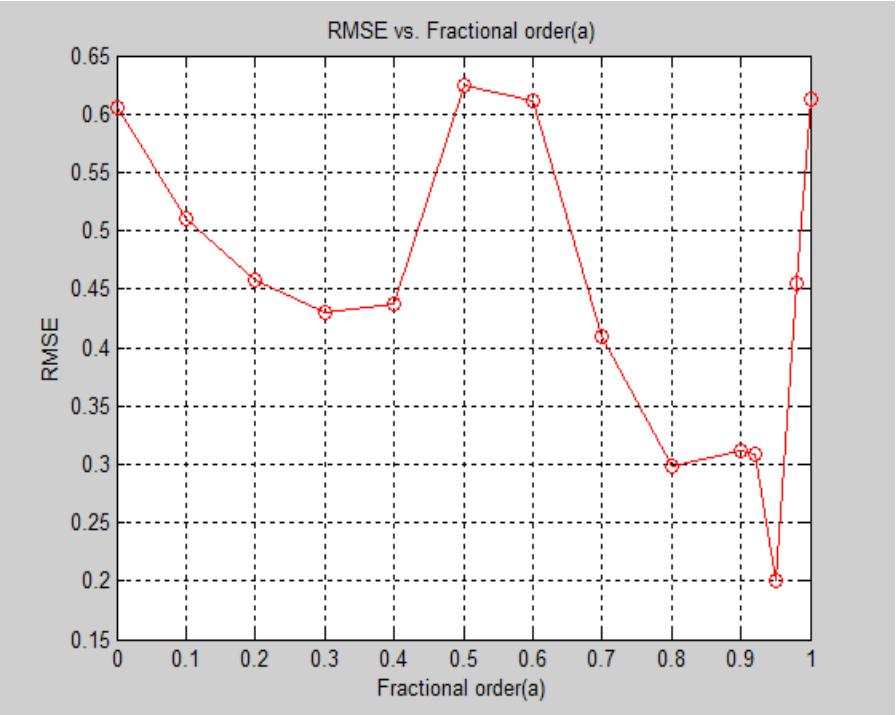
Figure 5.14(a)-(c) show the effect of variation of robustness coefficient (*k)* on the PSNR and MSE. As the robustness coefficient is increased the PSNR reduces hence reducing the image quality. This is true for all the techniques discussed above. However, higher the robustness coefficient more the robustness. Thus, a robustness coefficient is chosen, which maintain the robustness as well as quality of image.

5.6 Effect of watermark size:

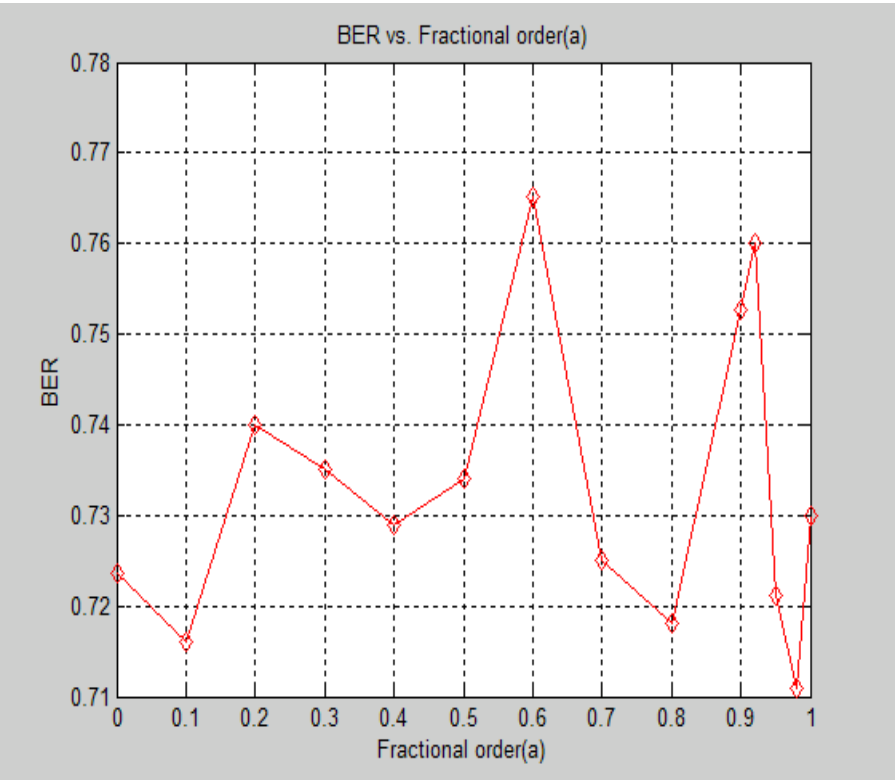
Figure 5.14(a)-(c), it is observed that as the size of watermark is decreased, the PSNR increases and MSE decreases. However, bit error rate decrease as the size of watermark is reduced as shown.



(a) Fractional order (*a*) v_s. PSNR



(b) Fractional order (*a*) v_s. RMSE



(c) Fractional order (*a*) vs. BER

Figure 5.14: (a) Fractional order (*a*) v_s. PSNR (b) Fractional order (*a*) v_s. RMSE

(c) Fractional order (*a*) v_s. BER

5.7 DWT Domain Watermarking:

Here 8-bit gray scale lena image as original (host) image of size 512 × 512 and for watermark THAPAR have been taken . Embedding the watermark into the host image, we

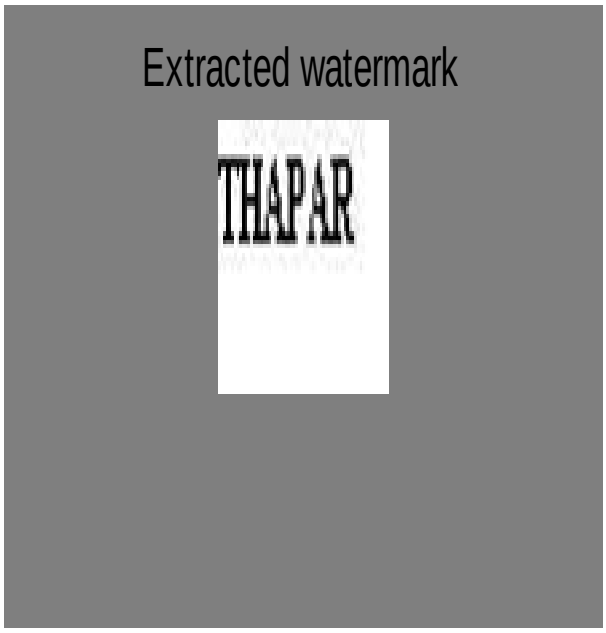
have used 2-level of decomposition using Haar\Daubechies filter bank. In the extraction, we are only selecting an image whose correlation coefficient is the greatest among all. This image is being used as the extracted primary watermark and this is used for extracting secondary watermark. In figure 5.15(a)-(b) original, watermarked images and extracted watermarks are shown. To investigate the robustness of the algorithm, the watermarked image is attacked by Average and Mean Filtering, JPEG and JPEG2000 compression, Gaussian noise addition, Rotation and Cropping.

The results are shown in figures 5.15(c)-(g). The compression has been shown in figure 5.15(c).

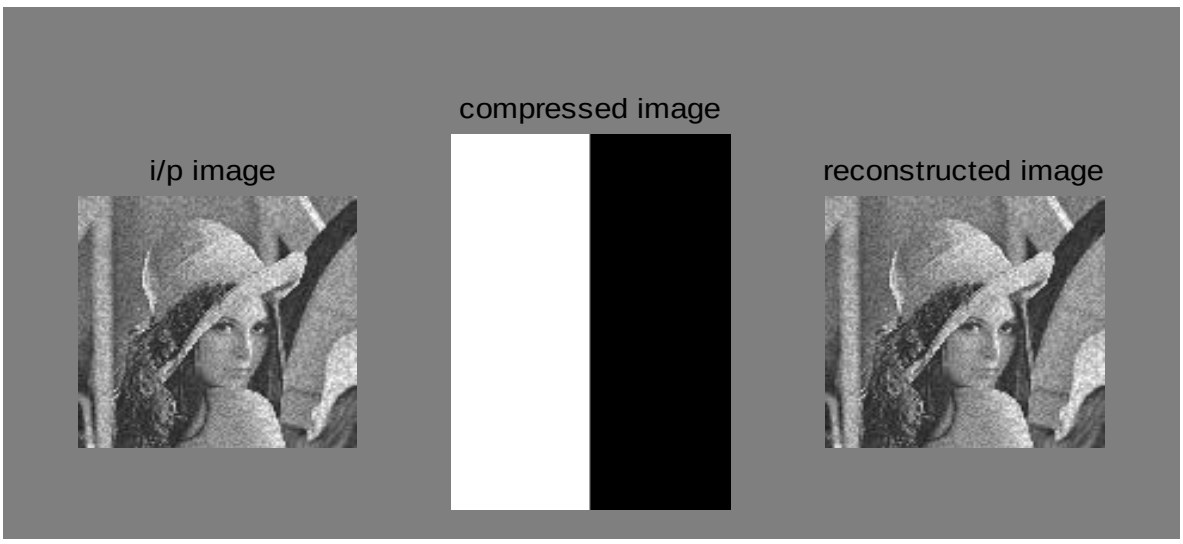
Haar wavelet has been used to embed the watermark and 2- level decomposition has been done.

Watermarked image and recovered watermark has been shown in figure 5.15(d)-(e)after Addition of 60% gaussian noise. Rotation and cropping has been shown in figure 5.15(f)-(g).

(a) Watermarked Image using Haar wavelet



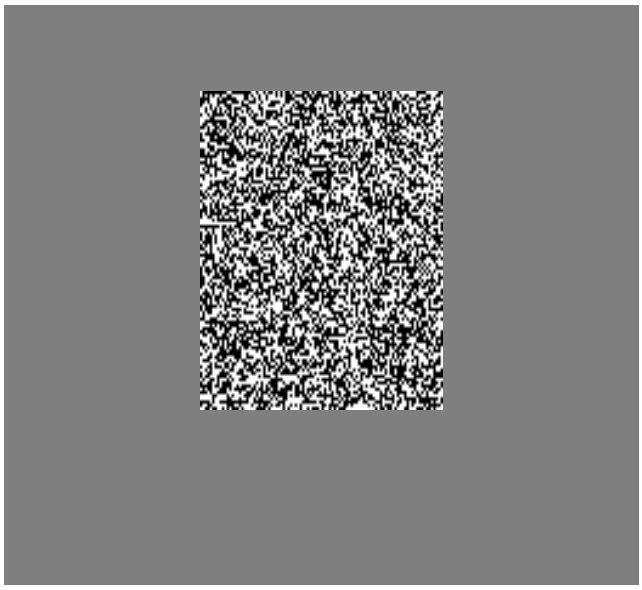
(b) Recovered watermark



(c) 2-Level decomposition of Lena image and Reconstruction using Haar wavelet (CR=83%)

(d) Noisy and cropped watermarked image after 60% Gaussian noise

(e) Recovered watermark



(f) Transposed and Cropped Lena image after addition of 60% Gaussian noise

(h) Recovered watermark

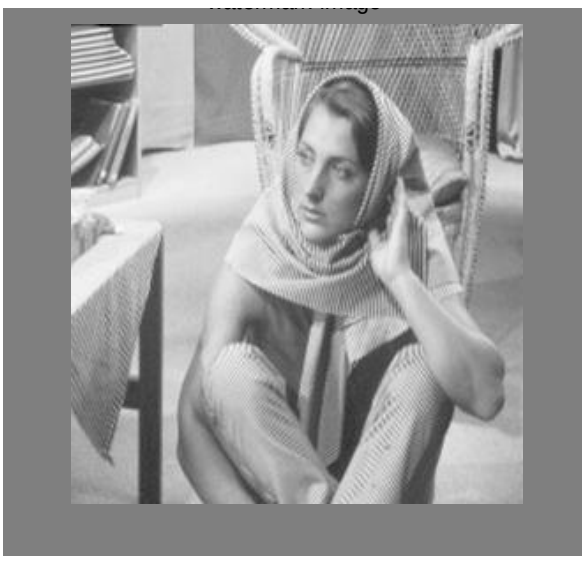
Figure 5.15: Watermarking in DWT domain and performance under attacks

5.8 DWT-DCT-SVD Watermarking:

The DWT-DCT-SVD based watermarking algorithm was found to be a very robust method of non-blind watermarking which can be used to embed copyright information in the form of a visual watermark or text. Watermark can be recovered even with the help of an attacked watermarked image. Embedding of watermark can be carried out in all the frequencies without reasonable distortion in the visual watermark. For textual embedding however, recovery was found to be difficult from the attacked watermarked image. We have seen that in most of the DCT-based watermarking schemes, the lowest frequency coefficients are not modified as it is argued that watermark transparency would be lost. In this approach, we did not experience any problem in modifying the coefficients. Watermarks inserted in the lowest frequencies are resistant to one group of attacks, and watermarks embedded in highest frequencies are resistant to another group of attacks. So, region of watermark embedding is of application dependent.

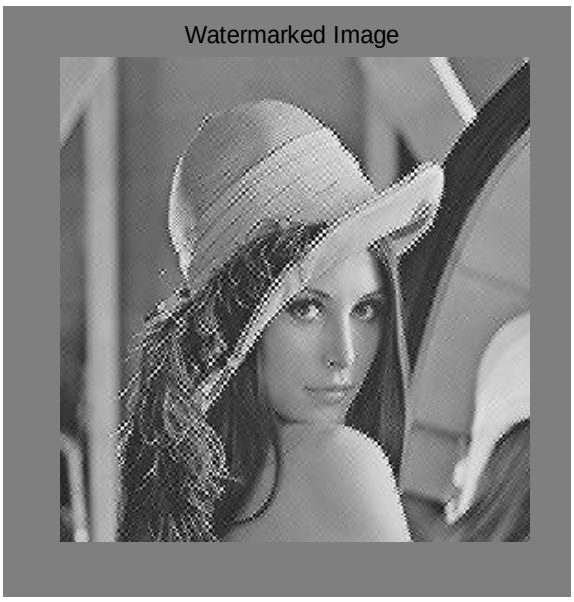
One advantage of SVD-based watermarking is that there is no need to embed all the singular values of a visual watermark. Depending on the magnitudes of the largest singular values, it would be sufficient to embed only a small set. This SVD property can be exploited to develop algorithms for lossy image compression.

(a) Original Image of Lena



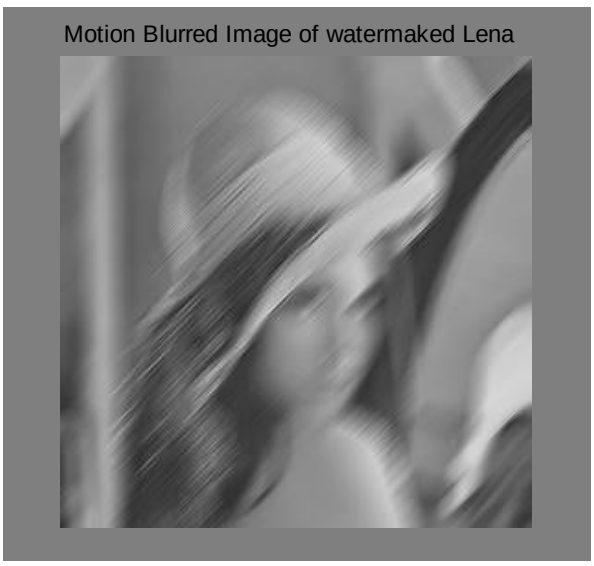
(b) Watermark to be embed

(c) Sub band of Lena image

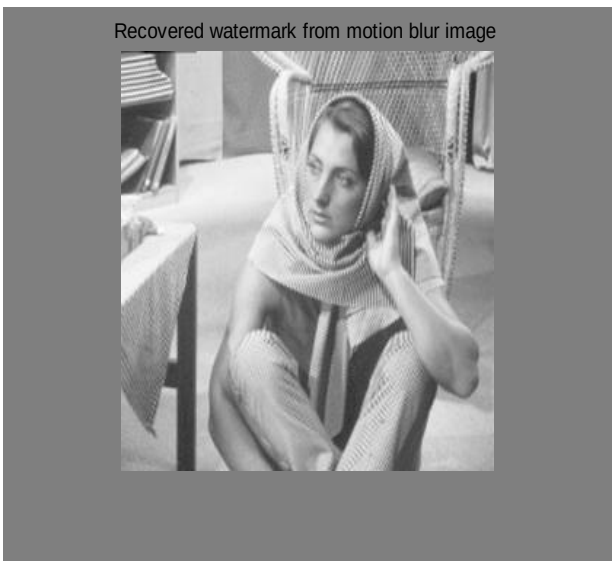


(d) Watermarked image using Haar wavelet

(e) Recovered watermark



(f) Motion Blurred image of watermarked Image



(g) Recovered watermark from Motion Blurred image of watermarked Image

Figure 5.16: Watermarking in DWT-SVD-DCT domain, recovered watermark and performance under attacks

In this domain the watermarking is very efficient and computationally good. The PSNR value upto 70 dB has been archived as shown in figure 5.17. Here motion blurring has been used to check the robustness of the technique as shown in figure 5.16(f) and watermark has been recovered perfectly as shown in figure 5.16(g).

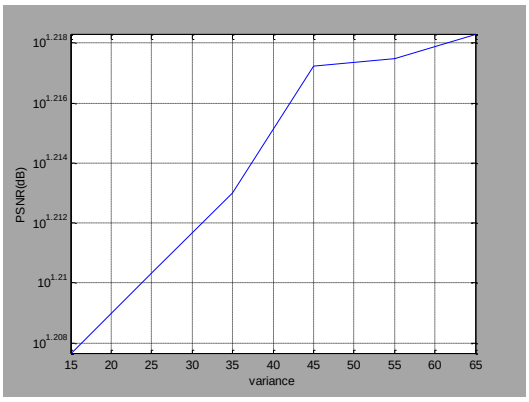


Figure 5.17: PSNR(dB) v_s Variance

CHAPTER 6

CONCLUSION

This study has introduced a number of techniques for the watermarking of digital images, as well as discussing the limitations and attributes of each technique.

LSB substitution is not a very good algorithm for digital watermarking due to its lack of even a minimal level of robustness. LSB embedded watermarks can easily be removed using techniques that do not visually degrade the image to the point of being noticeable. Furthermore, if one of the more trivial embedding algorithms is used, the encoded message can be easily recovered and even altered by an adversary. The LSB algorithm remains in the domain of steganography due to its tremendous information capacity. In spatial domain the watermark is embedded directly in to pixels of the image. Thus, the techniques in this domain proved fairly robust and carrying good capacity if small watermark is being used. In spread spectrum algorithm the watermark is converted into a sequence of PN codes known as gold sequence. This PN sequence have the attributes of the spread spectrum communication and very resistant to cropping or other attacks. An advantage of the spatial techniques in the thesis is that they can be easily applied to any image, regardless of subsequent processing (whether they survive this processing however is a different matter entirely). A possible disadvantage of spatial techniques is they do not allow for the exploitation of this subsequent processing in order to increase the robustness of the watermark

Another observation is that transform domain techniques are typically better for watermarking than spatial, for both reasons of robustness as well as visual impact. Embedding in the DCT domain proved to be highly resistant to JPEG compression as well as significant amounts of random noise as upto 50 dB of PSNR value has been achieved using varying processing gain k upto 30. By anticipating which coefficients would be modified by the subsequent transform and quantization, it is possible to produce a watermarking technique with moderate robustness, good capacity, and low visual impact. This holds true in general for watermarking; robustness can be improved significantly when the subsequent degradation techniques are known. This holds particularly true in the case of compression techniques, where the compression algorithms are well known.

Furthermore, The FRFT/FRDCT algorithm makes the watermarking more robust as an active adversary may know the watermark key and watermark key position, but the very

important he does not know, is the transformation angles. Without the knowledge of transformation angle ($\alpha = a\pi/2$) no one can detect the original watermark. This algorithm increases the capacity of watermarking as number of watermarks can be embedded on different transformation angle within the same image. Calculation complexity of the procedure for watermark embedding and detection is not significantly increased, since there are standard fast algorithms for the FRDCT calculation.

The wavelet domain as well proved to be highly resistant to both compression and blurring, with minimal amounts of visual degradation. This is all the more impressive when one considers that the wavelet technique described here is one of the most primitive currently known. More sophisticated wavelet-domain techniques will almost certainly improve on both of these, and hopefully lower it's computational requirements. The wavelet domain may be one of the most promising domains for digital watermarking yet found.

A dual watermarking scheme has been discussed in which the watermarks are either a gray scale image or visually meaningful gray scale logo instead of a noise type Gaussian sequence. Robustness of this method has been carried out by variety of attacks like Gaussian noise cropping and blurring. A newer approach of watermarking based on DWT-DCT-SVD has been also discussed. It has some very fair advantages over dual domain watermarking algorithm like DCT-SVD or DWT-DCT .The DCT-SVD based method is very time consuming though it offers better capacity and imperceptibility and highly resistant to geometric transformations. DWT-SVD method is found to be similar to the DCT-SVD scheme except that the process was fast. The new method was found to satisfy all the requisites of an ideal watermarking scheme such as imperceptibility, robustness and good capacity. This method can be used for authentication and data hiding purposes. The future work includes the extension of this technique to other category and formats of images, for example, color images and DICOM images.

REFERENCES

[1] A. J. Menezes, P. C. Van Oorschot, and S. A.Vanstone, *Handbook of Applied Cryptography*,Boca Raton, CRC Press, 1996.

[2] D. Kahn, *The Code breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, 2nd ed.,New York: Scribner, 1996.

[3] A. Kerkhoffs, "La Cryptographie Militaire," *Journal des Sciences Militaires*, 9th series, pp. 5–38, 161–191 January/February 1883.

[4] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, Vol. 28, No. 4, pp. 656–715 October 1949.

[5] C. A. Devours, *Selections from Cryptologia: History, People, and Technology*, Norwood, MA: Artech House, 1998.

[6] I. J. Cox, *Secure Spread Spectrum Watermarking for Multimedia*, NEC Research Institute, Tech.Rep.95-10, 1995.

[7] W. Bender, "Techniques for Data Hiding," *IBM Systems Journal*, Vol. 35, Nos. 3 4, pp. 313–336, 1996.

[8] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*, The Morgan Kaufmann Series in Multimedia Information and Systems, San Francisco:Morgan Kaufmann Publishers, 2002.

[9] M. Kutter, F. Hartung, S.C. Katzenbeisser, "Introduction to Watermarking Techniques", *Information Techniques for Steganography and Digital Watermarking*, Eds. Northwood, MA: Artec House, Dec. 1999.

[10] Inoue H., Miyazak A.,Katsura T.,"An Image Watermarking Method Based on the Wavelet Transform," *Kyushu Multimedia System Research Laboratory*.

[11] I. J. Cox, M.L. Miller, J.M.G. Linnartz, T. Kalker, "A Review of Watermarking Principles and Practices" *Proceedings of SPIE, Human Vision & Electronic Imaging II*, vol. 3016, pp. 92-99, February1997.

[12] F. A. P. Petitcolas ,"Watermarking Schemes Evaluation", *IEEE Signal Processing Magazine*, Vol 17, pp 58-64, September 2000.

[13] E. Koch, J. Zhao, I. Pitas, "Towards Robust and Hidden Image Copyright Labelling," *Proceedings of 1995 IEEE Workshop on Nonlinear Signal and Image Processing*, Neos Marmaras, Greece, pp. 452–455, June 1995,.

[14] N. R. Wagner, "Fingerprinting," *Proceedings of the 1982 IEEE Symposium on Security and Privacy (SOSP)*, pp. 18–22, Oakland, CA, April 1983.

[15] D. Kundur and Hatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication," *Proceedings of the IEEE*, vol. 87, no. 7, pp.1167–1180July 1999.

[16] N. F. Johnson and S. C. Katezenbeisser, "A Survey of Steganographic Techniques" *Information Techniques for Steganography and Digital Watermarking*, pp 43-75, Artec House, Dec. 1999.

[17] S. C. Katzenbeisser, J. Dugelay, and S. Roche, "A Survey of Current Watermarking Techniques", *Information Techniques for Steganography and Digital Watermarking*, pp 121-145, Artec House, Dec. 1999.

[18] P. Meerwald, A. Uhl, "Watermark Security Via Wavelet Filter Parameterization", *Proceedings of Internationl Conference on Image Processing*, Thessaloniki, Greece, 2001.

[19] G. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking Digital Image and Video Data", *in IEEE Signal Processing Magazine*, vol. 17, pp. 20-43, September 2000.

[20] I. Djurovic, S. Stankovic, and I. Pitas, "Digital watermarking in the fractional Fourier transformDomain", *Journal of Network and Computer Applications*, vol. 24, pp. 167-173, 2001.

[21] J. Guo, Z. Liu, and S. Liu, "Watermarking based on discrete fractional random transform", *Optics Communications*, vol. 272, no. 2, pp.344-348, 2007.

[22] J. Guo, Z. Liu, and S. Liu, "Erratum to the discrete fractional random cosine and sine transforms", *Optics Communications*, vol. 267, no. 2, pp.530, 2006.

[23] J. Guo, Z. Liu, and S. Liu, "A discrete fractional random transform", *Optics Communications*, vol. 55, no. 4, pp. 357-365, 2005.

[24] X. M. Niu and S. H. Sun, "Digital watermarking for still image based on discrete fractional Fourier transform" *J. Harbin Inst. Technology*, vol. 8, no. 3, pp. 309-311, 2001.

[25] S. C. Pei and M.H. Yeh, "The discrete fractional cosine and sine transforms", *IEEE Trans. Sig. Proc.*,vol. 49, pp.1198-1207, 2001.

[26] J. R. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis And a New Structure", *IEEE Trans. Image Processing*, vol. 9, pp 55-68, Jan. 2000.

[27] F. A. Petitcolas, "Introduction to information hiding" *Information Techniques for Steganography and Digital Watermarking*, Artec House, pp 1-11,Dec. 1999.

[28] S.C. Katzenbeisser, “Principles of Steganography” *Information Techniques for Steganography and Digital Watermarking*, Artec House ,pp 2-40, Dec. 1999.

[29] P. Meerwald and A. Uhl, “A Survey of Wavelet-Domain Watermarking Algorithms,” *Proceedings of Electronic Imaging 2001,Security and Watermarking of Multimedia*, pp.505–516,San Jose, CA, January 2001.

[30] D. Kundur and D. Hatzinakos, “Digital Watermarking using Multiresolution Wavelet Decomposition”, *Proc. IEEE Int. Conf On Acoustics, Speech and Signal Processing*, vol. 5, pp. 2969-2972, Seattle, Washington, May 1998