REGION AWARE DCT DOMAIN INVISIBLE

ROBUST BLIND WATERMARKING

FOR COLOR IMAGES

Sahasan Naraharisetti, B.Tech.

Thesis Prepared for the Degree of

MASTER OF SCIENCE

UNIVERSITY OF NORTH TEXAS

December 2008

APPROVED:

Saraju P. Mohanty, Major Professor
Elias Kougianos, Co-major Professor
Murali Varanasi, Committee Member
Krishna Kavi, Professor and Chair, Department of Computer Science and Engineering
Costas Tsatsoulis, Dean of the College of Engineering
Sandra L. Terrell, Dean of the Robert B. Toulouse School of Graduate Studies

Naraharisetti, Sahasan. Region aware DCT domain invisible robust blind watermarking for color images. Master of Science (Computer Engineering), December 2008, 61 pp., 9 tables, 40 figures, references, 30 titles.

The multimedia revolution has made a strong impact on our society. The explosive growth of the Internet, the access to this digital information generates new opportunities and challenges. The ease of editing and duplication in digital domain created the concern of copyright protection for content providers. Various schemes to embed secondary data in the digital media are investigated to preserve copyright and to discourage unauthorized duplication: where digital watermarking is a viable solution.

This thesis proposes a novel invisible watermarking scheme: a discrete cosine transform (DCT) domain based watermark embedding and blind extraction algorithm for copyright protection of the color images. Testing of the proposed watermarking scheme's robustness and security via different benchmarks proves its resilience to digital attacks. The detectors response, PSNR and RMSE results show that our algorithm has a better security performance than most of the existing algorithms.

ACKNOWLEDGEMENTS

I would like to express my gratitude to my major professor, Dr. Saraju P. Mohanty, for his constructive ideas, support, and constant guidance and for sharing his wisdom in the field of digital watermarking throughout the course of this research. I would sincerely like to thank my co-major professor, Dr. Elias Kougianos, for his support at various phases of my research work.

I would also like to thank my committee member, Dr. Murali Varanasi from electrical engineering department. for his time and support. I want to thank my colleagues Dhruva at the VLSI Design and CAD laboratory [VDCL] for their support during my graduate studies. I am also grateful to all the faculty and staff of the Department of Computer Science and Engineering for their support and help. I would also like to thank my friends Chiranjeevi, Swapnil, Sunil for their constant encouragement throughout my master’s program.

I would like to take this moment to thank God with whom everything is possible.

Special thanks to my parents Mr. Appa Rao Naraharisetti and Mrs. Vara Laxmi Naraharisetti, and my brother, Sirish Karthik.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

Page

CHAPTER 1

INTRODUCTION

This chapter presents the introduction to the thesis. Section 1.1 discusses the motivation behind the proposed research. Digital watermarking is introduced in section 1.2. The general framework for watermarking is presented in section 1.3. Various types of watermarking in current literature are discussed in section 1.4. The organization of this thesis is presented in section 1.5.

1.1 Motivation

Multimedia has exploded in the past few years primarily due to significant advantages of digital media over analog media. These advantages include higher quality, easier editing, perfect copying and more efficient transmission over information network. With the evolution of Internet, the duplication and distribution of the multimedia has become easier and much faster. The piracy of the multimedia data is an important issue for the owners of the products, so the need to address these issues which are mainly related to security has arrived. The owners or the media companies are looking for assurances that there will not be any unauthorized production. The significance of the multimedia security has increased with these issues. One solution is digital watermarking for copyright protection of multimedia data.

1.2 Introduction to Watermarking

Digital watermarking is a technique where a watermark is embedded into the original data and it can only be extracted or detected by the authorized user making it a viable solution for the copyright protection and verifying the content originality. The watermark can be declared as secure if the algorithms for insertion and extraction of the watermark are known only to the authorized user. Even if the quality of the host data is degraded, the watermark should always remain in the original data. Failure of detection of the watermark implies that the data has been modified and is no more authenticated. The watermark cannot be secure if it is not robust. The digital watermarking schemes are potentially used in the following applications [20, 29, and 2]:

- *Copyright protection:* Watermark can protect the content [identity of the owner, creator, and producer] from the unauthorized user.
- *Copy protection:* Watermark can limit the access to the copyrighted material and prohibits from copying.
- *Monitoring:* Watermarking can embed a watermark in the advertisements, news for verification of when, where and for how long the advertisements are broadcasted.
- *Fingerprinting:* In this technique, different watermarks are embedded in the copies by the owner to identify the source of illegal copies, i.e., the customer who broke the agreement.
- *Authentication:* Watermarking can verify the source and the owner of the data.
- *Filtering/ classification:* Watermarking can be used in filtering the content/ content identity to classify the content in a related database.
- *Forensic tracking:* Watermarking can be used to track where the content left the authorized environment.
- *Medical safety:* Watermarks can be used as a safety measure is to hide the data about the content in the content.

1.3 General Framework

The watermark can be embedded into an image, video, audio or text form of multimedia. Watermark can be more effective if it meets a set of specified requirements [2, 28]. However for a watermarking scheme to be successful, it needs to meet the requirements of the specific applications, which may be different for different applications.

Watermarking consists of four logical steps:

a. Selection of watermarks

b. Insertion of watermarks (encoding)

c. Extraction of watermarks (decoding)

d. Detection of watermarks

1.3.1 Selection of Watermarks

The watermark is to be selected depending on the type of application. There should not be any perceptible difference between the original data and the watermarked data. There can be different watermarks for the same owner. For example, a company has different kinds of products and for every product different unique watermark can be embedded by the algorithm.

1.3.2 Insertion of Watermarks

The process of insertion of watermarks is shown in the Figure 1.1. In this process, the original Image I was embedded with the watermark W**.** The insertion process resulted in a watermarked image $I^{'}$ as the output.

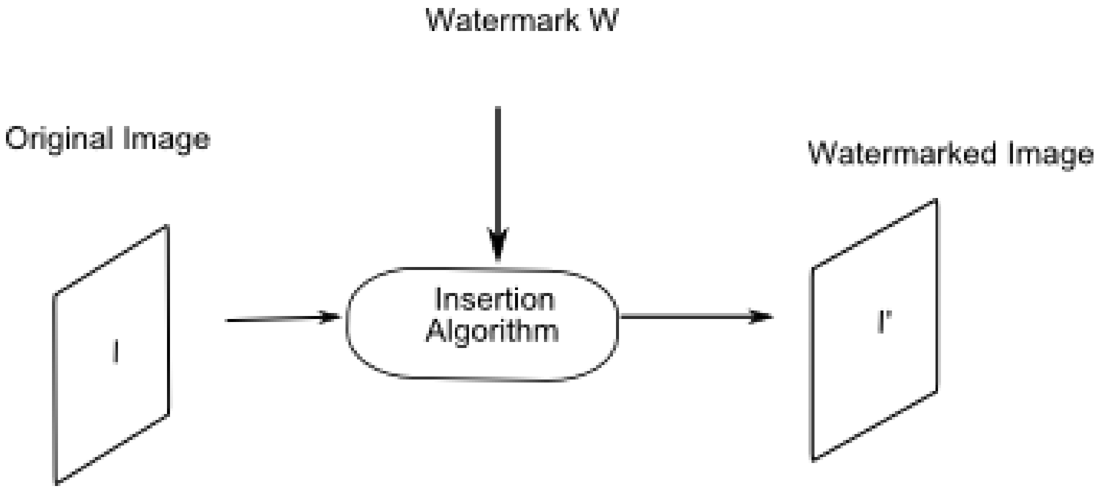


Figure 1.1. Watermarking insertion process

The embedding of the watermark can be imperceptible to the human eye if one cannot distinguish between the original and watermarked data. The watermark embedded must not affect the quality of the original data. However, for visible watermarking the watermark is visible along with the original image.

1.3.3 Extraction of Watermarks

The extraction of the watermark is a significant step in digital watermarking. This is needed for watermark authorization. The algorithm should ensure that the tapping of the multimedia data by unauthorized people results in very poor quality data or no data. Figure 1.2 schematically presents the extraction algorithm where watermarked image I**’** undergoes the extraction process to extract the watermark W’ which is embedded. Some extraction techniques use the original image for extra robustness (which is nonblind watermarking). Sometimes it is not possible to obtain the exact watermark as it depends up on the watermarking insertion algorithm and the way it is being embedded.

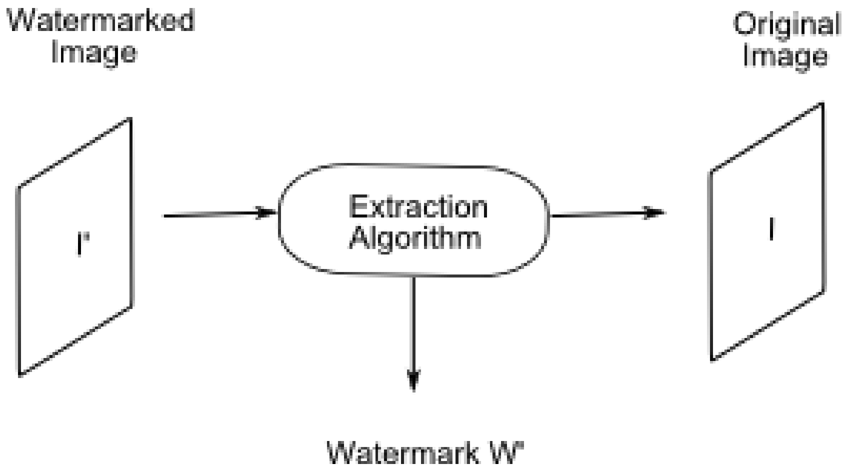


Figure 1.2. Watermarking extraction process

1.3.4 Detection of Watermark

Detection of watermark is different from the extraction process. The detection verifies the ownership whereas the extraction proves ownership. Detection of the watermark in the watermarked image can be calculated by correlating the watermark obtained after extraction with the original watermark. The watermarks with different keys have very low correlation value whereas the correlation value will be very high for the correct key.

1.4 Types of Digital Watermark

Watermarking techniques can be classified into various types as shown in figure 1.3. Based upon the type of document that is to be watermarked, the watermarking technique will vary for text, image, audio and video. Depending upon the insertion or extraction of the watermark, the original data can be converted into spatial or frequency domains like Fourier, discrete cosine transform (DCT), and wavelet transformation, where modifications can be made [2]. The frequency domain watermarking techniques are more robust to intentional and unintentional attacks compared to spatial domain watermarking.

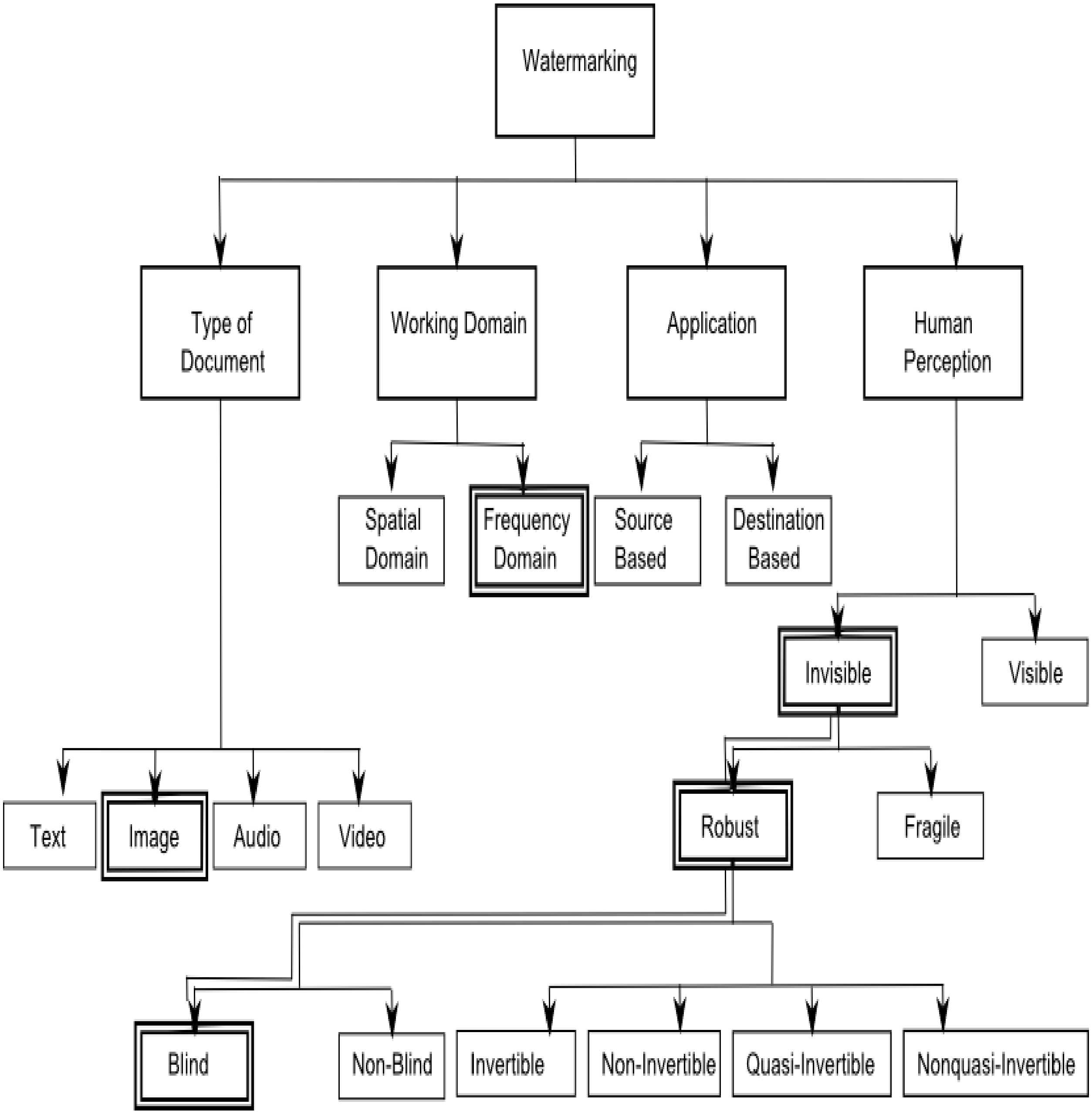


Figure 1.3. Types of digital watermarking schemes

For images, watermarking techniques are classified into two types based on perception:

- Visible
- Invisible

In the visible watermarking scheme, the watermark is embedded into the original (host) image such that it is translucently visible to the observer. In the case of invisible watermarking the watermark is imperceptible to the human eye. Invisible watermarking is divided into two categories as follows:

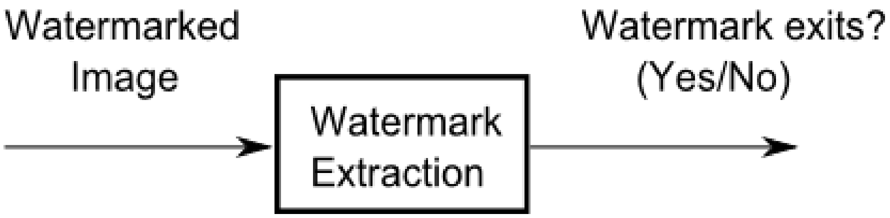
- Invisible-robust
- Invisible-fragile

In case of invisible-robust watermarking, the watermark is embedded in such a way that it is very difficult to alter and can only be recovered by the proper extraction algorithm. In case of invisible-fragile watermarking, the watermark can be altered or totally destroyed. They are used in different application scenarios.

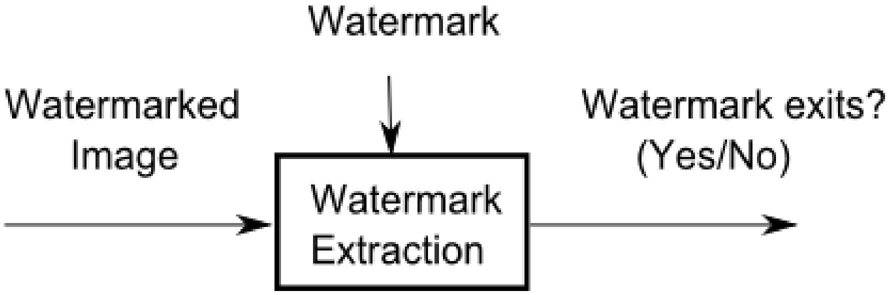
Invisible- robust watermarking is divided into two parts:

- Blind
- Nonblind

In applications like copyright protection, there will not be access to the original image where the extraction or detection will be much difficult known as blind or private watermarking as shown in Figure 1.4 (a). Figure 1.4 (b) shows nonblind watermarking. The original image is required for detection of the watermark and is used for copyright protection and data monitoring. Blind watermarking schemes are efficient for memory and processing time requirements. Since blind watermarking scheme does not need original image for extraction, it is better suitable for real-time applications.



(a) Blind watermarking technique



(b) Nonblind watermarking technique

Figure 1.4. Nonblind and blind watermarking schemes: a comparative perspective

The desired characteristics of a digital invisible blind watermark [1, 11] are as follows:

- The watermark should be robust to signal processing operations and attacker’s intentional distortions.
- The watermark should be imperceptible.
- The watermark should be able to detect the watermark without the original data.
- Increase in the robustness should not degrade the invisibility of watermark.
- The watermark should be able to unambiguously identify the true author or owner.

1.5 Organization of Thesis

The rest of the thesis is organized as follows: Chapter 2 describes the related research in the field of invisible watermarking for both blind and nonblind algorithms. In Chapter 3, the proposed invisible watermarking algorithm for insertion and extraction is discussed in detail. Chapter 4 discusses the experimental results of various test images and their detector's responses. Conclusions and future directions of this research are discussed in Chapter 5.

CHAPTER 2

REVIEW OF INVISIBLE WATERMARKING ALGORITHMS FOR IMAGES

2.1 Overview

The watermarking techniques proposed in the current literature are based on two working domains:

1. Watermarks embedded in spatial domain
2. Watermarks embedded in frequency domain

In this chapter the prior research related to the current invisible watermarking algorithms are briefly outlined, which is the scope of this thesis. Section 2.1 outlines the prior research on blind watermarking techniques. Section 2.2 presents prior research related to nonblind watermarking techniques.

2.2 Blind Watermarking Techniques

Wong et al. [5] propose three blind watermarking techniques. The first type called single watermark embedding (SWE) that embeds a watermark by two secret keys in a watermark space using spread spectrum technique. The second type of watermarking is called multiple watermark embedding (MWE) in which the same watermarking space embeds different watermarks simultaneously using different correlated secret keys. In the decoding of MWE, each watermark can be decoded separately as in SWE. The third technique is to embed the watermark into joint photographic experts group (JPEG)-compressed images ensuring that it is detectable. It is called iterative watermark embedding (IWE). The watermarked images obtained by these watermarking schemes produce perceptually high quality images.

Miller et al. [6] present an algorithm for robust image watermarking with large data payloads. It is based on informed coding and informed embedding to embed 1,380 bits of information in the images. In the information embedding, the watermark to be embedded is encoded and modified. Then it is inserted into the original host image. Constant robustness is maintained as the algorithm is designed to minimize the perceptual distance. The proposed system encodes the watermarks with modified trellis code and embedding is done using an iterative method. The robustness of the watermark is tested by volumetric scaling, lossy compression and noise addition. In this algorithm, 80% detection is achieved, which is effective for faithful detection.

Liu et al. [7] discusses the adaptive blind watermarking detection. The detector is designed based on generalized Gaussian distribution to establish statistical model for the subbands of the wavelet coefficients. The watermark is embedded in all the coefficients in the subbands of two-level discrete wavelet transform (DWT). An asymptotically optimal detection is used to analyze and estimate the shape parameter of wavelet coefficients. The experimental results prove that the detector is more practical.

An adaptive block-based blind watermarking scheme is proposed by Guannan et al. [8] using DWT. The proposed algorithm embeds a binary image into the original image. The selection of the subbands in which the watermark is embedded is performed after analyzing the coefficient characteristic. The watermarking embedding in this algorithm is realized by the modification of coefficients of the detail subbands using the statistic characteristic to adjust the embedding intensity adaptively. This block-based blind watermarking scheme is robust for image processing operations, noise addition, and lossy image compression.

In [9], an adaptive blind watermarking method based on zerotree wavelet is presented by Erhu and Fan. The authors have considered a method based on the types of image block as the solution to reduce the difficulty level in determining the threshold in the watermarking. After the integer wavelet transform is applied, each block is decomposed into three levels for watermark embedding. The authors show that using this technique increases the robustness against attacks.

Yu in [10] proposed a blind wavelet-based watermarking scheme changing the sign of DWT coefficients in order to indicate the watermarking bits. The polarity of the wavelet transformation coefficients, positive coefficients and negative coefficients are indicated by 1 and 0, respectively.

Choi and Seo in [11] present a statistical approach for watermark coefficients based on human visual system (HVS) blind watermarking approach. The watermarking scheme uses a two-step detection algorithm (TSDA). They have chosen a watermark gain in such a way that it is optimal in robustness and increase the performance of the watermarking techniques. The TSDA comprises of insertion and detection phases. In the insertion phase, each bit is placed in spreading pattern in the discrete cosine transform (DCT) coefficients and the detection part is done by estimate weighted binary hypothesis test (EWBHT). The two metrics, masked peak-signal-to-noise ratio (PSNR) and bit error rate (BER) used by the authors serve as a measure for invisibility and robustness.

A blind watermarking technique has been proposed by Zang et al. [12] based on 9/7 biorthogonal wavelet lifting transform. They discuss the first generation of wavelet lifting in which it analyzes the given image at multi resolution level so it can be useful in realization of the watermark embedding. It is known as integer wavelet lifting. The watermark is extracted from the low frequency domain.

In [13], Yen et al. have proposed a new blind watermarking technique based on the wavelet transform. By using the 3-level wavelet transform, the transformation of the noise watermark from the binary watermark is achieved and also the given image is resolved to ten sub bands. This noise watermark is employed to substitute the third and fourth bit of the absolute values of the coefficients. A 1D logistic map which is used to generate a pseudo random sequence and its parameters should be known for detection. The measure for invisibility, PSNR, for the proposed system is 43 *dB*.

Qiao et al. [14] present an adaptive blind watermarking scheme adopting the double embedding. Based on the HVS model the watermarking algorithm introduces a method for block classification in which the selection of quantization pedometers is done adaptively in order to embed the watermark in the most energy signal, DC component. This algorithm shows that by changing the order of the coefficients, the watermark can also be embedded into the midfrequency bands. This algorithm is robust to image processing operations and also for geometric distortions.

In case of blind watermarking, to accomplish perceptual invisibility, the watermark is embedded into the mid frequencies of the chosen DCT coefficients [23]. The two main reasons for considering mid-frequency DCT coefficients are as follows:

(a) Compression techniques such as JPEG will mainly affect the higher frequencies.

(b) Insertion of watermark in the lower frequencies may also cause problems if an attacker is interested in defeating the invisible watermarks.

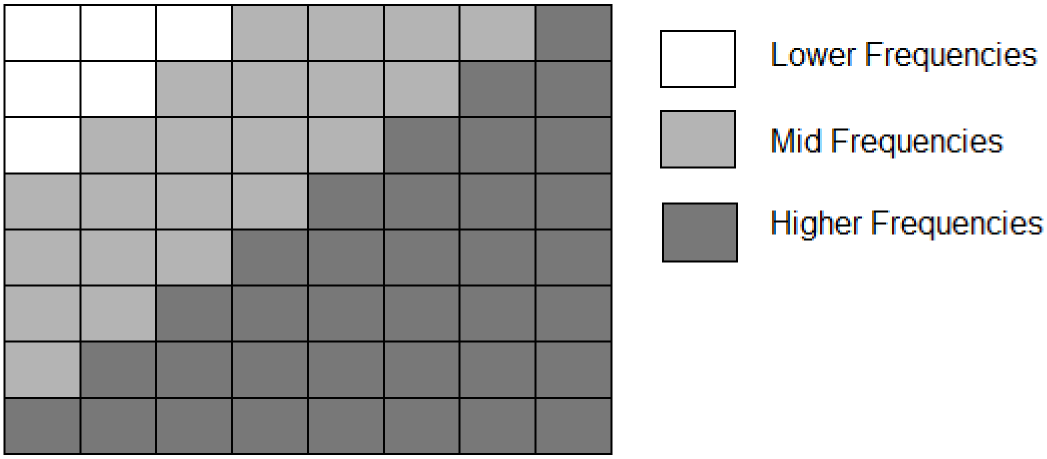


Figure 2.1. 8 X 8 DCT block showing various frequencies in transformed domain

Eventually this band of mid-frequencies is chosen to embed the watermark such that it survives lossy compression.

2.3 Nonblind Watermarking Techniques

Yongliang et al. [16] propose high security watermark detection schemes as the solution for faithful validity and unsecure problems. They propose the watermarking schemes based on zero knowledge protocol in which they implement the encryption tools so that the data can be hidden and while detecting, so that the information is not revealed. The encryption tool used is Rabin cryptosystem which is a public-key encryption scheme. The Rabin scheme is secure as the difficulty level is high for an attacker to find the square roots modulo of a composite number. In detection of the watermark, the owner sends his public-key to the verifier through a trustful judge so that either of them can fool the other. So this scheme is considered to be highly secure as compared to the conventional watermarking schemes. The approach provides both security and validity so that the attacker can either remove the watermark or can add a false watermark.

In [15], Khalfallah et al. propose a watermarking scheme using adaptive embedding strength so that the quality of the watermarked image does not get affected. The approach in turn improves the robustness of watermarking. The watermarking scheme is implemented on multiresolution field [wavelet 5/3] in which the image is transformed to multiresolution field followed by the selection of coefficients to be watermarked. Then the insertion of watermark is performed, which is followed by the inverse transformation. A daughter mark is being substituted instead of the regular referencing mark. This adapted embedding strength consists of two terms, one is fixed and the other is variable to reduce the computational errors. They have compared the results with the other existing algorithms and claim that they have obtained a better robustness and imperceptibility.

Safabakhsh et al. [17] present a digital watermarking technique based on two-dimensional DWT of still gray level images. This is a hierarchical transform for the signal to be analyzed at various resolutions. This technique embeds a watermark in high-pass wavelet coefficients without affecting the visual fidelity of an image. After the extraction of the original watermark from a binary logo image it is scrambled with a known PN sequence which is again used while extracting the watermark, improving the security level. They selected Antonini 7.9 wavelet for watermarking which is a biorthogonal wavelet and HVS model. The proposed method is approached on the entropy based and on the characteristic of the HVS model to select the wavelet coefficients in order to determine the watermarked coefficients. The experimental results show that they have achieved a better detection algorithm.

Eskicioglu and Ganic [18] propose a hybrid scheme based on wavelet transform and singular value decomposition domain (SVD). The 2-D DWT produces four bands of data at each level of decomposition and the watermark is embedded in the lower frequency for modification of the wavelet coefficients to increase the robustness. The SVD is applied to each band by the modifying the singular values which is resistant to most of the attacks. Unlike in other watermarking techniques even the low pass (LL) band is modified there will not be any loss of transparency. The removal of the watermark is difficult for an attacker as the same watermark is embedded in 4 blocks not only in low frequencies but also in high frequencies. The proposed watermarking scheme is resistant to various attacks including, image compression schemes, histogram equalization and geometric attacks.

Piper et al. [19] propose an algorithm which provides a solution for the tradeoff between the resolution and quality scalability by using characteristics of human visual system. They provided a spread spectrum image watermarking algorithm which uses a constant embedding strength and hence easy to implement. The authors also have developed a detection algorithm based on texture, focusing on texture regions. For each wavelet coefficient after implementing texture detection algorithm in wavelet domain a single resolution is used. The proposed HVS adaptive algorithm has achieved the quality scalability without any compromise on the resolution scalability.

Another digital watermarking algorithm has been proposed in [20] by Walter et al. based on complex wavelet transform (CWT) using error correction code to enhance the robustness of watermarking. The watermarking is performed in the spatial domain. The CWT is used for two reasons:

- Adapting a watermark in another image by visual masking.
- Selection of third and fourth level of CWT decomposition and employing the inverse CWT on every level so as to attain the two embedding channels.

By implementing additive spread spectrum, the watermark can be added to the attained embedding channels. The authors also perform the algorithm in DWT domain and the robustness is found to be better in CWT domain.

An efficient watermarking technique for gray level images is developed by Zaboli and Moin [21] based on the entropy using the human visual system (HVS) characteristics. This is performed in contourlet domain in which four levels are attained by the decomposition of the source image using curve scaling relation. After scrambling with a known PN-sequence [pseudorandom sequence] it is then watermarked with a logo image which increases the performance of detection in the extraction part. The quality of the extracted watermark can be increased by increasing the levels of decomposition.

In [22], Denis et al. present a watermarking algorithm for subdivision surfaces implementing in frequency domain addressing the tradeoff between the redundancy and imperceptibility by introducing error correcting codes (ECC) and a modulation technique respectively. This proposed algorithm is based on frequency domain decomposition and also on spectral coefficient modulation of subdivision control mesh. A synchronization process is used to retain the corresponding control mesh and also to extract the watermark by providing robustness against attacks.

CHAPTER 3

THE PROPOSED WATERMARKING ALGORITHM

The robust invisible watermarking algorithm with blind extraction is presented in this chapter. In section 3.1, the proposed insertion algorithm is explained. The extraction process is explained in section 3.2.

Table 3.1. Notations used to explain the proposed watermarking algorithms

O	Original color image
Y	Y-component after conversion of O [RGB] to YCbCr
A	Watermark, pseudo random numbers with zero mean and unit variance
O'	Watermarked image, also color image
O^*	Distorted image
$N \times N$	Dimension of the test images O and corresponding watermarked images O'
σ	Watermark detection ratio
Th_{σ}	Watermark detection threshold
α	Scaling constant , watermark strength factor

3.1 Watermarking Insertion Algorithm

In the proposed algorithm, I performed watermarking with color images of size $N \times N$ based on the procedure proposed by Mohanty et al. in [3] and A. Piva et al. in [27]. I initialized the process by transforming color images from RGB to YC_bC_r, where the Y component is considered for further watermarking insertion process. Figure 3.1 presents a schematic overview of my proposed robust invisible watermarking insertion algorithm. After the color transformation phase, the image Y was divided into equal number of 8 x 8 blocks and discrete wavelet transformation [DCT] was performed on each block.

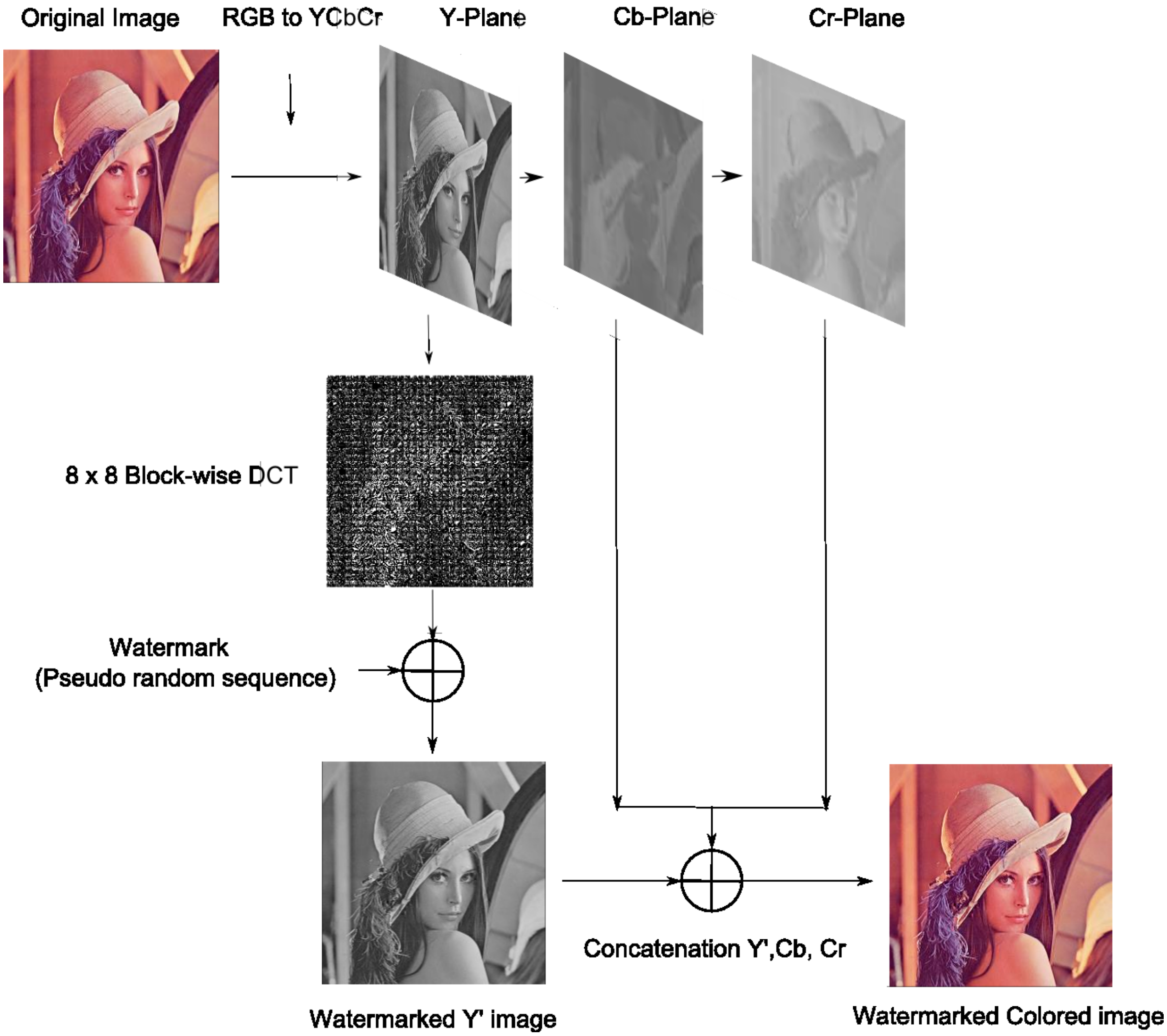


Figure 3.1. Schematic showing the insertion process.

The watermark can be placed anywhere in the image, but I chose to embed the watermark in the blocks of size 8 x 8 in the center quarter of the image. There are two specific reasons behind this decision:

(1) The center quarter of the image is gets more attention from the viewer. So, if an attacker tries to destroy the watermark, he will potentially destroy the image quality and its value.

(2) By not changing the rest 75% of the image effectively most portions of the image are left intact. This in turn reduces the amount of processing needed and maintains highest possible overall quality.

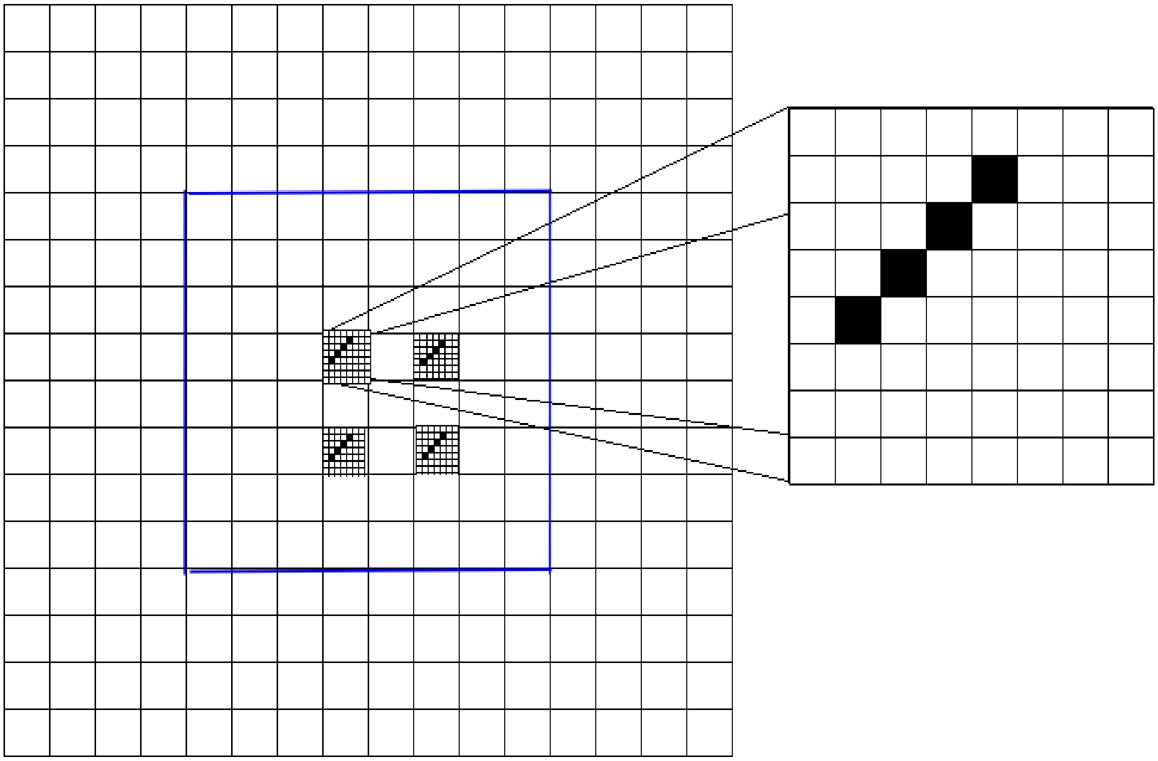
The selection of the blocks in the center quarter was critical through which four coefficients are chosen $C_{4,1}$, $C_{3,2}$,$C_{2,3}$,$C_{1,4}$. Through these coefficients I generated a vector R of size K which is the number of 8 x 8 blocks in the central quarter of the image:

$$R = \{ r_{1,i}, r_{2,i}, r_{3,i}, r_{4,i}, \ldots , r_{1,K}\ r_{2,K}\ r_{3,K}\ r_{4,K} \},$$

where $r_{x,y}$ was the coefficient of the selected block y and K was assumed to be the number of blocks in the center quarter of the image in which each block was numbered in the range [1,K]. A pseudorandom sequence chosen from 1,000 pseudorandom sequence of size $4 \times K$ was generated, which was used as the watermark represented by:

$$A = \{a_1, a_2, a_3 \ldots . a_{4 \times K}\},$$

where every element was of zero mean and unit variance.



(a) N x N image showing the center quarter blocks (b) Mid-frequencies of 8 x 8 blocks

Figure 3.2. Image showing the central quarter and mid frequencies of a block

.

To obtain a robust watermark, the watermark DCT coefficients were inserted into the midfrequencies of the image DCT coefficients ([23], [5], [6]). Figure 3.2 shows the *N x N* image with the central quarter blocks and also the 8 x 8 block showing the midfrequencies ($C_{4,1}$, $C_{3,2}$,$C_{2,3}$,$C_{1,4}$) where the watermark was exactly located to obtain more robustness. Table 3.2 explains step by step the invisible watermarking insertion algorithm discussed so far and also its pseudo-code.

Table 3.2. Watermarking insertion algorithm flow

Algorithm 1 Invisible watermarking insertion algorithm

```
Input:    Original image $O\ [N \times N]$, Watermark $X$
Output:  Watermarked image $O'$
Convert O=> Y, Cb, Cr
for component Y do
    8 x 8 block-wise DCT =>$Y'$
    Select coefficients $C_{4,1}, C_{3,2}, C_{2,3}, C_{1,4}$ from centered blocks
    form vector R= $\{ r_{1,i}, r_{2,i}, r_{3,i}, r_{4,i}, \ldots, r_{1,K}\ r_{2,K}\ r_{3,K}\ r_{4,K} \}$
    for size[R]
        generate watermark $A = \{ a_1, a_2, a_3, \ldots a_{4 \times K} \}$
        insert $A$ into $R$ forming
            $R' = \{ r'_1, r'_2, r'_3, \ldots r'_{4 \times K} \}$ by
                $r'_i = r_i + \alpha | r_i | a_i$
        reinsert $R'$ into corresponding blocks of $Y'$
        for image $Y'$
            8 x 8 block-wise inverse DCT =>$Y''$
        end
    end
end
Concatenation of Y"+ Cb+ Cr => $O'$
Compute PSNR and RMSE.
```

The watermark A was inserted into the DCT coefficients of the image of vector R according to equation [3.1]:

[3.1] $$r'_I = r_i + \underset{.}{\alpha} | r_i | \mathrm{a}_\mathrm{i}$$

This process formed a new vector $R' = \{ r'_1, r'_2, r'_3, \ldots\ldots r'_{4 \times K} \}$ of the same size as of the vector R where I = 1, 2, …4 x K, where α is the scaling constant to determine the watermark strength. To improve the performance of the watermark systems an optimal watermark strength ɑ̣ can be achieved by increasing its value [11], but the watermark became visible after a certain extent. By maintaining the invisibility of the watermark and at a maximum value of ɑ̣ the attacker cannot insert any signature to destroy the copyright or the ownership of the image unless it undergoes a strong degradation.

In figure 3.3, the flowchart clearly demonstrates the flow of the reinsertion of the new vector R' into the matrix of DCT coefficients of the corresponding blocks. Block-wise [8 x 8] IDCT [inverse discrete cosine transform] was applied to obtain the watermarked image *Y''* in spatial domain. In order to obtain the final watermarked image the C_b and C_r components were concatenated with the watermarked Y component Y'' to get O'.

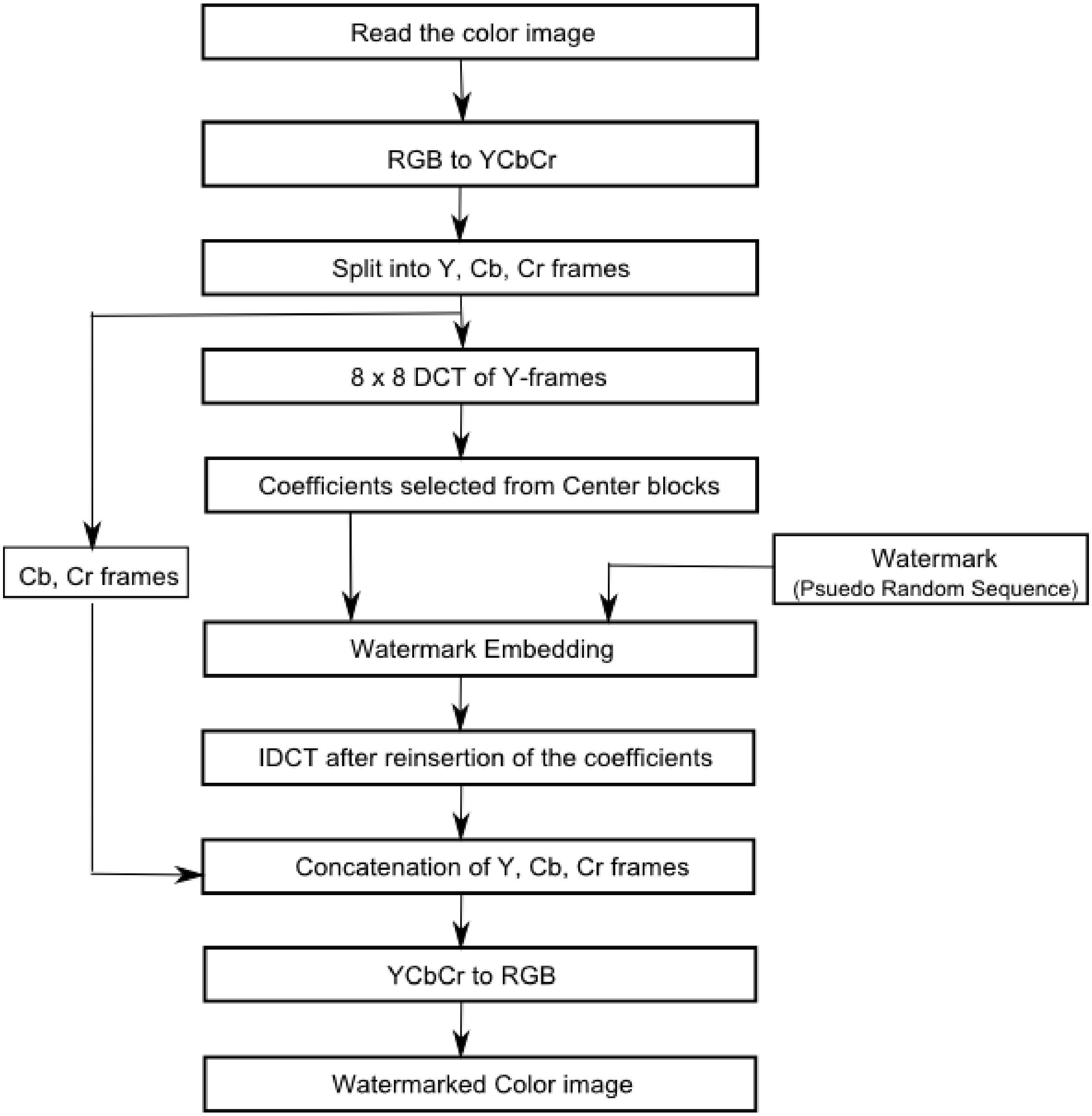


Figure 3.3. Flow chart of insertion algorithm

3.2 Watermarking Detection Algorithm

The detector has zero knowledge of the original image, which is a promising approach to overcome the security issue. As the original image is not required the memory and process requirement is reduced significantly. This is very attractive when the watermarking system is realized in hardware.

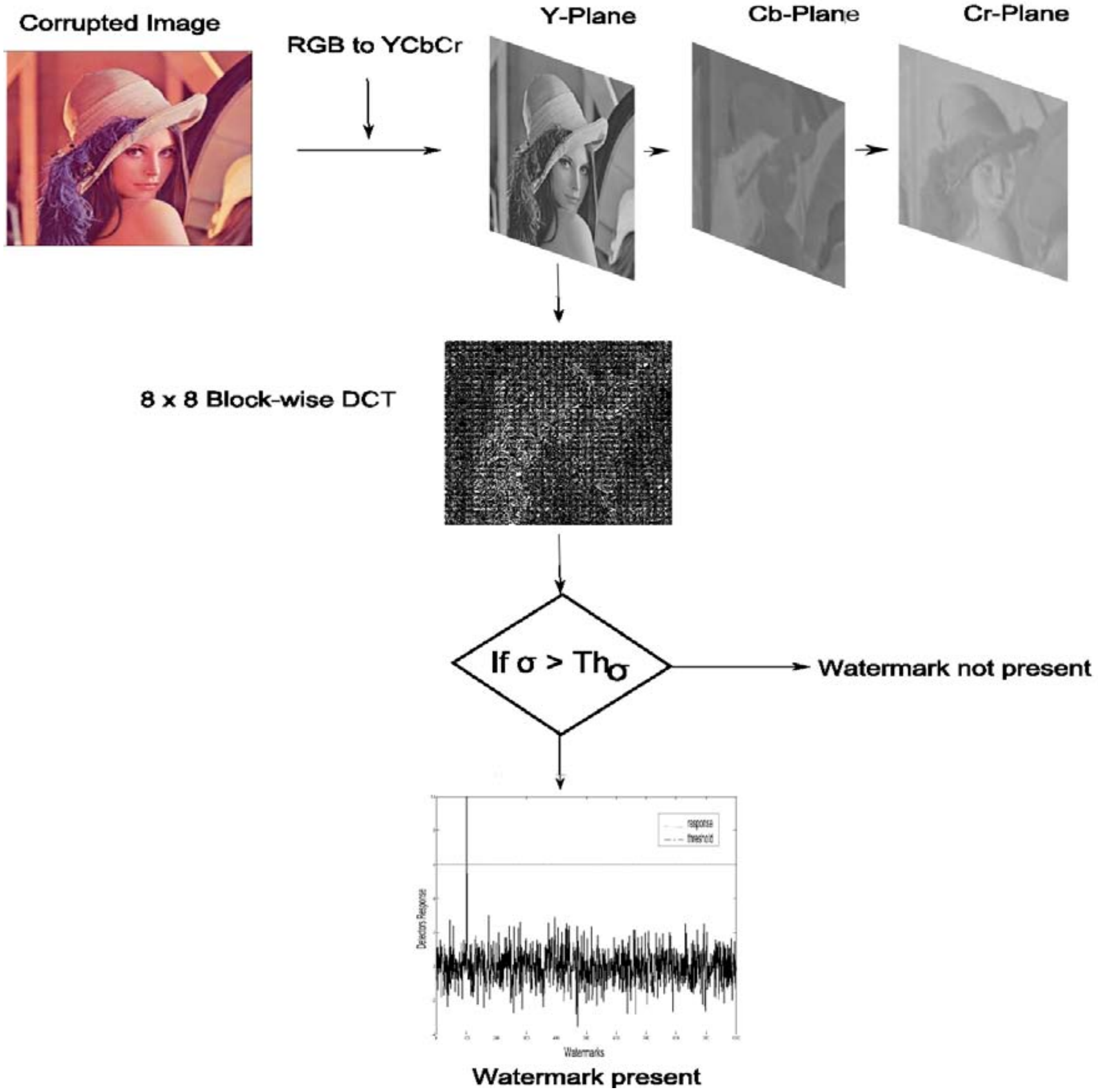


Figure 3.4. Schematic of the detection of watermark

Figure 3.4 depicts the schematic for the watermark extraction process in my proposed invisible watermarking scheme. As my watermark was inserted in the Y component of the image, I needed to transform the color image from RGB to YCbCr and I denoted this as *Y**.

In the ideal condition where the watermark is not corrupted by any attacker it is sufficient only to compute the 8 x 8 block- wise DCT coefficients of the watermarked image. There is a possibility of tampering effects by the unauthorized user or by transmission distortions by which I obtained a corrupted image O*.

Now the 8 x 8 block wise DCT is applied to O* to obtain the DCT coefficients. My proposed extraction process being blind, I did not need to have the availability of the original image O or the watermark. In Table 3.3, it clearly shows that the blocks of size 8 x 8 which are in the central quarter of the image are located to extract the watermark from the coefficients which are chosen during the watermarking insertion.

Table 3.3. Detection of watermark algorithm

Algorithm 2 Invisible watermarking extraction algorithm

```
Input:     Corrupted image $O^* [N x N]$
Output:  d
Convert O* => Y*, Cb, Cr
for component Y* do
      8 x 8 block-wise DCT
      extract watermark coefficients $C_{4,1}$,$C_{3,2}$ ,$C_{2,3}$ ,$C_{1,4}$ from centered blocks
      Generate vector $R^* = \{r^*_1, r^*_2, r^*_3 \ldots. r^*_{4 \times K}\}$.
end
Verification of the authentication
if [$\sigma > Th_\sigma$] then
      return d = watermark present
else d = watermark not present
```

From the chosen coefficients a vector is generated of size 4 x K,

$$R^* = \{r^*_1, r^*_2, r^*_3 \ldots . r^*_{4\,x\,K}\}$$

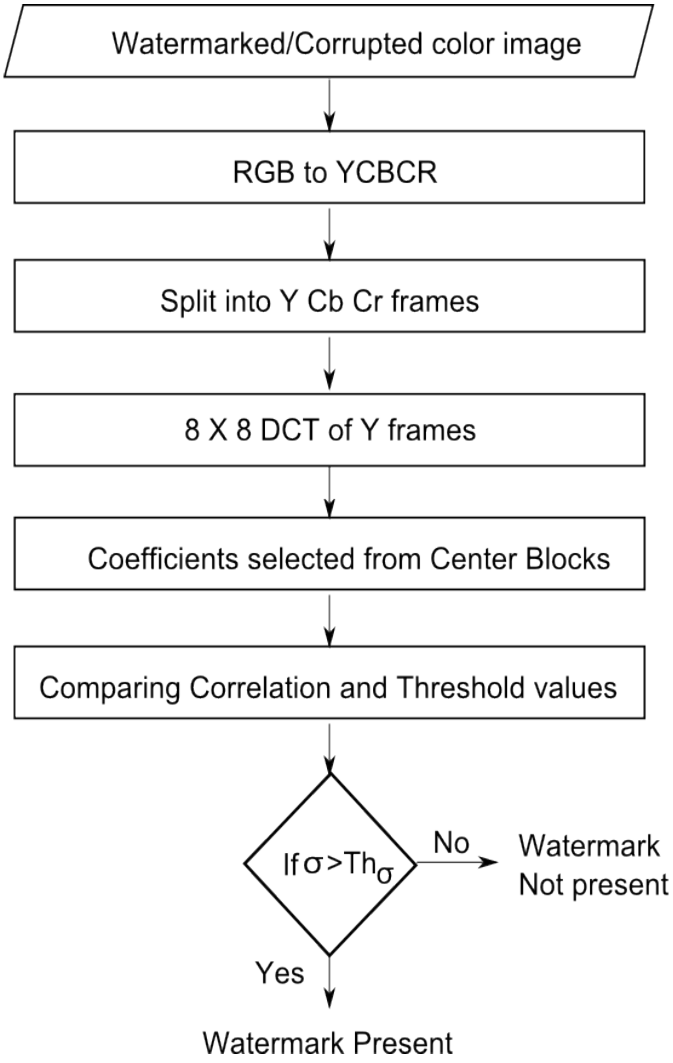

Watermarked/Corrupted color image
RGB to YCBCR
Split into Y Cb Cr frames
8 X 8 DCT of Y frames
Coefficients selected from Center Blocks
Comparing Correlation and Threshold values
If σ>Th$_\sigma$
No
Watermark Not present
Yes
Watermark Present

Figure 3.5. Flowchart for watermark detection

To determine the watermark presence as shown in the figure 3.5 I introduced a correlation coefficient “σ” equation [3.2] which computed the correlation between the extracted coefficients *R** and the watermark itself using the formula:

[3.2] $$\sigma = \frac{A.R^*}{K} = \frac{1}{K}\sum_{i=1}^{K} a_i r^*_{L+i}$$

I introduced “Th_{σ}” equation [3.3] which is a predefined value called the threshold. By comparing the value of “σ” and “Th_{σ}” it can be determined whether the watermark is present or not present, and it is defined as:

$$Th_{\sigma} = \frac{\alpha}{3\,K} \sum_{i=1}^{K} |r_i^*|$$

[3.3]

It has two states:

- $\sigma > Th_{\sigma}$ then watermark is present
- $\sigma < Th_{\sigma}$ then watermark is not present

By this can be made a decision whether the image is authentic or not.

CHAPTER 4

EXPERIMENTAL RESULTS

4.1 Experimental Setup

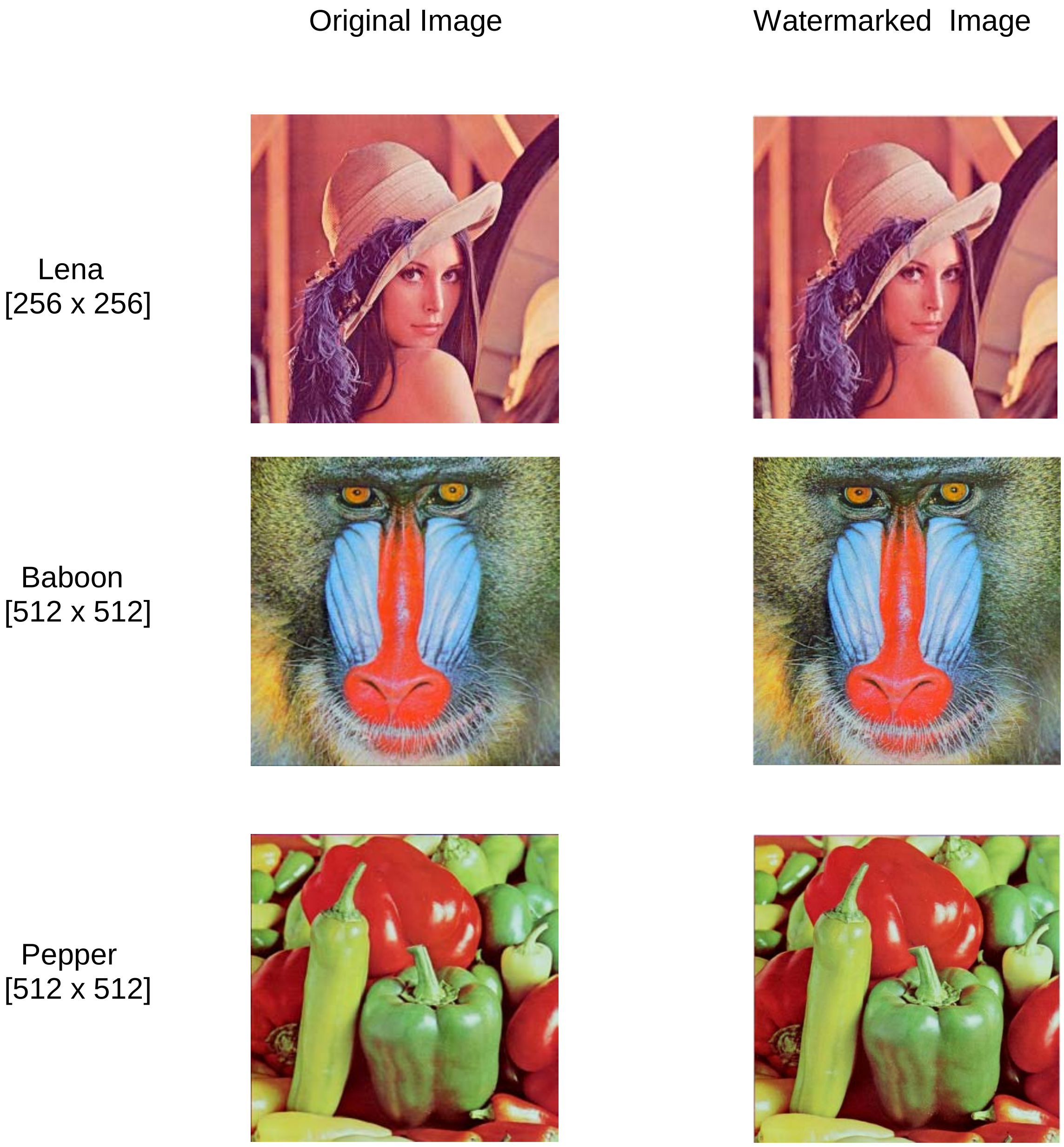
The primary goal of this experiment was to determine whether the proposed watermarking scheme improved the robustness without any loss in the quality of the image. The invisible watermarking algorithm was implemented in MATLAB® high-level language and interactive environment (The Mathworks, Inc., Natick, MA, www.mathworks.com). I performed extensive testing of the proposed algorithm for several test images. The details of the experiment can be found in the section 4.4.

4.2 Test of Insertion and Quality Assurance

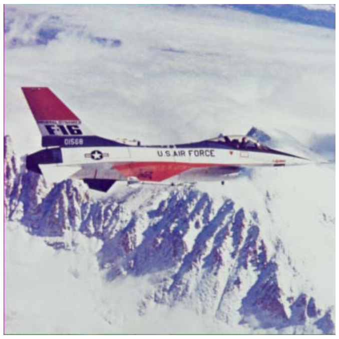
Each of the 9 images selected at random from large set of images was processed with the invisible watermarking insertion algorithm as discussed earlier in the section 3.2.

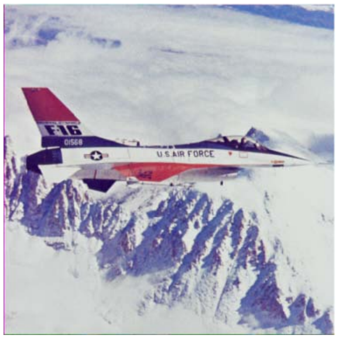
Figure 4. Figure 4 shows the various test images and their corresponding watermarked images. The test images are of different sizes, like 128 x 128 (winter greens [29]), 256 x 256 (Lena [4], trees [29], board [29], bear [26], kid [26]) and 512 x 512 (baboon [4], peppers [4], F-16 [4]). The performance of the proposed algorithm increases as the size of the image increases. In many schemes the insertion of the watermark is usually done in raw images. I implemented the algorithm in joint photographic experts group (JPEG) compressed images (.jpg files). The watermark is JPEG compatible, which can be decodable or detectable. I also executed the algorithm in portable network graphics (.png files) format. The experiments on these images

reveal the efficiency of the proposed algorithm in producing watermarked images with good visual quality presented in Figure 4.1.

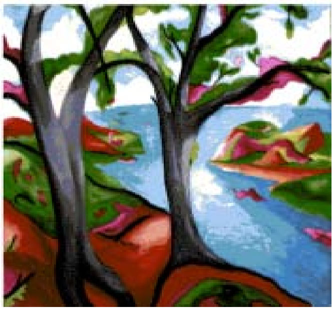


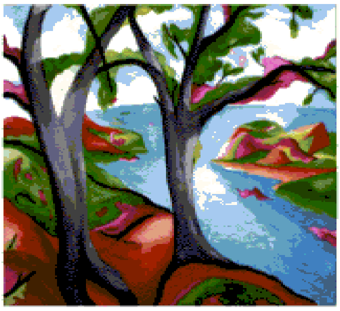
F-16
[512 x 512]



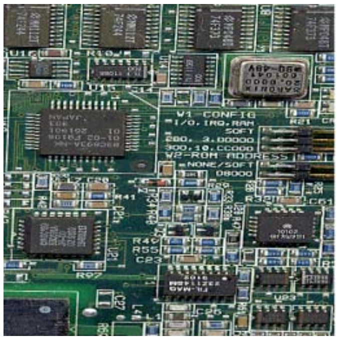


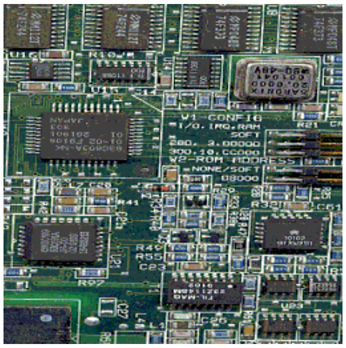
Trees
[256 x 256]



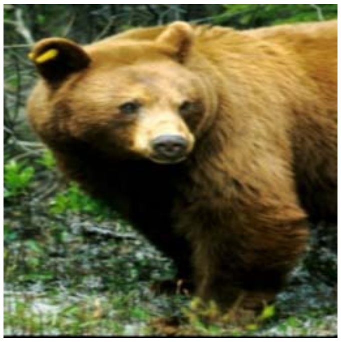


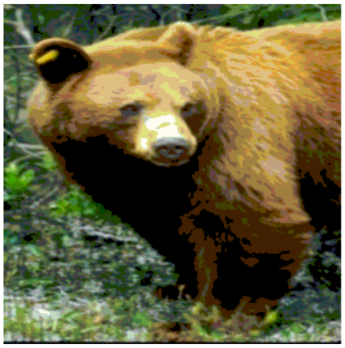
Board
[256 x 256]





Bear
[256 x 256]





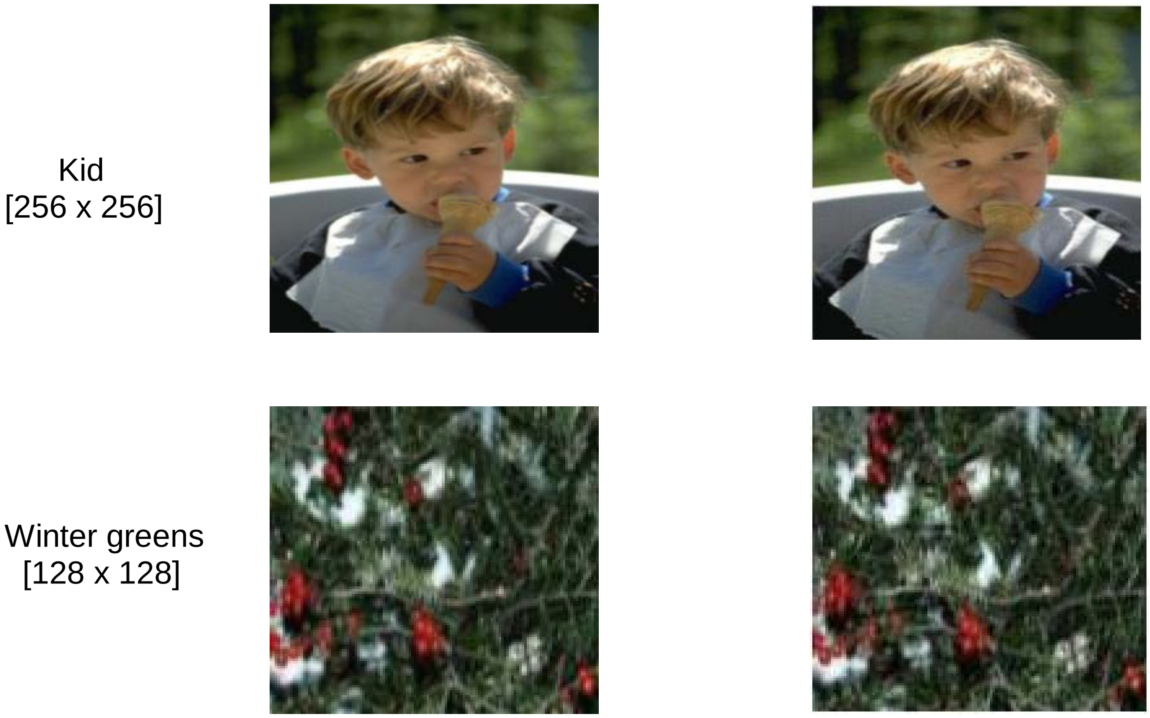


Figure 4.1. Original images and corresponding watermarked images

As observed in the original images above and the corresponding watermarked images, quality change cannot be seen by human eyes. Thus the watermarking scheme can be useful for copyright protection of high-quality images.

4.2.1 Graphs of Alpha vs. PSNR and Alpha vs. RMSE

In order to measure the robustness and invisibility of the watermark I used two performance measures, PSNR (peak signal-to-noise ratio) and RMSE (root mean squared error). RMSE of the extracted watermark O’ compared to that of the stored original O [24] of size m x n, is given by equation [4.1]:

$$RMSE = \sqrt{\frac{1}{mn}}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}||O(i,j) - O'(i,j)||\ ^{2}$$

[4.1]

The results of a quantitative analysis using RMSE are summarized in Table 4.1 for various test images for the range 0.2 ≤ α ≤ 0.65.

Table 4.1. RMSE values of the analyzed images

α	0.2	0.25	0.3	0.35	0.4	0.45	0.5	0.55	0.6	0.65
Lena	0.55	0.69	0.82	0.94	1.06	1.16	1.27	1.37	1.46	1.56
Baboon	0.37	0.46	0.55	0.63	0.72	0.81	0.89	0.97	1.04	1.12
Peppers	0.28	0.36	0.43	0.49	0.56	0.62	0.68	0.74	0.79	0.85
F-16	0.55	0.68	0.81	0.94	1.05	1.17	1.27	1.37	1.47	1.55
Trees	0.66	0.82	0.97	1.11	1.24	1.36	1.48	1.59	1.70	1.80
Board	1.02	1.27	1.52	1.74	1.94	2.14	2.31	2.47	2.62	2.76
Bear	0.37	0.46	0.55	0.64	0.73	0.82	0.90	0.98	1.05	1.12
Kid	0.25	0.31	0.37	0.43	0.49	0.55	0.61	0.67	0.73	0.79
Winter greens	0.59	0.74	0.89	1.03	1.18	1.31	1.45	1.57	1.68	1.80

The PSNR is the ratio between maximum possible energy of *O* and the power of corrupted image *O'* from watermarking [11] and is given by the equation [4.2]:

$$PSNR = 20.log_{10}\left(\frac{max_I}{RMSE}\right)$$

[4.2]

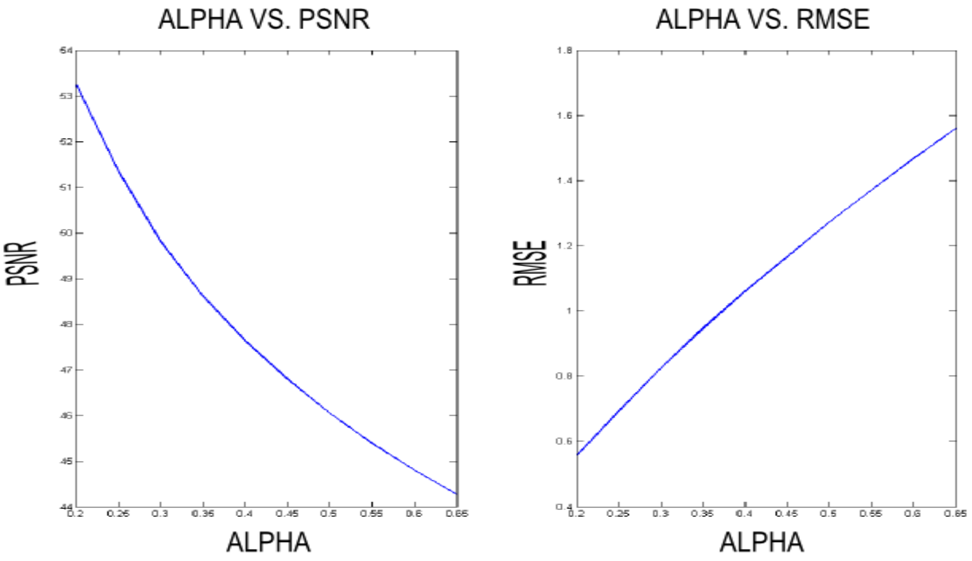
The metrics give the measure for invisibility. It can be observed from table 4.2 that the PSNR is maintained above 39 *dB* [20], [11] by utilizing α value so that the reduction of perceptual quality is very small. The results of this quantitative analysis using PSNR are summarized in table 4.2 for various test images for the range 0.2 ≤ α ≤ 0.65.

Table 4.2. PSNR values (*dB*) of the analyzed images

α	0.2	0.25	0.3	0.35	0.4	0.45	0.5	0.55	0.6	0.65
Lena	53.2	51.3	49.8	48.6	47.6	46.7	46.0	45.3	44.8	44.2
Baboon	56.7	54.6	53.3	52.0	50.9	49.9	49.1	48.3	47.7	47.1
Peppers	58.9	56.9	55.4	54.1	53.1	52.2	51.4	50.7	50.1	49.5
F-16	53.2	51.3	49.8	48.6	47.6	46.7	45.9	45.3	44.7	44.2
Trees	51.6	49.7	48.3	47.1	46.2	45.4	44.6	44.0	43.5	42.9
Board	47.9	46.0	44.4	43.3	42.3	41.5	40.8	40.2	39.7	39.2
Bear	56.6	54.7	53.1	51.9	50.7	49.8	49.0	48.2	47.6	47.1
Kid	60.1	58.1	56.6	55.3	54.1	53.1	52.3	51.5	50.7	50.1
Winter greens	52.5	50.6	49.1	47.8	46.6	45.7	44.9	44.1	43.5	42.9

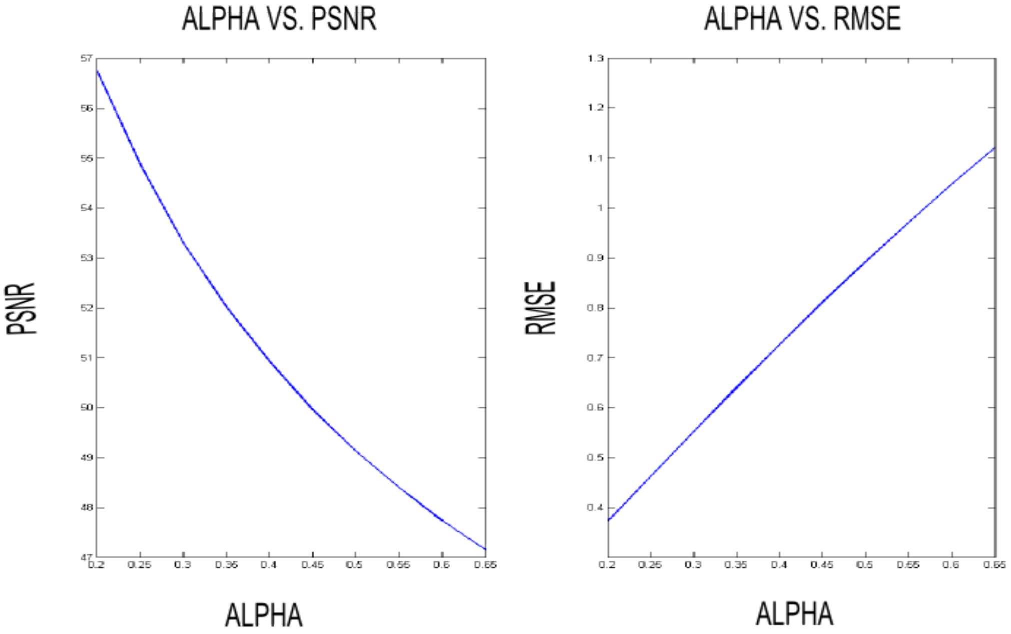
I observed that at greater PSNR the visual quality of watermarked images is very good and that it is almost indistinguishable for the human eyes from the original image.

Figure 4.2 through figure 4.10 show the various graphs for alpha vs. PSNR and alpha vs. RMSE. The robustness for every image was different depending upon the PSNR values. Figure 4.2 shows the graphs for Lena image with varying PSNR and RMSE values for 10 different α values ranging from 0.2 to 0.65. The average PSNR of the watermarked Lena image is 47.3 *dB* depicting a very high visual quality. In a similar kind of observation can be made for baboon image for different α values and the average PSNR was found to be 50.5 *dB* showing that it was more robust than the Lena image.



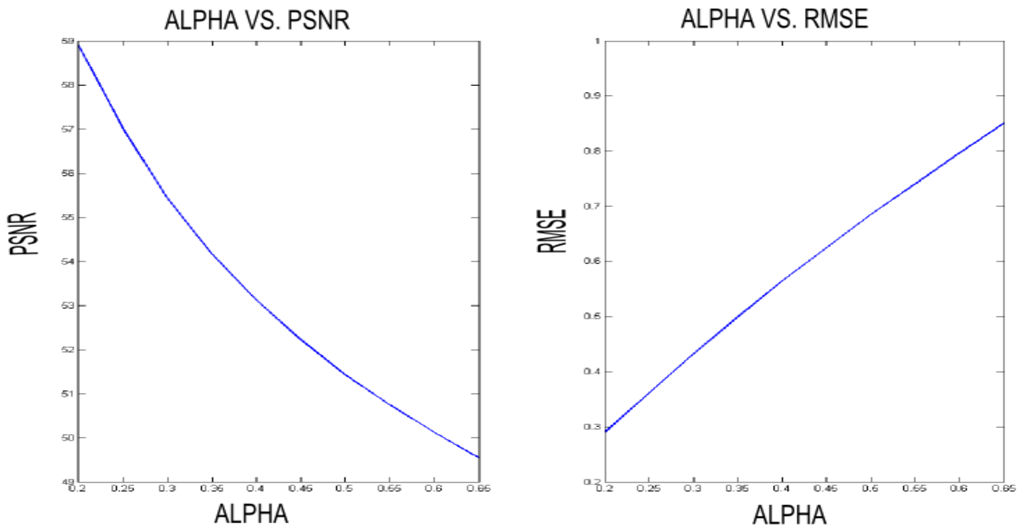
(a) Alpha vs PSNR (b) Alpha vs RMSE

Figure 4.2. Graphs of alpha vs. PSNR and alpha vs. RMSE for Lena image



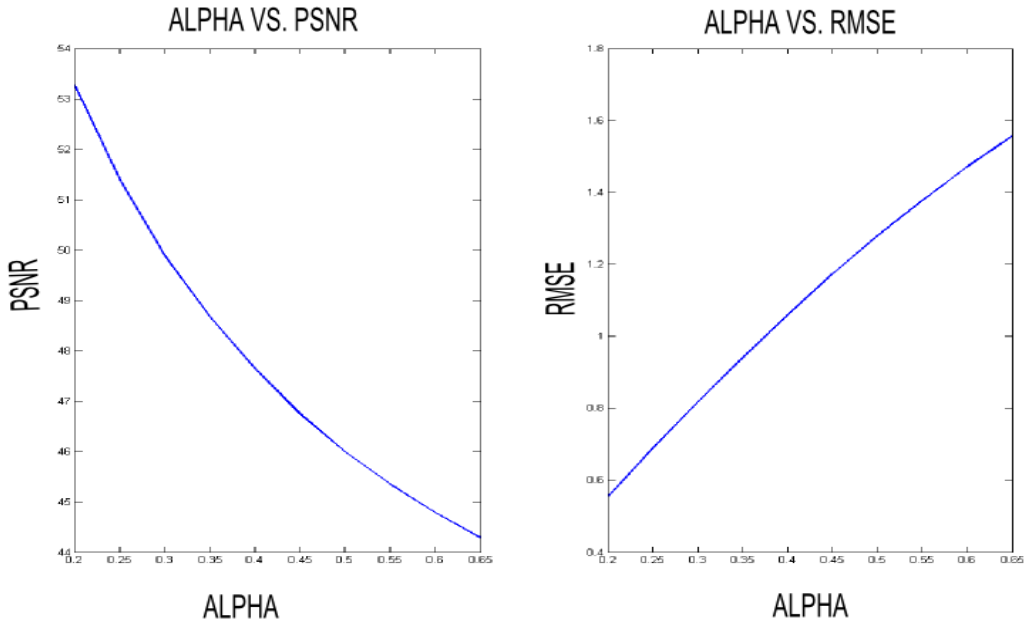
(a) Alpha vs. PSNR (b) Alpha vs. RMSE

Figure 4.3. Graphs of alpha vs. PSNR and alpha vs. RMSE for baboon image



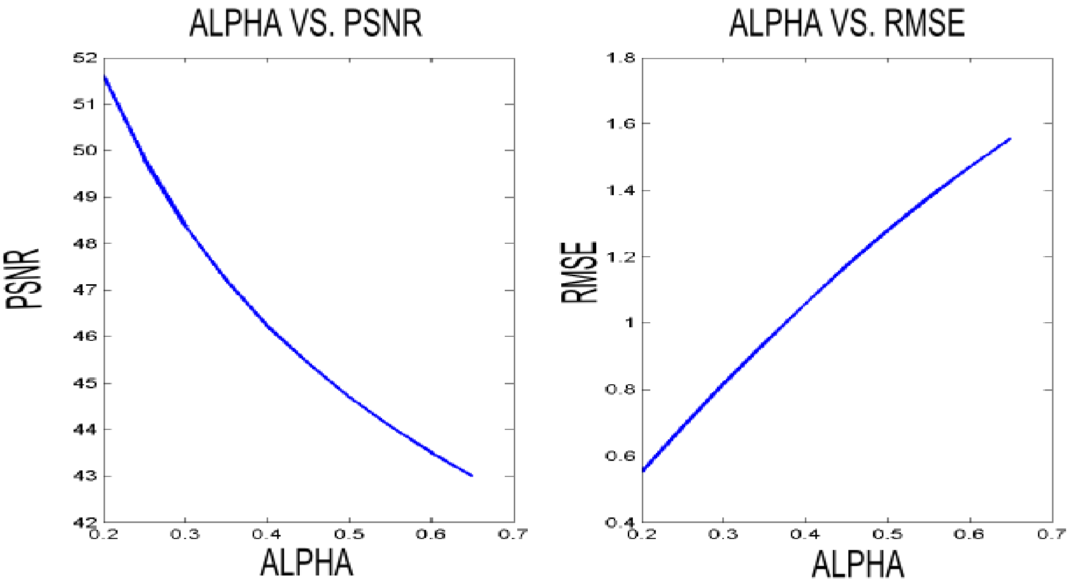
(a) Alpha vs. PSNR (b) Alpha vs. RMSE

Figure 4.4. Graphs of alpha vs. PSNR and alpha vs. RMSE for peppers image



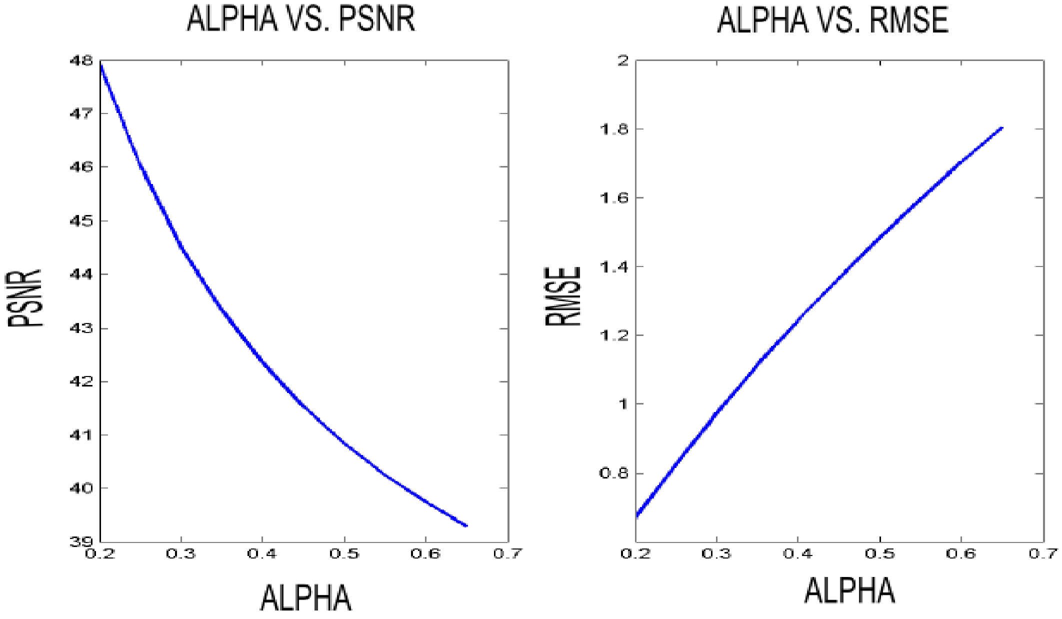
(a) Alpha vs. PSNR (b) Alpha vs. RMSE

Figure 4.5. Graphs of alpha vs. PSNR and alpha vs. RMSE for F-16 image



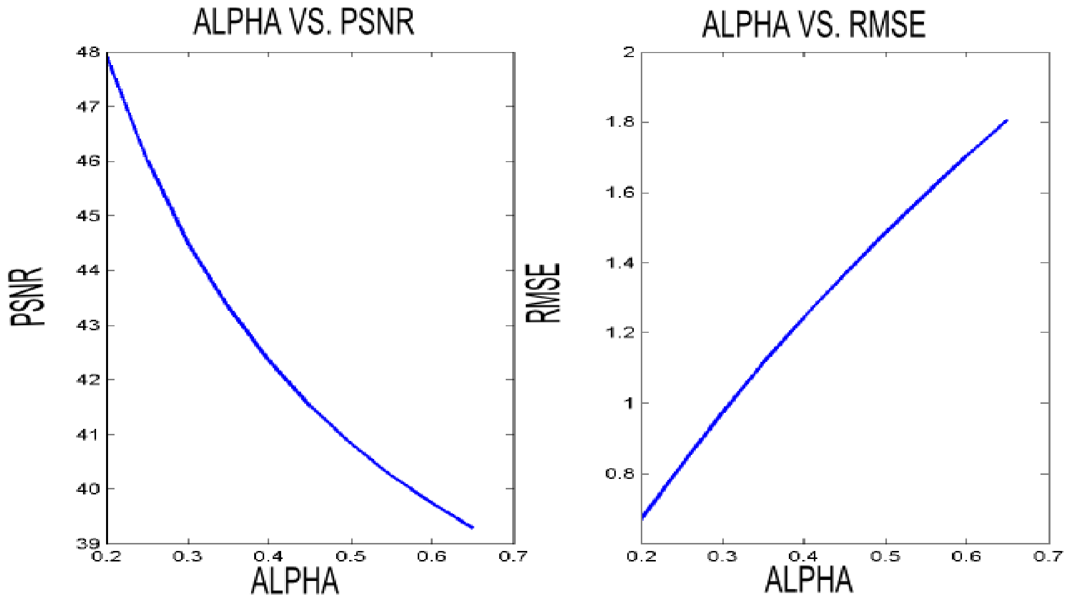
(a) Alpha vs. PSNR (b) Alpha vs. RMSE

Figure 4.6. Graphs of alpha vs. PSNR and alpha vs. RMSE for trees image



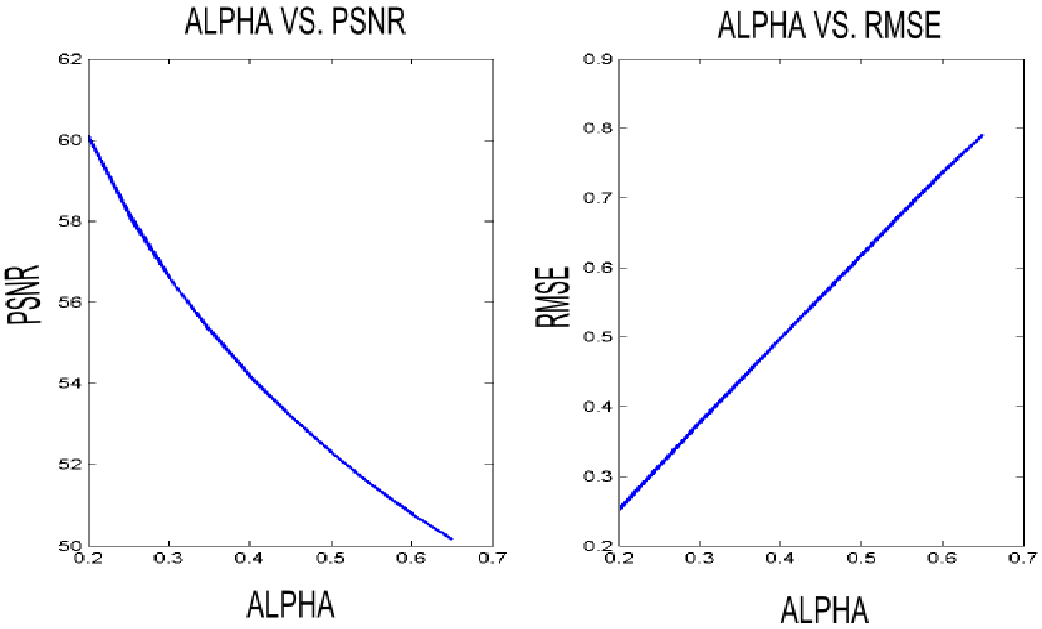
(a) Alpha vs. PSNR (b) Alpha vs. RMSE

Figure 4.7. Graphs of alpha vs. PSNR and alpha vs. RMSE for board image



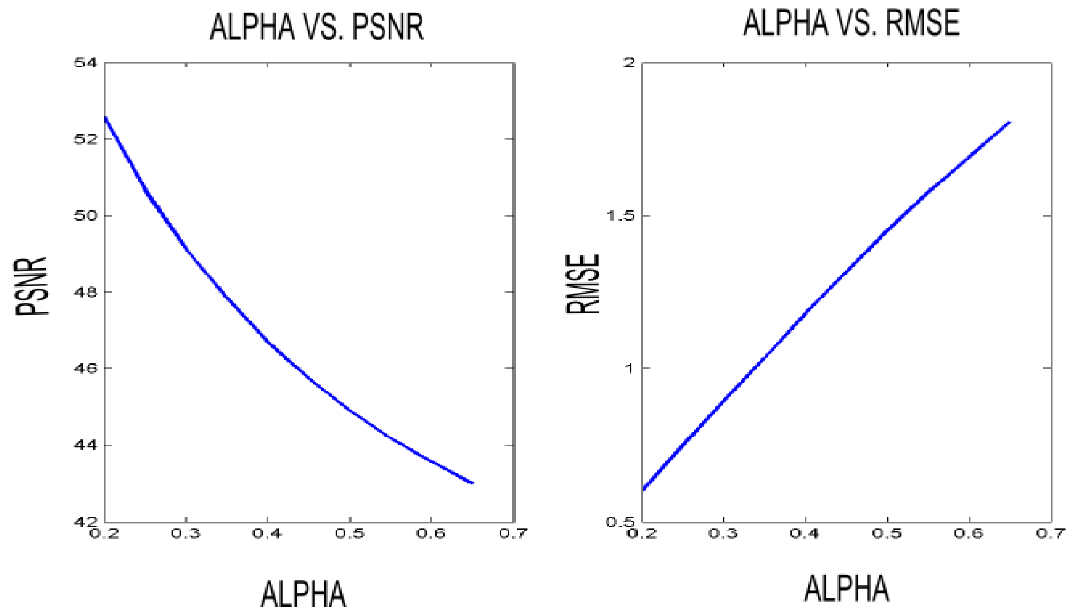
(a) Alpha vs. PSNR (b) Alpha vs. RMSE

Figure 4.8. Graphs of alpha vs. PSNR and alpha vs. RMSE for bear image



(a) Alpha vs. PSNR (b) Alpha vs. RMSE

Figure 4.9. Graphs of alpha vs. PSNR and alpha vs. RMSE for kid image



(a) Alpha vs. PSNR

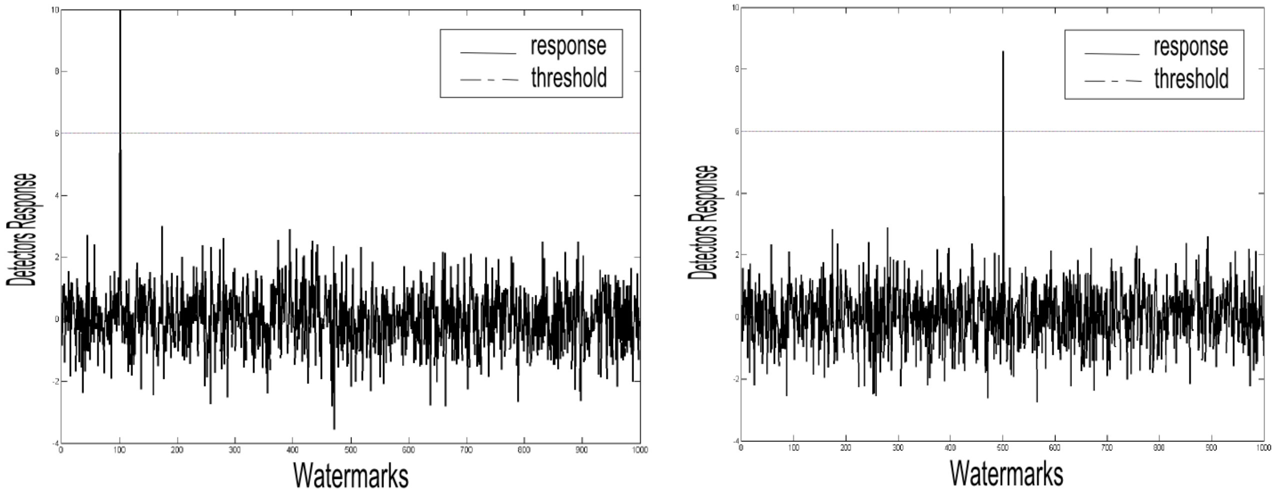
(b) Alpha vs. RMSE

Figure 4.10. Graphs of alpha vs. PSNR and alpha vs. RMSE for winter greens

Similarly in Figures 4.4, 4.5 4.6, 4.7, 4.8, 4.9, and 4.10, the graphs for alpha vs. PSNR and RMSE were observed for peppers, F-16, trees, board, bear, kid, winter greens images. A strong watermark was embedded in the peppers image.

4.3 Extraction Testing

In this section I provided the watermarked images and their corresponding detectors response for all the test images. The response of the detector of Lena image shown in figure 4.11(a) was obtained for random number sequences (watermarks) with 1,000 different seeds for evaluating the discrete wavelet transformation (DCT) domain. It can be observed that only the watermark with seed = 100 passed the threshold level, while in figure 4.11(b) the response for seed = 500 are shown.

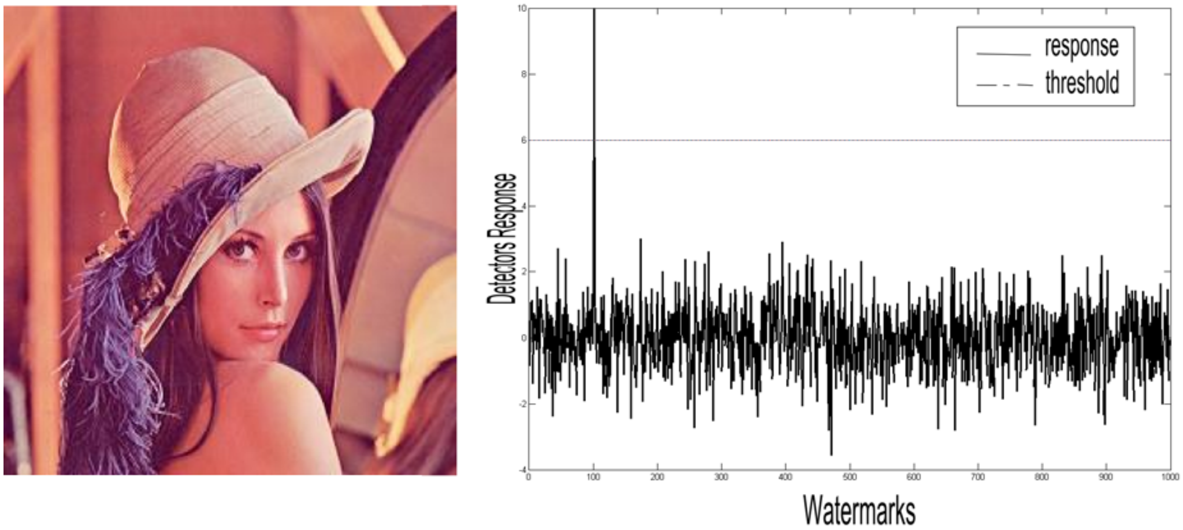


(a) Seed = 100

(b) Seed = 500

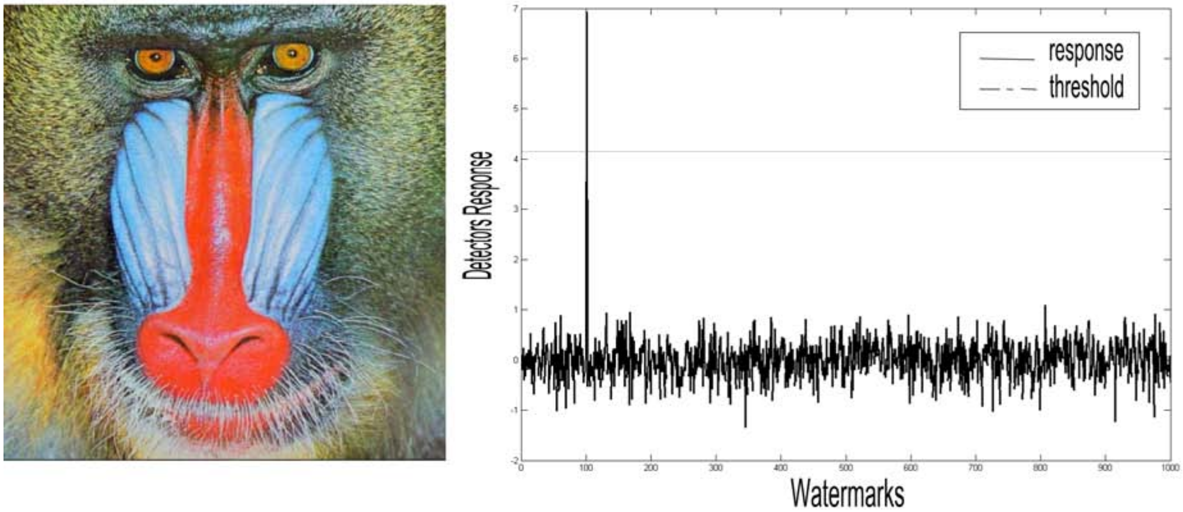
Figure 4.11. Detector response of Lena with (a) seed = 100 and (b) seed = 500

Figure 4.12 depicts the watermarked Lena image [256 x 256] with a scaling constant α = 0.35 and its PSNR value is 48.607 *dB*. The corresponding detector response to the 1,000 randomly generated watermarks is also shown: The response to the correct watermark was much larger than the other watermarks. This suggests that the proposed watermarking scheme was effective and also the probability of achieving very low false positive and false negative rates. Similarly, in Figure 4..13, the watermarked baboon image (512 x 512) can be seen with a scaling constant α = 0.4 and PSNR value of 50.915 *dB*. In figures 4.14, 4.15, 4.16, 4.17, 4.18, 4.19, and 4.20, an increase in the scaling constant from 0.4 to 0.65 and their corresponding detectors response can be observed.



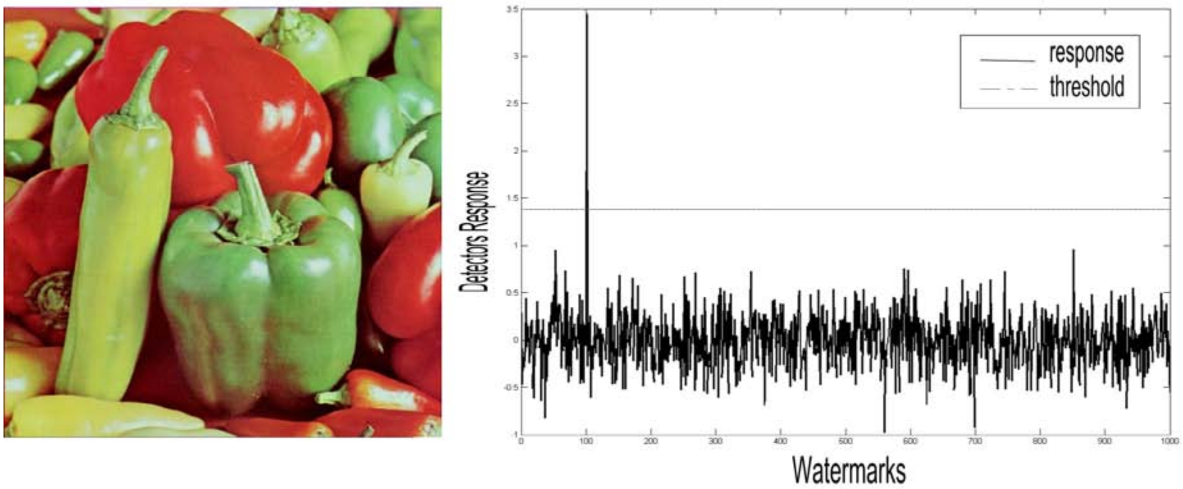
(a) Watermarked Lena image (b) Detectors response

Figure 4.12. The watermarked Lena image with α = 0.35 and corresponding detector response to 1,000 randomly generated watermarks



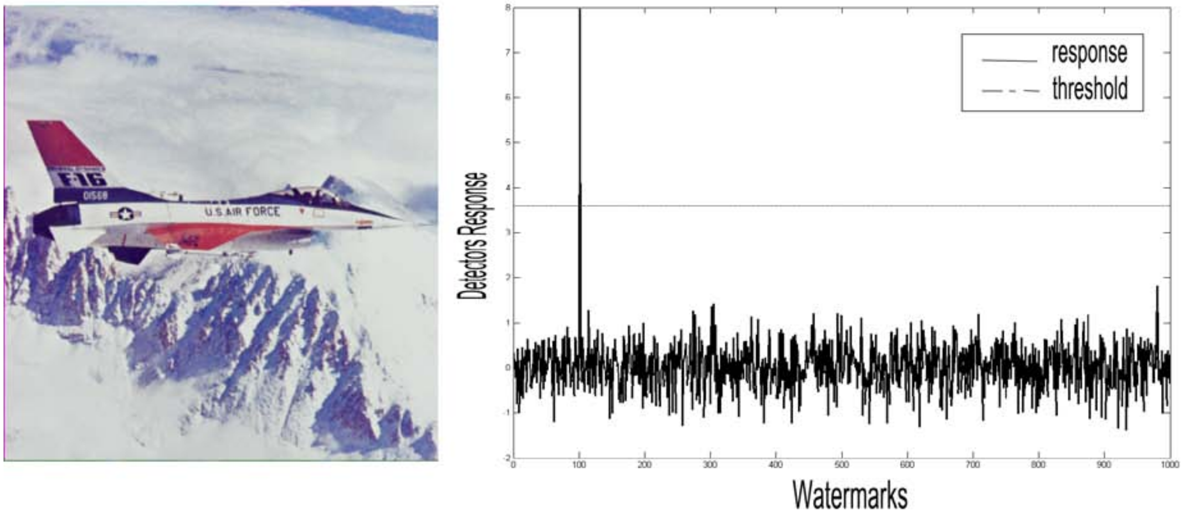
(a) Watermarked baboon image (b) Detectors response

Figure 4.13. The watermarked baboon image with α = 0.4 and the corresponding detector response to 1,000 randomly generated watermarks



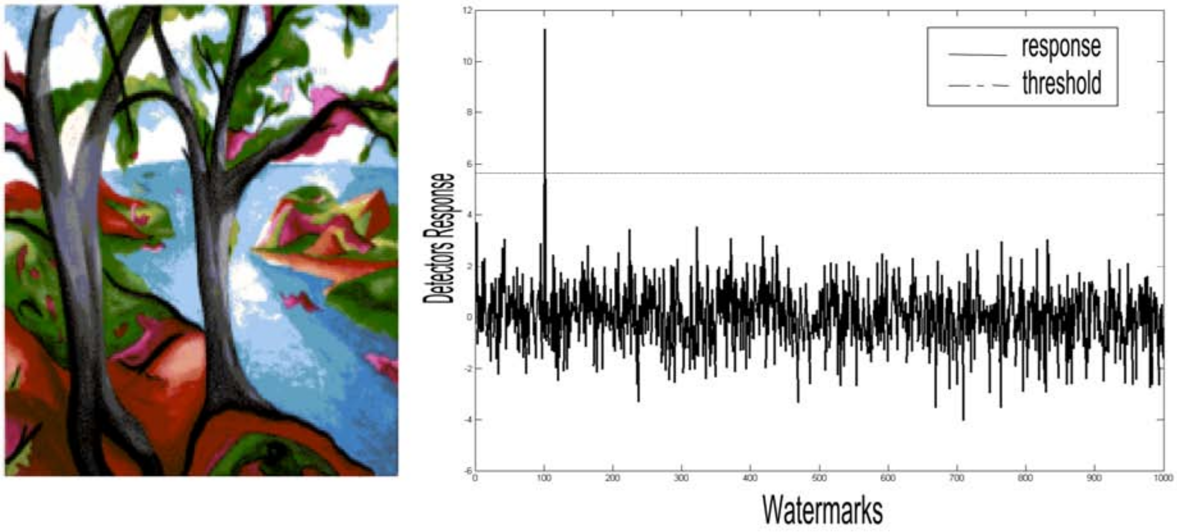
(a) Watermarked peppers image (b) Detectors response

Figure 4.14. The watermarked peppers image with α = 0.4 and the corresponding detector response to 1,000 randomly generated watermarks



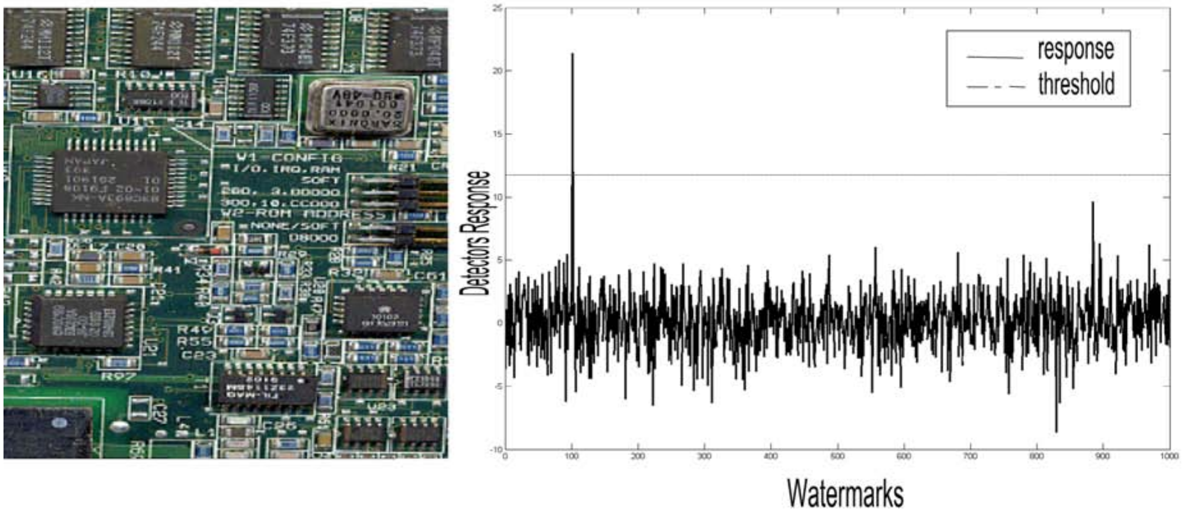
(a) Watermarked F-16 image (b) Detectors response

Figure 4.15. The watermarked F-16 image with α = 0.45 and the corresponding detector response to 1,000 randomly generated watermarks



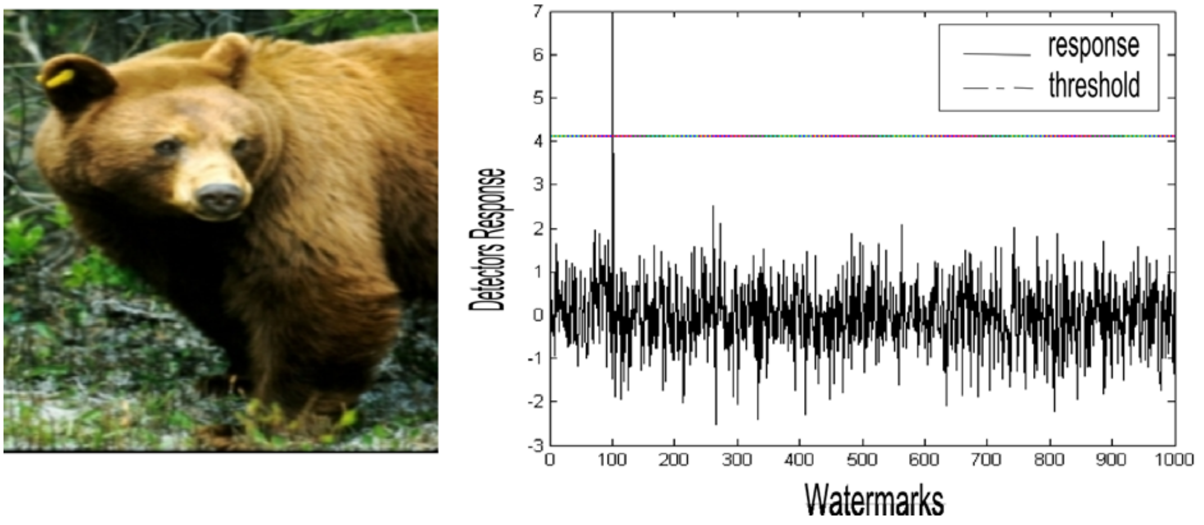
(a) Watermarked trees image (b) Detectors response

Figure 4.16. The watermarked trees image with α = 0.5 and the corresponding detector response to 1,000 randomly generated watermarks



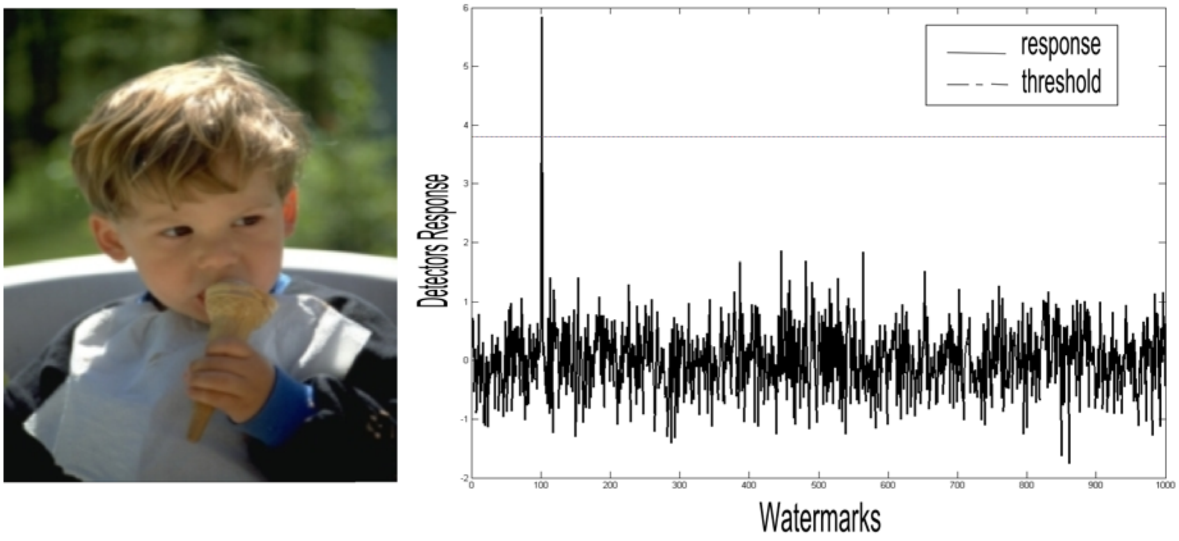
(a) Watermarked board image (b) Detectors response

Figure 4.17. The watermarked board image with α = 0.55 and the corresponding detector response to 1,000 randomly generated watermarks



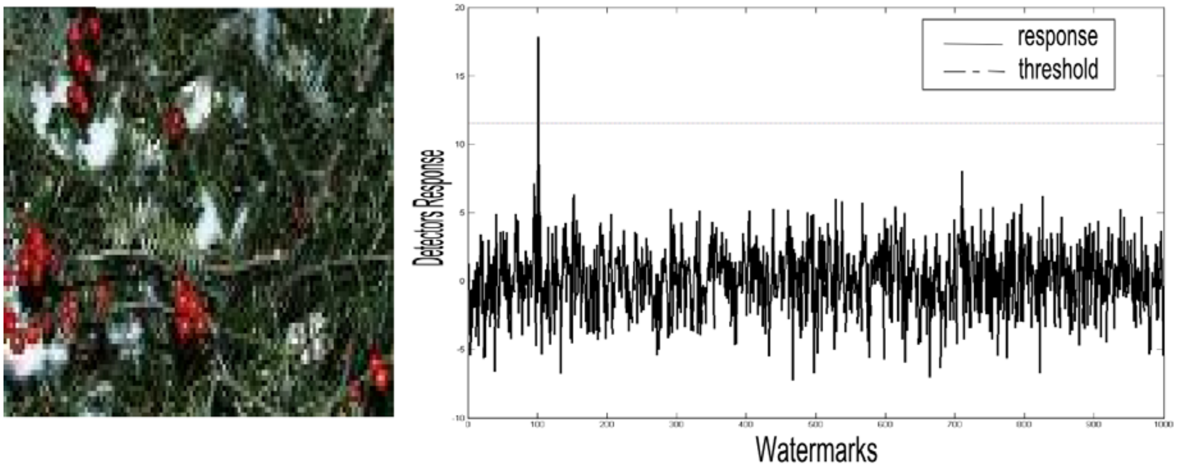
(a) Watermarked bear image (b) Detectors response

Figure 4.18. The watermarked bear image with α = 0.6 and the corresponding detector response to 1,000 randomly generated watermarks



(a) Watermarked kid image (b) Detectors response

Figure 4.19. The watermarked kid image with α = 0.65 and the corresponding detector response to 1,000 randomly generated watermarks



(a) Watermarked winter greens image (b) Detectors response

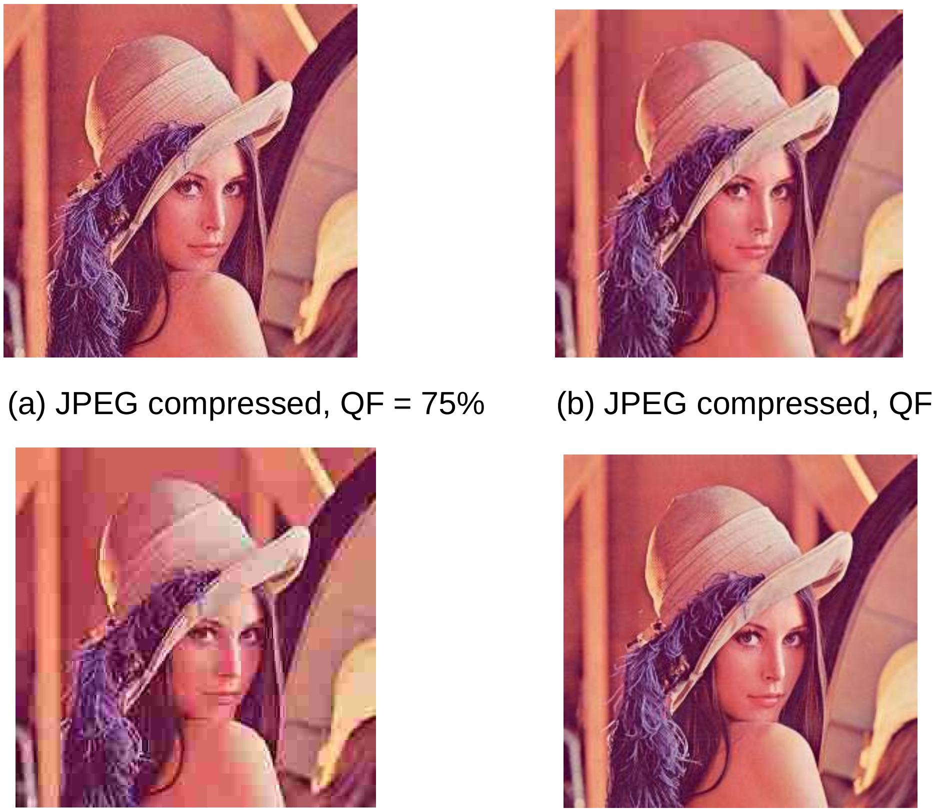
Figure 4.20. The watermarked winter greens image with α = 0.65 and the corresponding detector response to 1,000 randomly generated watermarks

4.4 Testing with Different Attacks

There was a need to analyze how attacks can modify the watermarked images and their corresponding detectors response. The primary purpose of the various attacks on the watermarked images is to know the survival, i.e., whether the watermark has survived or not. Survival of the watermark shows that it can be extracted as a replica of the original watermark. However, the extracted watermark was degraded due to channel noise while broadcasting and other intentional attacks. The watermarked image has been tampered with the built-in functions of ImageMagick® software suite for creating, editing, and composing bitmap images (ImageMagick Studio LLC, Landenberg, PA, www.imagemagick.org) [30]. The attacks I performed are as follows: joint photographic experts group (JPEG) compression, blurring, sharpen, spread and Pixelise.

4.4.1 Attack 1: JPEG Compression

Joint photographic experts group (JPEG) compression is a widely used algorithm in image compression. Any watermarking scheme will undergo some damaged compression. Figure 4.21 shows the extracted watermark images after the JPEG compression attack for the quality factors (QF) 75%, 50%, 25%, and 10%.



(a) JPEG compressed, QF = 75%

(b) JPEG compressed, QF = 50%

© JPEG compressed, QF = 25%

(d) JPEG compressed, QF = 10%

Figure 4.21. Watermarked image of Lena subjected to JPEG compression with quality factors (a) 75% (b) 50% (c) 25% (d) 10%

By observing the results in

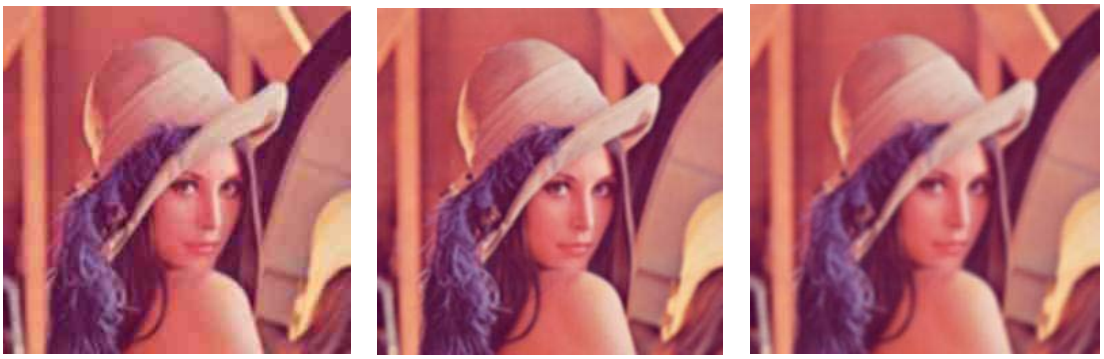
Table 4.3, it can be concluded that the robustness of the proposed algorithm was higher against JPEG compression. The watermark survived until the quality factor was larger than 8% for Lena image.

Table 4.3. Observation of JPEG compression with different quality factors (QF)

Tampering operation	Lena (256x256)
JPEG compression, QF 75%	Identical
JPEG compression, QF 50%	Identical
JPEG compression, QF 25%	Recognizable
JPEG compression, QF 10%	Survived

4.4.2 Attack 2: Blurring

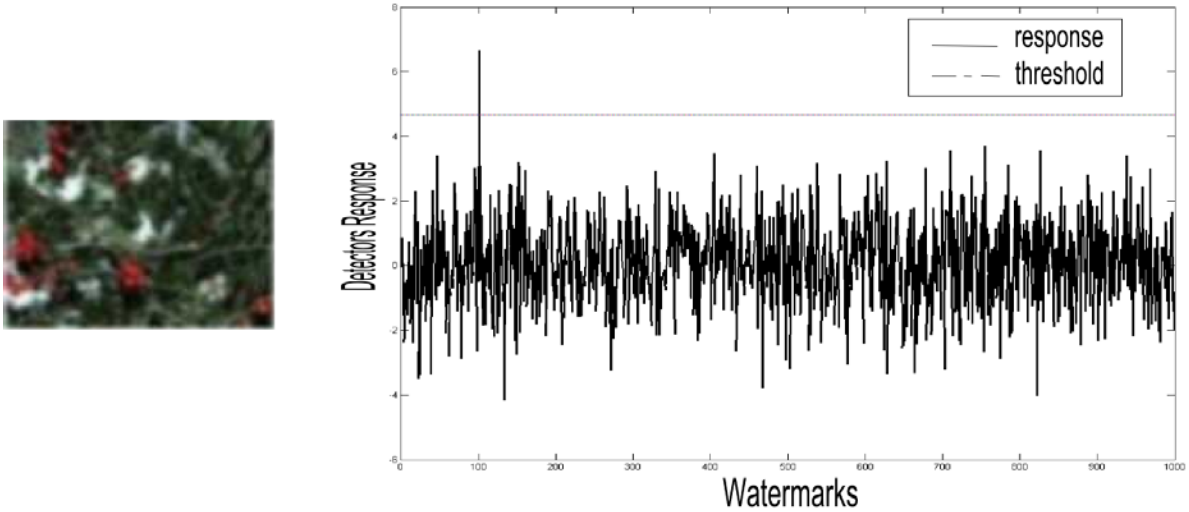
Figure 4.22 shows the watermarked images of Lena after blurring attack along with JPEG compression for 2 x 2 with QF of 25% and 75%, and 3 x 3 blur with QF of 75% from which the watermark can be extracted. I considered images of different sizes in this type of attack. These images were subjected to JPEG compression with different quality factors followed by blurring effect.



(a) 2x2 blur, QF 25% (b) 2x2 blur, QF 75% (c) 3x3 blur, QF 75%

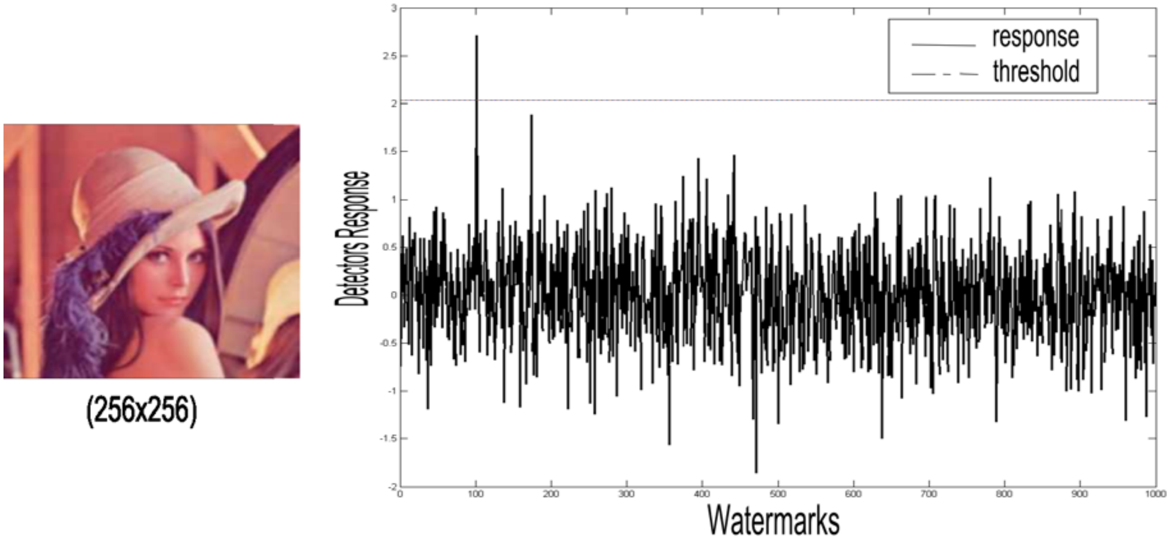
Figure 4.22 Watermarked images of Lena after blurring

Figure 4.23 shows the watermarked image of winter greens [128 x 128] after 2 x 2 blurring, compressed with a QF of 50 and its corresponding detectors response at seed = 100. The detectors response decreased by 39% after this effect.



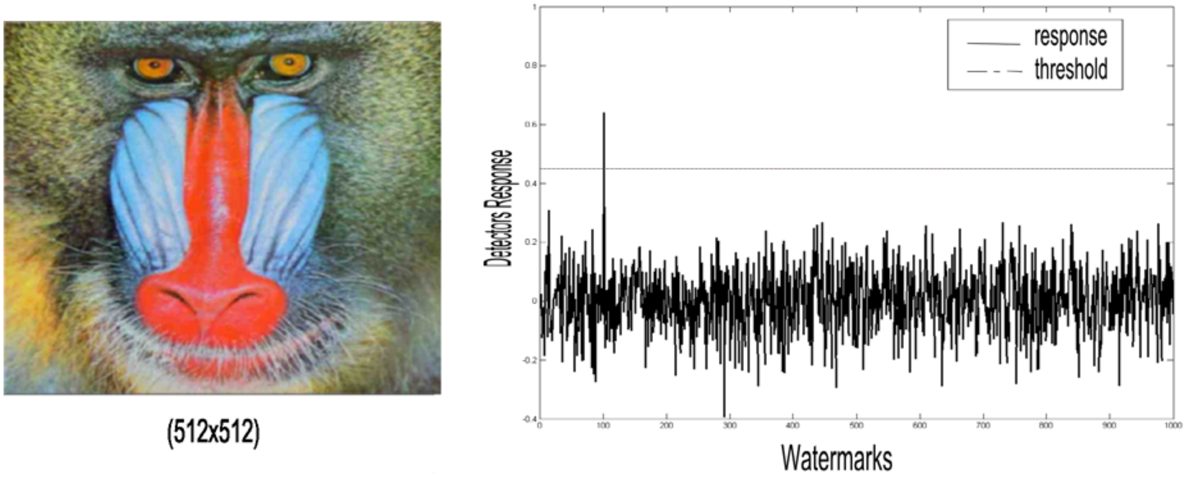
(a) Blurred winter greens image (b) Detectors response

Figure 4.23 The 2x2 blur, QF = 50 winter greens image and the corresponding detector response to 1000 randomly generated watermarks



(a) Blurred Lena image (b) Detectors response

Figure 4.24 The 2x2 blur, QF = 50 Lena image and the corresponding detector response to 1,000 randomly generated watermarks



(a) Blurred baboon image (b) Detectors response

Figure 4.25. The 3x3 blur, QF = 25 baboon image and the corresponding detector response to 1,000 randomly generated watermarks

Figure 4.24 shows the watermarked image of Lena image after 2 x 2 blurring, compressed with a quality factor of 50 and its corresponding detectors response at seed = 100. It was observed that the detectors response was decreased to 38%. Figure

4. shows the watermarked image of baboon image after 2 x 2 blurring, compressed with a quality factor of 50 and its corresponding detectors response at seed = 100, but with a decreased response to 10%.

Table 4.4 shows six different situations of blurring attack, JPEG compressed with different quality factors that were attacked on three images: winter greens, Lena and baboon.

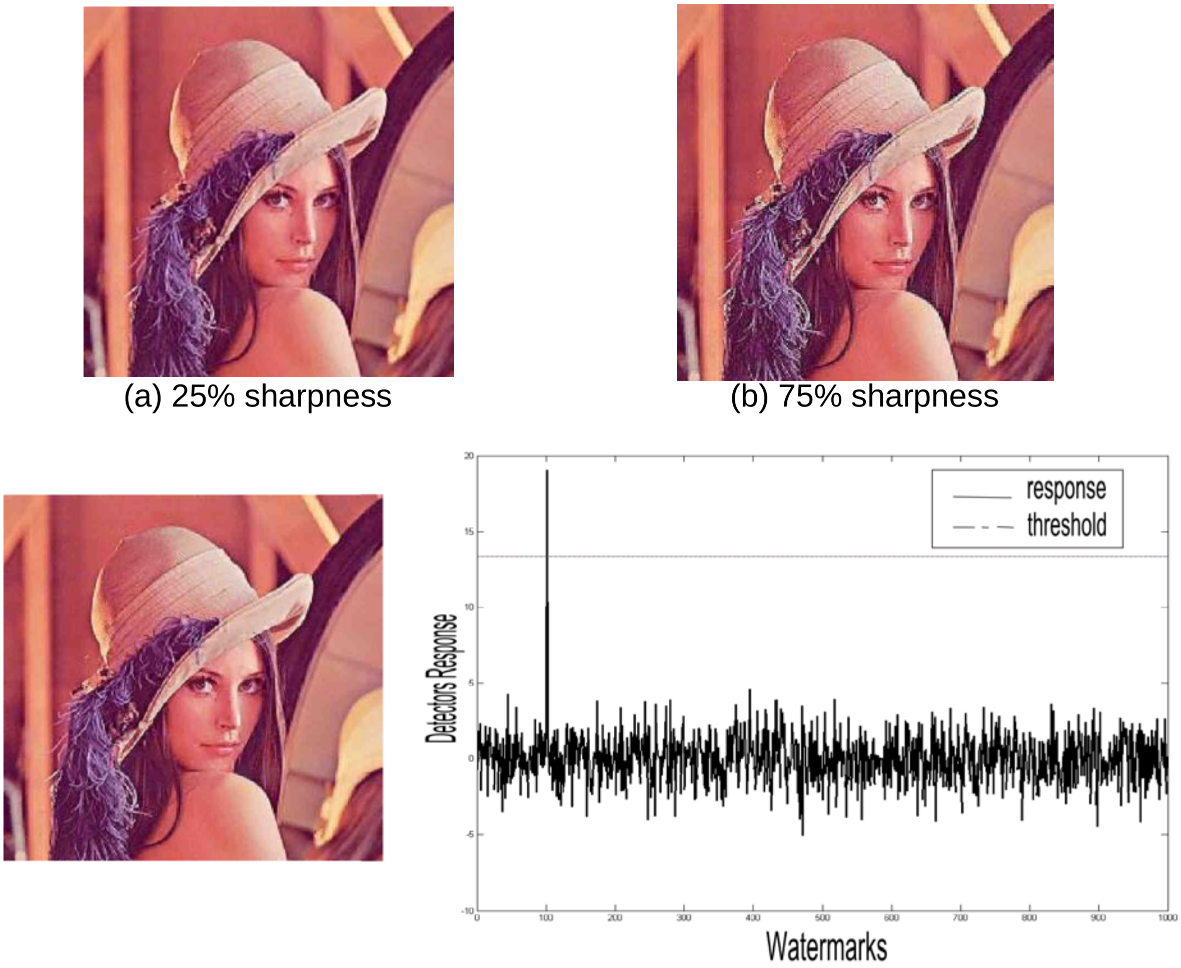
Table 4.4. Blurring attack on different images

Tampering Operations	Winter greens [128x128]	Lena [256x256]	Baboon [512x512]
2x2 blur, JPEG compression, QF 25%	Identical	Identical	Identical
2x2 blur, JPEG compression, QF 50%	Identical	Identical	Identical
2x2 blur, JPEG compression, QF 75%	Identical	Identical	Identical
3x3 blur, JPEG compression, QF 75%	Blurred	Survived	Identical
5x5 blur, JPEG compression, QF 90%	Unrecognizable	Unrecognizable	Unrecognizable
5x5 blur, JPEG compression, QF 50%	Too noisy	Heavily Blurred	Survived

For the winter greens image the watermark was sustained for 2 x 2 blur, JPEG compressed up to QF of 25 and it could not be recovered for 3 x 3 and 5 x 5 blur attacks. For the Lena image the watermark survived up to 3 x 3 blur, JPEG compressed with QF of 75 but could not withstand for 5 x 5 blur and beyond. There was a greater survival of baboon image for the 2 x 2 and 3 x 3 blur, JPEG compressed for various quality factors 75%, 50%, 25%. The watermark can be extracted up to the 5x5 blur till to a quality factor of 75.

4.4.3 Attack 3: Sharpening

The watermarked images after sharpening are shown in Figure 4. with 25% (a) and 75 % (b) sharpness in which the watermark still survived, (c) the watermarked image with 50% sharpness, JPEG compressed with quality factor of 25 and [d] its corresponding detectors response where the watermark is recognized can be observed.



(a) 25% sharpness

(b) 75% sharpness

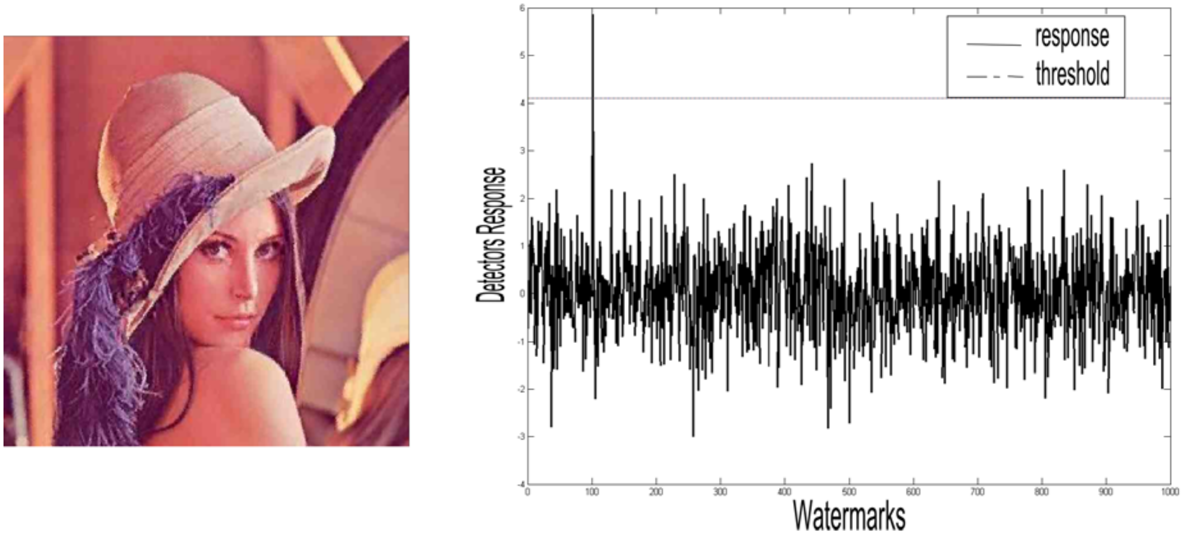
(c) 50% sharpness, QF=25

(d) corresponding detector response

Figure 4.26. Watermarked images Lena after sharpening

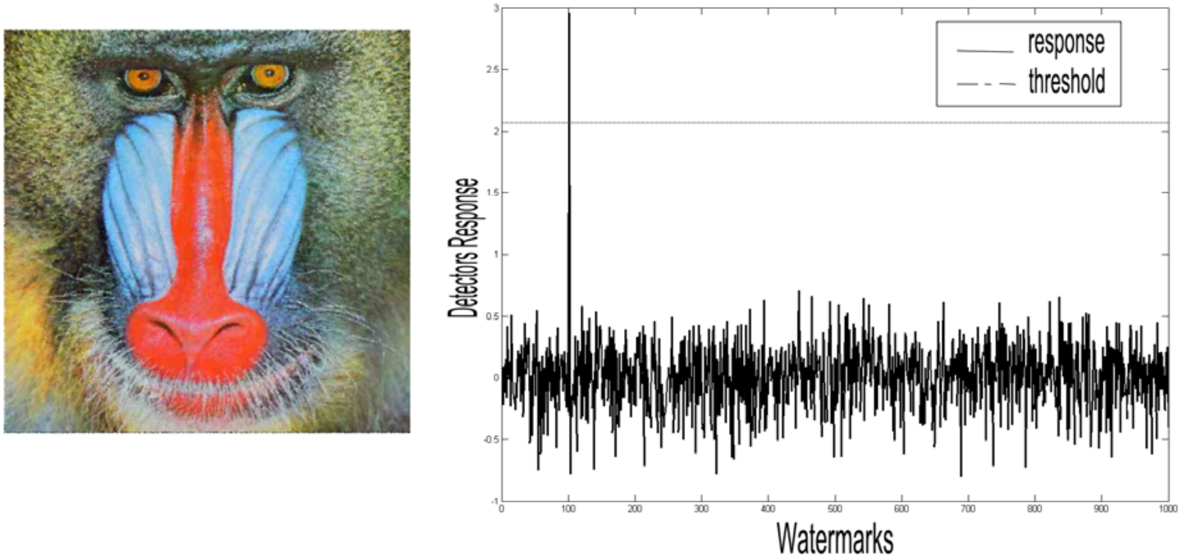
4.4.4 Attack 4: Spread

Another attack using the spread filter on the three images was implemented. Figure 4.27 shows the watermarked image of Lena image after 3 x 3 spread, compressed with a quality factor of 25 and its corresponding detectors response at seed = 100, with a decreased response by 32%. Figure 4.28 shows the watermarked image of baboon image after 5 x 5 spread, compressed with a quality factor of 25 and its corresponding detectors response at seed = 100 with a decreased response by 57%.



(a) 3x3 Spread, QF= 25 (b) Corresponding detector response

Figure 4.27 Watermarked image of Lena after spread and its response



(a) 5x5 spread, QF= 25 (b) Corresponding detector response

Figure 4.28. Watermarked image of baboon after spread and its response

As can be seen from Table 4.5, the winter greens watermarked image only survived a 5 x 5 spread filter, JPEG compressed with quality factor of 90%. The Lena image survived both for 3 x 3 and 5 x 5 spread with various quality factors while the baboon image survived to all the attacks up to a 7 x7 window showing its robustness.

Table 4.5. Tampering of test images with spread filter

Tampering operation	Winter Greens [128x128]	Lena [256x256]	Baboon [512x512]
3x3 spread, JPEG compression, QF 25%	Identical	Identical	Identical
5x5 spread, JPEG compression, QF 25%	Unrecognized	Survived	Recognized
5x5 spread, JPEG compression, QF 90%	Survived	Recognized	Identical
7x7 spread, JPEG compression, QF 25%	Too noisy	Too noisy	Survived

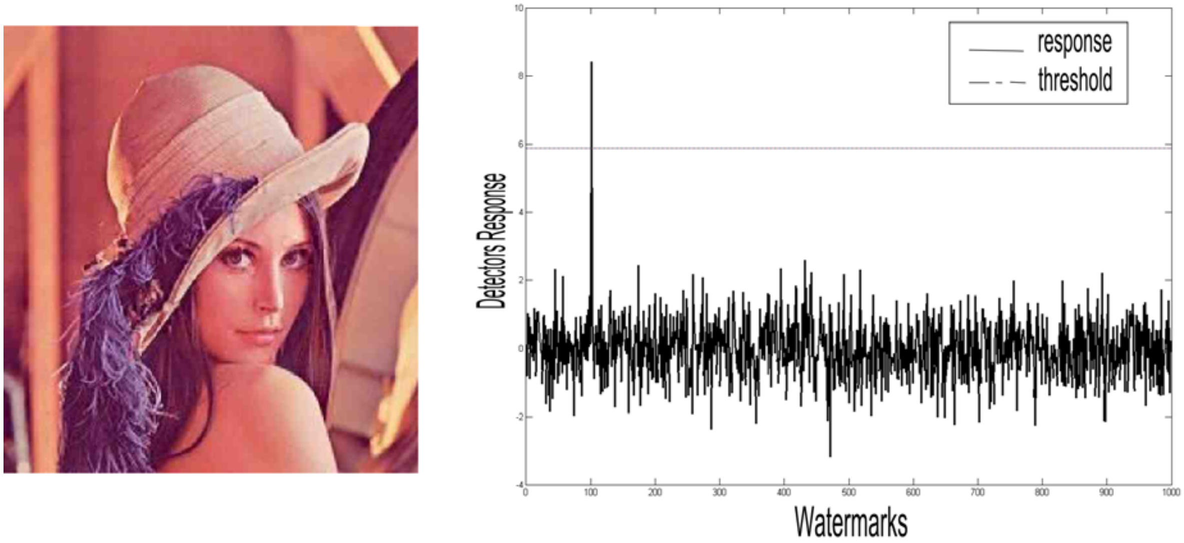
4.4.5 Attack 5: Pixelise

Table 4.6 shows the various pixel windows of sizes 2 x 2, 3 x 3, and 5 x 5 on different images. In this attack the winter greens survived for only 2 x 2 filter, Lena image survived until the 3 x 3 filter is implemented while the watermark was still recognized till 5 x 5 filter; for a baboon image till the quality factor is 25% after JPEG compression.

Table 4.6. Attacking with various pixel size

Tampering Operation	Winter greens (128x128)	Lena (256x256)	Baboon (512x512)
Pixel size 2x2, JPEG compression, QF 25%	Identical	Identical	Identical
Pixel size 3x3, JPEG compression, QF 75%	Unrecognized	Survived	Identical
Pixel size 5x5, JPEG compression, QF 25%	Too noisy	Unrecognized	Recognized

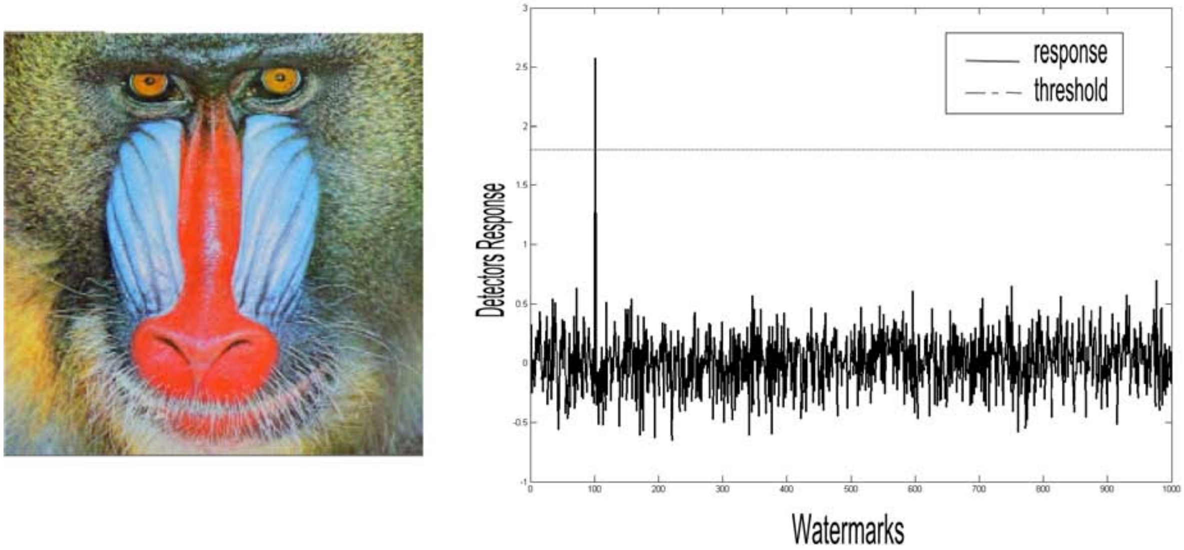
Figure 4.29 (a) shows watermarked image of Lena after pixel size 2 x 2, compressed with a quality factor of 25 and its corresponding detectors response (figure 4.29 (b)) at seed = 100 with a decreased response by 20%.



(a) Pixel size 2x2, QF = 25 (b) Detector response

Figure 4.29. Watermarked image of Lena after Pixelise and its response

Figure 4.4.30 (a) shows the watermarked image of baboon image after pixel size 3 x 3, compressed with a quality factor of 25 and its corresponding detectors response (Figure 4(b)) at seed = 100 with a decreased response by 64%.



(a) Pixel size 3x3, QF = 75 (b) Detector response

Figure 4.30 Baboon watermarked image after Pixelise and its response

From the results I concluded that the proposed watermarking algorithm is robust to the attacks and also maintained good visual quality for the watermarked images.

CHAPTER 5

CONCLUSIONS AND FUTURE RESEARCH

An effective invisible watermarking technique for copyright protection is being proposed. I inserted the watermark in color images in the Y component. Watermark inserted in the midband frequencies were more resistant to the attacks. The blind extraction of the invisible watermark was helpful for authentication.

By visually analyzing the Lena image I concluded that for the obtained peak signal-to-noise ratio (PSNR) values the watermark is invisible and the same is valid for all the other images. Comparing various watermarking schemes and the proposed algorithm, the PSNR values under no attack 47.75 *dB*, were much higher than the PSNRs obtained by image adaptive watermarking [14] (40.054 *dB*), image adaptive watermark creation [26] , [11] (35.17 *dB*, 45 *dB*), zerotree of wavelet [9] (44.18 *dB*) and 9/7 biorthogonal wavelet lifting [12] (36.44 *dB*).

An exhaustive test with nine images on the proposed algorithm proved the quality and also the recognizability of extracted watermark, showing that it can survive various kinds of attacks like joint photographic experts group (JPEG) compression, blurring, median filtering, sharpening. The effectiveness of the proposed algorithm increased with the size of images. This is an advantage as the big-sized images are always valuable images.

The algorithm can be extended toward its power-efficient versions. This can be extended to its real-time version. Very large scale integration (VLSI) architectures and chips using the invisible robust blind watermarking technique can be implemented.

Other possible extensions include:

- Insertion of multiple watermarks in the host image.
- Use wavelet transforms for insertion of strong watermarks.
- Other types of multimedia like video.

BIBLIOGRAPHY

1. S. P. Mohanty, “Digital Watermarking: A Tutorial Review.” Report, Dept. of Electrical Engineering, Indian Institute of Science, Bangalore, India, 1999.

2. G.C. Langelaar, I. Setyawan, & R.L. Lagendijk. “Watermarking digital image and video data. A state-of-the-art overview.” *Signal Processing Magazine IEEE*, 17:5 [September 2000]: 20-46.

3. S. P. Mohanty, N. Pati, & E. Kougianos. "A Watermarking Co-Processor for New Generation Graphics Processing Units." *Proceedings of the 25th IEEE International Conference on Consumer Electronics* [2007]: 303-04.

4. S. P. Mohanty, R. Sheth, A. Pinto, & M. Chandy. "CryptMark: A Novel Secure Invisible Watermarking Technique for Color Images." *Proceedings of the 11th IEEE International Symposium on Consumer Electronics* [2007]: 1-6.

5. Peter H. W. Wong, Oscar C. Au, & Y. M. Yeung. “A Novel Blind Multiple Watermarking Technique for Images.” *IEEE Transactions on Circuits and Systems for Video Technology*, 13:8 [September 2003]: 813-30.

6. M.L. Miller, G.J. Doerr, & I.J. Cox.”Applying informed coding and embedding to design a robust high-capacity watermark.” *IEEE Transactions on Image Processing,* 13:6 [June 2004]: 792-807.

7. Xiao-Yun Liu, Gao Kun, & Wu-Fan Chen. “A Blind Watermarking Optimal Detection Based on the Wavelet Transform Domain.” *IEEE International Conference on Machine Learning and Cybernetics* [2007]: 1779-83.

8. Zhang Guannan, Wang Shuxun, & Wen Quan. “An adaptive block-based blind watermarking algorithm.” *7th International Conference on Proceedings of Signal Processing* [2004]: 2294- 97.

9. Zhang Erhu & Zhao Fan. “Adaptive Image Blind Watermarking Method Based on Zerotree Wavelet.” *8th International Conference on Electronic Measurement and Instruments* [2007]: 2-799 to 2-802.

10. Pengfei Yu. "Blind Watermarking Scheme Based on the Sign of Wavelet Coefficients." 8th *International Conference on Signal Processing* [2006]: 16-20.

11. B.C Choi & D. I. Seo. “A statistical approach for optimal watermark coefficients extraction in HVS-based blind-watermarking system.” *The 7th International Conference on Advanced Communication Technology* [2005]: 1085-88.

12. Zhang Hong-cai, Liu Zhi-bo, & Fan Jiu-lun. “A blind watermarking algorithm based on wavelet lifting transform.” *The 7th International Conference on Signal Processing* [2004]: 843-47.

13. Jui-Cheng Yen, Hun-chen Chen, & Jui-hsiang Juan. “Blind Watermarking Based on the Wavelet Transform.” *The 7th International Conference on Parallel and Distributed Computing, Applications and Technologies* [*2006*]: 474-78.

14. Xiao-hua Qiao, Shu-xun Wang, Quan Wen, & Zhao Xu. “A Robust Watermarking Algorithm Adopting Double Embedding.” *Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing* [2006]: 63-66.

15. A. Khalfallah, F. Kammoun, M.S. Bouhlel, & C. Olivier. “A new scheme of watermarking in multi-resolution filed by 5/3 wavelet: Family signature combined with the adapted embedding strength.” *2nd Information and Communication Technologies* [2006]: 1145-52.

16. Liu Yongliang, Xiaolin Yang, Hongxun Yao, Tiejun Huang, & Wen Gao. “Watermark detection schemes with high security.” *International Conference on Information Technology: Coding and Computing* [2005]: 113-17.

17. R. Safabakhsh, S. Zaboli, & A. Tabibiazar. “Digital watermarking on still images using wavelet transform.” *International Conference on Information Technology Coding and Computing* [2004]: 671-75.

18. Emir Ganic & Ahmet M. Eskicioglu. “Robust DWT-SVD domain image watermarking: embedding data in all frequencies.” *Proceedings of the 2004 Workshop on Multimedia and Security* [2004]: 166-74.

19. Angela Piper, Reihaneh Safavi-Naini, & Alfred Mertins. “Resolution and quality scalable spread spectrum image watermarking.” *Proceedings of the 7th Workshop on Multimedia and Security* [2005]: 79-90.

20. Nataša Terzija & Walter Geisselhardt. “Digital image watermarking using complex wavelet transform.” *Proceedings of the 2004 Workshop on Multimedia and Security* [2004]: 193-98.

21. S. Zaboli & M.S. Moin. “CEW: A Non-Blind Adaptive Image Watermarking Approach Based on Entropy in Contourlet Domain.” *IEEE International Symposium on Industrial Electronics* [2007]: 1687-92.

22. Guillaume Lavoué, Florence Denis, & Florent Dupont. “Subdivision surface watermarking.” *Computers & Graphics,* 31:3 [June 2007]: 480-92.

23. Gererdo Pineda Betancourth, Ayman Haggag, Mohamed Ghoneim, Takashi Yahagi & Jianming Lu. “Robust watermarking in the DCT domain using dual detection.” *IEEE International Symposium on Industrial Electronics* [2006]: 579-84.

24. O. B. Adamo, S. P. Mohanty, E. Kougianos, M. Varanasi, & W. Cai. "VLSI Architecture and FPGA Prototyping of a Digital Camera for Image Security and Authentication." *Proceedings of the IEEE Region 5 Technology and Science Conference* [2006]: 154-58.

25. S. P. Mohanty, N. Ranganathan, & K. Balakrishnan. "A Dual Voltage-Frequency VLSI Chip for Image Watermarking in DCT Domain." *IEEE Transactions on Circuits and Systems II [TCAS-II]*, 53:5 [May 2006]: 394-98.

26. S. P. Mohanty, P. Guturu, E. Kougianos, & N. Pati. "A Novel Invisible Color Image Watermarking Scheme using Image Adaptive Watermark Creation and Robust Insertion-Extraction." *Proceedings of the IEEE International Symposium on Multimedia* [2006]: 153-60.

27. A. Piva, M. Barni, F. Bartolini, V. Cappellini. “DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image.” *Proceedings of the IEEE International Conference on Image Processing [*1997]: 520-23.

28. Borivoje Furht & Darko Kirovski. *Multimedia Security Handbook*. CRC Press, 2005.

29. MATLAB®, The MathWorks, Inc., Natick, MA, http://www.mathworks.com

30. ImageMagick®, ImageMagick Studio LLC, Landenberg, PA, http://www.imagemagick.org