DIGITAL WATERMARKING FOR IMAGES

AILEEN KOAY YEE HOON

Universiti Sains Malaysia

2006

ABSTRAK

Kecanggihan Internet membolehkan penyebaran maklumat secara sewenang-wenangnya. Kemudahan penghasilan semula dan penyebaran dokumen berdigit merupakan suatu masalah kepada pemilik dokumen yang ingin menghalang berlakunya penggunaan dokumen oleh orang lain secara haram dan tanpa pengetahuan pemilik. Bagi mengatasi masalah tersebut, teknik tera air bagi melindungi hak milik telah diperkenalkan. Dalam disertasi ini, suatu sistem tera air bagi imej berwarna untuk tujuan melindungi hak milik telah dicadangkan. Tera air yang dapat dicam, logo berwarna dan disembunyikan di dalam imej berwarna. Transformasi *wavelet* yang digunakan oleh imej berwarna dalam projek ini ialah *Stationary Wavelet Transform (SWT)* peringkat pertama dan peringkat kedua. Bagi memperoleh saluran model warna RGB yang bersesuaian bagi sistem tera air, tiga saluran model warna RGB yang berlainan telah diuji dengan menggunakan imej berwarna dan tera air yang berlainan. Keputusan eksperimen menunjukkan teknik yang dicadangkan adalah kebal terhadap *Gaussian filtering, Gaussian noise, salt and pepper noise, speckle noise* dan *JPEG compression.*

ABSTRACT

The success of the Internet allows for the prevalent distribution of multimedia data easily. Meanwhile, the ease of reproduction and distribution of digital documents create problems for authorized parties that wish to prevent illegal use of such documents. To solve this problem, a digital watermarking method for copyright protection is introduced. In this dissertation, a color image watermarking system for copyright protection is proposed. A visually recognizable watermark is used and embedded in the wavelet decomposition of the color host image. The wavelet decomposition of host image used in this project is Stationary Wavelet Transform (SWT) level 1 and level 2. In order to identify the suitable channel of RGB color model for watermarking, three different channels of RGB color model are tested by using different host images and watermarks. The experimental results show that the proposed watermarking scheme is robust to Gaussian filtering, Gaussian noise, salt and pepper noise, speckle noise and JPEG compression.

ACKNOWLEDGEMENT

First and foremost, I would like to express my sincere gratitude to my supervisor, Dr. Khoo Bee Ee for her guidance and valuable suggestions towards the success of this project. She also has provided me with necessary intellectual and material support for this project.

I am also thankful to Master Research student, Mr. Lim Say Yarn, for his effort to guide me learning MATLAB and Image Processing Toolbox and his willingness to share his experience with me and helped me a lot in this completion of my final year project.

Besides, I also would like to acknowledge the support and friendship I received from Mr Chia Chun Kwang, Miss Yap Shu Shin and Mr Saw Si Xing.

Finally, I wish to thank my parents for all the support, love and understanding they have given me throughout the years.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Table **Page**

CHAPTER 1

INTRODUCTION

1.1 Motivation

The rapid expansion of the Internet in the past years has quickly increased the availability of digital data such as audios, images and videos to the public. As we have witnessed in the past few months, the problem of protecting multimedia information becomes more and more significant and a lot of copyright owners are concerned about protecting any illegal duplication of their data or work. Some serious work needs to be done in order to maintain the availability of multimedia information but, in the meantime, the industry must come up with ways to protect intellectual property of creators, distributors or simple owners of such data. This is an interesting challenge and this is probably why so much attention has been drawn toward the development of digital images protection schemes. There are number of technologies to provide protection from illegal copying. A favourable method of copyright protection is digital watermarking.

1.2 Objectives and Scopes of Dissertation

In this dissertation, a methodology for embedding a color watermark into a color image is proposed. The main objective of this project is to find the most suitable level of wavelet transform for the proposed watermarking scheme. The suitable channel of RGB color model of color image to embed color watermark is also need to be investigated. Four color images (512 x 512) and four color logo (32 x 32) were selected as host images and watermarks respectively in this project.

1.3 Dissertation Outline

This dissertation is organized into 7 chapters as follows. Chapter 2 presents a basic knowledge on digital watermarking, the requirements, classifications, attacks, applications of digital watermarking. Besides, two types of wavelet transforms, RGB color model and performance measurements are also included. The relationships among wavelet coefficients is investigated in Chapter 3. In Chapter 4, we determine the quantization parameter value and employ the theory described in Chapter 2 and Chapter 3 and propose blind wavelet-based watermarking method. Our proposed watermarking scheme is divided into two sections – embedding process and extraction process. Chapter 5 provides the graphical user interface (GUI) of watermarking system. Experimental results and discussions are reported in Chapter 6. In Chapter 7, we present conclusions and intended future research directions of the results obtained so far.

CHAPTER 2

LITERATURE REVIEW

2.1 Basic on Digital Watermarking

Digital watermarking is a technique to hide or embed information data (watermark) into a digital data. Generally, a watermark can be a piece of meaningful information, a random signal or a logo. The watermark can be extracted for copyright protection and must be difficult for an attacker to remove the watermark purposely.

A watermark can be embedded in the spatial domain or the frequency domain [Vallabha, 2007].In the spatial domain, the watermark is embedded by modifying the color values of selected pixel values directly. In the frequency domain, the pixel values are transformed to frequency coefficients and the watermark is then embedded by modifying the coefficients. Some examples of transformations are Discrete Cosine Transform (DCT) ,Discrete Fourier Transform (DFT) ,Stationary Wavelet Transform (SWT).Generally, the robustness of the watermark embedded in the spatial domain is often weaker than that in the frequency domain.[Hsieh et al., 2001]

2.2 Digital Watermarking Requirements

Generally, a good watermark at least should comply with the following requirements [Hsieh et al.,2001] :

1) Readability

A watermark should convey as much information as possible. A watermark should be statistically undetectable. Moreover, retrieval of the digital watermark can be used to identify the ownership and copyright unambiguously.

2) Security

A watermark should be secret and must be undetectable by an unauthorized user in general. A watermark should only be accessible by authorized parties. This requirement is regarded as a security and the watermark is usually achieved by the use of cryptographic keys. As information security techniques, the details of a digital watermark algorithm must be published to everyone. The owner of the intellectual property image is the only one who holds the private secret keys.

3) Imperceptibility

One of the main requirements for watermarking is the perceptual transparency. The digital watermark should not be noticeable to the viewer. The data embedding process should not introduce any perceptible artefacts into the original image and not degrade the perceived quality of the image.

4) Robustness

The digital watermark is still present in the image after attacks and can be detected by the watermark detector, especially on the attacks from compression. Possible attacks include linear or nonlinear filtering, image enhancements, requantization, resizing, and image compression.

2.3 Digital Watermarking Schemes

There are three types of watermarking schemes that can be classified by the watermark detection or extraction schemes [Kusyk and Eskicioglu, 2007]:

a) Non-blind scheme

- Also called non-public or non-oblivious watermarking system.
- Both the original image and the secret key(s) are needed.

b) Semi-blind scheme

- Also called semi-private or semi-oblivious watermarking system.
- The secret key(s) and the watermark are needed.

c) Blind scheme

- Also called public or oblivious watermarking system.
- Only the secret keys are needed.

2.4 Attacks

A watermark should resist with a variety of attacks. It is meaningless if the watermark embedded in the media is not robust to malicious attacks. Once the watermark in the media is destroyed, the media is considered as unprotected and easily manipulated by other users. There are many kinds of attacks can be listed as following [Hartung et al.,1999]:

a) Simple attacks (Noise attacks / Waveform attacks)

The aim of a simple attack is to impair the embedded watermark by manipulating watermarked image without an attempt to identify or remove the watermark. Examples include linear and general non-linear filtering,waveform-based compression (JPEG,MPEG),addition of noise, cropping.

b) Detection-disabling attacks (Synchronization attacks)

These types of attacks are attempt to break the correlation and make the recovery of watermark impossible for a watermark detector, mostly by geometric distortions such as cropping, rotation, pixel permutation or any other geometric transformation of data.

c) Ambiguity attacks (Confusion attacks / Deadlock attacks / Inversion attacks / Fake-watermark attacks / Fake-original attacks)

The goal of ambiguity attacks are to make confusing by producing fake original data or fake watermarked data. An example is the inversion attack by Craver et al. [16-18] (sometimes referred to as 'IBM attack') that tries to discredit the authority of the watermark by embedding one or several additional watermarks to confuse which is the first, authoritative of the data owner.

d) Removal attacks

These kind of attacks are attempt to analyze the watermarked data, estimate the watermark or the host data, separate the watermarked data into host data and watermark, and discard only watermark. For example, in a collusion attack, even if attackers have no special knowledge of a specific algorithm, they can estimate the watermark or the original if they have different watermarked works with same watermark. Again, an approximation of the original can be determined if the attacker has the same watermarked work with different watermarks. These attackers can construct a new copy without watermark from the original watermarked work after they made estimation or approximation.

2.5 Digital Watermarking Applications

Digital watermarking has a broad array of applications as following:

1) Copyright protection

Copyright protection is the most prominent application of watermarking today. The copyright owner protects his or her intellectual property from being manipulated by a user in an illegal way in effort to remove or destroy the watermark or replace it with his or her own one.

2) Fingerprinting

In order to trace the source of illegal copies, the owner embed different watermarking keys in the copies that are supplied to different customer. Owner embedding a unique serial number-like watermark is a good way to detect customers who break their license agreement by copying the protected data and supplying it to a third party.

3) Authentication

In image authentication, the watermark conveys some kind of summary of the content and if any part of the content is modified, its summary will change and making it possible to detect that some kinds of tampering has taken place. It is also possible to locate the exact location of the tamper and recover the tamper area using watermark. The watermark used in the content authentication is called fragile watermark because it is designed to become invalid if even slight modifications of digital content taken place.

4) Copy and Playback Control

It is possible for digital recording and playback device to react to embed signal. The watermarked information can directly control the behaviour of the digital recording device. In copy control scenario, the recording device might inhibit certain recording process if it detects a watermark represents a copy-permission bit stream that controls the recording process. In the playback control scenario, the watermark will act as display permission, a secure module can be added into playback equipment to automatically extract this permission information and the playback device will react according to the permission.

5) Secure communications

The watermarked media (main channel) conveys side-channel information to the end user. There are three types of side-channel information: public, private and hidden. A public side-channel watermark contains information about the content in which it is embedded, meant to be accessed by any legal buyer or user of the product. A private side-channel watermark contains information that is intended only for specific authorized users. A hidden side-channel watermark is the only important information and the cover media is just the carrier.

6) Broadcast and Internet Monitoring

Digital watermarks allow data owners and distributors to track traditional broadcast and Internet dissemination of their data. Multimedia data is embedded with a unique identifier – distributor and/or date and time information. Detectors are placed where broadcasts can be received and processed. The digital watermarking is decoded and used to reference a database, resulting in reports to the owner or distributor that the data has been played in the given market, at a given time, and whether it played to full-length.

2.6 Wavelet Transform

In the latest few years wavelet transform has been widely studied in signal processing and image compression [Potdar, 2007]. Two types of wavelet transforms are discussed below :

2.6.1 Discrete Wavelet Transform (DWT)

The Discrete Wavelet Transform (DWT) is identical to a hierarchical subband system, where the subbands are logarithmically spaced in frequency [Hsieh et al., 2001]. The critically sampled DWT is widely used in signal compression.

In the DWT, a fundamental computational step is down-sampling. In one-dimensional DWT, the input discrete sequence X is convolved with high-pass and low-pass analysis filters, and each result is downsampled by two, yielding the transformed signals L1 and H1 [Watson et al.,1997]. The approximation is the low-frequency component; the detail is the high-frequency component. For a two-dimensional image, a two-dimensional wavelet transform is required. The two-dimensional wavelet transform can be computed using one-dimensional decomposition algorithm. Wavelet transform is first performed in one dimension (horizontally) and then the other dimension (vertically).

One level DWT decomposition of an image results into 4 subbands identified as LL1, HL1, LH1, HH1 by downsampling horizontal and vertical channels using filters [Potdar, 2007]. The LL1 band is termed as approximate subband while the others such as HL1, LH1, HH1 are termed as detailed subbands. The transformation is done using wavelet filters. Some common examples of wavelet filters are Haar Wavelet Filter, Daubechies Orthogonal Filters (e.g. D-4, D-6, D-8, D-10 and D-12), Daubechies Bi-Orthogonal and so forth.

The wavelet reconstruction process consists of upsampling by two and filtering. Those subbands can be assembled back into the original image with no loss of information using Inverse Discrete Transform (IDWT).

Figure 2.1 shows the one-dimensional DWT that decomposes X into one level and Figure 2.2 depicts the two-dimensional DWT that decomposes X into one level.

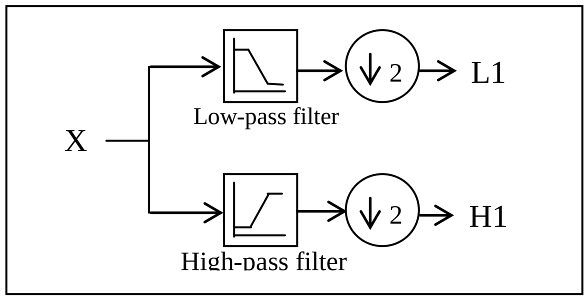


Figure 2.1: One-dimensional DWT (1-level)

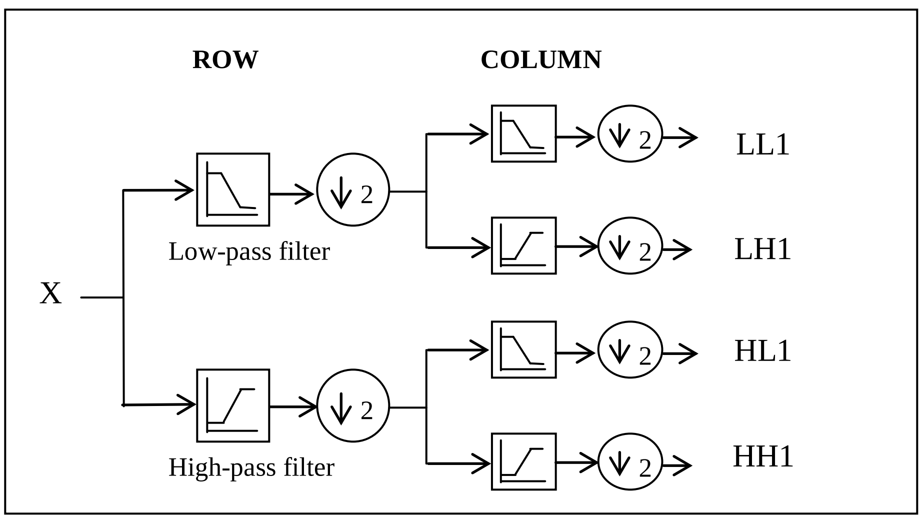


Figure 2.2: Two-dimensional DWT (1-level)

Figure 2.3 shows a single level 2-D DWT decomposition of an image. The approximate subband can be further be decomposed by another level (n-levels) of DWT. Figure 2.4 shows a second level 2-D DWT decomposition of an image. Here, the approximate band is considered as a new image and the DWT decomposition is applied on LL_1.

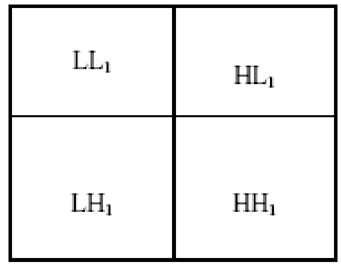


Figure 2.3 : Single level DWT Decomposition

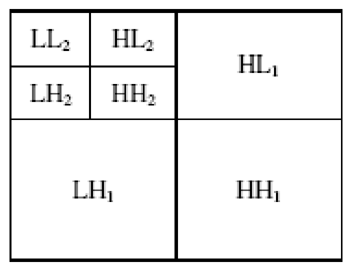


Figure 2.4 : Two level DWT Decomposition

2.6.2 Stationary Wavelet Transform

The usual DWT technique will down sample the coefficients to half when the level of resolution increased [Lim, 2006]. By removing the downsampling operation, the decomposition obtained is then redundant and is called Stationary Wavelet Transform (SWT) or the *a trous* algorithm. The shift variance of the DWT arises from its use of downsampling, while the SWT is shift invariant since the spatial sampling rate is fixed across scale [Fowler,2004]. Therefore, the size of each subband in a SWT is same as the size of input signal.

Figure 2.5 shows the one-dimensional SWT that decomposes X into one level. Figure 2.6 illustrates the two-dimensional SWT that decomposes X into one level and Figure 2.7 illustrates the two-level, two-dimensional SWT of an image.

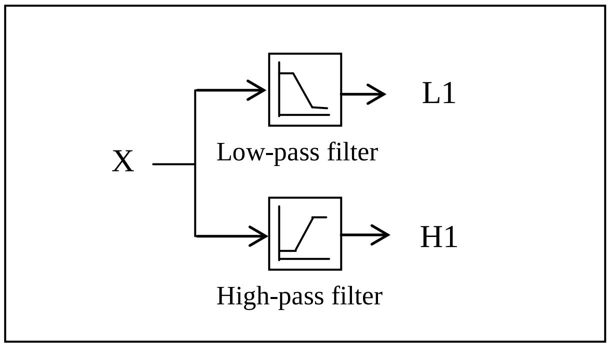


Figure 2.5: One-dimensional SWT (1-level)

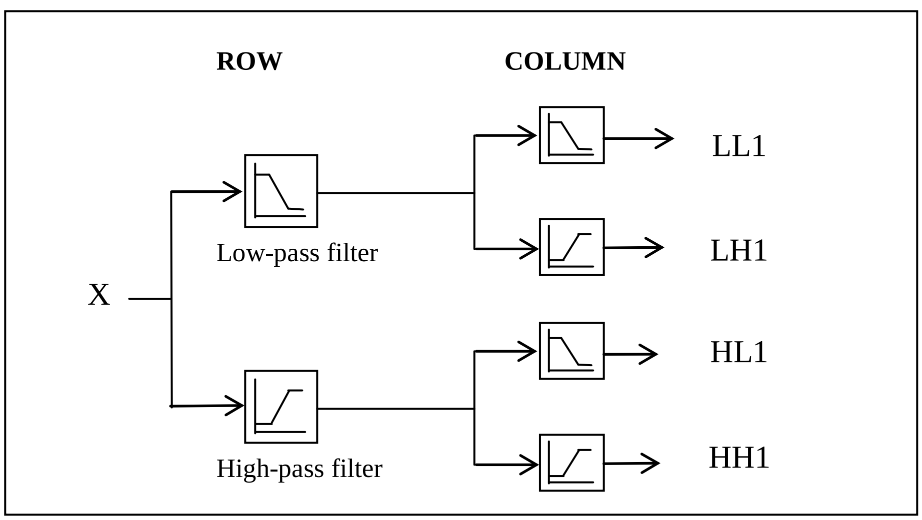


Figure 2.6 : Two-dimensional SWT (1-level)

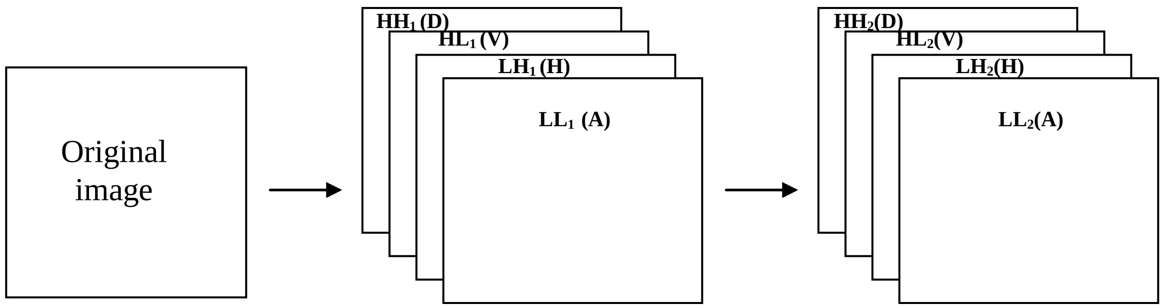


Figure 2.7 : Two-dimensional SWT (2-level)

2.7 Color Representation

2.7.1 Color Model

The purpose of a color model (also called color space or color system) is to facilitate the specification of colors in some standard, generally accepted way. In essence, a color model is a specification of coordinate system and subspace within that system where each color is represented by a single point.

RGB Color Model

The primary colors are Red, Green, Blue. It is an additive model, in which colors are produced by adding components. When red, green, blue are all mixed together, an entire spectrum of colors make up a color space of colors that can represented by a cube. The RGB color space cube is shown as below. There are three axes, each representing one of the primary colors of red, green, or blue.

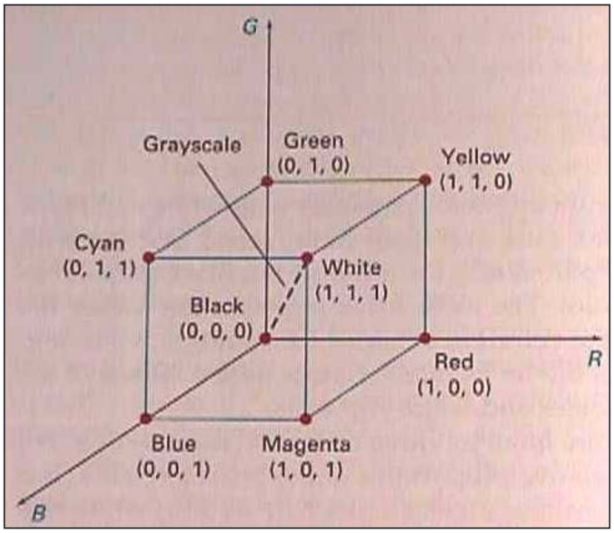


Figure 2.8 : RGB Color Cube

2.8 Performance Measurements

2.8.1 Peak Signal-to-Noise Ratio (PSNR)

PSNR is the most commonly used method for measuring the quality of the watermarked image compare with an original image. PSNR is measured in decibels(dB) and is defined as below:

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \quad dB \tag{2.1}$$

$$MSE = \frac{1}{3xmxn}\sum_{k=1}^{3}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(A_{ijk} - B_{ijk}\right)^2 \tag{2.2}$$

where A_{ij1} = original image pixel value (Red channel)

A_{ij2} = original image pixel value (Green channel)

A_{ij3} = original image pixel value (Blue channel)

B_{ij1} = distorted image pixel value (Red channel)

B_{ij2} = distorted image pixel value (Green channel)

B_{ij3} = distorted image pixel value (Blue channel)

where Mean Square Error(MSE) = mean-square error between a watermarked (or an attacked watermarked) image and its original image.

The lower the MSE is, the lower the error between two images, which means the more similar are the two images.

2.8.2 Correlation

The similarity measurement between the original watermark *A* and the extracted watermark *B* of size mxn is defined as below :

$$correlation = \frac{\sum_m \sum_n (A_{mn} - \tilde{A})(B_{mn} - \tilde{B})}{\sqrt{\left[\sum_m \sum_n (A_{mn} - \tilde{A})^2\right]\left[\sum_m \sum_n (B_{mn} - \tilde{B})^2\right]}} \qquad (2.3)$$

where A_{mn} = original watermark value

$\tilde{A}$ = original watermark average value

B_{mn} = extracted watermark value

$\tilde{B}$ = extracted watermark average value

Usually, the correlation value is between -1.0 and +1.0, where -1.0 and +1.0 represent the highest correlation. Usually if correlation is larger than a predefined threshold

T, the owner can declare the copyright. The higher the value of the correlation is, the higher the legibility is.

For a color watermark, the average correlation can be used to measure the similarity. The average correlation is shown as below :

$$average\ correlation = \frac{correlationR + correlationG + correlationB}{3} \qquad (2.4)$$

where correlationR = correlation of Red channel

correlationG = correlation of Green channel

correlationB = correlation of Blue channel

CHAPTER 3
RELATIONSHIPS AMONG WAVELET COEFFICIENTS

In this chapter, the Discrete Wavelet Transform (DWT) coefficients and the Stationary Wavelet Transform (SWT) coefficients of color images are investigated and compared. The purpose of this investigation is to find out the relationship between DWT coefficients and SWT coefficients.

A color image, Lena is selected as host image and is decomposed by using SWT and DWT to get the SWT coefficients and DWT coefficients respectively. The R channel of color images is selected to decompose using one level and second level of DWT and SWT to get approximation, horizontal, vertical , and diagonal bands (A, H, V, and D bands). The wavelet basis that we used is Haar basis.

3.1.1 Comparison between DWT Coefficents and SWT Coefficients

Table 3.1 : Selected DWT coefficients and SWT coefficients at level 1 from host image (Lena)

Subband	DWT Level 1						SWT Level 1					
Approximation	188	197	200	197	213	212	188	191	197	200	200	197
	180	200	196	190	208	206	183	188	198	201	197	192
	178	193	193	191	200	199	180	188	200	204	196	188
	181	183	195	192	201	194	181	188	195	196	196	191
	170	184	189	188	198	188	178	186	193	191	193	193
	164	189	191	185	192	182	177	186	192	193	195	193
Horizontal	-2	3	3	2.5	-1.5	2	-2	0	3	3.5	3	2
	-4	2	0	0.5	2.5	0	7	3	-4	-5	0.5	3.5
	0	-1.5	3	-2	3	-0.5	-4	-3	2	2	0	0.5
	-5	7.5	4	0	0	3.5	3	3	3.5	6.5	0	-3.5
	2	-1.5	0	1.5	2.5	1.5	0	-0.5	-1.5	-1.5	3	1
	0	0	0	0	0	0	1	0.5	2	-0.5	-4.5	-0.5
Vertical	0	-3	-1	-3.5	3.5	-7	0	-3	-3	0.5	-1	4
	0	-4	8	-2.5	-2.5	0	0	-5	-5	2	2.5	2.5
	0	0.5	-4	-2	-2	-1.5	0	-8	-4	0	8	0.5
	0	0.5	-0	-4	2	-3.5	0	-7	0.5	-1.5	1	4.5
	0	-0.5	1	3.5	4.5	-0.5	0	-7.5	0.5	1.5	-4	4
	0	3	3	-1	4	-4	0	-8.5	2	-2.5	0.5	1.5
Diagonal	0	-1	0	-1.5	-0.5	-3	0	-2	-1	0.5	0	1
	0	-4	-2	-1.5	0.5	0	0	4	3	-2	-3.5	0.5
	0	0.5	-4	-3	1	-2.5	0	-1	-4	4	-2	1.5
	0	3.5	1	0	5	0.5	0	-0	-0.5	-2.5	9	-5.5
	0	0.5	-4	-2.5	1.5	5.5	0	0.5	0.5	-0.5	-4	6
	0	0	0	0	0	0	0	0.5	-2	4.5	-0.5	-3.5

Table 3.2: Selected DWT coefficients and SWT coefficients at level 2 from host image (Lena)

Subband	DWT Level 2						SWT Level 2					
Approximation	898	907	905	893	886	891	898	898	898	903	907	908
	900	909	905	898	894	895	898	898	898	903	907	908
	895	904	903	903	902	901	899	899	899	903	908	908
	907	906	901	904	904	903	901	900	901	904	909	910
	902	901	906	908	908	903	900	900	901	903	909	909
	901	904	908	909	908	900	900	900	901	903	908	908
Horizontal	0	0	0	0	0	0	0	0	0	0	0	0
	0.75	-0.25	0.5	-2.5	-2.5	-2	0	0	0	0	0	0
	0.5	-1.25	-0.5	-0.8	-2	-1	-1.3	-1	-1.3	0.25	-0.75	-0.3
	-0.3	-1	1.5	0.25	-2.25	0.25	-3	-2	-2.5	-0.8	-2	-1.8
	1.5	-0.25	0.5	-3.7	0	2	0.75	0.25	-0.2	-0.2	-0.25	-0.5
	-1.2	0.25	1.5	-1.8	2.5	-0.5	4.25	2.25	2.5	2	3.25	3.5
Vertical	6	-3	-1	5	-2	1	6	0	-6	-5	-3	0
	4.25	-2.75	0	2	0.5	-2.5	6	0	-6	-5	-3	0
	0.5	1.25	-1	-4.2	6.5	-3	5.75	1.5	-5.7	-5.2	-2.75	-0.3
	4.25	0	-4	0.25	3.25	1.75	6	2.5	-5.5	-6.2	-3	0.25
	4.5	-1.75	-2	-0.3	1	1	4.25	2.75	-5.2	-5.7	-2.75	-0.5
	3.25	-1.25	-6.5	-1.7	3	0	3.25	2.75	-4	-5.5	-3.25	-0
Diagonal	0	0	0	0	0	0	0	0	0	0	0	0
	1.25	0.25	0	-0.5	-1	0.5	0	0	0	0	0	0
	0.5	-3.25	1	-1.7	-1	0	0.25	-1.5	-0.3	0.25	-0.25	0.25
	-0.8	1.5	3	0.75	1.25	-0.7	0	-2.5	-0.5	1.25	-0	-0.3
	0.5	1.25	-1.5	-0.8	-2.5	-4	1.25	0.25	-0.3	0.25	0.25	0
	-0.8	0.25	-3	-2.2	0.5	-2.5	2.75	2.25	-1	-2	0.25	0.5

3.2 Discussions

3.2.1 Discussions of Comparison between DWT Coefficents and SWT Coefficients

From the Table 3.1, we discover that the first, second and third DWT coefficients in the first row are identical with the first, third and fifth SWT coefficients in the same row respectively at level 1. For second and third rows, first, second and third DWT coefficients are same with first, third and fifth SWT coefficients in the third and fifth row respectively. The distance between each DWT coefficient in SWT coefficients is 1.

At level 2, we realize that the first and second DWT coefficients in first row from Table 3.2 are equivalent to the first and fifth SWT coefficients in the same row individually. For second row, first and second DWT coefficients are equal to the first and fifth SWT coefficients in the fifth row respectively. Each DWT coefficient in SWT coefficients has a distance at 3.

In conclusion, the distance between each DWT coefficient in SWT coefficients is given a formula :

$$\textit{Distance each DWT coefficient in SWT coefficients} = 2^N - 1 \quad (3.1)$$

where N = level of SWT

CHAPTER 4
THE PROPOSED APPROACH

The purpose of this chapter is to describe our proposed blind wavelet-based watermarking technique. The watermark used is a visually identifiable color logo. Before the watermark is embedded in the wavelet coefficient of host image, the permutation process is applied on it to prevent tampering or unauthorized access. Besides, the secret keys also used in permutation to increase security.

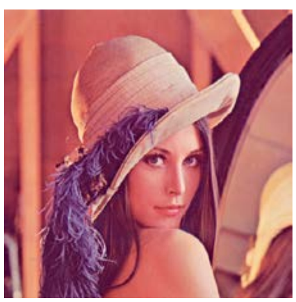
In the proposed watermarking scheme, the host image that we used is a color image. The two-dimensional wavelet transform is applied to the selected channel of the host image. The Haar wavelet basis is selected due to its simple and fast. It is memory efficient because it does not require a temporary array to store intermediate result and reversible withhout an edge effect which is an issue with other wavelet transforsm [Potdar et al., 2007]. In addition, for our proposed watermarking method, the watermark is embeded in the horizontal (HL) band and diagonal (HH) band as they are more robust to attack.

For more effective and practical watermarking methods the watermark detection process should be blind, meaning that the host image (unwatermarked image) is not needed for detecting the presence of watermarks. That is, the copyright owners require no extra disk space to preserve the host image.

4.1 Analysis

Before embedding and extraction process are performed**,** a watermark is embedded into the different location of SWT and DWT coefficients of color image, various value of quantization parameter, Q at different level of SWT and DWT. SWT coefficients of color images before and after attacks are being tested to discover which location of SWT coefficients is suitable to embed watermark, which value of quantization parameter, Q is appropriate to be used at different level of SWT and DWT and which subband is more robust against a variety of attacks such as filtering, compression, noise addition and rotation respectively. This is important for us to design a more robust digital watermarking system.

The color images that we used in our experiments are shown in Figure 4.1 below.



(a) Lena

(b) Baboon

(c) Peppers

(e) Water Lilies

Figure 4.1 Original color images of size 512x512

4.1.1 Comparison on Embedding Watermark in Different Combination of Subbands of Color Image for SWT and DWT (Level 1 ,Level 2)

Table 4.1 : Correlation value of watermark that is embedded in different combination of subbands for SWT level 1 (using Lena as host image, without attack)

Quantization Parameter,Q	**Correlation**		
	Horizontal Band + Vertical Band	**HorizontalBand + Diagonal Band**	**Vertical Band + Diagonal Band**
0	invalid	invalid	invalid
5	0.8589	0.8559	0.8629
10	0.9214	0.9226	0.9221
20	0.9985	0.9986	0.9995
30	0.9952	0.9986	0.9977
40	0.9990	0.9990	0.9998
50	0.9989	0.9990	0.9990
100	1	1	1
185	1	1	1

Table 4.2 : PSNR of watermarked image in different combination of subbands for SWT level 1 (using Lena as host image, without attack)

Quantization Parameter,Q	**Peak Signal-to-Noise Ratio (PSNR)**		
	Horizontal Band + Vertical Band	**Horizontal Band + Diagonal Band**	**Vertical Band + Diagonal Band**
0	+11.27 dB	+11.27 dB	+11.27 dB
5	+59.28 dB	+59.24 dB	+59.33 dB
10	+54.31 dB	+54.33 dB	+54.24 dB
20	+48.65 dB	+48.72 dB	+48.67 dB
30	+45.33 dB	+45.39 dB	+45.37 dB
40	+42.97 dB	+43.02 dB	+42.98 dB
50	+41.12 dB	+41.16 dB	+41.11 dB
100	+35.20 dB	+35.21 dB	+35.20 dB
185	+29.94 dB	+29.94 dB	+29.94 dB