A Robust Framework for Watermarking System

By

Adham Mohsin Saeed Alshamary

Supervised By
Prof. Nidal Shilbayeh

Master Thesis

Submitted in Fulfillment of the Requirements
for the Degree of Master of Science in
Computer Information System

Middle East University
Faculty of Information Technology

April 2010

Middle East University
Authorization statement

I, Adham Mohsin Saeed Alshamary, authorize Middle East University for Graduate Studies to supply copies of my thesis to Libraries, establishments or individuals on request, according to the university regulations.

Name: Adham Mohsin saeed Alshamary

Signature:

Date: 14-4-2010

قرار لجنة المناقشة

نوقشت هذه الرسالة وعنوانها: **A Robust Framework for Watermarking System**

أعضاء لجنة المناقشة

التوقيع

1- الأستاذ الدكتور : نضال فوزي شلباية مشرفا وعضوا

2- الدكتور : محمد عصام ملكاوي رئيسا وعضوا

3- الأستاذ الدكتور : رياض فرحان الشلبي عضوا خارجيا

DEDICATIONS

This thesis is dedicated to:

My Parents, who taught me the love of knowledge

My Sister and Brother

Adham M. Alshamary

ACKNOWLEDGEMENTS

In the name of Allah the most Gracious and the most merciful, I would like to thank all of the people who assisted and supported me to complete this thesis.

First, I'm very grateful to my advisor, Prof. Nidal Shilbayeh for his availability, patience, suggesting comments and great ideas about this thesis.

Finally, many thanks to all faculty members for their encouragement and help.

ABSTRACT

This study aims at proposing a system to solve problems of modification, forgery, illegal manipulation and distribution of digital image. Digital watermarking has been proposed as one of the possible ways to deal with the problem of forging and manipulation of digital media, to keep information safe. The main idea of the proposed system in this thesis "A Robust Framework for Watermarking System" is to overcome the problems of attack that happens during transmitting the image via communication links. Therefore, there is a vital need to construct a framework for image watermarking against all types of attacks, i.e., illegal manipulation and distribution of digital image via Internet. The proposed system represents a new method (HWT-DWT) constructed by cascading two different but complementary techniques for image protection by using watermarking techniques which is one of the powerful and robust schemes in protection process. Wavelet transformation (HWT-DWT) provides robust resistance of the protected image against modification and forgery attacks. The main significance of the proposed system is to solve problems of modification, forgery attacks, illegal manipulation and distribution of digital image. The study findings prove the efficiency of the proposed system since it suggests a new method to protect the image for the purposes of ownerships, copyright and intellectual property. This is done through using the PSNR to compare the results of attacks of the watermarked image with those of the original image through several examples conducted in this study.

الخلاصة

لقد هدفت هذه الدراسة لاقتراح نظام "Digital Watermarking" كأحد الطرائق الممكنة للتعامل مع مشكلة قرصنة الوسائل الرقمية والتلاعب بها بأسلوب غير قانوني من أجل المحافظة على سلامة هذه البيانات والمعلومات.

إن الفكرة الرئيسية للنظام المقترح في هذه الرسالة " A Robust Framework for Watermarking System" هي التغلب على مشاكل القرصنة التي تحدث خلال إرسال الصورة عبر روابط الاتصال. وبناء عليه، توجد حاجة ماسة لبناء إطار لـ Image Watermarking ضد أنواع القرصنة جميعها: التلاعب غير القانوني ونشر الصورة الرقمية عبر شبكة الانترنت ويمثل النظام المقترح أسلوباً جديداً تم إنشاؤه بواسطة مكاملة أسلوبين مختلفين ولكن متكاملة لحماية الصورة باستخدام Watermarking وهذان الأسلوبان لهما فعالية عالية في عملية الحماية. ويوفر نظام Wavelet مقاومة قوية للصورة المحمية ضد القرصنة. والأهمية الأساسية للنظام المقترح هو الحماية من مشاكل القرصنة والنشر والتلاعب غير القانوني للصورة الرقمية. وقد أثبتت نتائج هذه الدراسة فاعلية هذا النظام المقترح حيث يقترح أسلوب جديد لحماية الصورة الرقمية لغايات حفظ الملكية وحق النسخ والملكية الفكرية رغم وجود العديد من الأنظمة الأخرى لحماية الصورة الرقمية من خلال استخدام نظام PSNR لمقارنة نتائج الهجمات على الصورة الأصلية مع صورة العلامة المائية وتوضيح ذلك من خلال عدة أمثلة أجريت في هذه الدراسة.

Contents

Chapter 1		**Introduction**	
	1.1	Introduction	2
	1.2	Statement of the problem	4
	1.3	Objective of study	4
	1.4	Thesis Significance	5
	1.5	Thesis organization	5
Chapter 2		**Literature Survey**	
	2.1	Watermarking Overview	7
	2.1.1	Watermarking Applications	7
	2.1.2	Properties of Watermarking System	7
	2.1.3	Watermarking Techniques	8
	2.1.3.1	Spatial Domain Watermarking	8
	2.1.3.2	Frequency domain watermarking	9
	2.1.3.2.1	Discrete Fourier Transform (DFT)	10
	2.1.3.2.2	The Discrete Cosine Transform (DCT)	10
	2.1.3.2.3	The Wavelet Transform Based Techniques (WT)	11
	2.1.4	Digital watermarking system	11
	2.1.5	Attacks on Digital Watermarks	12
	2.2	Related works	13
Chapter 3		**A cascade Haar-DWT Based digital Watermarking system**	
	3.1	Introduction	18
	3.2	Haar Wavelet Transform Subsystems	20
	3.3	Discrete Wavelet Transform Subsystems	30
	3.3.1	Hide (embedding) part	31
	3.3.2	Extract (recover) part	33
Chapter 4		**Experimental Results and Discussion**	
	4.1	Experimental Results	37
	4.2	Robustness Test Result	42
	4.3	Discussions	47
Chapter 5		**Conclusions and Future Work**	
	5.1	Conclusions	53
	5.2	Future Works	54
References			56

LIST OF TABLES

3.1	Decomposition to lower resolution	22
4.1	Comparing PSNR of Al-Haj's with Proposed Method	51

LIST OF Figures

3.1	General Structure of the proposed system	19
3.2	HWT subsystem	20
3.3	Structure of 2D Haar wavelet proposed systems	25
3.4	Structure of wavelet decomposition	25
3.5	A 8x8 image	26
3.6	2D arrays to representing	26
3.7	Transformed array after operation	28
3.8	Final Transformed Matrix after one step	28
3.9	Embedding of a watermarking in the wavelet domain	29
3.10	DWT subsystem	30
3.11	Subblock of size 3*3	31
3.12	Extraction Scheme Using ICA	34
4.1	Wavelet Transform subsystems	37
4.2	original image	37
4.3	Line Transform	38
4.4	Column Transform	38
4.5	2Layer WT	39
4.6	3Layer WT	39
4.7	4Layer WT	39
4.8	First watermarking processes	40
4.9	Final result of Hide part	41
4.10	the extracted watermarked image	41
4.11	Image Attack structure	42
4.12	Invert Attack	43
4.13	Crop Attack	43
4.14	Rotate Attack	44
4.15	Scale Attack	44
4.16	Extact orgiginal image from attack image scale	45
4.17	Extact orgiginal image from attack image invert	45
4.18	Extact orgiginal image from attack image rotate	46
4.19	Extact orgiginal image from attack image crop	46
4.20	HWT image without attack	49
4.21	HWT image after Invert and Noise attack	49
4.22	HWT-DWT image without attack	49
4.23	HWT-DWT images after Invert and Noise attack	49
4.24	HWT-DWT image without attack	50
4.25	HWT-DWT images after Invert	50
4.26	HWT-DWT image without attack	50
4.27	HWT-DWT images after Noise attack	50

.

List of Abbreviations

HWT	Haar Wavelet Transform
DWT	Discrete Wavelet Transform
WT	Wavelet Transform
DFT	Discrete Fourier Transform
DCT	Discrete Cosine Transform
FDCT	Fast Discrete Curvelet Transforms
ICA	Independent Component Analysis
PSNR	Peak Signal-to-Noise Ratio

CHAPTER ONE

INTRODUCTION

Chapter one

Introduction

1.1 Introduction

In the recent years, a huge amount of digital information circulated through out the world by means of the rapid and extensive growth in Internet technology; therefore, there is a pressing need to develop several newer techniques to protect copyright, ownership and content integrity of digital media. Most of such data is exposed and can be easily forged or corrupted, consequently the need for intellectual property rights protection arises. This necessity arises because the digital representation of media possesses inherent advantages of portability, efficiency and accuracy of information content on one hand; but on the other hand, this representation also puts a serious threat on easy, accurate and illegal perfect copies of unlimited number. Unfortunately, the currently available formats for image, audio and video in digital form do not allow any type of copyright protection. Digital watermarking has been proposed as one of the possible ways to deal with this problem to keep information safe.

Digital watermarking, an extension of steganography, is a promising solution for content copyright protection, it imposes extra robustness on embedded information. In other words, digital watermarking is the art and science of embedding copyright information in the original files. The information embedded is called ‘watermarks’.

Information hiding, watermarking and Steganography are defined in the coming section, though these three terms share many similarities and could even be interchangeable in some literature. Therefore, certain fundamental differences lead us to define them as follows:

Information hiding is a general practice encompassing a broad range of applications in which the messages are embedded into the other media content for varying purposes, while watermarking and steganography are two types of information hiding. Steganography, which is derived from Greek words means, covered writing that hides the secret message into innocuous host content to achieve covert communication (Lin and Delp, 1999). In order to act as a successful camouflage to conceal the very existence of the secret message, the host media content is usually chosen to have nothing to do with the hidden information. Similar to Steganography, watermarking is also a procedure of imperceptibly embedding the information, i.e., a digital watermark, into the content. However, a digital watermark usually represents the ownership of the content. The legitimate content user or other information used to help protect the content. In other words, there exists a strong relationship between the embedded digital watermark and the host content. Besides, in order to achieve the intended functions, the existence of a digital watermark is usually known to the users, in contrast to the fact that the hidden information in Steganography is kept secret to the public. Therefore, the dependency between the host media content and hidden information is a differentiating factor between digital Watermarking and Steganography (Cachin, 1998).

1.2 Statement of the problem

Some sorts of techniques can use a copyright material image to ensure its ownership authentication. The main idea of the proposed system in this thesis is to overcome the problems of attack that happens during transmitting the image via communication links. Therefore, there is a vital need to construct a framework for image watermarking "A Robust Framework for Watermarking System" against all types of attacks, i.e., illegal manipulation and distribution of digital image via Internet.

1.3 Objective of study:

The primary objective of the proposed system is summarized as follows:

- Cascading two algorithms are based on the wavelet technique and evaluation in terms of robustness and security. New robust watermarking method that compiles two watermarking techniques (HWT&DWT) are put forward.

- Adding a private key to watermarking that will increase the privacy and gives more security. Further it will give more protection in wavelet transform that enhances resistance against attack.
- Using colored images is efficient and more secured from other techniques because of coupling between DWT, HWT and adding a private key.
- More robust against all types of attacks (Invert, Rotate, Crop, and Scale), which means that the embedded original image is not effected.

1.4 Thesis Significance:

The main significance of the proposed system is to solve problems of modification, forgery, illegal manipulation and distribution of digital image. Although there are many ways to protect the images, the proposed system suggests a new method to protect the image for the purposes of ownerships, copyright and intellectual property.

1.5 Thesis organization:

In addition to this chapter, the thesis includes four other chapters. As follows:

Chapter two provides an overview of watermarking techniques along with listing and explaining different related works in the area of the proposed system. Chapter three explains in detail the proposed system architecture and the different models and algorithms that are used in all parts of the proposed system. Also it shows the user interface in the details of all options that represent activities and tasks in the proposed system, as well. Chapter four represents a complete experimental result through step-by-step examples provides the robustness of the generated images based on the proposed system. This is performed by using different types of attacks against the watermarking image.

Finally, chapter five is divided into two sections which are, conclusion and future works including recommendations.

CHAPTER TWO

LITERATURE SURVEY

Chapter Two

Literature Survey

2.1 Watermarking Overview

"Digital watermarking" means embedding information into digital material in such a way that it is imperceptible to a human observer but easily detected by computer algorithm. A digital watermark is a transparent, invisible information pattern that is inserted into a suitable component of the data source by using a specific computer algorithm. It is a signal added to digital data (audio, video, or still images) that can be detected or extracted later to make an assertion about the data(Amin, et al., 2003).

2.1.1 Watermarking Applications

Digital watermarking is described as a viable method for the protection of ownership rights of digital image, and other data types. It can be applied to different applications including digital signatures, fingerprinting, broadcast and publication monitoring, authentication, copy control, and secret communication (Cox, et al., 1997, 2000; Katzenbeisser and Petitcolas, 2000).

2.1.2 Properties of Watermarking System

When designing a watermarking system, several properties must be observed, among which are the following (Kutter and Hartung, 2000):

1 Imperceptibility – the watermark should be invisible not to degrade data quality and to prevent an attacker from finding and deleting it.

2 Readily detectable – the data owner or an independent control authority should easily detect the watermark.

3 Unambiguous – retrieval of it should unambiguously and unequivocally identify the owner of the data with a high degree of confidence.

4 Robust – difficult to remove without producing a remarkable degradation in data fidelity.

5 Security – unauthorized parties should not be able to read or alter the watermarking.

2.1.3 Watermarking Techniques:

There are many different watermarking techniques. They range from the very simple to the complex (Anirban, et al., 2010). Obviously the type and the value of the content should determine the watermarking technique to be used. For the image watermarking, there are a number of schemes of varying robustness that have been implemented (Haldar, 2008). These techniques have their strong and weak points. Typically they fall into two categories: Spatial and Transform domain (Yeung, et al., 1998).

2.1.3.1Spatial Domain Watermarking:

Watermarking was the first scheme that introduced works directly in the spatial domain. By some image analysis operations (e.g. edge detection), it is possible to get perceptual information key, directly in the intensity values of predetermined regions of the image (Paquet, 2001). Those simple techniques that provide a simple and effective way for embedding an invisible watermark into an original content but don't show robustness to common alterations, (Cox, et al., 2002; Wolfgang, et al., 1999). One of the most famous spatial techniques is Least Significant Bit (LSB) (Hanjalic, et al., 2000).

One straightforward and rapid technique is based on the principle of generating a pseudo-generated noise pattern and integrating it into specific chrominance or

luminance pixel values (Darmstaedter, et al., 1998). Such pseudo-random noise patterns consist of black (1), white (–1), and neutral values (0). The pseudo noise is generated with a "secret" key and algorithm. Additionally, the process could be adjusted to the image components or feature vectors to achieve a higher level of invisibility. In general, the watermark W(x, y) is integrated into the image components I (x, y) by a factor that allows amplification of the watermarking values in order to obtain the best results. K (key), W(x, y) (watermark image), I (x, y) (image components).

$$I_W(x,y) = I(x,y) + k * W(x,y)$$

2.1.3.2 Frequency domain watermarking:

It is also known as transforming domain watermarking (Grans, 2003). Another way to produce high quality watermarked content is by first transforming the original content (e.g. image) into the frequency domain by the use of Fourier, discrete cosine or wavelet transform. With this technique, the marks are not added to the intensities of the image but to the values of its transform coefficients (Robi, 2004), then inverse transforming the marked coefficients from the watermarked image. The use of frequency based transform allows the direct understanding of the content of the image (Grans, 2003). Therefore, characteristics of the Human Visual System (HVS) can be taken into account more easily when it is time to decide the intensity and position of the watermark to be applied to a given image (Kunder and Hatzinko, 2001). Because high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies

containing important elements of the original image (Fionn, 2007). The following are some techniques of the frequency transform domain.

2.1.3.2.1 Discrete Fourier Transform (DFT):

The scholar Joseph Fourier in 1822 produced what is know as Fourier analysis, which is a method to present periodic signals by using a series of sine and cosine.

The transformer transfers the signal from the space of time to space of frequency and vice versa, and Fourier transform is mathematically defined as the following:

$$x(f) = \int_{-\infty}^{+\infty} x(t).e^{-jwt}.dt$$

But the problem is that the Fourier transform becomes inactive for the non-stationary signals (variable frequency) because it does not provide us with information on the frequency content over time (Dittmann, 2000).

2.1.3.2.2 The Discrete Cosine Transform (DCT):

DCT is a real domain transform which represents the entire image as coefficients of different frequencies of cosines (which are the basis vectors for this transform). The DCT of the image is calculated by taking (8X8) blocks of the image, which are then transformed individually. DCT also forms the basis of JPEG image compression algorithm, which is one of the most widely used image data storage formats. The DCT approaches are able to withstand some forms of attack (Chiou-Tign and Ja-Ling-Wu, 1998; Dittmann, 2000).

2.1.3.2.3 The Wavelet Transform Based Techniques (WT):

The wavelet transform provides the time frequency transformation of a given signal (Paquet, 2001). Wavelet transform is capable of providing the time and frequency information simultaneously, hence giving a time-frequency representation of the signal.

The problem is the huge number of wavelet resulting from the use of all the gradations in the process of analysis and the reams of information, which also produced for the same reason, and therefore the treatment process requires a very long time. Two transformers (DWT and HWT) are using limited number of gradations, rather than making the conversion for all the gradations, and are done by selecting time domains in the signal (Kunder and Hatzinko, 2001, Inoue, et al., 1999, Radomir and Bogdan, 2003). This conversion produces a sufficient quantity of information, with less time of accounting and maintaining the basic information of the depicted reference (i.e. without the loss of important information)

2.1.4 Digital watermarking system

All watermarking methods share the same building blocks:

- Digital watermark embedding system, and
- Digital watermark embedding extraction or recovery system.

Any generic embedding system should have as inputs: (data/image)/hiding medium, watermark symbol (image/text/number) and a key to enforce security. The output of the embedding process is always the watermarked data/image (Leung, et al., 2009; Al-Haj, 2007). The generic watermark extract/recovery process needs the watermarked data, the secret key or public key and, depending on the

method, the original data and /or the original watermark as inputs, while the output is the extracted/recovered watermark with some kind of confidence measure for the given watermark symbol or an indication about the presence of watermark in the cover image under inspection (Haldar, 2008).

2.1.5 Attacks on Digital Watermarks

Watermarking research has produced a wide range of watermarking techniques that can be subdivided into various methodological complexity levels. Each of these methods attempts to reduce vulnerability in various attack scenarios. Attacks on digital watermarks can be mainly classified into two major groups:

(i) Friendly and malicious attacks (Hanjalic, et al., 2000; Hartung, et al., 1999).

(ii) Conventional image or data operations applied in the normal use of computer technology can destroy the watermark information. Different operation of the classical image processing field, such as scaling, color and gamma corrections, and so forth, can be identified at this point. Today, compression techniques can also be placed in the field of classical operations, but often separated as a single element in watermarking research. The friendly attack has two common features. It is generally described as an unintentional event where the user has no suppose and/or knowledge of the watermark and its embedded procedure. The second type of attack, the malicious one, occurs with the intention of eliminating the information (Hanjalic, et al., 2000).

2.2 Related works

In this section we will illustrate several related works in order to find out the position of this proposed system and to define the gaps and difference between this work and the previous works. Also to determine the major research techniques and methodologies used, finally, to recognize key ideas, theories and conclusion, and to set the differences and similarities. In the following, we will summarize some of such related works:

Houng-Jyh, et al., (1998) investigated a wavelet-based watermark casting scheme and a blind watermark retrieval technique. An adaptive watermark casting method is developed to first determine significant wavelet subbands and then select a couple of significant wavelet coefficients in these subbands to embedding watermarks. A blind watermark retrieval technique that can detect the embedded watermark without the help from the original image is proposed. Experimental results show that the embedded watermark is robust against various signal processing and compression attacks.

Taskovski, et al., (1999) argued that the wavelet coefficients of the watermark are embedded to the most significant coefficients at the low and high frequency bands of the discrete wavelet transform of an image. A multiresolution nature of wavelet transform can be exploiting in the process of detection. Experimental results show that the proposed watermarking method results in almost invisible difference between the watermarked image and the original image. Moreover, proposed watermarking method is robust to DCT and wavelet based lossy image

compression techniques, and some image processing operations like image resizing and cropping.

Radomir, et al., (2003) gives brief survey of basic definitions of the Haar wavelet transform where some recent developments and state-of-the art in Haar transforms include efficient symbolic calculation of Haar spectrum and some applications of Haar wavelet transform. The authors believe that this survey can be useful to researchers working in different disciplines where the Haar transform is used.

Stephan, (2005) embedded watermarking in still images (BMP) true color, this method applies embedding watermark in large coefficients and in high frequency subbands by using discrete wavelet transform. The watermark in this method is capable of surviving against the JPEG2000 compression and the watermark extracted using original image (non-blind watermark).The research applied to many images, and the results for this method is robust against extraction watermarking on the average 90-95%.

Lepik, (2007) demonstrates that the Haar wavelet method is a powerful tool for solving different types of integral equations and partial differential equations. This method with less degree of freedom and with smaller CPU time provides better solutions than classical ones. The main advantage of this method is its simplicity and small computation costs, resulting from the sparsity of the transform matrices and the small number of significant wavelet coefficients.

Cabir and Serap, (2007) suggests a new digital image watermarking algorithm that combines the strengths of the moment based image normalization and two dimensional discrete wavelet transform was proposed by the researchers. Normalization provides robustness against geometrical degradations, whereas discrete wavelet transform achieves immunity for compression, linear and non-linear filtering by taking the properties of the human visual system into consideration. Simulation results show that the method provides promising robustness results for various kinds of image manipulations.

Wu a .N.-I, et al., (2008) propose a novel watermarking method to solve the problem of copyright protection. Their new method makes a difference by providing the user with the power to process masses of digital image watermarking tasks using just one private key. The results of the authors' extensive experiments have proven both the capability of the proposed technique as an efficient management mechanism and the robustness of it against various image processing attacks such as Joint Photographic Experts Group compression, low pass filtering and high pass filtering as well as noise contamination

Min-Jen, (2009) studied novel visible watermarking algorithm based on the content and contrast aware (COCOA) technique with the consideration of Human Visual System (HVS) model. In order to determine the optimal watermark locations and strength at the watermark embedding stage, the COCOA visible watermarking utilizes the global and local characteristics of the host and watermark images in the discrete wavelet transform (DWT) domain. The experimental results demonstrate that COCOA technique not only provides high PSNR values for the watermarked images, but also preserves the watermark

visibility under various signals processing operations, especially the watermark removal attack.

Leung, et al, (2009) proposed a selective curvelet coefficient digital watermarking algorithm. The selective band provides an addition security feature against any physical tampering. Their reported goal was to give an intensive study on the robustness of watermarking using selective curvelet coefficients from a single band and to find out the best band for embedding watermark. Wrapping of specially selected Fourier samples is employed to implement Fast Discrete Curvelet Transforms (FDCT) to transform the digital image to the curvelet domain.

Ilker and Ivan, (2009) developed an over complete discrete wavelet transform (DWT) based on rational dilation factors for discrete- time signals. It was implemented using self-inverting FIR filter banks. It is approximately shift-invariant, and can provide a dense sampling of the time-frequency plane. This algorithm is based on matrix spectral factorization. The analysis/synthesis functions (discrete-time wavelets) can be very smooth and can be designed to closely approximate the derivatives of the Gaussian function.

Chapter Three

A CASCADE HAAR-DWT BASED DIGITALWATERMARKING SYSTEM

Chapter Three

A cascade Haar-DWT Based digital Watermarking system

3.1 Introduction

The content is watermarked by converting copyright information using an algorithm that is perceptible only to the content creator. Digital watermarks can be read only by using the appropriate reading software. These are resistant to filtering and stay with the content as long as originally purposely degraded.

The technique facilitates access of the encrypted data only for valid key holders but fails to track any reproduction or retransmission of data after decryption. On the other hand, in digital watermarking, an identification key is embedded permanently inside a cover image which remains within that cover invisibly even after decryption process. This requirement of watermarking technique, in general, needs to possess the following characteristics:

(a) Imperceptibility for hidden information.

(b) Redundancy in distribution of the hidden information inside the cover image to satisfy robustness in watermark extraction process even from truncated (cropped) image.

(c) A key to achieve cryptographic security of hidden content.

Besides these general properties, an ideal watermarking system should also be resilient to insertion of additional watermarks to retain the rightful ownership. The perceptually invisible data hiding needs insertion of watermark in higher spatial frequency of the cover image since human eye is less sensitive to this frequency

component since in most of the natural images, majority of visual information are concentrated on the lower end of the frequency band, so the information hidden in the higher frequency components might be lost after quantization operation of lossy compression.

The proposed system in this thesis is called "A Robust Framework for watermarking system". The system generally consists of two independent, but complementary, subsystems. The first subsystem is called the "Haar Wavelet Transform (HWT)" and the second subsystem is called the "Discrete Wavelet Transform (DWT)". The general structure of the proposed system is shown in figure 3.1.

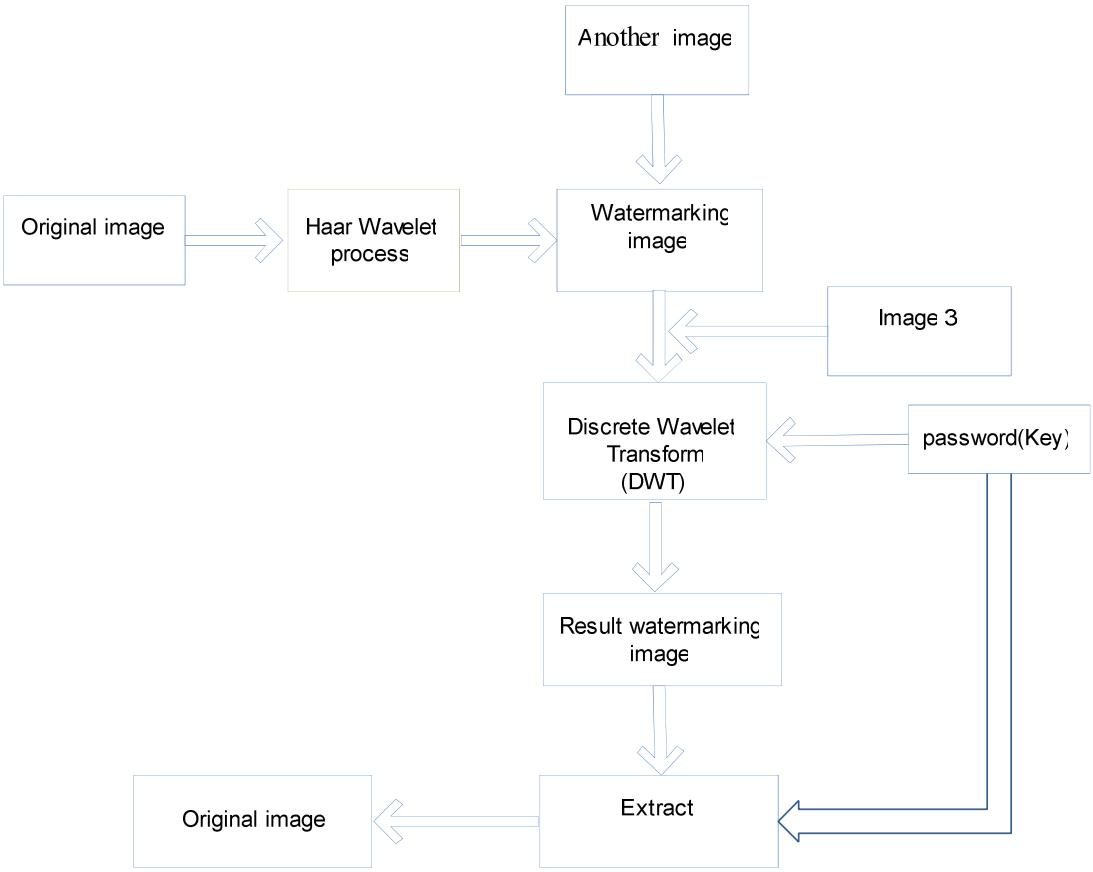

Figure 3.1 General Structure of the proposed system

3.2 Haar Wavelet Transform Subsystems (HWT)

The main tasks of the HWT subsystems:

1. A standard decomposition of a 2-D signal (image), this is done by performing a one dimensional transformation on each row followed by a one dimensional transformation of each column.

2. Construct a function that Haar Transforms an image for differed levels.

Figure 3.2 represents the general structure of the HWT and shows its main parts. Essentially, each part is cascading for the other parts, and represents a task in the HWT Process.

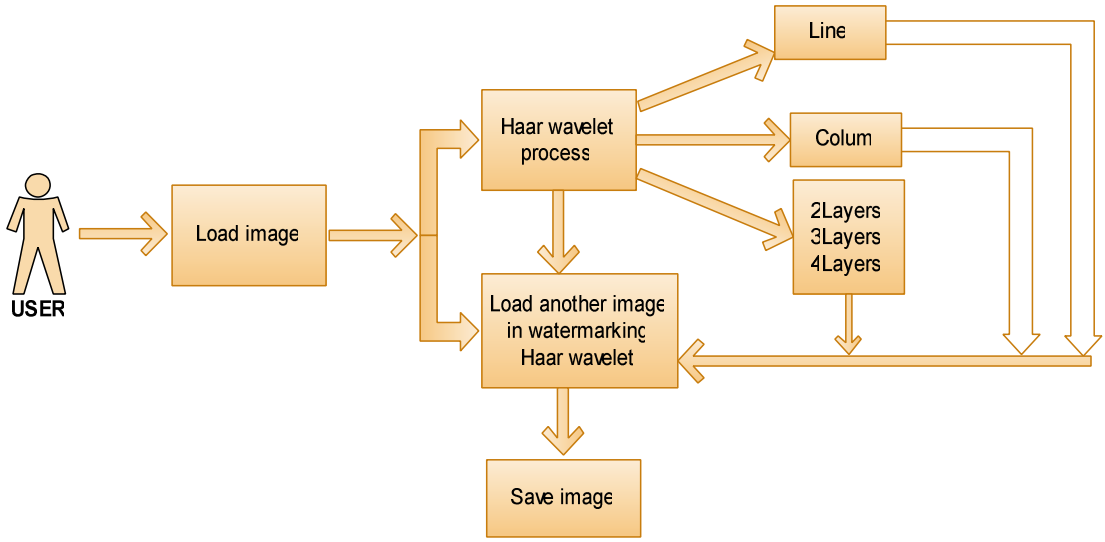

Figure 3.2 HWT subsystem

This subsystem applies wavelet transform by using Haar Wavelet. The main function of HWT can be explained through the following steps:

1. Load an image (300x300 pixel)

2. Apply HWT Process. It consists of the following processes:

a. Line transformation: This also is called row. It decompose the image into rows using the flowing code (Talukde and Harada, 2007):

```
/*row transformation*/
for(i=0;i<row;i++){w=col;
do{ k=0;
/*averaging*/ for(j=0;j<w/2;j++)
a[j]=((mat[i][j+j]+mat[i][j+j+1])/2);
/*differencing*/ for(j=w/2;j<w;j++,k++)
a[j]=mat[i][j-w/2+k]-a[k];
for(j=0;j<row++) mat[I] [j]=a[j];
w=w/2;
}while(w!=1);
}
```

b. Columns transformation: it decompose the image into columns using the following code: another image (Talukde and Harada, 2007):

```
}
/*column transformation*/
for(i=0;i<col;i++){ w=row;
do{k=0;
/*averaging*/ for(j=0;j<w/2;j++)
a[j]=((mat[j+j][i]+mat[j+j+1][i])/2);
/*differencing*/for(j=w/2;j<w;j++,k++)
a[j]=mat[j-w/2+k][i]-a[k];
for(j=0;j<w;j++) mat[j][i]=a[j];
w=w/2;
}while(w!=1);
}
```

c. Two, Three, Four Layers Wavelet transformation:

It decomposes the image into two, three, or four layers. To understand how the Haar Wavelets Transform works, let us consider the following simple example; suppose one dimension vector we have image with a resolution of four pixels having values [8 6 3 7]. Haar wavelet basis can be used to represent this image by computing a wavelet transform. To do this, we find the average of the two pixels together, results

the pixel values [7 5]. Clearly, some information is lost in this averaging process. We need to store some detail coefficients to recover the original four pixel values from the two averaged values. In our example. 1 chosen for the first detail coefficient, since the average computed is 1 less than 8 and 1 more than 6. This single number is used to recover the first two pixels of our original four-pixel image. Similarly, the second detail coefficient is -2. 3-5=-2 and since 5+ (-2) =3 and 5- (-2) =7. Thus, the original image is decomposed into a lower resolution (two – pixel) version and a pair of detail coefficients.

Regarding this process recursively on the averages gives the full decomposition shown in Table 3.1:

Resolution	Averages	Detail coefficients
4	[8 6 3 7]	
2	[7 5]	[1 -2]
1	[6]	[1]

Table 3.1: Decomposition to lower resolution

Thus, for the one-dimensional Haar basis, the wavelet transform of the original four-pixel image is given by [6 1 1 -2]. We call the way used to compute the wavelet transform by recursively averaging and differencing coefficients, filter bank.

We can reconstruct the image to any resolution by recursively adding and subtracting the detail coefficients from the lower resolution version.

Compression of 2-D image with Haar Wavelet Technique: It has been shown in the previous section how 1-D image can be treated as sequences of coefficients. Alternatively, we can think of images as piecewise constant functions on the half-open interval [0, 1). To do so, the concept of a vector space is used. A one-pixel image is just a function that is constant over the entire interval [0, 1). Let V^0 be the vector space of all these functions. A two pixel image has two constant pieces over the intervals [0, 1/2) and [1/2, 1). We call the space containing all these functions V^1. If we continue in this manner, the space V^j will include all piecewise-constant functions defined on the interval [0, 1) with constant pieces over each of 2^j subintervals. Note that because these vectors are all functions defined on the unit interval, every vector in V^j is also contained in V^{j+1}. For example, we can always describe a piecewise constant function with two intervals as a piecewise-constant function with four intervals, with each interval in the first function corresponding to a pair of intervals in the second. Thus, the spaces V^j are nested; that is, $v^0 \subset v^1 \subset v^2 \subset \ldots$ this nested set of spaces V^j is α necessary ingredient for the mathematical theory of multiresolution analysis. It guarantees that every member of V^0 can be represented exactly as a member of higher resolution space V^1. The converse, however, is not true: not every function G (x) in V^1 can be represented exactly in lower resolution space V^0.

Now we define a basis for each vector space V^j. The basis functions for the spaces V^1 are called scaling functions, and are usually denoted by the symbol ϕ. A simple basis for V^j is given by the set of scaled and translated box functions (Talukde and Harada, 2007).

$\Phi_i^j(x) := \Phi(2^j x - i) \qquad i = 0, 1, 2 \ldots 2^j - 1$ Where

$$\Phi(x) := \begin{cases} 1 & for \;\; 0 \le x < 1 \\ 0 & otherwise \end{cases}$$

The wavelets corresponding to the box basis are known as the Haar wavelets, given by (Talukde and Harada, 2007):

$$\Psi_i^j(x) := \Psi(2^j x - i) \qquad i = 0, 1, 2 \ldots 2^j - 1 \quad \text{Where}$$

$$\Psi(x) := \begin{cases} 1 & for \;\; 0 \le x < 1/2 \\ -1 & for \;\; 1/2 \le x < 1 \\ 0 & otherwise \end{cases}$$

Thus, the HWT for an image as a 2-D signal will be obtained from 1-D DWT. We get the scaling function and wavelet function for 2-D by multiplying two 1-D scaling functions: Ø (x, y) = Ø (x) Ø (y). The wavelet functions are obtained by multiplying two wavelet functions for wavelet and scaling function for 1-D. For the 2-D case, there exist three wavelet functions that scan details in horizontal Ψ(1) (x , y)= Ø (x) Ψ(y) , vertical Ψ(2) (x , y)= Ψ(x) Ø (y) and diagonal directions; Ψ(3) (x , y)= Ψ(x) Ψ (y). This may be represented as a four-channel perfect reconstruction filter bank. Now; each filter is 2-D with the subscript indicating the type of filter high pixels frequency (HPF) or low pixels frequency (LPF) for separable horizontal and vertical components. By using these filters in one stage, an image is decomposed into resolution: horizontal (HL), vertical (LH), and diagonal (HH). The operations can be repeated on the low low (LL) band using the second stage of identical filter bank.

Thus, a typical 2-D Haar transform, used in image compression and can be represented as a four-channel perfect reconstructions as shown in figure 3.3.

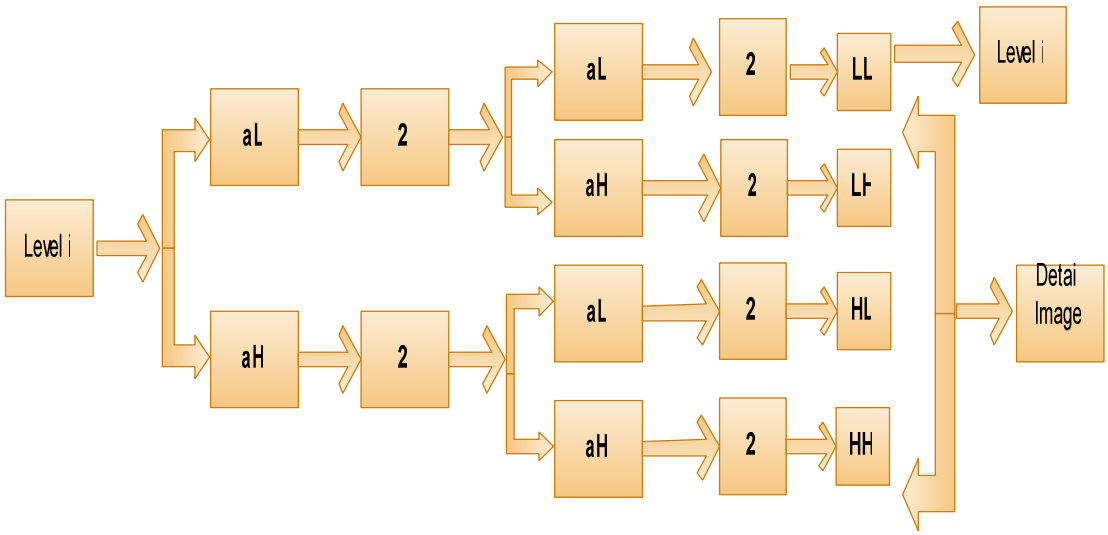

Figure 3.3 Structure of 2D Haar wavelet proposed systems

The WT (Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to compute multiple "scale" wavelet decomposition, as in the three scales WT which is shown in figure 3.4.

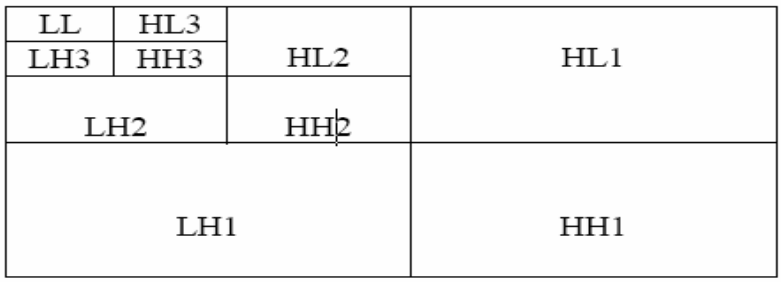

Figure 3.4 Structure of wavelet decomposition

The transformation of the 2-D image is a 2-D generalization of the 1-D wavelet transform which is already discussed. This operation provides us with an average value and detail coefficients for each row. Next, these transformed rows are treated as if they were themselves an image and apply the 1-D transform to each column. The resulting

values are all detail coefficients except a single overall average coefficient. In order to complete the transformation, this process is repeated recursively only on the quadrant containing averages.

Now let us see how the 2-D Harr Wavelet Transformation is performed. The image is comprised of pixels represented by numbers. Consider the 8x8 image taken from a specific portion of a typical image shown in Figure 3.5. The matrix (a 2D array) representing this image is shown in Figure. 3.6.

Now we perform the operation of averaging and differencing to arrive at a new matrix representing the same image in a more concise manner. Let us look how the operation is done. Consider the first now in Figure. 3.6.

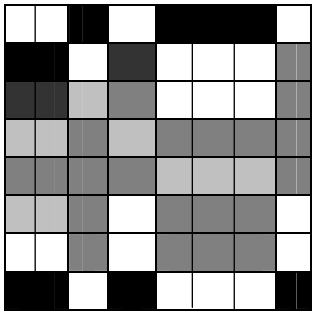

Figure 3.5 A 8x8 image

$$\begin{pmatrix} 56 & 10 & 1 & 63 & 58 & 8 & 10 & 54 \\ 11 & 53 & 52 & 14 & 14 & 50 & 51 & 16 \\ 20 & 44 & 46 & 37 & 22 & 42 & 40 & 24 \\ 39 & 27 & 26 & 38 & 34 & 32 & 31 & 34 \\ 31 & 35 & 34 & 30 & 30 & 36 & 40 & 24 \\ 40 & 24 & 23 & 43 & 44 & 20 & 19 & 47 \\ 50 & 14 & 15 & 51 & 52 & 12 & 11 & 55 \\ 7 & 57 & 58 & 6 & 3 & 63 & 62 & 2 \end{pmatrix}$$

Figure 3.6 2D arrays to represent the image in Figure 3.5.

Averaging :(56+10)/2=33, (1+63)/2=32, (58+8)/2=33, (10+54)/2=32.

Differencing: 56-33=23, 1-32=-31, 58-33=25 and 10-32=-22.

So, the transformed now becomes (33 32 33 32 23 – 31 25 - 22). Now the same operation on the average values i.e. (32.5 32.5 0.5 0.5 23 -31 25 -22) is performed. Then we perform the same operation on the averages i.e. first two elements of the new transformed row. Thus the final transformed row becomes (32.5 0 0.5 0.5 32 -31 25 -22). The new matrix we get after applying this operation on each row of the entire matrix of Figure 3.6 is shown in Figure 3.7. Performing the same operation on each column of the matrix in Figure 3.7,

We get the final transformed matrix as shown in Figure 3.8. This operation on rows followed by columns of the matrix is performed recursively depending on the level of transformation which means that more iteration provides more transformations. It is known that the left-top element of Figure 3.8 i.e. 32.5 is the only averaging element which is the overall average of all elements of the original matrix and all the remaining elements are details coefficients. The point of the wavelet transform is that regions of little variation in the original image manifest themselves as small or zero elements in the wavelet transformed version. A matrix with a high proportion of zero entries is said to be sparse. For most of the image matrices, their corresponding wavelet transformed versions are much sparser than the original. Sparse matrices are easier to store and transmit than ordinary matrices of the same size. This is because the sparse matrices can be specified in the data file solely in terms of locations and values of their non-zero entries.

32.5	0	0.5	0.5	23	-31	25	-22
32.5	0	- 0.5	- 0.5	-21	19	-18	18
32.5	0	- 0.5	- 0.5	-12	-4	-10	7
32.5	0	0.5	0.5	6	-6	1	-2
32.5	0	0.5	0.5	-2	2	-3	8
32.5	0	- 0.5	- 0.5	8	-10	12	-14
32.5	0	- 0.5	- 0.5	18	-18	20	-22
32.5	0	0.5	0.5	-24	26	-30	30

Figure 3.7 Transformed array after operation

32.5	0	0	0	-0.5	-3.75	-0.375	0.375
0	0	0	0	- 0.5	-3.75	-0.125	-0.125
0	0	0	0	-2	0 .5	4	-2.25
0	0	0	0	3	-4	4.75	-3.5
0	0	0.5	0.5	22	-25	21.5	-20
0	0	- 0.5	- 0.5	-9	1	-5.5	4.5
0	0	- 0.5	- 0.5	-5	6	-7.5	11
0	0	0.5	0.5	-4	-22	25	-26

Figure 3.8 Final Transformed Matrix after one step.

Therefore, a lot of zero entries can be found in the final transformed matrix. From this transformed matrix, the original matrix can be easily calculated just by the reverse operation of averaging and differencing i. e. the original image can be reconstructed from the transformed image without loss of information. Thus, it yields a lossless compression of the image. However, to achieve more degree of compression, we have to think of the lossy compression (if applicable).

Figure 3.9 shows the embedding of a watermarking in the wavelet domain.

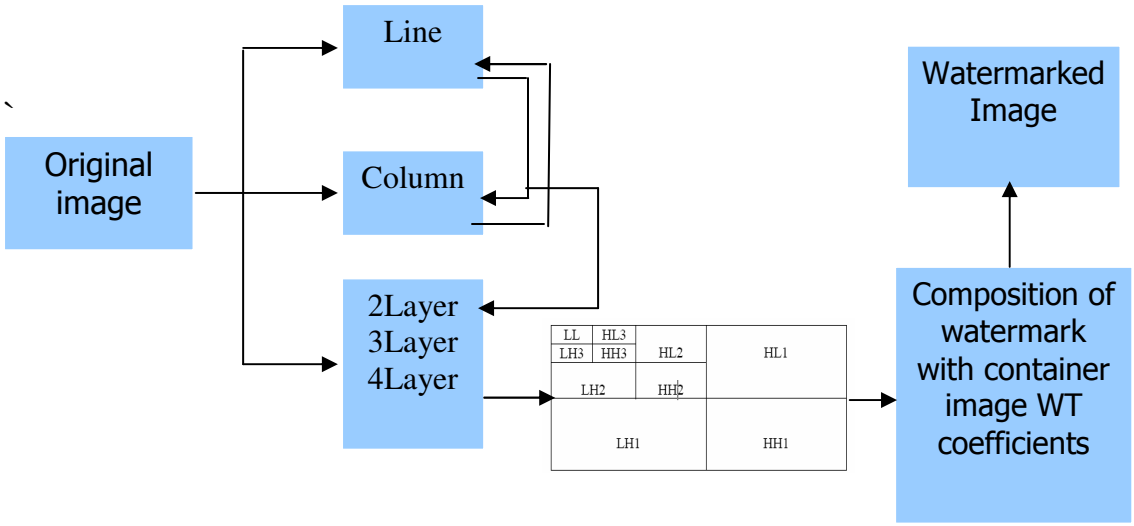

Figure 3.9 Embedding of a watermarking in the wavelet domain

The embedding algorithm is described in the following steps:

Step1: Input the original image, anther image.

Step2: The size of the two images should be the same.

Step3: Decompose image by using Haar wavelet transform.

Step4: Load the watermark into the suitable subband of the original image.

Step5: Convert the watermark into a stream of bits (zeroes, and ones).

Step6: The watermark will match the size of the matrix.

Step7: Convert every image from RGB to matrix color format.

Step8: Save watermarked color image.

Step9: Display watermarked image.

Algorithm for Embedding Watermark in Haar Wavelet Transform

3.3 Discrete Wavelet Transform Subsystems

The second subsystem is the Discrete Wavelet Transform (DWT). Figure 3.10 represents the general structure of the DWT and shows its main parts.

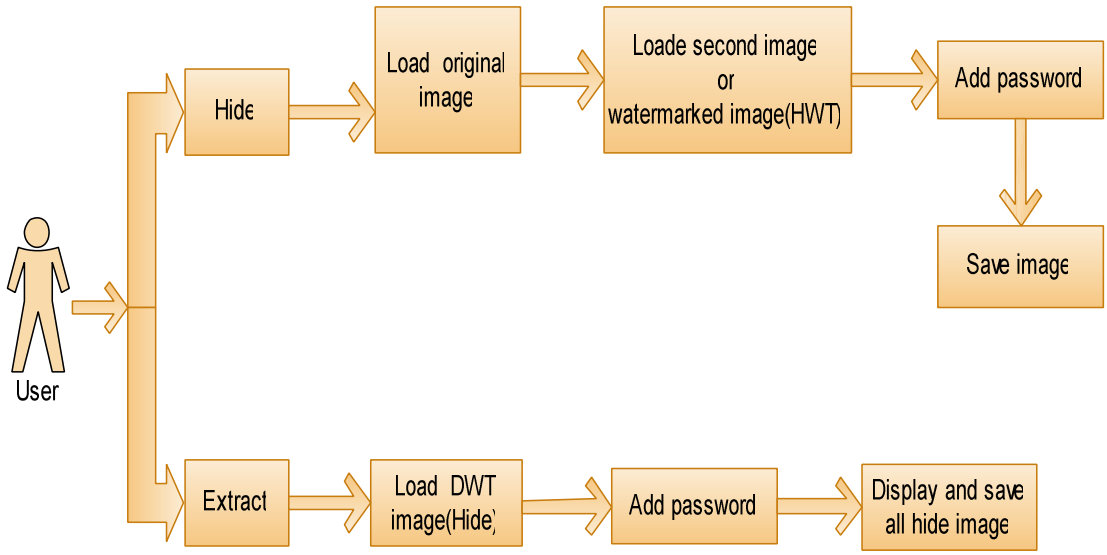

Figure 3.10 DWT subsystem

The DWT consists of two parts, which are Hide and Extract.

3.3.1 Hide (embedding) part

To understand the embedding technique, we will describe it through the following:

Let I be a color image with M*N pixels which consists of channels R, G and B. The three channels are divided into a set of n*n (n is odd) non-overlapping subblocks. In general, the size of the subblock has an influence on the robustness of the watermark. Each watermark bit can be embedded into one subblock by modifying the values of the subblock's middle pixel (m) and the other pixels (μ). Let us define m as the middle pixel value and μ as the mean value of the other pixels. For example, it is supposed have a 3*3 subblock as shown in Figure. 3.11. In this case, P5 is the middle pixel value m and the mean value of the other pixels can be computed by μ

(P1+P2+P3+P4+P6+P7+P8+P9)/8. To control the balance between the robustness and image quality, the robustness coefficient value T must be used; different robustness coefficient values for channels R, G and B are used:

P_1	P_2	P_3
P_4	P_5	P_6
P_7	P_8	P_9

Figure 3.11 Subblock of size 3*3

TR is the robustness coefficient value of channel R, TG is for channel G, and TB is for channel B.

Basically, the visual effect to modify the R, G and B channels is different in terms of the human visual sensitivity. In addition, the B channel has the larger tolerance to be modified than that of other channels. For these reasons, the robustness coefficient value TB used in the scheme is the largest value. TR and TG are the secondly and minimal respectively. The other advantage to adopt varied robustness coefficient is that the whole survival rate of watermark bit can be enhanced.

The Hide part process can be done by the following step:

1-Load the DWT image which has a size larger than the size of second image (HWT /embedded image).

2- Load the HWT image which has size smaller than the DWT image. The HWT image may be a watermarked image generated by the first subsystem (HWT).

3- Save DWT image.

4- Add a password to DWT image.

This part is giving more security for the watermarked image because it's an embedded image, which differs from other techniques. The application of

watermarking along with adding the password key would give additional security for the watermarked image.

The procedure of the embedding algorithm is as follows:

1. Input original image, image watermarking.

2. Divide channels R, G and B into a set of n*n non-overlapping subblocks respectively.

3. Set the robustness coefficient values TR, TG and TB for channels R, G and B respectively. In the next step, T represents TR, TG and TB when channels R, G and B are chosen to hide the watermark respectively.

4. Modify m (middle pixel) and μ (other pixels) for watermark embedding in the following:

$IF(W_k = 1) \quad and \quad (m - u \geq T)$

No Modify

Else

$$(m,u) = (m + \left\lceil \left| (m-u) - \frac{T}{2} \right| \right\rceil, u - \left\lfloor \left| (m-u) - \frac{T}{2} \right| \right\rfloor) \text{.....(1)}$$

$IF(W_k = 0) \quad and \quad (u - m \geq T)$

No Modify

Else

$$(u,m) = (u + \left\lceil \left| (u-m) - \frac{T}{2} \right| \right\rceil, m - \left\lfloor \left| (u-m) - \frac{T}{2} \right| \right\rfloor) \text{.....(2)}$$

5. Add the password (owner PRK) to watermarking to hide part.

6. Save watermarked image.

In equations (1) and (2), the μ value can be adjusted by subtracting or adding the pixel values P1, P2, P3, P4, P5, P6, P7, P8 and P9 respectively. When the first watermark bit has been embedded on channel R, the same location on channels G and B are also chosen to embed the first watermark bit.

Algorithm for Embedding Watermark in Discrete Wavelet Transform

3.3.2 Extract (recover) part

In the method of watermark Extraction in Wavelet, we need to input the watermarking image where the output is the original image. Watermark extraction needs to have some original data (original image). It is performed using Independent Component Analysis (ICA) which is applied to the bands of original and watermarked images and extracted by the backward embedding formula. The procedures of an extraction after various attacks are realized on purpose to check the watermark robustness against attacks. The quality of the extracted watermark is calculated using the correlation coefficient.

The advantages of ICA algorithm approach include storage of less information by the image's owner and better quality of the extracted watermark in the case of attacks.

Independent Component Analysis (ICA) is a statistical and computational technique for revealing hidden factors that underlie sets of random variables, measurements, or signals. ICA defines a generative model for the observed multivariate data, which is typically given as a large database of samples. In the model, the data variables are assumed to be linear mixtures of some unknown latent variables, and the mixing system is also unknown. The latent variables are assumed to be not Gaussian and mutually independent and they are called the independent components of the observed data. These independent components, also called sources or factors, can be found by ICA which is superficially related to principal component analysis and factor analysis. ICA is a much more powerful technique, however, capable of finding the underlying factors or sources when these classic methods fail completely.

The steps of the Extract part process are discussed in the Flowing paragraph as shown in figure 3.12:

1- Load the DWT image (generated in Hide part).

2- Add password (that used in Hide part).

3- Display and save all Hided images.

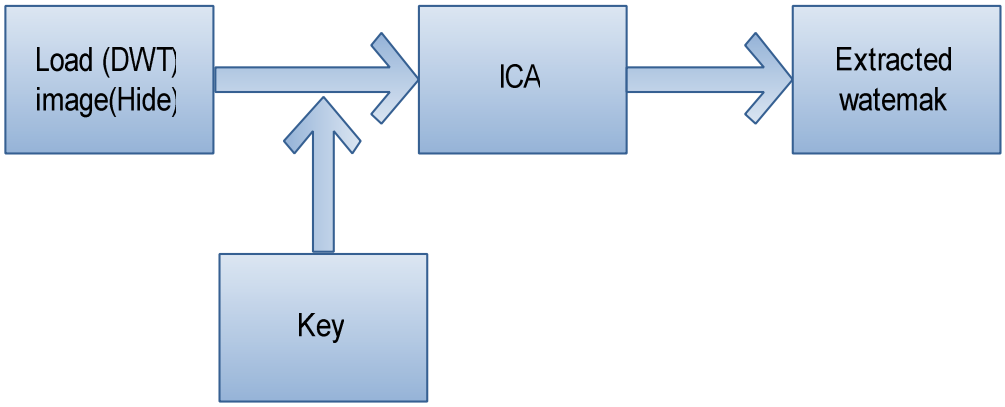

Figure 3.12 Extraction Scheme Using ICA

The extraction algorithm is described in the following steps:

1: Input watermarked image.

2: Add the password (owner PRK) to the watermarked image.

3: Divide channels R, G and B into a set of n*n non-overlapping subblocks respectively.

4: Compute the middle pixel value m and the mean value μ of the subblock.

5: Recover the watermark bit by comparing m with μ according to the following statements

If $m>\mu$

The watermark bit '1' is extracted

Else

The watermark bit '0' is extracted

6: Read the next watermarked subblock and repeat Steps (4) and (5) until all the watermark bits are extracted.

7: Display original image.

When the first watermark bit is extracted from channel R, the watermark bit hidden on channels G and B can also be extracted using the proposed extracting algorithm.

Algorithm for Extraction Watermark in Wavelet Transform

CHAPTER FOUR

EXPERIMENTAL RESULTS AND DISCUSSION

Chapter Four

Experimental Results and Discussion

4.1 Experimental Results

This section will demonstrate the steps of using the proposed system Figure 4.1 Wavelet Transform subsystems:

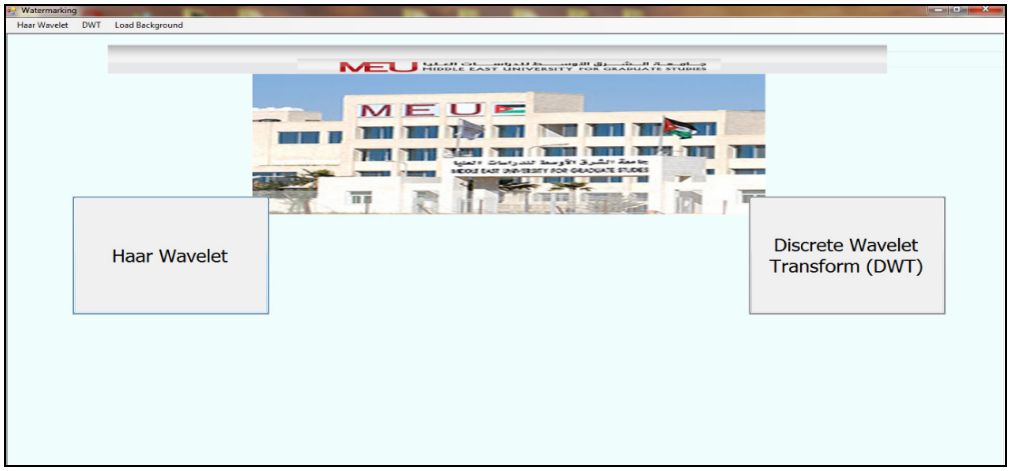

Figure 4.1 Wavelet Transform subsystems

The selected image (original image) will be show in Figure 4.2.

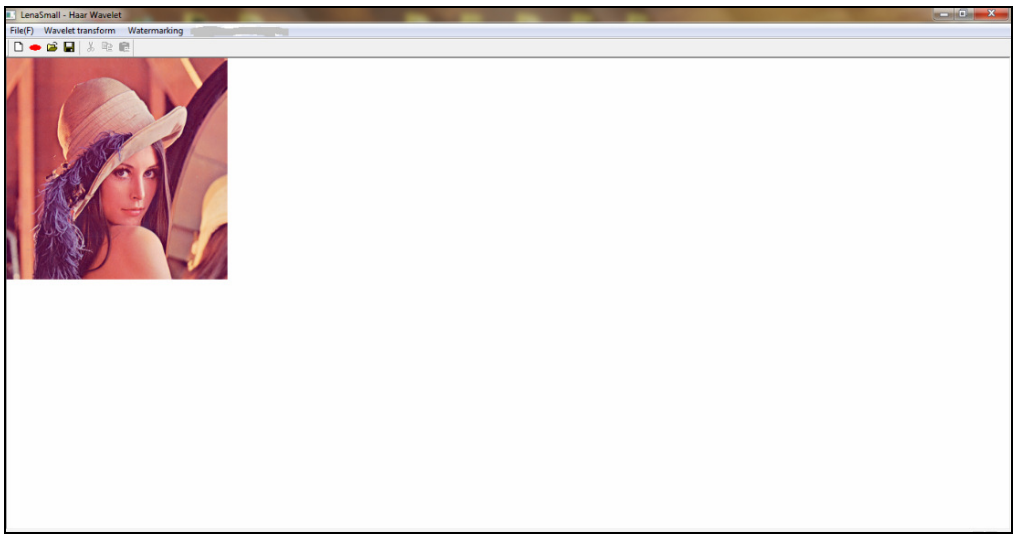

Figure 4.2 original image

Figure 4.3 and 4.4 shows the effect of choosing the Line Transform and the Column Transform processes.

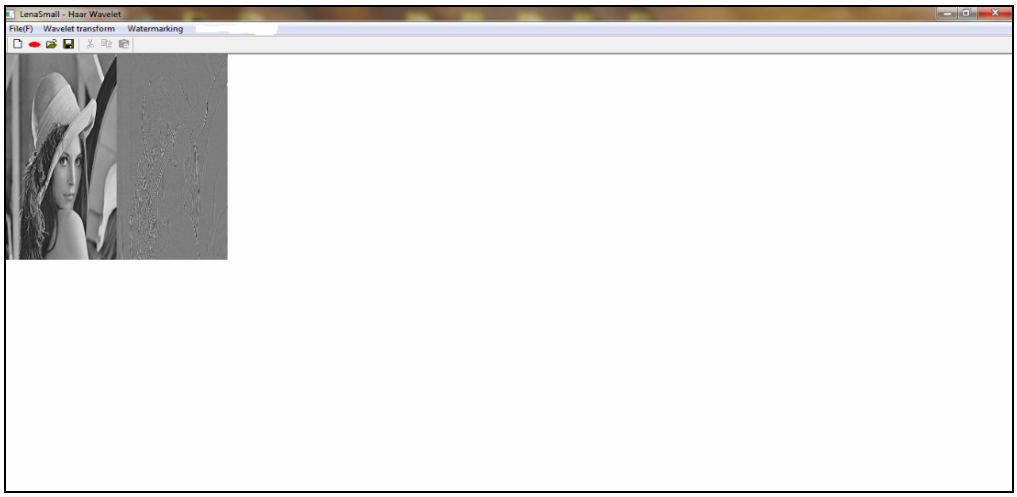

Figure 4.3 Line Transform

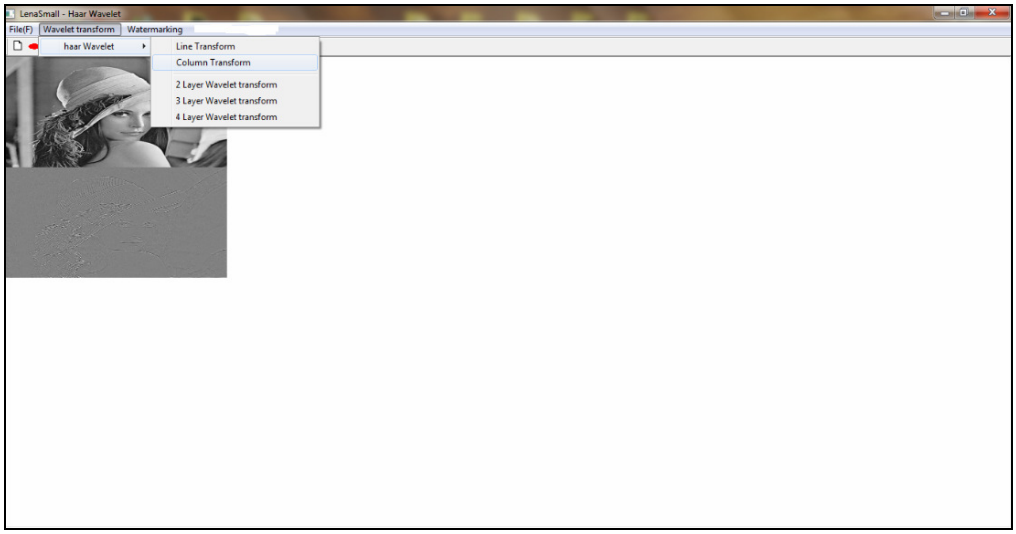

Figure 4.4 Column Transform

Figure 4.5, 4.6 and 4.7 shows the effect of 2Layer WT, 3Layer WT and 4 Layer WT on the selected image respectively.

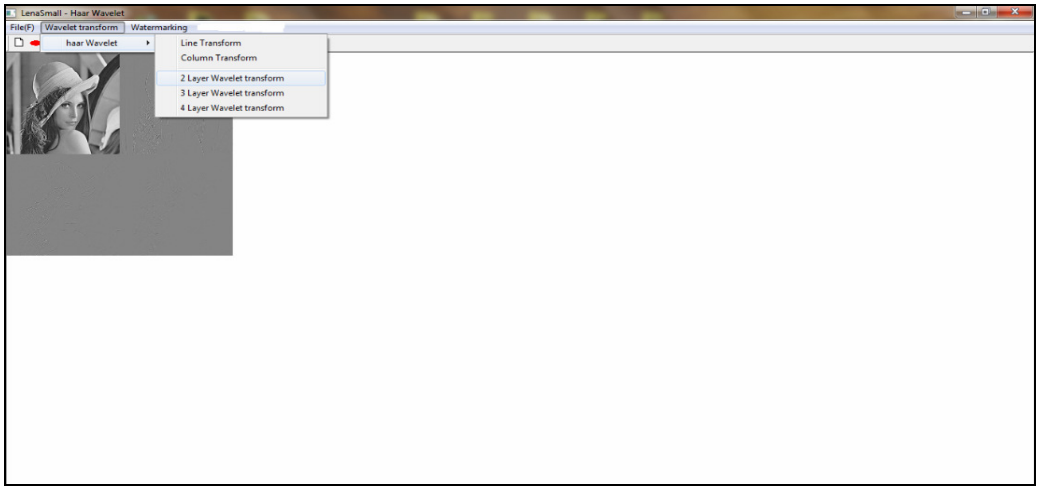

Figure 4.5 2Layer WT

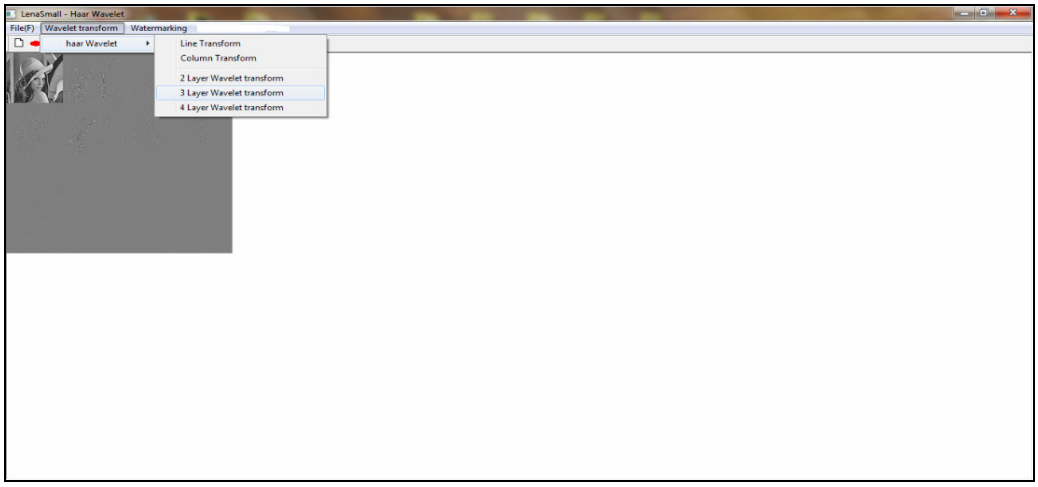

Figure 4.6 3Layer WT

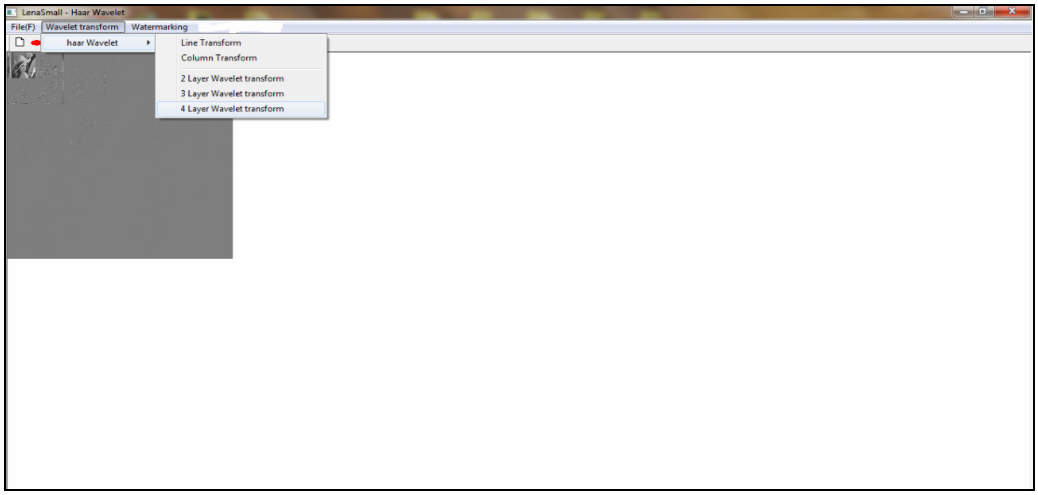

Figure 4.7 4Layer WT

The processes of HWT can be selected randomly and in any combination. After selecting the desired HWT, the next step is selecting the 'watermarking' option from the main menu and chooses another image (using the same steps of open option) Figure 4.8. shows process of watermarking on the original image

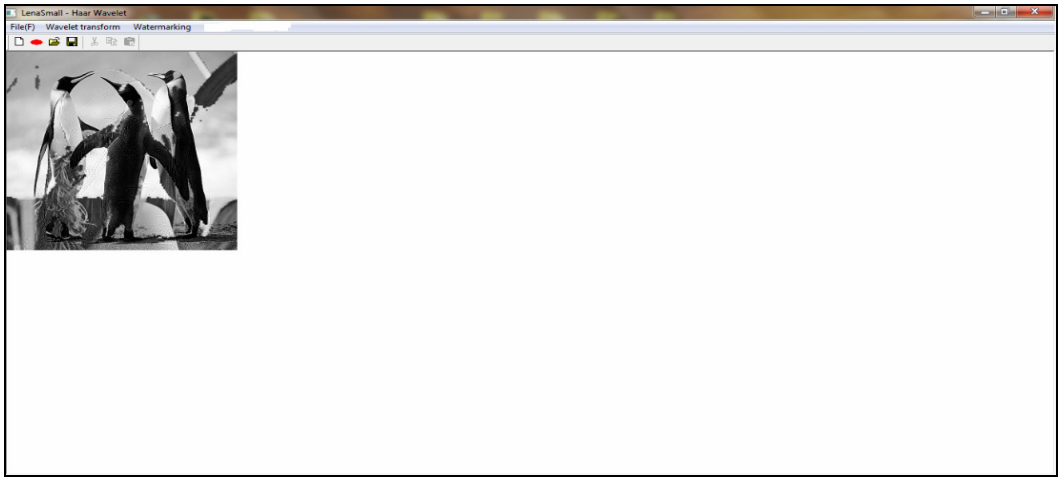

Figure 4.8 First watermarking processes

The next step, the user should choose "Discrete Wavelet Transform (DWT)" process. DWT process consists of two parts Hide and Extract.

- The Hide (embedding) part: this part is to hide/embed an image (or HWT) inside original image. It consists of the following steps:
    a) Load the original Image.
    b) Load HWT image.
    c) Save resulted image.
    d) Add password.
    e) Hide button.

Figure 4.9 shows the result of the hide (embedding) part.

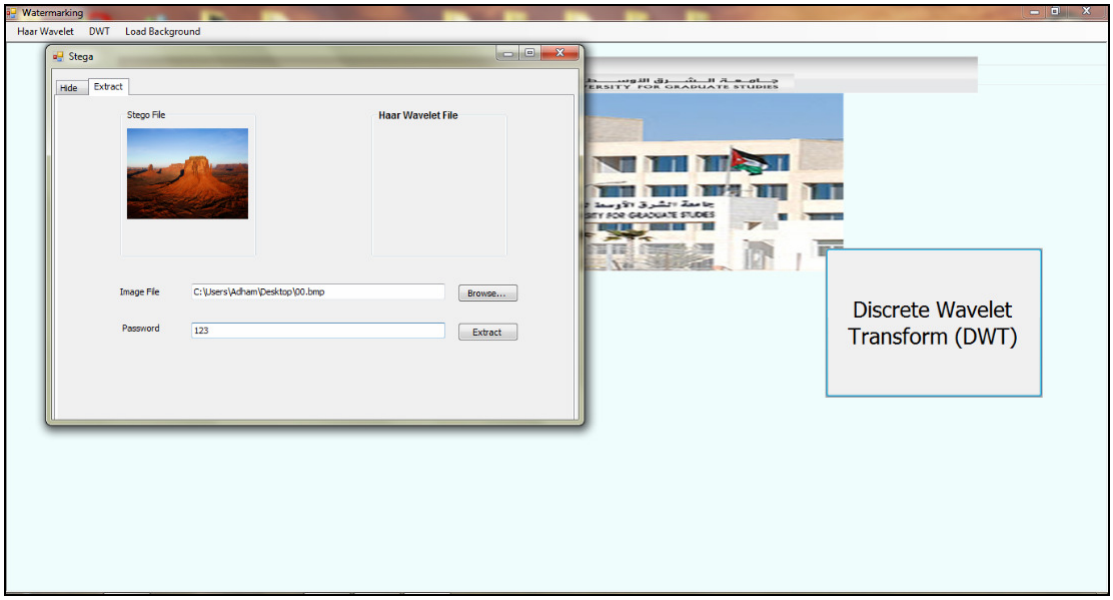

Figure 4.9 Final result of Hide part

- The Extract (recover) part: The task of this part is to extract /recover the images that embedded in the Hide part. It consists of the following steps:

  a) Load the DWT image.

  b) Put the password.

  c) Extract the watermarked image.

Figure 4.10 shows the extracted watermarked image.

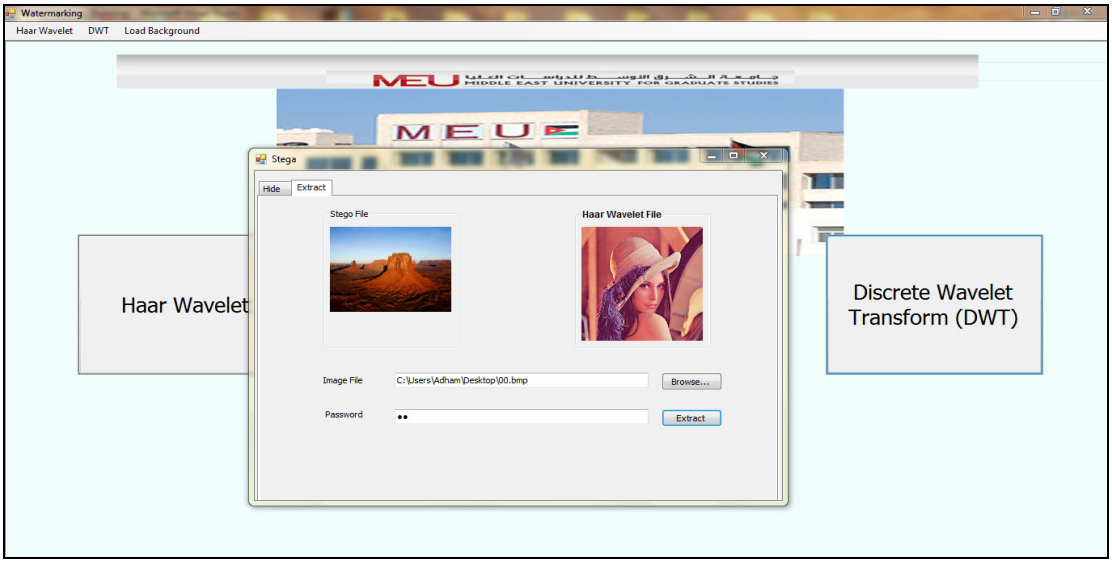

Figure 4.10 the extracted watermarked image

4.2 Robustness Test Result

In this section we will check the robustness of the watermarking image produced by using our proposed system.

For this purpose we created a program called "Image Attack" that will be used to attack the watermarking image resulted from the proposed system in the previous chapter. Figure 4.11shows the general structure for our Image program attacks.

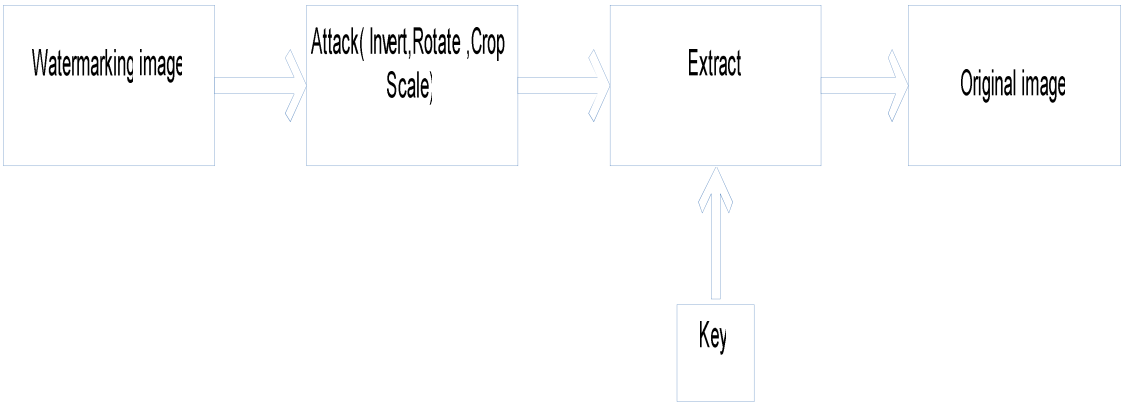

Figure 4.11 Image Attack structure

The watermarking image resulted from our system has been tested using the following different attacks: Invert, Rotate, Crop and Scale.

Figure 4.12, 4.13, 4.14, 4.15 shows the different types of attacks (Invert, Crop, Rotate, and Scale) applied to watermarking image respectively.

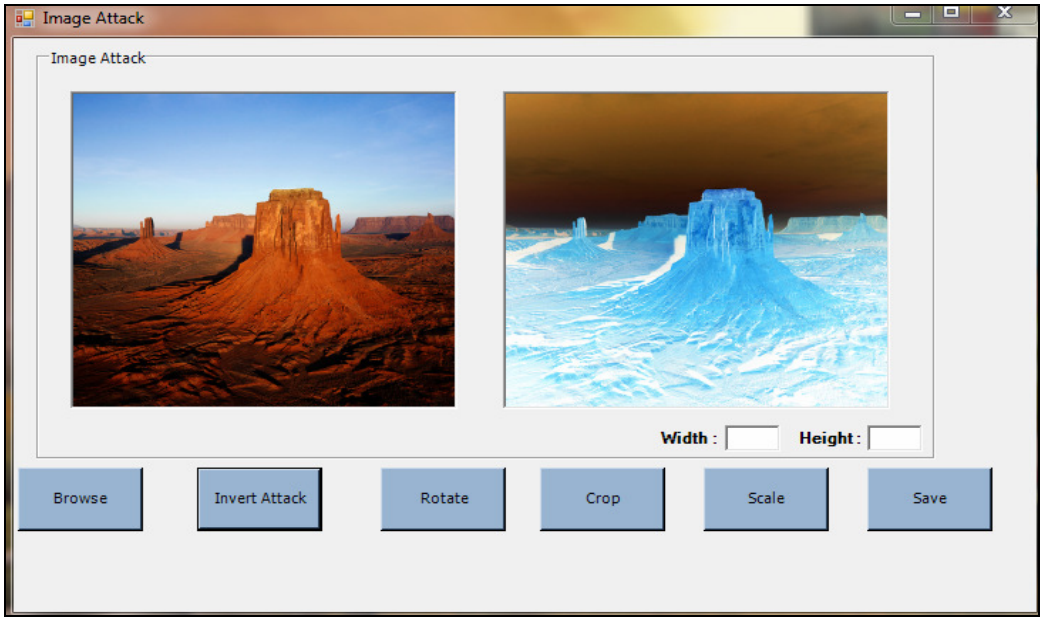

Figure 4.12 Invert Attack

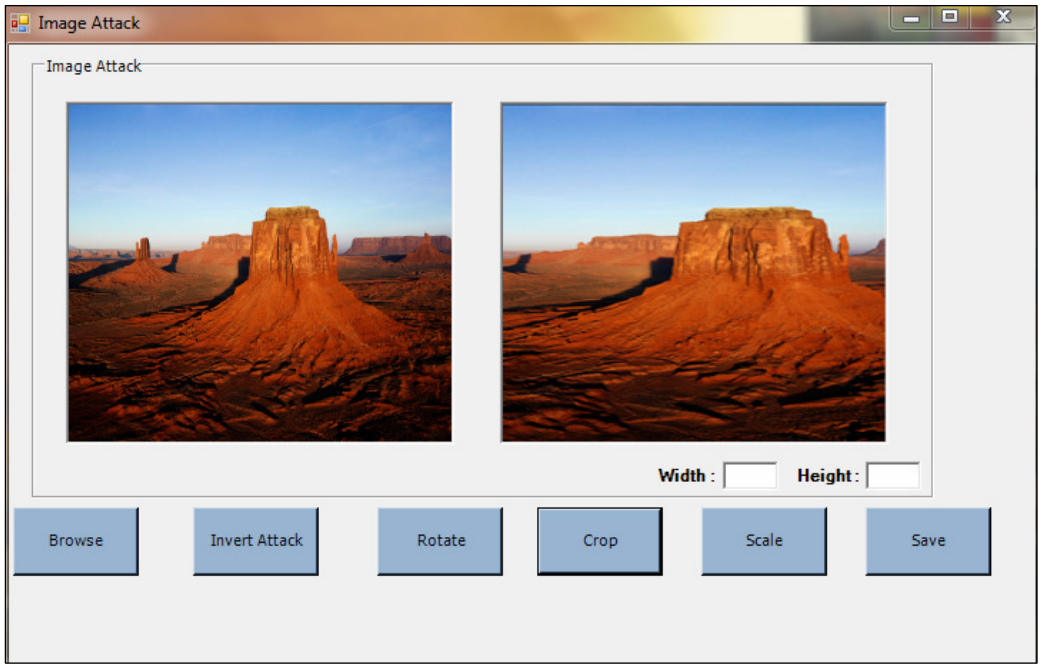

Figure 4.13 Crop Attack

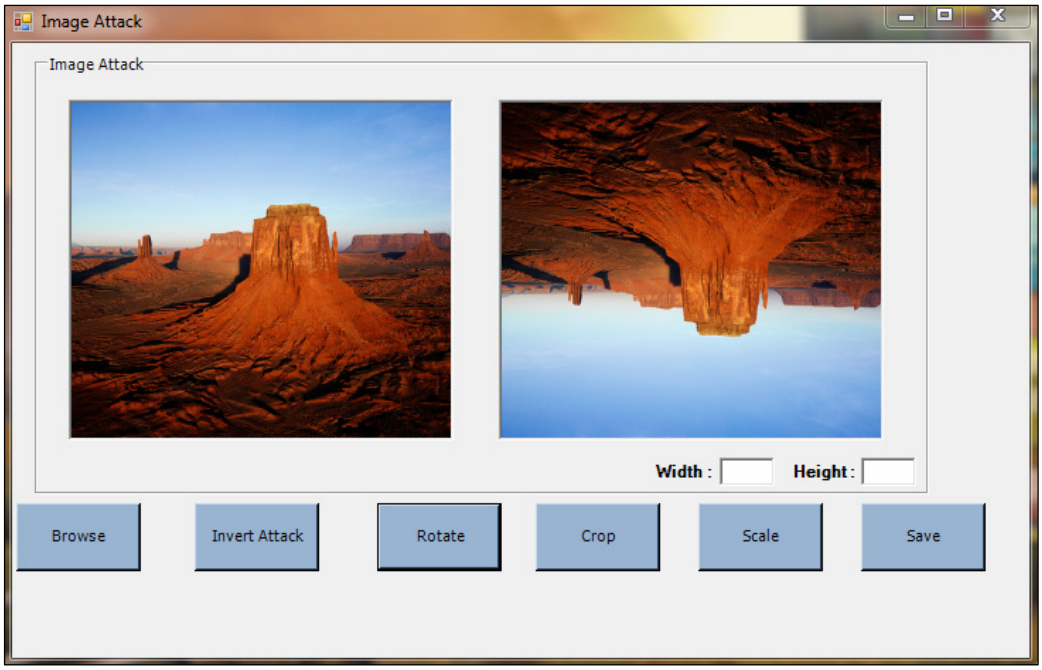

Figure 4.14 Rotate Attack

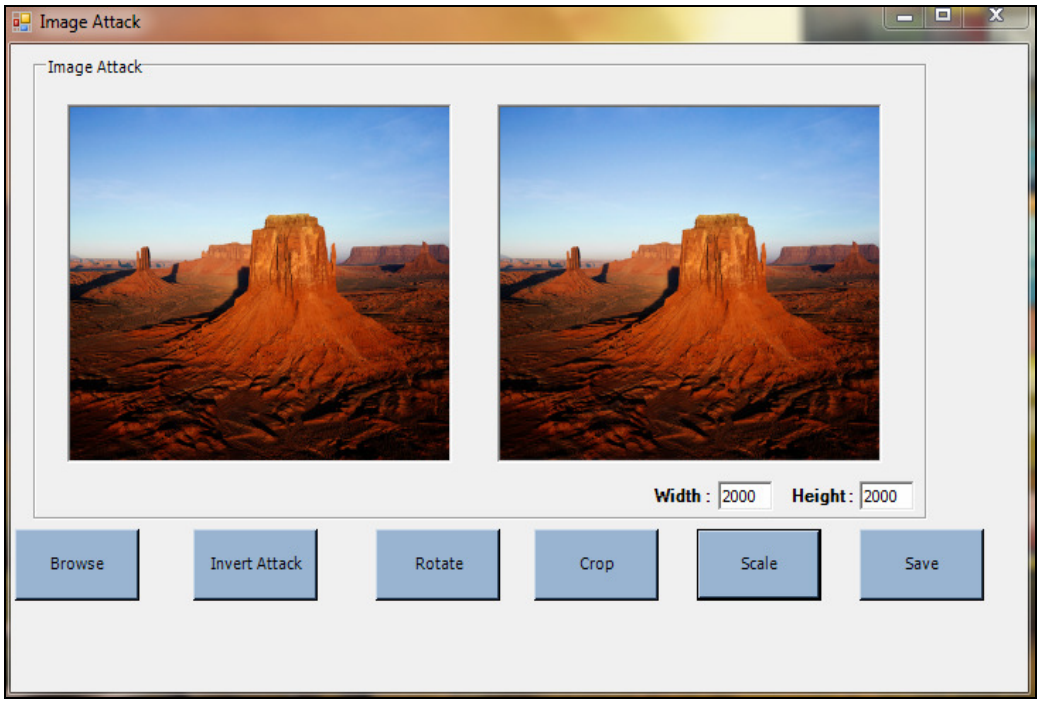

Figure 4.15 Scale Attack

After attacking the above image, we can extract the original image using the Extract part of the DWT process.

Figures 4.16, 4.17, 4.18, 4.19 show the attack image using the Image Attack and how the original images are extracted without any effects of attack process.

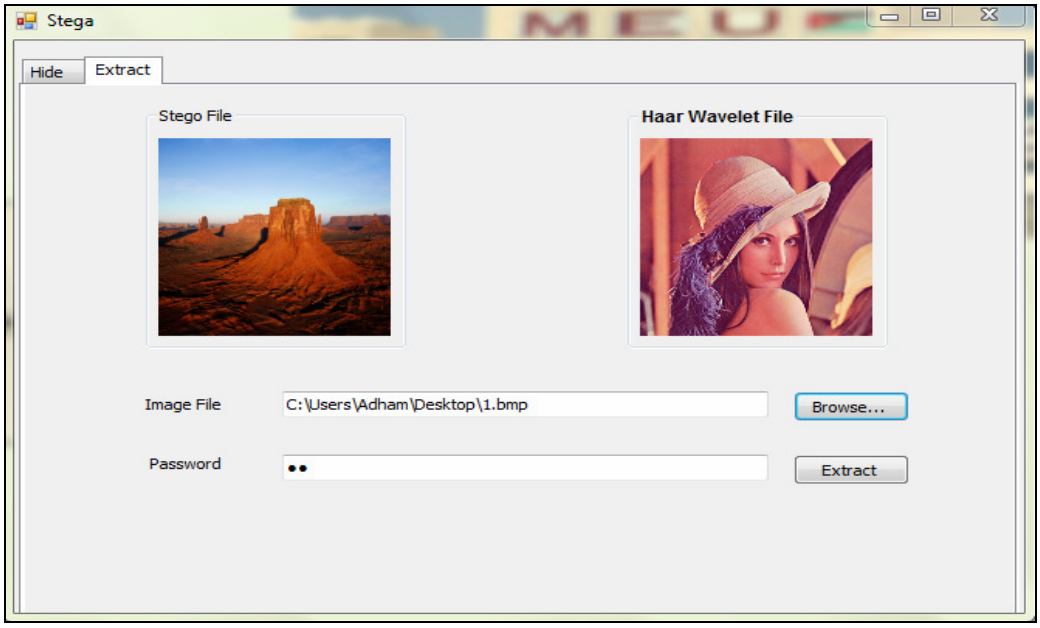

Figure 4.16 Extact original image from attack image scale

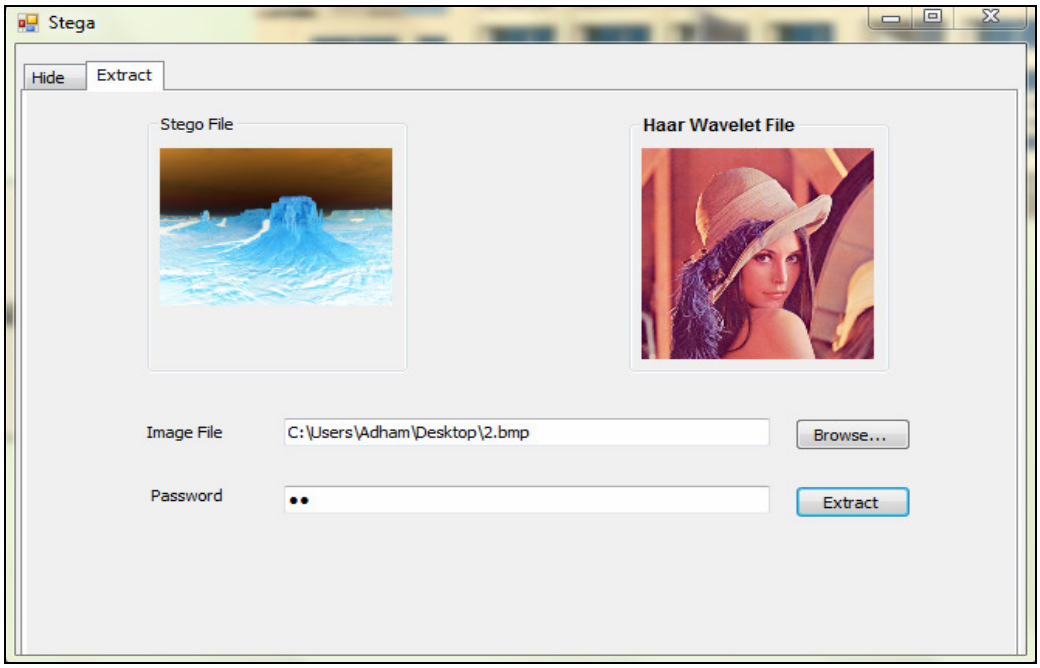

Figure 4.17 Extact original image from attack image invert

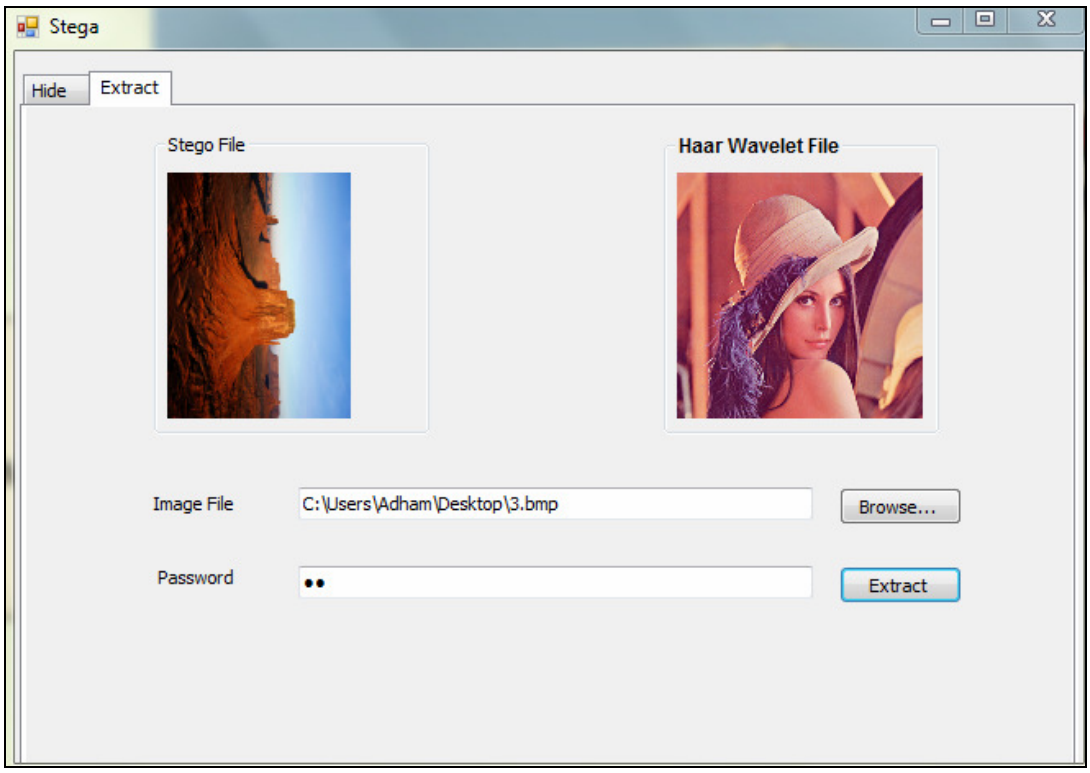

Figure 4.18 Extact original image from attack image rotate

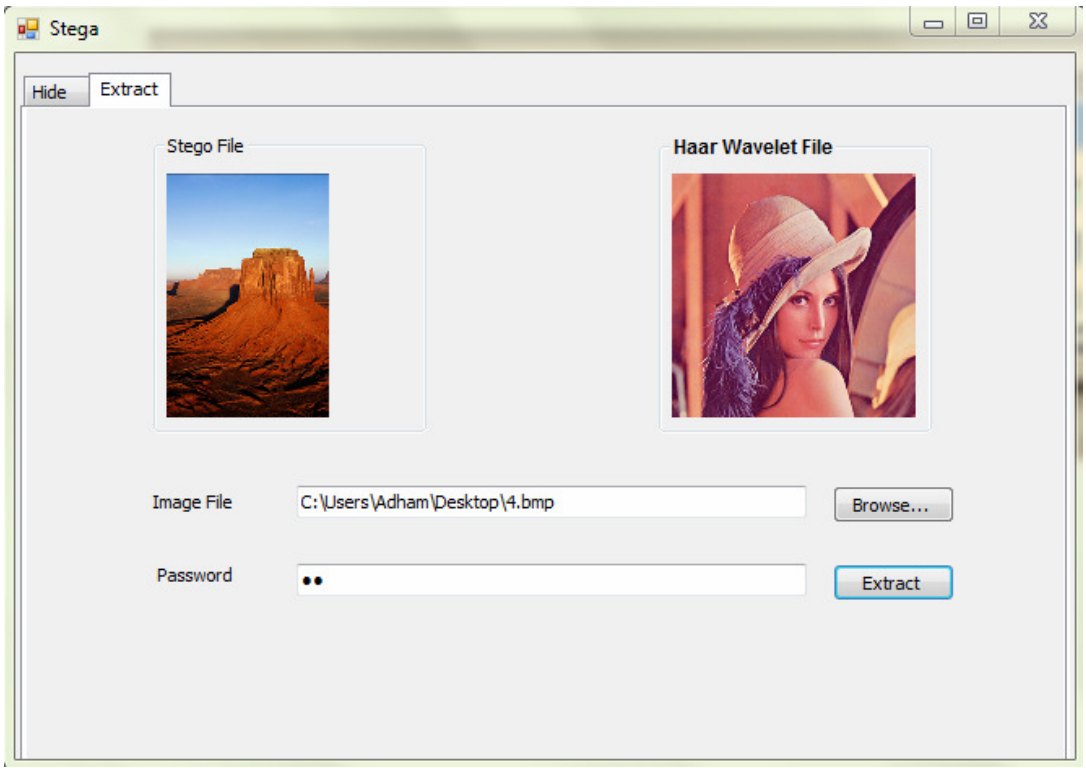

Figure 4.19 Extact original image from attack image crop

4.3 Discussions

The robustness of the generated images based on the proposed system is tested using different types of attacks (Invert, Rotate, Crop, and Scale). We created a program called "Image Attack" that will be used to attack the watermarking image resulted from the proposed system.

The proposed digital image watermarking algorithm is constructed by cascading two different but complementary techniques: the Discrete Wavelet Transform and Haar Wavelet Transform to provide robustness image to all attacks. The algorithm proved resistance against numerous image manipulations. Furthermore, the method is easy to implement and suitable for real time applications. Adding a private key to the new technique gives more robustness and security to the watermarked image against attacks.

The based embedding in the second algorithm allows watermark image to be hidden in this image that gives a clear superiority of the algorithm. This technology has been proposed to solve the problem of illegal manipulation and distribution of digital image. Therefore, DWT and HWT techniques are used in our proposed system, and because it is more robust against transmission and decoding errors, it is computationally efficient and can be implemented by using simple filter convolution.

DWT- HWT are compared with HWT, both methods are the digital watermarking techniques coming from Transform Domain category, therefore, they have some features in common. However, they have some variant characteristics. Performance comparison between DWT- HWT and HWT is summarized in the next paragraphs. Moreover, we used in this comparison the PSNR (Peak Signal-to-Noise Ratio), to show the effects of the attacked images and how it robustness against different types of attacks.

The PSNR is defined as:

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right)$$
$$= 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right)$$

Here, MAX1 is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented using linear with B bits per sample, MAX1 is 2B-1.

It is most easily defined via the Mean Squared Error (MSE) which for two m*n monochrome images I and K where one of the images is considered a noisy approximation of the other is defined as:

$$MSE = \frac{1}{m\,n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

The following examples show the effect of different types of attacks on the images that watermarked using HWT-DWT and HWT.

(Note: the results are generated by using the PORCUPINE software, Version 1.2.2)

Figure 4.20 HWT image without attack.

PSNR value=16.7838db.

Figure 4.21 HWT image after Invert and Noise attack.

PSNR value=12.5846db.

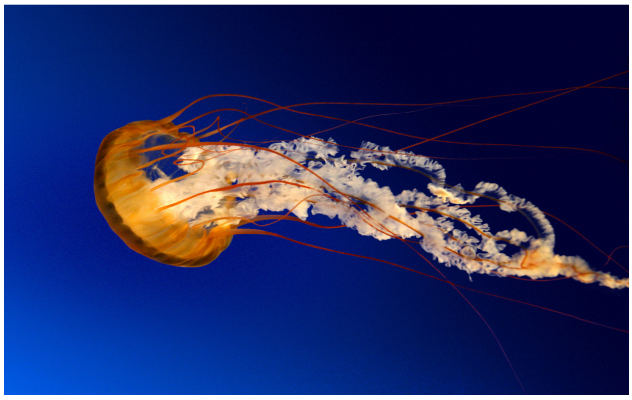

Figure 4.22 HWT-DWT image without attack

PSNR value=37.52231db.

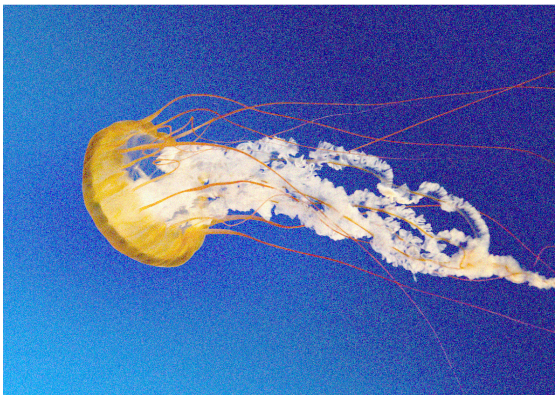

Figure 4.23 HWT-DWT images After Invert and Noise attack.

PSNR value=28.3914db.

Figure 4.24 HWT-DWT image without attack

PSNR value=49.3914db.

Figure 4.25 HWT-DWT images

After Invert.

PSNR value=38.5894db.

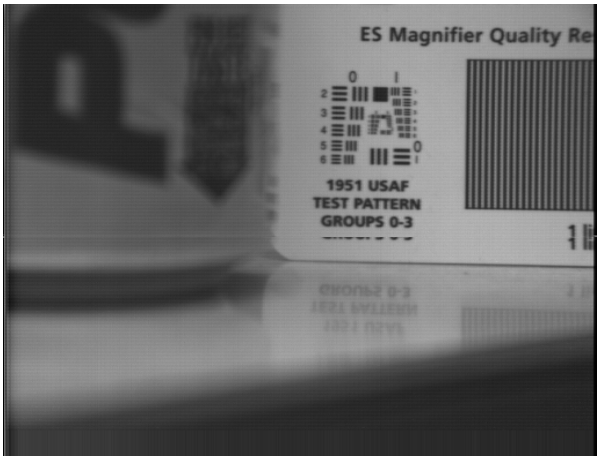

Figure 4.26 HWT-DWT image without attack

PSNR value=50.3914db.

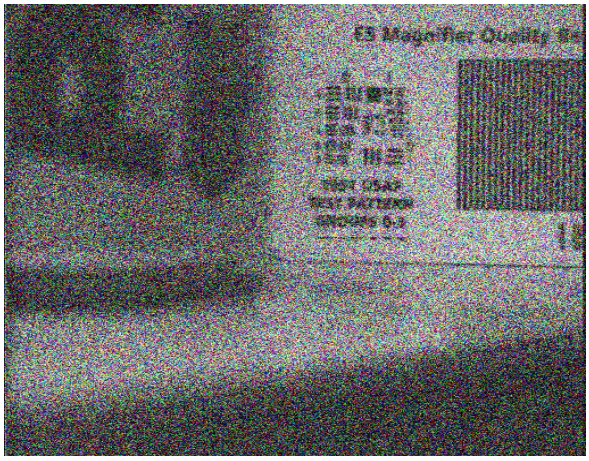

Figure 4.27 HWT-DWT images

After Noise.

PSNR value=39.2714db.

Therefore, from the above examples we can show that the robustness of the proposed system has been improved by using two powerful techniques HWT and DWT. For the sake of performance and comparison, we also evaluated the watermarking when HWT-only were used. The evaluated results show better performance using the cascaded HWT and DWT.

Furthermore, comparing our proposed method (HWT-DWT) with (DWT-DCT) (Al – Haj, 2007) exploits strength of two common frequency domains method; HWT and DWT, to obtain higher efficiency and performance. The quality of each watermarks, which is extracted by exploiting the proposed method, is superior to that of why DWT-DCT method. In the following several watermarking attacks, including inverting and noising, are simulated to investigate the robustness of our watermarking method. The experimental results for the cases of attacks related to figures (4.25 and 4.27), are shown it table 4.1.

Figure No.	PSNR	
	Al-Haj's	Proposed Method
(4.27) HWT-DWT images After Noise.	37.88db.	39.2714db.
(4.25) HWT-DWT images After Invert.	37.26db.	38.5894db

Table 4.1 Comparing PSNR of Al-Haj's with Proposed Method

CHAPTER FIVE

CONCLUSIONS AND FUTURE WORKS

Chapter Five

Conclusions and Future Works

5.1 Conclusions

It is concluded from this thesis relating the proposed system that represents a new method (HWT-DWT) constructed by cascading two different but complementary techniques for image protection by using watermarking technique. Such technique is considered one of the powerful and robust schemes in protection process. Wavelet transformation (HWT-DWT) provides robust resistance to the protected image against manipulation and forgery attacks. Adding a private key (password) to the watermarking will increase the privacy and security, but by embedding watermark along with adding the private key (password) more protection in wavelet transform will result, leading to more resistance against attacks. A new technique has been proposed to solve the problem of illegal manipulation and distribution of digital image, i.e. HWT and DWT system. By comparing the response of this system with that of the DWT-DCT, it (HWT-DWT) shows the robustness of our proposed method in illustrating through comparing different types of attacks on the images and the relevant generated values (PSNR).

5.2 Future Works

In order to expand the system that proposed in this thesis, several recommendations for future works are suggested including improving the proposed system to deal with different types and size of image files as well as, expanding the proposed system to include a new embedding algorithms and encryption keys. It is recommended to use new techniques for wavelet transformation, such as, wavelet net or multiple wavelets. Also the proposed system could be extended to cover the protection of other files such as document, audio and video files. The neural technique could also be used to choose a region from the image to embed the watermarking one.

REFERENCES

References

Al-Haj, A. (2007). "Combined DWT-DCT Digital Image Watermarking". Princess Sumaya University for Technology Department of Computer Engineering, PP.1549-3636.

Amin, M.M., Salleh, M., Ibrahim, S., & Katmin, M. (2003). "Information Hiding Using Steganography", work paper 4th National Conference on Telecommunication Technology Proceeding 2003, Concorde Hotel, Shah Alam, Selangor,PP.21-25.

Anirban, D., Anindya, H., & Swapna Banerjee. (2010). “An Efficient Architecture for 3-D Discrete Wavelet Transform”. IEEE Transactions on Circutts and Systems for Video Technology, VOL. 20, NO. 2.

Cabir, V., & Serap., K. (2007). “Image Normalization and Discrete Wavelet Transform Based Robust Digital Image Watermarking”.Computer Engineering Sakarya University, VOL. 56 Part B.

Cachin, C. (1998). “An Information-Theoretic Model for Steganography”. 2nd Information Hiding Workshop, VOL. 1525, PP.306-318.

Chiou-Tign, H., & Ja-Ling-Wu. (1998). “DCT-Based Watermarking for Video”. IEEE Transactions on Consumer Electronics, VOL. 44, NO.1.

Cox, I.J., Kilian, J., Leighton, F.T., & Shamoon, T. (1997). “ Secure Spread Spectrum Watermarking for Multimedia”. IEEE Transactions on Image Processing, VOL. 6, NO. 12, PP.1673–1678.

Cox, I.J., Miller, M.L. & Bloom, J.A. (2000). “Watermarking and Their Properties”. Proceedings of the International Conference on Information Technology: Coding and Computing, ITCC 2000, Las Vegas, NV.

Cox, I.J., Miller, M.L., & Bloom, J.A., (2002), "Digital Watermarking", San Francisco: Morgan Kaufmann Publishers.

Darmstaedter, V., Delaigle, J.F., Quisquater, J.J., & Macq, B. (1998). "Low Cost Spatial Watermarking". Computer & Graphics, VOL. 22, NO.4, PP.417-424.

Dittmann, J. (2000). "Digitale Wasserzeichen: Grundlagen, Verfahren, Anwendungsgebiete". Berlin: Springer IEEE Computer Society Press Los Alamitos, VOL 8 , Issue 4 , PP 54 - 65.

Fionn M. (2007). "The Haar Wavelet Transform of a Dendrogram". Royal Holloway, Journal of Classification.University of London NO.24, PP.3-32.

Grans L. (2003). "Multiresolution Watermark Based on Wavelet Transform for Digital Images". University of British Columbia.

Haldar P. (2008). "Watermarks". parallax, VOL.14, NO.4, PP. 101–113.

Hanjalic, A., Langelaar, C., van Roosmalen, G., Biemond, J., & Langendijk, L. (2000). "Image and Video Databases: Restauration, Watermarking and retrieval". Elsevier, scieule,1stED.

Hartung, F., Su, J.K., & Girod, B. (1999). "Spread Spectrum Watermarking: Malicious Attacks and Counterattacks". Proceedings

of SPIE Electronic Imaging '99, Security and Watermarking of Multimedia Contents, San Jose, CA.

Houng-Jyh, S., & Kuo .C.-C, J. (1998). "Wavelet-Based Digital Image Watermarking". University of Southern California,optics Exprecs, Issue 12, VOL.13, NO.491.

Ilker, Bayram., & Ivan W. Selesnick. (2009). "Overcomplete Discrete Wavelet Transforms With Rational Dilation Factors". VOL.57, NO. 1, PP. 131-145.

Inoue, H., Miyazaki, A., & Katsura, T. (1999). "An Image Watermarking Method Based on the Wavelet-Transform". Proc. Of ICIP, VOL. 3, PP.296-300.

Katzenbeisser, S., & Petitcolas, F. (2000). " Information Hiding: Techniques for Steganography and Digital Watermarking". Norwood, MA: Artech House Books, Neswpape Article from:Telecom Worldwire,ISBN:1-58053-035-4 .

Kunder, D., & Hatzinko, D. (2001). "A Robust Digital Image Watermarking Method Using Wavelet-Based Fusion". University of Toronto.

Kutter, M., & Hartung, F. (2000). "Introduction to Watermarking Techniques".In S. Katzenbeisser & F.A.P. Petitcolas (Eds.),

Information Hiding Techniques for Steganography and Digital Watermarking. Boston:Artech House.

Lepik, Ü. (2007). "Application of the Haar wavelet Transform to Solving Integral and Differential Equations". Institute of Applied Mathematics, University of Tartu, Proc. Estonian Acad. Sci. Phys, VOL. 56, NO. 1, PP.28–46.

Leung, Y., Cheng, M., & Cheng, L. (2009). "A Robust Watermarking Scheme Using Selective Curvelet Coefficients". Department of Electronic Engineering, City University of Hong Kong, VOL. 7, NO. 2, PP.163–181.

Lin, T., & Delp, J. (1999). "A Review of Data Hiding in Digital Images". in Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference, PICS '99, Ed., PP.274-278.

Min-Jen, Tsai. (2009). "A Visible Watermarking Algorithm Based on The Content and Contrast Aware (COCOA) Technique". National Chiao Tung University, Institute of Information Management, J. Vis. Commun. Image R, NO. 20, PP.323–338.

Paquet, A. (2001). "Multiresolution Watermark Based on Wavelet Transform for Digital Images". Project Report, University of British Columbia.

Radomir, S., & Bogdan, b. (2003). "The Haar Wavelet Transform: Its Status and Achievements". Nanyang Technological University, School of Electrical and Electronic Engineering.

Robi, P. (2004). "The Wavelet Tutorial". Rowan University, College of Engineering.

Stephan, J. (2005). "Image Watermarking Using Wavelet Transform". University Sts. Cyril and Methodius, Faculty of Electrical Engineering.

Taskovski .D, Bogdanova .S., & Bogdanov , M. (1999). "Digital Watermarking in Wavelet Domain", University Sts. Cyril and Methodius, Faculty of Electrical Engineering.

Talukder, K., & Harada, K. (2007), "Haar Wavelet Based Approach for Image Compression and Quality Assessment of Compressed Image". IAENG International Journal of Applied Mathematics, online publication, VOL.36, pp.1-9.

Wolfgang, B., Podilchuk, I., & Delp J. (1999). "Perceptual Watermarks for Images and Video". Proceedings for IEEE, Trans.on Image Processing VOL. 87, NO.7.

Wu a, N.-I., Wanga, C.-M., Tsaib, C.-S., & Hwangb, M.-S. (2008). "A Certificate-Based Watermarking Scheme for Colored Images".

aInstitute of Computer Science and Engineering, National Chung Hsing University, VOL. 6.

Yeung, M., Teo, B., & Holliman M. (1998). “Digital Watermarks: Shedding Ligith on The Invisible”. Intel Corporation.