



**COPYRIGHT PROTECTION USING DIGITAL WATERMARKING**

**HASSAN FAKHRY HASSAN ALLAYLA**

**FEBRUARY 2017**

**COPYRIGHT PROTECTION USING DIGITAL WATERMARKING**

**A THESIS SUBMITTED TO  
THE GRADUATE SCHOOL OF NATURAL AND APPLIED  
SCIENCES OF  
ÇANKAYA UNIVERSITY**

**BY  
HASSAN FAKHRY HASSAN ALLAYLA**

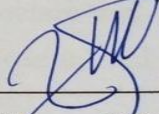
**IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE  
DEGREE OF  
MASTER OF SCIENCE  
IN  
THE DEPARTMENT OF  
COMPUTER ENGINEERING**

**FEBRUARY 2017**

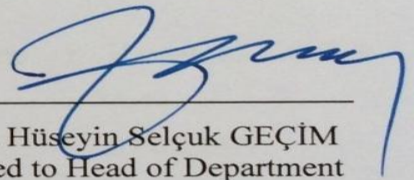
The title of the Thesis: **Copyright Protection Using Digital Watermarking.**

Submitted by **Hassan Fakhry Hassan Allayla**

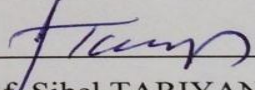
Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.

  
\_\_\_\_\_  
Prof. Dr. Halil Tanyer EYYÜBOĞLU  
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

  
\_\_\_\_\_  
Prof. Dr. Hüseyin Selçuk GEÇİM  
Entrusted to Head of Department

This is to certify that we have read this thesis and that in our opinion; it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

  
\_\_\_\_\_  
Assist. Prof. Sibel TARIYAN ÖZYER  
Supervisor

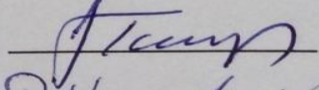
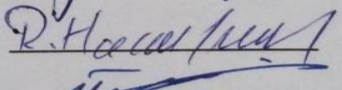
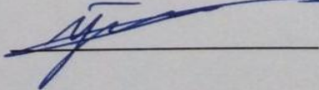
**Examination Date: 07.02.2017**

**Examining Committee Members**

Assist. Prof. Sibel TARIYAN ÖZYER (Çankaya Univ.)

Assist. Prof. Reza Zare HASSANPOUR (Çankaya Univ.)

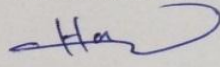
Assist. Prof. Uğur BAÇ (Atılım Univ.)

## STATEMENT OF NON-PLAGIARISM PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : Hassan ALLAYLA

Signature : 

Date : 07.02.2017

## **ABSTRACT**

### **COPYRIGHT PROTECTION USING DIGITAL WATERMARKING**

ALLAYLA, Hassan Fakhry

M.Sc., Department of Computer Engineering

Supervisor: Assist. Prof. Dr. Sibel TARIYAN ÖZYER

February 2017, 64 pages

The digital techniques have greatly smooth data representation and data storage. However, the content of the data without distortion is easy to edit and copy in digital media, and this situation has resulted in a series of security problems over the widespread of using the network. For example, users can easily access, edit, or distribute data in digital media. Therefore, how to guarantee copyright protection and the integrity of the content of digital media has become an emergent issue. Digital watermarking has been proposed as a solution to the problem of resolving copyright ownership of multimedia data (image, audio, and video). In this thesis, we have proposed a copyright protection using private watermarking algorithm. The algorithm is based on multi techniques of frequency domain such as: Two Dimensional Discrete Cosine Transform and Multi-Level Two Dimensional Discrete Wavelet Transform. The proposed

algorithm is built by using the secret key which is coded in the embedding side by using the secure hash algorithm (SHA-1) to increase the security of the proposed study.

In this thesis, we used some fidelity criteria (such as: the peak signal to noise ratio, the normalized cross correlation and the normalized hamming distance) for measuring the performance on some different standard gray scale images. The robustness of the proposed algorithm was tested on different types of noises.

**Keywords:** Copyright protection; Digital watermarking, Two Dimensional Discrete Cosine Transform, Multi-level Two Dimensional Discrete Wavelet Transform.

## ÖZ

### SAYISAL DAMGALAMA KULLANARAK TELİF HAKKI KORUMASI

ALLAYLA, Hassan Fakhry

Yüksek Lisans, Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı: Yrd. Doç. Dr. Sibel TARIYAN ÖZYER

Şubat 2017, 64 Sayfa

Sayısal teknikler fazlasıyla düzgün veri temsiline ve veri depolamasına sahiptirler. Bununla birlikte, sayısal ortamda verinin içeriğinin bozukluk olmadan düzenlemesi ve kopyalaması kolaydır, ve bu durum ağ kullanımında yaygın bir dizi güvenlik problemine neden olmaktadır. Örneğin, sayısal ortamda kullanıcılar kolaylıkla veriye ulaşabilirler, düzenleyebilirler, ve dağıtabilirler. Bu nedenle, telif hakkı korumasının nasıl garanti edileceği ve sayısal ortamın bütünlüğü yeni bir konu olarak ortaya çıkmaktadır. Sayısal damgalama, çoklu ortam (görüntü, ses, video) verisinin telif hakkı çözmesinde çözüm olarak sunulmuştur. Bu tezde, özel damgalama algoritması kullanarak telif hakkı koruması sunmaktayız. Algoritma, frekans alanında çoklu teknik temellidir: İki boyutlu ayrık kosinüs dönüşümü, Çok katmanlı iki boyutlu ayrık dalgacık dönüşümü gibi. Önerilen algoritma gizli anahtar kullanılarak gömülü tarafta gizli hash algoritması (SHA-1) kodlanması ile sunulan çalışmanın güvenilirliğini artırmak için yapılmıştır. Bu tezde, uygunluk derecesi (sinyal gürültü oranı, normalize edilmiş çapraz korelasyon ve normalize edilmiş hamming mesafe gibi) farklı standartlardaki gri görüntüler

üzerindeki performansı ölçmek için kullandık. Önerilen algoritmanın sağlamlığı farklı gürültü türlerinde test edilmiştir.



**Anahtar Kelimeler:** Telif hakkı koruması, Sayısal damgalama, İki boyutlu ayrık kosinüs dönüşümü, Çok katmanlı iki boyutlu ayrık dalgacık dönüşümü.



## ACKNOWLEDGMENTS

Foremost, I am grateful to Allah for giving me the force that was necessary to complete this thesis.

I would like to thank my supervisor Assist. Prof. Sibel Tariyan for her continuous support, encouragement and advice in writing my thesis. Thanks are due to all the academic staff in the department of computer engineering for their efforts throughout the study period.

I would like to thank, my parents and my family for their unconditional support, kindness, and for having allowed with their efforts, to get to where I am now.

## TABLE OF CONTENTS

STATEMENT OF NON PLAGIARISM.....	iii
ABSTRACT.....	iv
ÖZ.....	vi
ACKNOWLEDGEMENTS.....	viii
TABLE OF CONTENTS.....	ix
LIST OF FIGURES.....	xiii
LIST OF TABLES.....	xv
LIST OF ABBREVIATIONS.....	xvi

### CHAPTERS:

<b>1. INTRODUCTION.....</b>	<b>1</b>
<b>1.1. General Review .....</b>	<b>1</b>
<b>1.2. Information of Data Hiding .....</b>	<b>1</b>
<b>1.2.1. Cryptography.....</b>	<b>2</b>
<b>1.2.2. Steganography.....</b>	<b>3</b>
<b>1.2.3. Watermarking.....</b>	<b>3</b>
<b>1.3. Literature Review.....</b>	<b>3</b>
<b>1.4. Thesis Aim.....</b>	<b>5</b>
<b>1.5. Thesis Organization.....</b>	<b>6</b>
<b>2. BACKGROUND THEORY.....</b>	<b>7</b>
<b>2.1. Overview.....</b>	<b>7</b>
<b>2.2. Watermarking Copyright Protection .....</b>	<b>7</b>
<b>2.3. Stimulus.....</b>	<b>7</b>
<b>2.4. Watermarking Embedding Process .....</b>	<b>8</b>
<b>2.5. Watermarking Properties.....</b>	<b>8</b>

2.6.	Digital Watermark Application.....	9
2.7.	Classification of Watermark Algorithms.....	10
2.8.	Attacks on Watermarking.....	13
2.8.1.	Classification of Watermarking Attacks.....	13
2.8.2.	Effect of Noise Attacks on Watermarks.....	14
3.	WATERMARKING ALGORITHMS AND THE SECURE HASH ALGORITHM.....	15
3.1.	Overview .....	15
3.2.	Spatial Domain.....	16
3.2.1.	Least Significant Bit Adjustment.....	16
3.2.2.	Spread Spectrum Modulation (SSM).....	16
3.3.	Watermarking Hiding Operations.....	16
3.4.	Watermark Extraction Operations.....	18
3.5.	Transform Domain.....	19
3.5.1.	Transform Domain Watermark Insertion and Detection.....	19
3.5.2.	Discrete Fourier Transform (DFT).....	20
3.5.3.	Discrete Cosine Transform (DCT).....	20
3.5.3.1.	One Dimension Discrete Cosine Transform.....	20
3.5.3.2.	The Two Dimensional Discrete Cosine Transform....	21
3.5.3.3.	Advantages of DCT.....	22
3.5.3.4.	Disadvantages of DCT.....	22
3.5.4.	The Discrete Wavelet Transforms (DWT).....	22
3.5.4.1.	The One Dimensional Discrete Wavelet Transform..	23
3.5.4.2.	The Two Dimensional Discrete Wavelet Transform..	24
3.5.4.3.	Advantages of DWT.....	26
3.5.4.4.	Disadvantages of DWT.....	26
3.6.	The Secure Hash Algorithm.....	26

3.6.1.	Secure Hash Algorithm Family (SHA).....	26
3.6.2.	Hash Message Authentication Code (HMAC).....	27
4.	THE PROPOSED ALGORITHMS AND THE MEASURMNET.....	29
4.1.	The Proposed Copyright Watermark Embedding Algorithm.....	30
4.2.	The Suggest Copyright Watermark Extracting Algorithm.....	34
4.3.	Metrics for Quality.....	36
4.3.1.	Peak Signal to Noise Ratio (PSNR).....	36
4.3.2.	Normalized Correlation Coefficient (NCC).....	37
4.3.3.	Normalized Hamming Distance (NHD).....	38
4.4.	The Graphical User Interface Model.....	38
4.4.1.	The Graphical User Interface Model of Embedding and Extracting.....	38
5.	THE NOISE EFFECT OF THE COPYRIGHT WATERMARKING ALGORITHM.....	44
5.1.	Noise Modelling and Digital Image Filtering .....	44
5.2.	Noise Types.....	45
5.2.1.	Impulse Noise (Salt and Pepper Noise).....	45
5.2.2.	Gaussian Noise (Amplifier Noise).....	47
5.2.3.	Poisson Noise.....	48
5.2.4.	Speckle Noise.....	49
5.2.5.	Gamma Noise.....	49
5.2.6.	Mean Filter.....	50
5.2.7.	Median Filter.....	51
5.2.8.	Adjustment Filter.....	51
5.3.	The Graphical User Interface Model of Multi Type of Noise.....	52
6.	CONCLUSIONS AND FUTURE WORK.....	62
6.1.	Conclusion.....	62

6.2. Future Works.....	64
REFERENCES.....	R1
APPENDICES A.....	A1
CURRICULUM VITAE.....	A1



## LIST OF FIGURES

### FIGURES

<b>Figure 1</b>	Types of Information Hiding .....	2
<b>Figure 2</b>	Process of embedding watermark.....	8
<b>Figure 3</b>	Classification of Watermarking algorithms.....	12
<b>Figure 4</b>	Watermarking techniques classification.....	15
<b>Figure 5</b>	Watermark hiding algorithm.....	17
<b>Figure 6</b>	Watermark extraction algorithm .....	18
<b>Figure 7</b>	Block diagram of the transform domain watermark insertion...	19
<b>Figure 8</b>	Block diagram of the transform domain watermark detection...	20
<b>Figure 9</b>	The one dimensional discrete wavelet transforms.....	23
<b>Figure 10</b>	The three levels one dimensional discrete wavelet transforms..	24
<b>Figure 11</b>	The block diagram of one level 2D –DWT.....	25
<b>Figure 12</b>	Sub-bands after applying second and third decomposition levels.....	25
<b>Figure 13</b>	The hashing Process.....	27
<b>Figure 14</b>	The block diagram of HMAC.....	28
<b>Figure 15</b>	The block diagram preconditioning operations.....	31
<b>Figure 16</b>	The time diagram of proposed alorithm.....	32
<b>Figure 17</b>	The flowchart of the copyright watermarking algorithm.....	33
<b>Figure 18</b>	The proposed copyright watermark extracting algorithm.....	35
<b>Figure 19</b>	The graphic user interface of the proposed algorithm.....	39
<b>Figure 20</b>	The implementation of step 1,2,3 and 4 of our GUI model.....	39
<b>Figure 21</b>	The message of correct password.....	40
<b>Figure 22</b>	The message of false password.....	40
<b>Figure 23</b>	The implementation extracting part our GUI model.....	41
<b>Figure 24</b>	Gray scale image before and after watermarking and the message.....	41
<b>Figure 25</b>	The central pixel value is corrupted by Pepper noise.....	45
<b>Figure 26</b>	The likelihood density function of salt & pepper noise.....	46
<b>Figure 27</b>	The Salt &Pepper noise with different density of noise.....	46
<b>Figure 28</b>	The probability density function of gaussian noise.....	47
<b>Figure 29</b>	The effect of gaussian noise.....	48
<b>Figure 30</b>	The effect of poisson noise.....	48

<b>Figure 31</b>	The effect of speckle noise.....	49
<b>Figure 32</b>	The probability density function of gamma noise.....	50
<b>Figure 33</b>	The effect of gamma noise.....	50
<b>Figure 34</b>	The effect of different type of size of mean filter.....	50
<b>Figure 35</b>	The effect of median filter.....	51
<b>Figure 36</b>	The effect of image adjustment.....	51
<b>Figure 37</b>	The eight types of noise in GUI model.....	52
<b>Figure 38</b>	The message of choosing variance value.....	52
<b>Figure 39</b>	The message of salt & pepper density.....	53
<b>Figure 40</b>	The question message of choosing gamma.....	55
<b>Figure 41</b>	The gray scale images used to show noise effect.....	57
<b>Figure 42</b>	The PSNR in dB of different references and our study without noise.....	63
<b>Figure 43</b>	The effect of many type of noises in watermarking algorithms..	63

## LIST OF TABLES

### TABLES

<b>Table 1</b>	The fidelity criteria of the proposed algorithm .....	42
<b>Table 2</b>	the results for applying three level on standard images.....	43
<b>Table 3</b>	The gaussian noise with $\sigma=0.005, 0.015$ and $0.10$ .....	53
<b>Table 4</b>	The effect of salt and pepper with $d=0.01, 0.02$ and $0.04$ .....	54
<b>Table 5</b>	The effect of many type of noises.....	55
<b>Table 6</b>	The effect of adjustment noise with $\text{Gamma}=0.4, 0.8$ and $1.5$ ....	56
<b>Table 7</b>	The Effect of different noise on the used images.....	58
<b>Table 8</b>	Effect of gaussian noise for different variance values.....	59
<b>Table 9</b>	Effect of salt & peppers for different density values.....	60
<b>Table 10</b>	Effect of adjustment noise for different gamma values.....	61



## LIST OF ABBREVIATIONS

DIAS	Digital Image Authentication System
DWT	Discrete Wavelet Transform
SVD	Singular Value Decomposition
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio
DCT	Discrete Cosine Transform
DFT	Discrete Fourier transform
2-D DWT	Two Dimension Discrete Wavelet Transform
FT	Fourier Transform
SSM	Spread Spectrum Modulation
MD	Message-Digest algorithm
MD5	Message-Digest algorithm 5
SHA	Secure Hash Algorithm
NIST	National Institute of Standards and Technology
HMAC	Hash-based Message Authentication Code
MAC	Message Authentication Code
db	decibel
NCC	Normalized Cross Correlation
NHD	Normalized Hamming Distance
GUI	Graphical User Interface
PDF	Probabilty Density Function

## **CHAPTER 1**

### **INTRODUCTION**

#### **1.1. General Review**

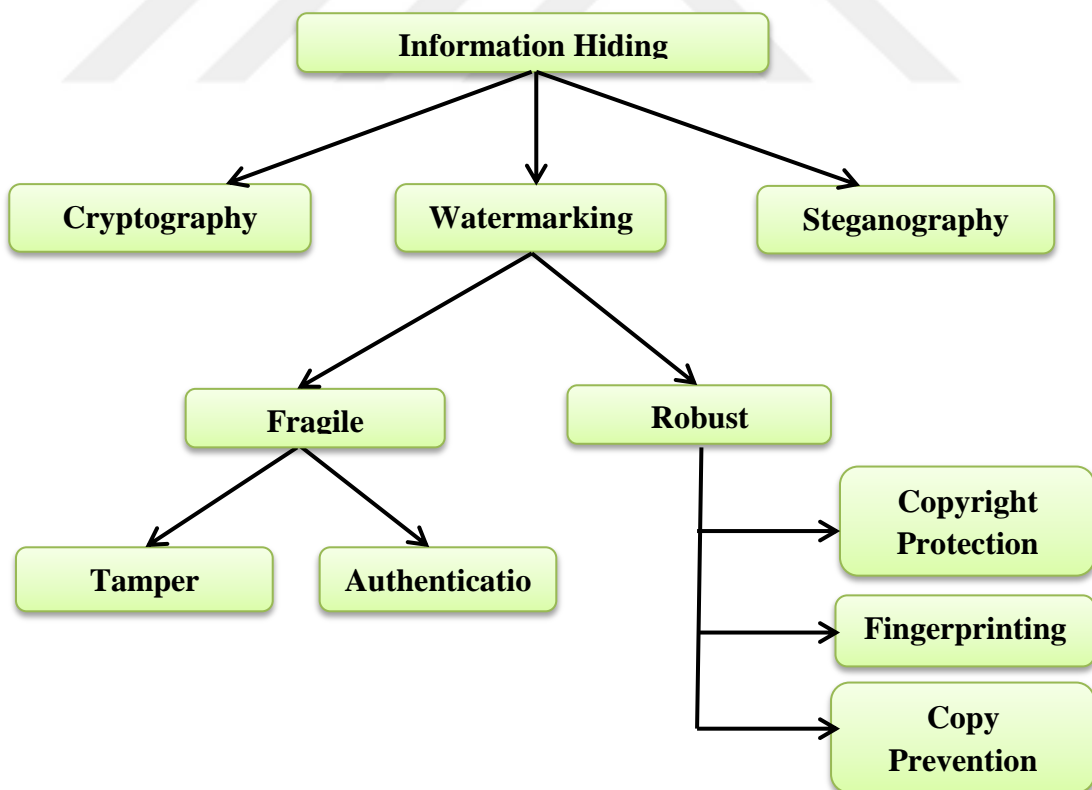
The expansion of the internet and digital information usage for many applications, clinical, scientific, and social opportunities have led to greater demand for the authentication of the given information [1]. The entrance for an authenticating client has become generic, which leads to the problem of copyright assurance of data. Copyright assurance of outsourced data is considered as a genuine aim in today's online database utilization and in numerous applications. WATERMARKING is a procedure for hiding information that's utilized to validate the provenance of information. Unauthorized copying can be detected; It has depended on the availability of a noise transmission area with which the information can be adjusted while retaining its fundamental properties [2].

#### **1.2. Information Hiding**

Information hiding means that the system hides a special piece of data (such as a signature) which refers to the owner in the original data and recovers the original data from any multimedia data. The multimedia data include: image, sound, video and text. Information hiding is a general term containing of three forms: cryptography, steganography and watermarking. (It appears in Figure 1). According to the application type the watermarking can be strong or delicate [3].

### 1.2.1. Cryptography

It is one of the techniques of transforming copyrighted digital content into an ambiguous format. Generally, the information that can be recognized without extraordinary transaction is called plaintext. The protected plain content, which is messy, is called cipher textual content. The technique of changing plain content into cipher text content is referred to as encryption. The protected message is available to the trusted users only if they have the unscramble key. The process of changing back cipher text to its initial plaintext is called decryption. We use encryption to guarantee that the information is not validated to every one even who can see the secured information. Just authenticated users who have a mystery key that can decode the information message in plain content. Cryptography is utilized to secure email data, SMS, MasterCard date, passwords, and other mystery data. It is the most established approach to hide vital information while going over the computerized correspondence medium [3].



**Figure 1** Types of information hiding [3].

### **1.2.2. Steganography**

The term steganography originates from the Greek Stefanos, which indicate to cover and graph. Steganography is the realization of important data, so that the unauthorized person can not discover it. The data is encoded in a way that the very presence of this data is covered up. The fundamental objective of steganography is to import data safely in an undetectable style. In the event that a steganography strategy gives the trust to suspect user to transporter medium, then the technique has been unsuccessful [3].

### **1.2.3. Watermarking**

The term watermarking (data hiding) means data covering, a watermarking technique used to hide (embed) given information (data ownership, name, logo or signature) in digital data (text documents, picture and video). This hidden data can later be extracted or detected in the multimedia for security aim.

A watermark is characterized as an undetectable recognizable code that is for all time inserted in the important data, to send concealed information. It stays present the data even after the unscrambling procedure. The watermarking gives copyright assurance of protected innovation, also it is used to perceive the true copyright proprietor of the item [3].

## **1.3. Literature Review**

There are numerous previous works of watermarking in different form here we describe some of them:

In 2010, Jiang Xuehua built a system model of digital watermarking. It had two stages: inserting and extraction. He had utilized Two Dimensions Discrete Cosine Transform (2D-DCT) in his work. He proved that the watermark based on DCT was well as a different image processing such as: cropping, compression and other processing, the watermark data can be extracted regardless of the possibility that it has been assaulted [4].

In 2012, Shankar Thawkar presented a hidden image watermarking scheme for copyright protection. He had used a secret key encryption for concealing the watermark using Least Significant Bit (LSB) technique at the DCT coefficients. The watermark extraction process had used the same key as in encryption, and hence, it can be used for copyright protection of digital media (images, video and audio), this work has minimum computations and a high capacity provided [5].

Also in 2012, Neeraj Bhargava and Et Al. Had been introduced a Digital Image Authentication System (DIAS). The DIAS system is used to specify the ownership of images using watermarking. It consisted of two steps: embedding information inside the image and other for detecting information. In this work, digital watermarking had been performed utilizing Discrete Wavelet Transform (DWT). They proved that the quality of the images did not affect watermarking and the watermark image could be easily read [6].

In 2014, Kumar Ashwani, implemented watermarked image by utilizing a 3-levels DWT transformed. He was embedding the watermark bits into the edges and textures of the picture, i.e. (HL3) and (LH3) sub bands of the image. The outcomes appearance that the watermarking procedure didn't influence on the picture quality and the watermark information can be extracted. He concluded that the security of his work was depending on the embedding and extraction of the watermark. [7].

In 2015, Furqan, Asna, and Munish Kumar, presented digital image watermarking procedure to solve copyright security issue. They utilized DWT and Singular Value Decomposition (SVD) strategies were combining them to get a robust watermarked image. Then applying different attacks on the watermarked image to examine the watermarked strongest, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) values were calculated. This work proved that, a DWT-SVD technique was robustness against attacks such as: geometric attacks and other kinds of signal processing attacks [8].

From the previous literature review of existing related research work, it is concluded that the watermark has been implementing by DWT and DCT because they are simple and robust against attack more than other techniques and most of the other

techniques are complex, and the robustness of the algorithm on variant deformation was not examined enough.

In this thesis, we have proposed a copyright protection using a private watermarking algorithm based on multi techniques of frequency domain such as: (Two Dimensional Discrete Cosine Transform and Multi-level Two Dimensional Discrete Wavelet Transform). The proposed algorithm is built by using the mystery key which is coded in the embedding side by using the Secure Hash Algorithm (SHA-1) to increase the security of the proposed architecture.

#### **1.4. Thesis Aim**

We used digital watermarking to provide copyright protection for digital image. The watermark was considered as a good solution to protect important data such as digital image. There is a big chance to steal images from the web, If you have not integrated your digital image; then a good solution to prove that is inserting a watermark on that image.

In this thesis, we are trying to realize the following goals:

- A strong and robust watermarked image.
- We are done to get the maximum of the PSNR (it is a one of the measurements used to measure the integrity watermarked image).
- We are done to get maximum Normalized Cross Correlation (NCC) (it is a one of the metrics used to calculate the similarity between images).
- We are done to get minimum Normalized Hamming Distance (NHD) (it is used to calculate the identical between the original data and the extracted watermarked data).

To prove the previous goal, has been suggested:

- A new algorithm to realize image copyright protection; therefore we implemented some commonly mathematical principles of transformation in watermarking such as 2D- DCT and 2D- DWT together with other technique such as SHA-1.
- The result of combinations between DWT, DCT and using the Secure Hash Algorithm (SHA-1) giving a robust watermarked image better than other

previous work not only in image quality, but also against some common noise such as: salt & pepper, speckle noise and etc.

## 1.5. Thesis Organization

This thesis consists of six chapters and one appendix where a brief description of each of them at the below:

**Chapter one:** This chapter is an introduction to the copyright protection and watermarking introduced. Then some previous work and attempts to authenticate information and copyright saving by using the watermarking is offered.

**Chapter two:** In this chapter, an overview on the watermark was offered. The base concept of watermarking, watermarking properties, watermarking applications, classification of watermark, then some of the attack and noise on the watermark had been presented.

**Chapter Three:** This chapter has been explaining the purpose of using the transform domain. Then has been discussed the important transformation such as DFT, DCT and multi-level 2D-DWT, has discussed the advantage and the disadvantage of the DCT and DWT has been discussed.

**Chapter Four:** In this chapter, explaining the proposed watermarking algorithm using the 2D-DWT and 2D-DCT with a secure hash algorithm (SHA-1), then have been presented the MATLAB 2015a and its GUI tools have been used to display that algorithm. Then the results will be discussed which can be represented by measure: PSNR, NCC, and NHD.

**Chapter Five:** In this chapter, the noise effect on watermarking has offered noise on different images has been applied and their effects have been shown.

**Chapter Six:** The conclusions and future work.

**Appendices A:** Personal information is offered.

## CHAPTER 2

### BACKGROUND THEORY

Digital watermarking technology is a new algorithm suggested, as a solution to resolve the copyright ownership problem and the originality of digital data, also to prevent illegal modifying, copying and distribution of the data

#### 2.1. Overview

The embedding of a given digital piece of information into digital data (text content, image, audio, video), is called digital watermarking, in which it can be extracted or detected later. It is the preferred decision over the other strategy. For example the cryptography; when we utilize the watermarking the content of the digital data has not been effected. The information of the watermarking inserted through data bits, not only in the headers. Watermarking framework has three phases: generation, encryption and decoding [9].

#### 2.2. Watermarking For Copyright Protection

Digital watermark is the best option for copyright protection of the important information. The robust watermark cannot be directly removed from the watermarked information without extremely corrupting the original data quality, thus; it's suited for copyright protection. It permits the identification of the copyright holder thus protecting user content distribution [10].

#### 2.3. Stimulus

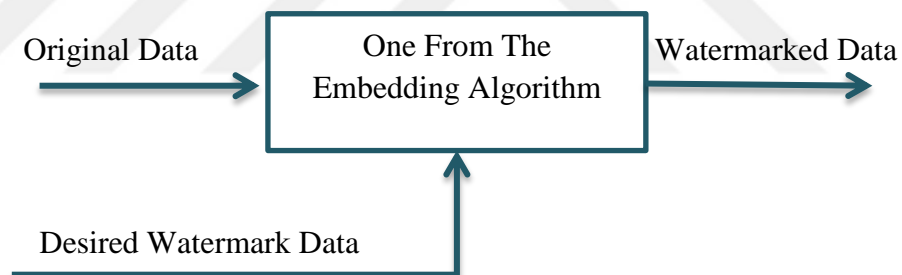
There are many different algorithms in frequency domains and the spatial domains that are used for digital watermarking. The technique in the spatial domain is not strong enough to lousy image compression and other image processing. Same times, a noise in the watermarked image maybe remove the watermark data.



Furthermore, the techniques of the frequency domain can hide additional bits for the watermark and more powerfully against attacks. Various transforms (such as: DCT and DWT) are applied for watermarking applications in the frequency domain. These transforms are being applied in several multimedia standards, for example: MPEG-2, MPEG-4, and JPEG2000 [11].

#### 2.4. Watermarking Embedding Process

The watermark embedding process can be described (Figure 2). The input data is the original data and the desired watermark data. The watermark data may contain the secret key or combination of mystery key and the original data. The first step of the watermarking process is the embedding step. In this step, a cover data is considered and the watermarking data are embedded using a secret key. Before the embedding stage should be selected the watermark data and secret key indicating to the owner. The output of the watermark embedding process is the watermarked data [10].



**Figure 2** Process of embedding watermark [10].

#### 2.5. Watermarking Properties

There are many properties of digital watermarking, the importance of them depending on the application that the watermarking used in it. Some of the common properties are [37] :

- 1- **Transparency (invisibility):** It is indicated to the similarity between watermarked data and the original data. The watermarking should not be effected on the original data or quality of the content.
- 2- **Robustness:** The watermark process is called robust if it is undetectable even some signal processing, such as: lousy compression, spatial filtering, rotation, and translation. The watermark may be robust against some process and fragile against another. A watermark just should be robust against the some signal processing based on the type of application.
- 3- **Capacity:** A watermarking technique should enable to embed amount of information into an original data. That information is called data payload. The information payload in watermarked picture implies the amount of bits secured with the picture.
- 4- **Security:** The watermarked information ought to resist malicious attacks. It must not be easy for an attacker to remove the watermark without harm the information. Specially, he couldn't change the watermark without having the mystery watermark key.
- 5- **Complexity:** The insertion of the watermark might be done just once or many times depending on the application. Consequently, the complexity of the watermark algorithms ought to be simple.

## 2.6. Digital Watermark Application

Digital watermarking applied in many applications. We discuss some of them [40] :

- 1- **Copyright Protection:** It is an application of the watermark, especially in image watermarking. In fact, it inserts copyright information (the rules of using and copying) into the digital data without damage of quality.

- 2- **Owner Identification:** The proprietor distinguishing proof can be embedded as watermark data in the original information to confirm the information ownership.
- 3- **Copy Control:** There are numerous strategies for copy prevention, for example, a client control system to forestall replicating of the information by embedding a never-duplicate watermarking or limit the quantity of replicating times.
- 4- **Authentication:** it means that the ability to find any variation in the information, with the goal that data required for validating the original information.
- 5- **Fingerprinting:** The main trouble here is to mark the source of illegitimate copies so that the owner can be embedded various watermarks into every duplicate that share to a several customer.

## 2.7. Classification of Watermark Algorithms

There are various classifications of watermarking depending on different things such as: a form of data, human perception, data for extraction and transformation domain [38].

Firstly, the watermarking can be split according to the form information:

- Text watermarking
- Image watermarking
- Video watermarking
- Audio watermarking

Secondly, the watermarking can be split based on human perception as:

- Visible watermarking: Visibility is related to the ability of the human's eye to discover the watermark data, so that if the watermark is hiding the information in

the way which can be noticed without extraction, it is considered as visible watermark that are utilized in text document and video.

- Invisible watermarking: An invisible watermarking cannot be noticed by the human eye. So it is hiding the information without changing the contents and could be extracted from the authenticated person only. For example, pictures are exposed over the web and watermarked for copying security.

Thirdly, watermarks are categorized according to the data for extraction as:

- Public watermarking: In this type of watermarking, there is no need for the original data through the extraction operation to discover the watermark. Only the mystery key is desired.
- Private watermarking: In this type of watermarking, the original data is needed for extracting the watermark.
- Semi-blind watermarking: In this type we may need additional data for recognizing the watermark.

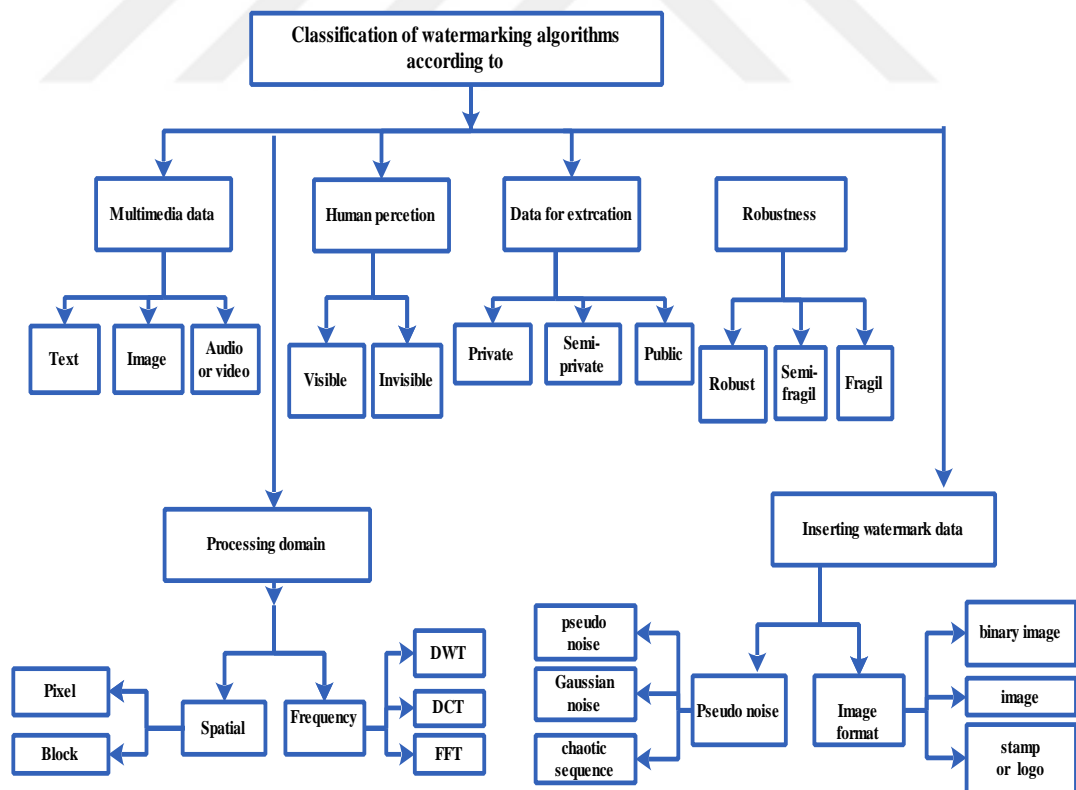
Lastly, watermarking techniques can be classified into two groups:

- Spatial domain: It puts the watermark data through image pixels. It is considered a simple technique and can be utilized for every image, however, it has some drawbacks. It can be easily destroyed. The watermarking in the spatial domain is not hard to harm utilizing a few assaults [39].
- Transform domain: It is also called frequency domain in order to values of frequency can be adjusted through transforms process. In this process, transform coefficients are modified for hiding the watermark information. Regularly methods utilized as a part of this technique are: DCT and DWT.

Furthermore, classification of the watermark as indicated by the watermarking robustness as:

- **Robust watermark:** A watermark is strong in the event that it can be extracted after some basic handling process as lossy compression and filtering.
- **Fragile watermark:** A watermark is delicate in the event that it can be pulled out after any distinction in the information furthermore conceivable to distinguish the information before alteration. This form of watermark can be utilized for the credibility of the original information.
- **Semi-fragile watermark:** A watermark is semi-delicate on the off chance that it is basic to some scope of the modification on the watermarked picture.

The classification of digital watermarking is illustrated in (Figure 3) [11].



**Figure 3** Classification of watermarking algorithms [11].

## 2.8. Attacks on Watermarking

There are numerous operations applied on the watermarking may damage it. Those operations that harm the watermark information are called attacks. Digital information is put in lossy compressed format. These compressions isolate essential parts of information; this operation may be causing damage the watermark information. Subsequently, a small attack is compressed information in a lossy and harm the watermark. In the state of picture a scaling or rotation can change pixel values causing harm the watermark [11].

### 2.8.1. Classification of Watermarking Attacks

There are many types of attacks can be classed as:

- 1- **Active attacks:** When the attacker attempts to remove the watermark, then it is called active attack. These types of attacks produce a large issue in copyright protection, as copy control and fingerprinting.
- 2- **Passive attacks:** The attacker attempt to locate if a given mark is present or not. This type of attack was important in secret communications where the straightforward knowledge of the occurrence of the watermark has been enough to begin attacking.
- 3- **Collusion attacks:** The aim of attacker is the same as for the active attacks yet the process are distinctive, the attacker examines a few duplicates of the similar information, but with various watermark, each marked with a key, to build another duplicate with no watermark.
- 4- **Forgery attacks:** In this type the attacker tries to hide a new watermark rather than removing it.
- 5- **Ambiguity attacks:** Here the attacks try to confound by creating forged original information or forge watermarked information.

6- **Protocol attacks:** In this type of attack the aim is an entire thought at the watermarking application [12].

### 2.8.2. Effect of Noise Attacks on The Watermarks

The effect of some kinds of noise on the robustness of watermarks is considered below:

- 1- **Salt and pepper noise:** It is normally observed in the picture. This appears to be random in process white and black pixels. Salt and pepper noise appears in pictures in the state through speedy transients.
- 2- **Speckle noise:** It is decay the quality of the image. It is the impact from irregular variation in the return signal from an object that is not greater than a single picture handling component. It raises the mean grey level of a local area. It is creating the hardness for picture translation.
- 3- **Gaussian noise:** It is factual noise, its likelihood intensity function equivalent to that of the ordinary circulation, which is additionally called gaussian distribution. A common situation is white gaussian noise, in which the values of any sets of times are factually isolated. In many applications, gaussian noise is most generally utilized for additive white noise to produce additive white gaussian noise.

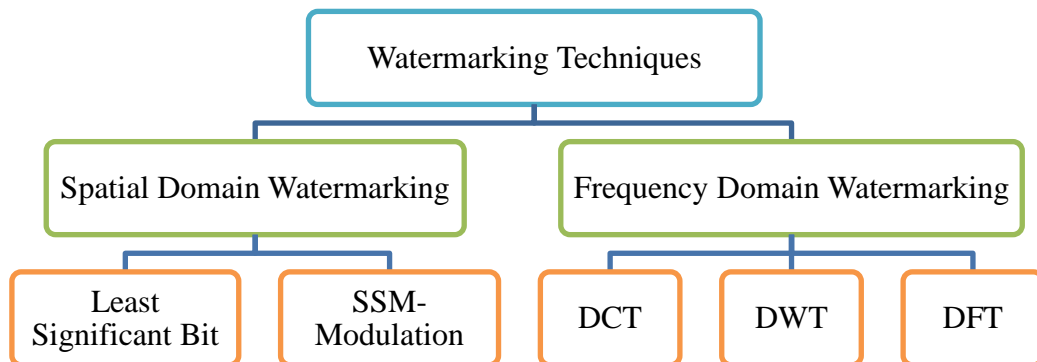
There are many other attacks like Cropping, Resizing JPEG compression, Rotation, etc. that impact the quality of the watermark extracted [13].

## CHAPTER 3

### WATERMARKING ALGORITHMS AND THE SECURE HASH ALGORITHM

#### 3.1. Overview

Two processing domain has been offered for digital watermarking algorithms, there are spatial domain and frequency domain (See Figure 4). Watermark technique setup on spatial domain is expending, watermarks information hiding in the picture element value; this lead to uses a little modified in the pixel intensity amount. For strongest hide to the watermark information should be adjusted the significant parts of low- frequency components of images. However, in the spatial domain, the techniques are not sufficiently strong to lousy image compression and other operation. Such as, a small noise may be removing the watermark. On the other side, the techniques in frequency domain can hide more bits for the watermark information and it is stronger against attack. Also the transform domain does not utilize the original image for hiding the watermark information so it is stronger to image doctrinaire [13]. In this chapter, we discuss the important transformation as DWT, DCT, and DFT.



**Figure 4** Watermarking techniques classifications.



## **3.2. Spatial Domain**

The simplest way of hiding the watermark is modifying the pixel values for host image as the technique in spatial domain. It considered a simple executing procedure, but it is powerless compared with the transform domain technique. It is inserted the watermark in pixel values in the form of changing some of bits from 1 to 0 or from 0 to 1 [14].

### **3.2.1. Least Significant Bit Adjustment**

The digital image contains a sample average of the function at discrete locations or pixels. These averages are indicating the pixel domain or image performance. Spatial domain insert message into that image pixels [14].

### **3.2.2. Spread Spectrum Modulation (SSM)**

The SSM techniques are generated the energy at discrete frequencies spread in time or frequency domains. When used the SSM for watermarking, we embed the watermark information by combining the host image with a small noise signal that is modulated by the embedded watermark [15].

## **3.3. Watermark Hiding Operations**

The hiding of the watermark is applied by selecting a part of pixel from the picture and change the least significant bit of all the selected pixels by the watermark bits. The hiding operations can be listed below:

1: Load picture (I).

2: Load watermark (W).

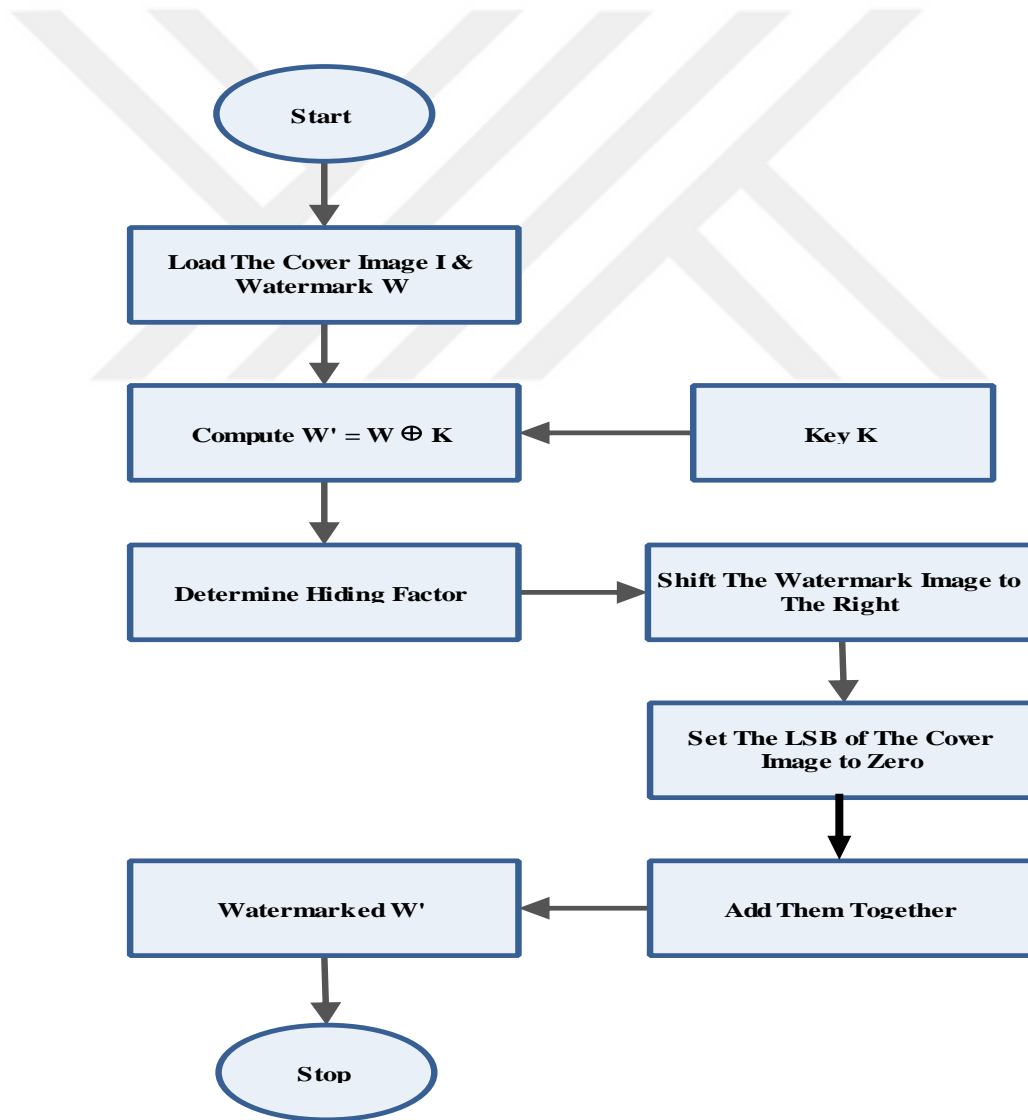
3: Preprocess the watermark: Load the mystery key (K) (K: it is a sequence in a binary form). Then calculate  $\{W' = W \oplus K\}$ , where  $\oplus$  is the bitwise XOR symbol.

4: For every value of the watermark picture move to right, it hides a message matrix (8-N) areas to move the higher 4-bits to the right end.

5: Change the lower bits of every value of the original picture to zero. These bits are exchanged by the higher bits of the watermark picture.

6: Add a cover picture with the watermark picture making the watermarked picture.

7: Store the watermarked picture. (Figure 5) demonstrates the watermark hiding operation [16].

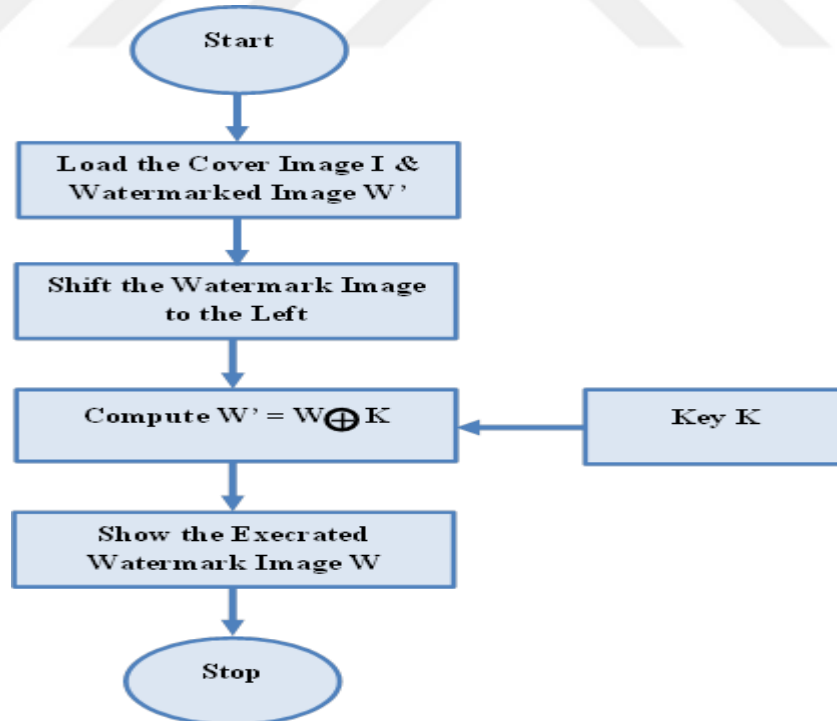


**Figure 5** Watermark hiding algorithm [16].

### 3.4. Watermark Extraction Operations

To acquire the original data (such as a picture) from the watermarked data, the list below is implementing:

- 1: Open the watermarked picture.
- 2: Shift the watermarked picture matrix to the left bits by (8-N) to make these four bits the highest significant bits.
- 3: Load K which is the mystery key.
- 4: Process the (W') with the key array (K) to acquire the watermark (W) by:  $\{W = W' \oplus K\}$ .
- 5: Display recovered watermark picture. (Figure 6) shows the watermark extraction algorithm [16].



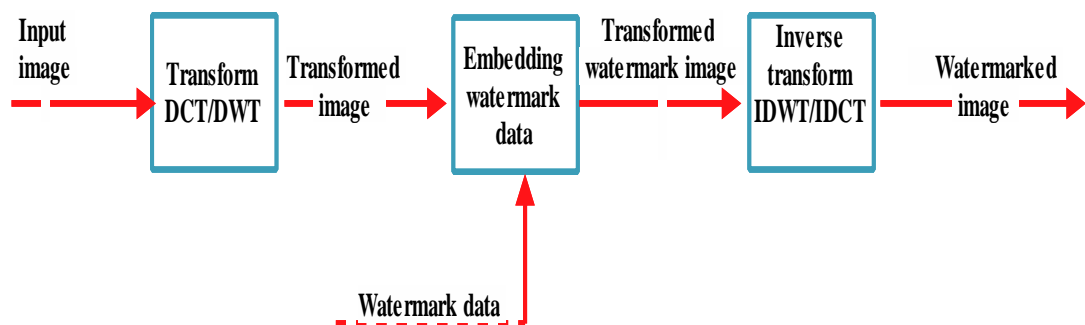
**Figure 6** Watermark extraction algorithm [16].

### 3.5. Transform Domain

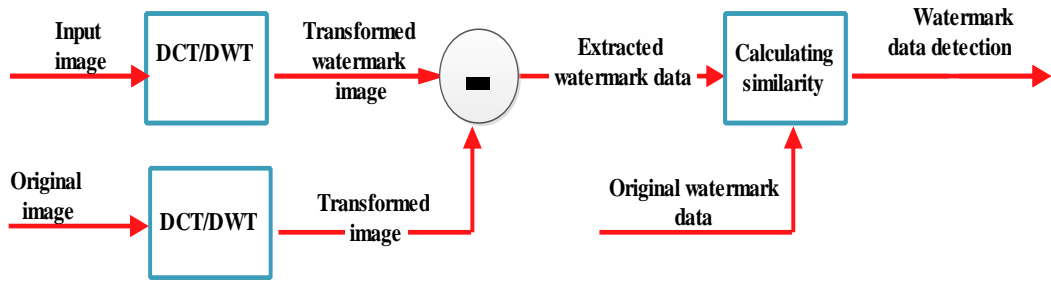
It is modifying the transform component of the cover data message to hide the data message. Generally, transform domain has an impact in the spatial domain as split the hide information over varying order bits in the strong way. There are many transforming algorithms used for digital data, applied in watermarking. As: DFT, DCT and DWT [14].

#### 3.5.1. Transform Domain Watermark Insertion and Detection

Initially, the input image is transformed utilize a transform such as the DWT or DCT. See Figure 7 describe the block diagram for transforming domain watermark insertion. In public, any frequency domain transform can be used. The watermark data are embedded in a transformed image. In other words, the watermark data is put into the transformed component, the inverse transform is used in the transformed watermarked image. The watermark extracted process is the inverse step of the watermark insert process as is seen in Figure 8. As this figure shown, to decode the watermark data, first, transforming the watermarked and the original image using the DCT or DWT. Secondly subtracted transformed image from the transformed watermarked image. This is because the watermark data is the difference between the original picture and the watermarked picture. Finally, the similarity of the original watermark data and the extracted watermark data is calculated. The likeness is depending on the amount of the embedding watermark data and the watermark attacks. Since the DCT and DWT are generally utilized for watermarking in the frequency domain [11].



**Figure 7** Block diagram of the transform domain watermark insertion [11].



**Figure 8** Block diagram of the transform domain watermark detection [11].

### 3.5.2. Discrete Fourier Transform (DFT)

It converts a function in continuous form to its frequency components. The synonymous changes in discrete valued function demand the DFT. In picture handling, the functions that are not periodic can be changed over to the necessary of (sine) or potentially (cosine) duplicated by a weighting value. Fourier transforms allows investigation and preparing of the signal in its frequency domain [14].

### 3.5.3. Discrete Cosine Transform (DCT)

It breaks the picture into various frequency bands. Arranged the frequency components in sequential order (low, mid, and high frequency) as other transforms, the DCT tries to de-correlate the picture data. After de-correlation, can be encoded the transform coefficient independently without damage compression quality [14].

#### 3.5.3.1. One-dimensional Discrete Cosine Transform

The DCT form of a one-dimensional sequence of length (N) is defined as [17]:

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

Where  $u = 0, 1, 2, \dots N-1$ .

The inverse of DCT is:

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

Where  $x = 0, 1, 2, \dots, N - 1$ . In each excerption (1) and (2)  $\alpha(u)$  is as:

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N}} & \text{For } u = 0 \\ \sqrt{\frac{2}{N}} & \text{for } u \neq 0 \end{cases} \dots\dots\dots 3$$

It is evident from the equation (1) for  $u=0$ ,

$$C(u = 0) = \sqrt{\frac{1}{N}} \sum_{x=0}^{N-1} f(x) \dots\dots\dots 4$$

The first transform coefficient is indicated to as the DC coefficient. The other transforms coefficients are called the AC coefficients [17] [18].

### 3.5.3.2. The Two-Dimensional Discrete Cosine Transform

DCT depends on DFT; it is transforming a signal from the time domain to frequency components. It contains the real parts of the DFT coefficients. It has a strong energy compaction and generality the signal information directed to be in a few low-frequency components of the DCT [14].

The transform of a specific signal is another state of representing that signal. It does not effect on the information in the signal.

The 2-D DCT is an expansion of the 1-D and is given by equation [19][20]:

$$C(u, v) = \frac{2}{N} \alpha(u)\alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right] \dots\dots\dots 5$$

For  $u, v = 0, 1, 2, \dots, N - 1$  and  $\alpha(u)$  and  $\alpha(v)$  are defined in equation (6).

$$\alpha(k) = \begin{cases} 1/\sqrt{2} & \text{for } k = 0 \\ 1 & \text{otherwise} \end{cases} \dots\dots\dots 6$$

The inverse of DCT is:

$$f(x, y) = \frac{2}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \alpha(u)\alpha(v) C(u, v) \cos \left[ \frac{\pi(2x+1)u}{2N} \right] \cos \left[ \frac{\pi(2y+1)v}{2N} \right] \dots\dots\dots 7$$

For x, y = 0,1,2,..., N -1.

### 3.5.3.3. Advantages of DCT

There are many advantages of transforming algorithm DCT some of them are listed below:

- 1- Agreeable robustness.
- 2- Sensible implementation time.
- 3- Fast and suitable for JPEG compression.
- 4- Its genuine transform with better efficiency than DFT [14].

### 3.5.3.4. Disadvantages of DCT

There are many disadvantages of transforming algorithm DCT some of them are listed below:

- 1- Cropping picture effect.
- 2- The blocking effect.
- 3- Not as robust against geometric attacks. [14]

### 3.5.4. The Discrete Wavelet Transforms (DWT)

DWT is a time domain analysis method commonly used in digital image processing, as compression and watermarking. The transforms are depending upon little waves, it is called wavelet changing in frequency. A wavelet series is representing a square integral function of a certain orthonormal chain made by a wavelet. The DWT

separate a picture into four subbands a lower resolution image (LL), horizontal (HL), vertical (LH) and diagonal (HH) detail segments [15].

### 3.5.4.1. The One-Dimensional Discrete Wavelet Transform

The discrete time wavelet transformation of one dimension applies the convolution mathematics between one dimensional signal such as  $x(n)$  and wavelet filter  $H(n)$  for the lowpass filter to make the approximation coefficients  $A(n)$  and high pass filter  $G(n)$  for high pass filter to produce the detail coefficients  $D(n)$ . As shown in (Figure 9). The equation 8 and 9 describe this operation.

$$A(n) = \sum_{n=0}^{N-1} H(n)x(n - k) \dots\dots\dots 8$$

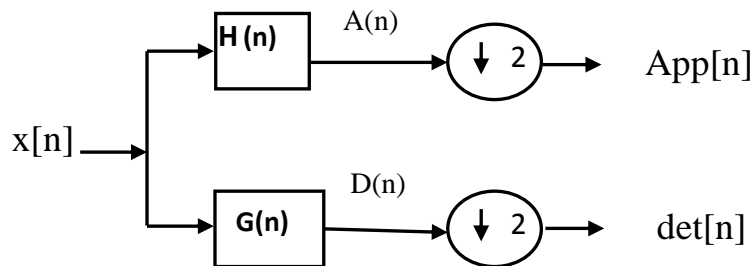
$$D(n) = \sum_{n=0}^{N-1} G(n)x(n - k) \dots\dots\dots 9$$

$N$ : is representing a number of samples in the signal.

The down sampling operation is used to pick up one sample and remove the other; this operation is done by developing the above equations as shown below:

$$App(j, n) = \sum_{n=0}^{N-1} H(n)x(n - 2^j k) \dots\dots\dots 10$$

$$Det(j, n) = \sum_{n=0}^{N-1} G(n)x(n - 2^j k) \dots\dots\dots 11$$

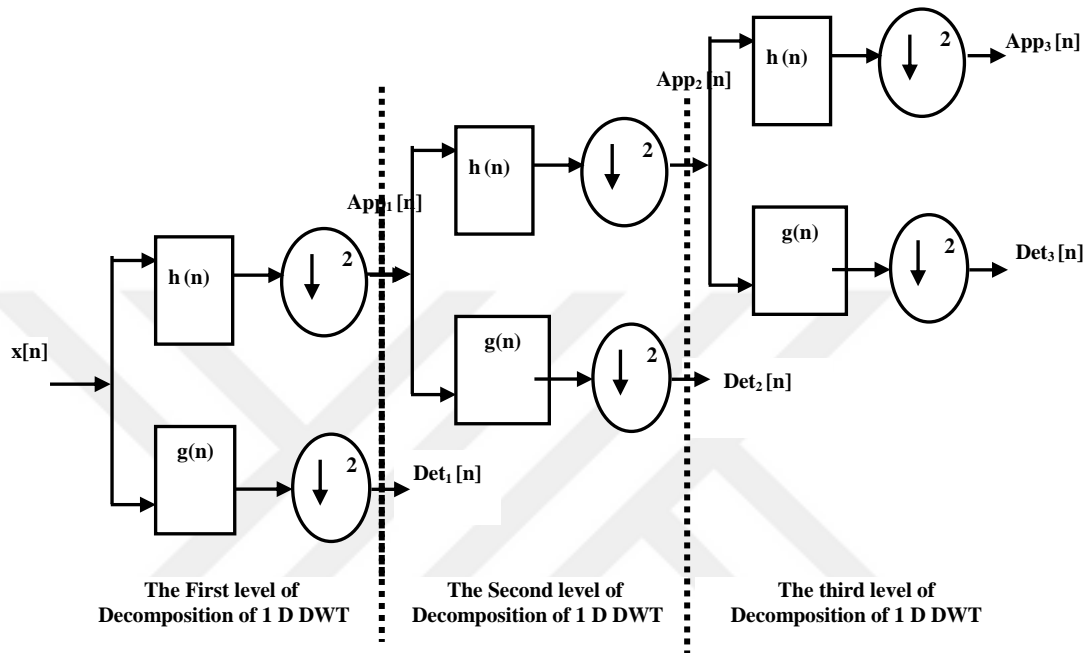


**Figure 9** The one dimensional discrete wavelet transforms.

A multi-level of one-dimensional discrete wavelet transform can be represented by using the low-pass filter (which is expressed by  $(h(n))$  and high-pass filters (which



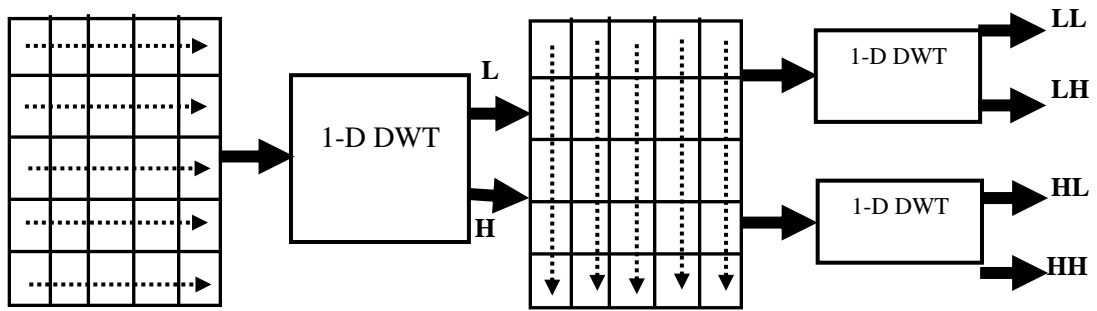
are expressed by  $g(n)$ ) (Figure 10 shows that). At each level, the high-pass filter produce detailed image pixel data ( $det_j(n)$ ) where (j) refer to the level number, however the low pass filter generate the coarse approximations of the input image  $App_j(n)$ . At the last level, each output of the lowpass and highpass filtering are down-sampled by two ( $\downarrow 2$ ) [11].



**Figure 10** The three levels one dimensional discrete wavelet transforms [11].

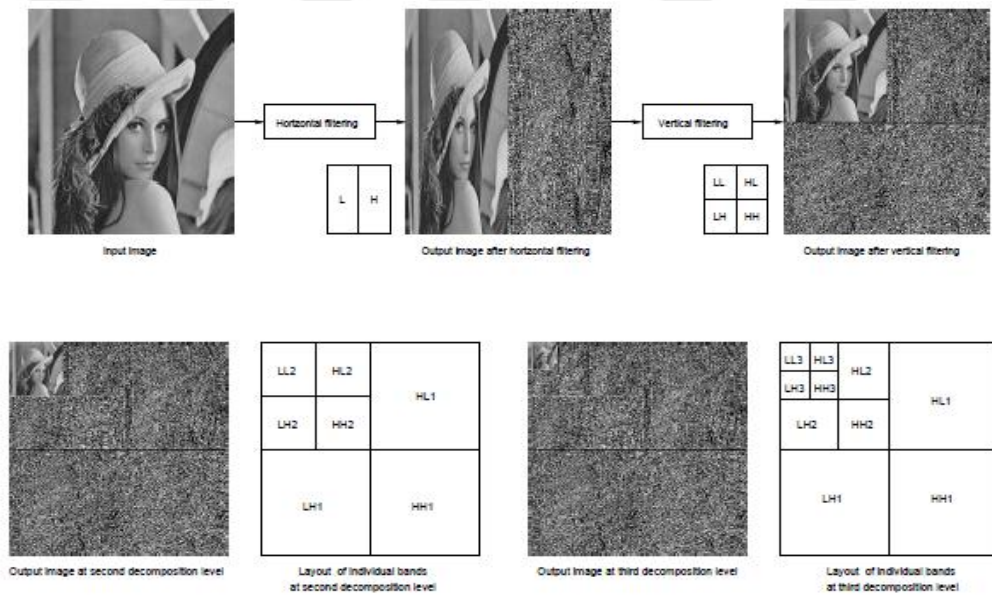
### 3.5.4.2. The Two-Dimensional Discrete Wavelet Transform

It is computed by a lowpass and a highpass filter. A 1D DWT is applied twice in both horizontal and vertical scan to giving 2D DWT. In other words, a 2D DWT can be done by first implement a 1D DWT on every row, which is indicate to as horizontal scanning of the image and the approximation coefficient and detail coefficients are called (L) and (H) followed by a 1D DWT on each column, which is named a vertical scan. Here, the 1-D DWT operation performed twice [11]. As shown below in (Figure 11), once for implementing the 1-D DWT on (L) coefficients to produce (LL) and (LH) coefficients and another 1-D DWT perform the vertical scan on each (H) coefficient to produce (HL) and (HH) results.



**Figure 11** The block diagram of one level 2D –DWT.

In 2D applications, after the first level of decomposition, there are four subbands{LL1, LH1, HL1, and HH1}. For each sequential level of decomposition, the (LL) sub-band of the former level is utilized as the input. To implement DWT at the next level, they perform DWT on (LL1) and for three level decomposition, they apply DWT on (LL2) to get 4 sub-band of three levels {LL3, LH3, HH3, HL3} [11] [21]. As shown in (Figure 12).



**Figure 12** Sub-bands after applying second and third decomposition levels.

### **3.5.4.3. Advantages of DWT**

There are many advantages of transforming algorithm DWT some of them are listed below:

- 1- It has a perfect localization both in the spatial domain and in the frequency domain.
- 2- The transformation of the whole image, presents inherent scaling
- 3- A good identification of datum is relevant to the human eye.
- 4- Flexibility; Wavelet function ability is free chosen [14].

### **3.5.4.4. Disadvantages of DWT**

There are numerous disadvantages of transforming algorithm DWT some of them are recorded below:

- 1- May be a large cost of calculating DWT as compared to DCT.
- 2- Using a larger DWT basic function or wavelet filters lead to blurring and ringing noise close to edge regions in images.
- 3- It has a long compression time [14].

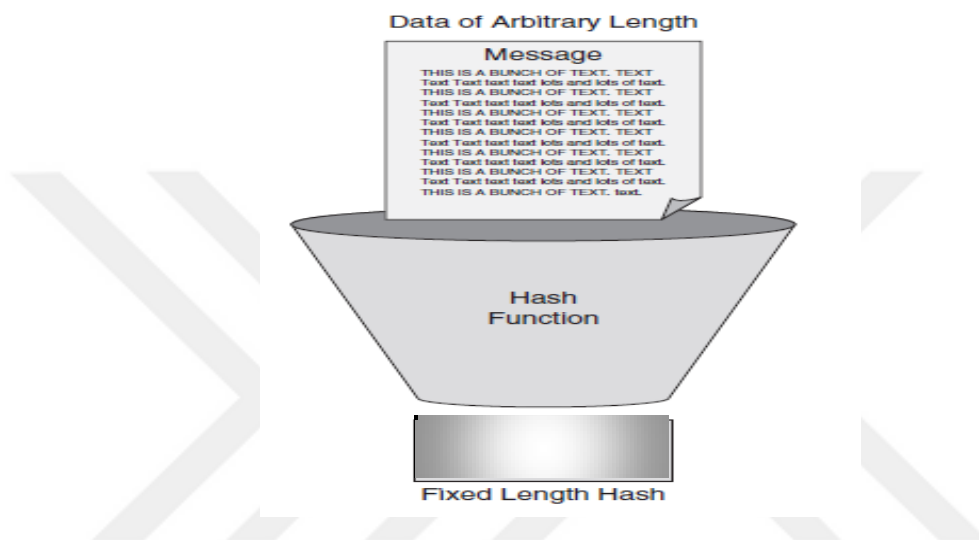
## **3.6. The Secure Hash Algorithm (SHA)**

One of the methods to produce a data message authentication code depending on hash functions. A hash function produces extra security characteristics to make it appropriate in different information security applications, as authentication and message integrity. Hash functions are generally applied to secure password contents and interacting authentication on the web service. There are some of public hash algorithms some of them: Message Digest algorithm (MD), MD5, SHA-0, and SHA-1 in data security applications [22] [23].

### **3.6.1. Secure Hash Algorithm Family**

The SHA family is used in cryptographic application and produced by the National Institute of Standards and Technology (NIST). SHA-0 is the first type of SHA family. The development version of SHA-0 is a SHA-1 version, another model has

issued by NIST with increased output and a variant design: SHA-22, SHA-256, and SHA-512. In this thesis, we used the SHA-1. The SHA-1 algorithm is depending on basics such as MD (Message Digest algorithm). It generates a 160-bit digest within a message block consist of 512 bits. SHA-1 is frequently powerful against attacks. The hash gets the information of arbitrary length and input it into the hash function for treating it to make it a fixed-length hash, the fixed-length hash is named a digest or fingerprint. (Figure 13 shows the hashing process) [22].



**Figure 13** The hashing process.

The algorithm which applies to create the fingerprint called hash sums or hash values/ hash codes.

Cryptographic hashes serve information security applications. They are applied to make integrity message checks and digital signatures on different data security applications, as authentication and message security [23].

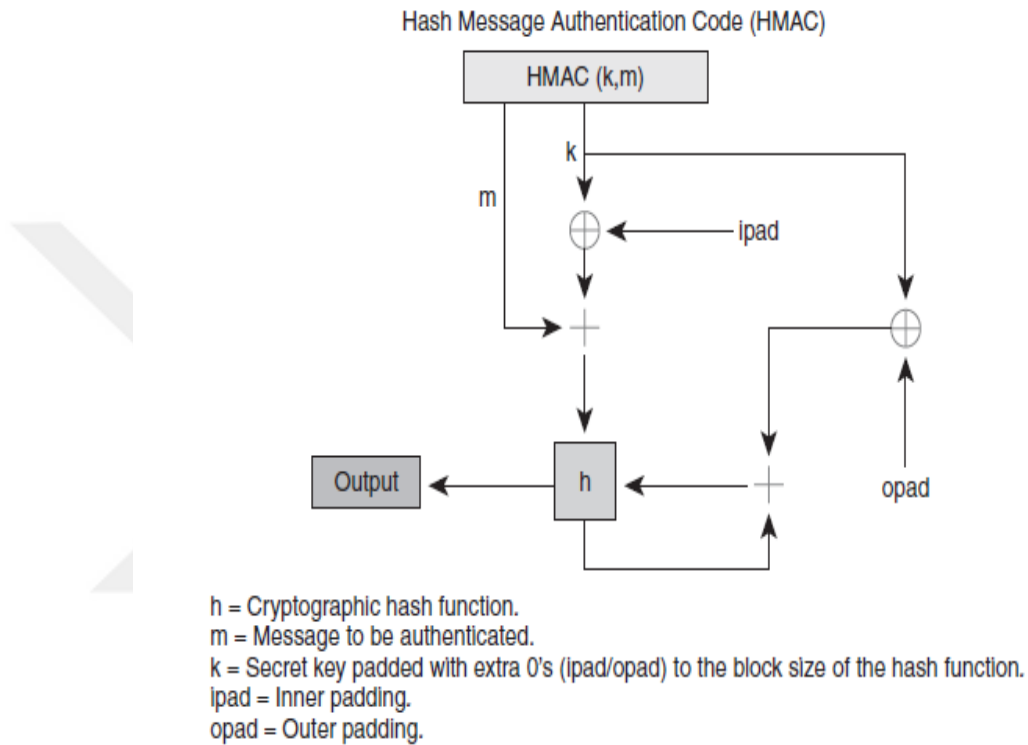
### **3.6.2. Hash Message Authentication Code (HMAC)**

One type from the Message Authentication Code (MAC) is HMAC; it is determined by using a cryptographic hash function with a secret key. It is used to verify the data's integrity and the message's authenticity at the same time.

When used SHA-1 to calculate the HMAC the MAC algorithm is called HMAC-SHA-1. The cryptographic strength at using a hash function, depends on the size and

quality of the key and the size of the hash output length in bits, show (Figure 14) describes HMAC [24].

SHA-1 divide message into pieces of a fixed size, and after that restore them with a compression function. For instance, SHA-1 works on 512-bit blocks, the size of the HMAC output is 160 bits, but we can amputate this if you want. When the hash image is amputated, the security of the MAC is reduced [23].



**Figure 14** The block diagram of HMAC.

## CHAPTER 4

### THE PROPOSED ALGORITHMS AND THE MEASUREMENTS

In this chapter, we focused on explaining the proposed watermarking algorithm using the 2D-DWT and 2D-DCT with a secure hash algorithm (SHA-1), the proposed algorithm is begin by applying the multi-level (one, two or three levels) of 2D-DWT on gray scale host images then two different types of embedding processing are performed in parallel form.

The first type of embedding depends on replacing the coded secret key with some elements of 2D-DCT coefficients which is implemented on (HL) sub band image of 2D-DWT.

The second type of embedding is performed by applying the 2D-DCT on watermark information and adding it with (LL) sub band image of the host image. The purpose of embedding different information in different sub band images is to increase the security of the algorithm and do not merge the secret key with the watermark information even some one suggest the place of watermark information, he cannot reach the place of the secret key. So he cannot destroy the information or get it. Another benefit of using a different type of sub bands image is allowing performing the parallel processing which reduces the time required for executing the proposed embedding algorithm.

In this thesis, The MATLAB program 2015a and its GUI tool are used to implement our proposed algorithm. The GUI Tools are very useful to build the suitable graphic interface to make the execution of our work is very easy.

The performance of our study can be measured by using some fidelity criteria such as: PSNR, NCC and NHD. To measure the performance, we use some different host standard gray scale images (Gold Hill, Baboon, Barbara, Cameraman, Boat and peppers).

#### **4.1. The Proposed Copyright Watermark Embedding Algorithm**

The essential idea of the suggested algorithm is to supply image integrity and copyright protection which uses a watermark technique for copyright protection and hash function for image integrity. The working of the suggested algorithm include following steps:

##### **Step1: The Host Image Preconditioning**

- 1- Select the grey scale  $256 \times 256$  image as a host image.
- 2- Select the numbers of levels, which can be one, two or three levels of 2D-DWT. If you choose one level the output of this step is (LL<sub>1</sub>, LH<sub>1</sub>, HL<sub>1</sub>, and HH<sub>1</sub>), if you choose 2 levels 2D-DWT the output are: (LL<sub>2</sub>, LH<sub>2</sub>, HL<sub>2</sub>, HH<sub>2</sub>, LH<sub>1</sub>, HL<sub>1</sub>, and HH<sub>1</sub>), and if you choose the three levels 2D-DWT, the output is (LL<sub>3</sub>, LH<sub>3</sub>, HL<sub>3</sub>, HH<sub>3</sub>, LH<sub>2</sub>, HL<sub>2</sub>, HH<sub>2</sub>, LH<sub>1</sub>, HL<sub>1</sub> and HH<sub>1</sub>). As shown in (Figure 15).

##### **Step2: The Password or Secrete Key Preconditioning**

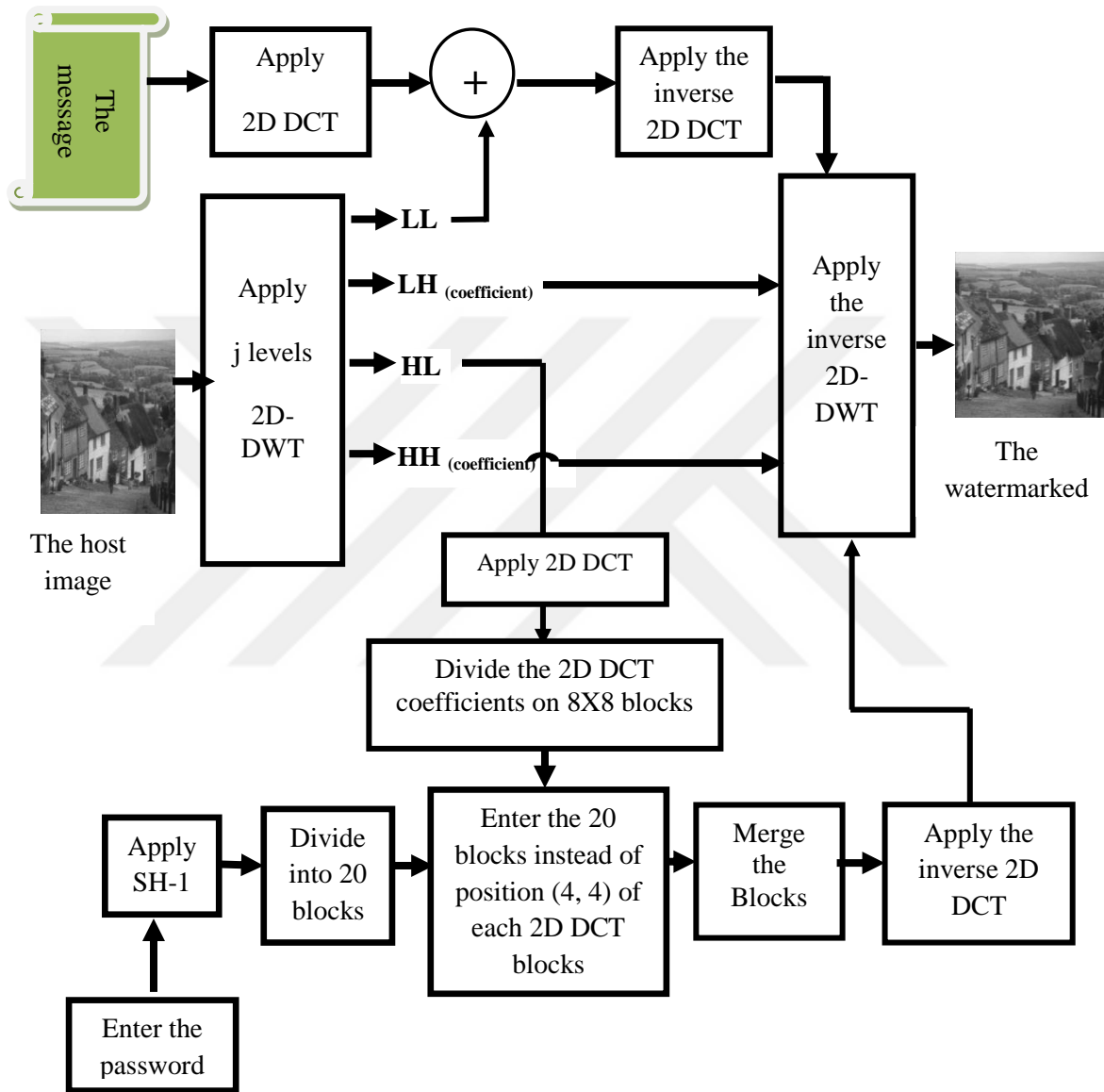
- 1- Enter your password or secret key.
- 2- Apply the SHA-1 on the password and save the output result which is contain 160- Bit.
- 3- Divide the 160- bit on 20 blocks each block is 8-bit only.

The password preconditioning is described in (Figure 15).

##### **Step3: The Message Preconditioning**

- 1- Select the bitmap  $64 \times 64$  message.
- 2- Apply the 2-D DCT onto the message.

These steps are explained in (Figure 15).



**Figure 15** The block diagram of preconditioning operations.



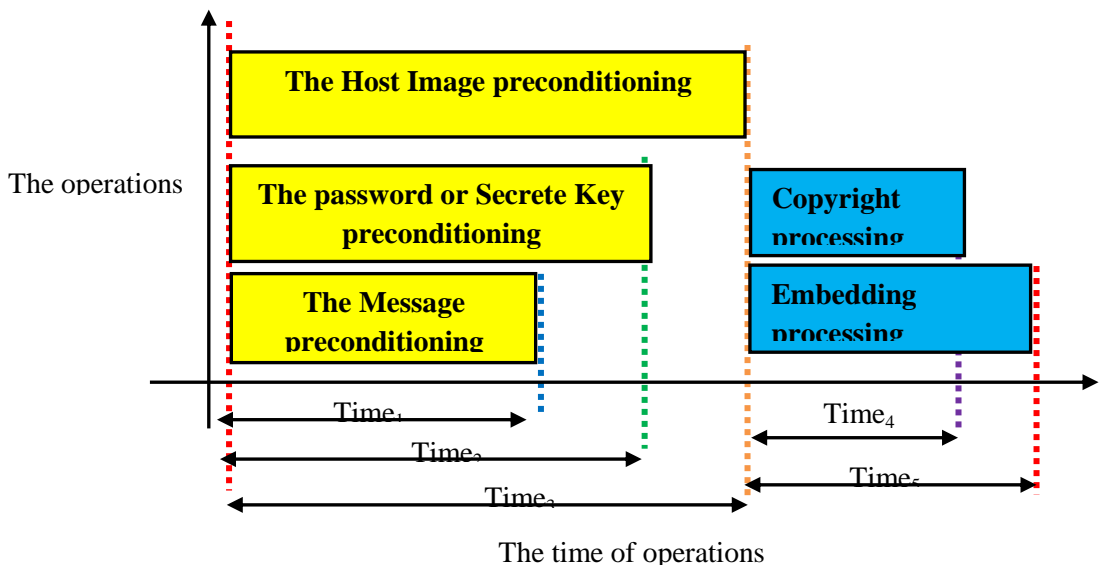
#### Step4: Copyright Processing

- 1- The beginning of this step, we must select the  $HL_j$  which  $j$  is representing the level number of 2D-DWT ( $j=1, 2$  or  $3$ ).
- 2- Apply the 2D-DCT on  $HL_j$ .
- 3- Divide the 2D-DCT coefficients on  $8 \times 8$  blocks.
- 4- Sub-bands the position  $(4, 4)$  on each  $8 \times 8$  block of 2D-DCT coefficients by SHA-1 blocks.
- 5- Merge all the  $8 \times 8$  blocks.
- 6- Apply the inverse 2D-DCT.

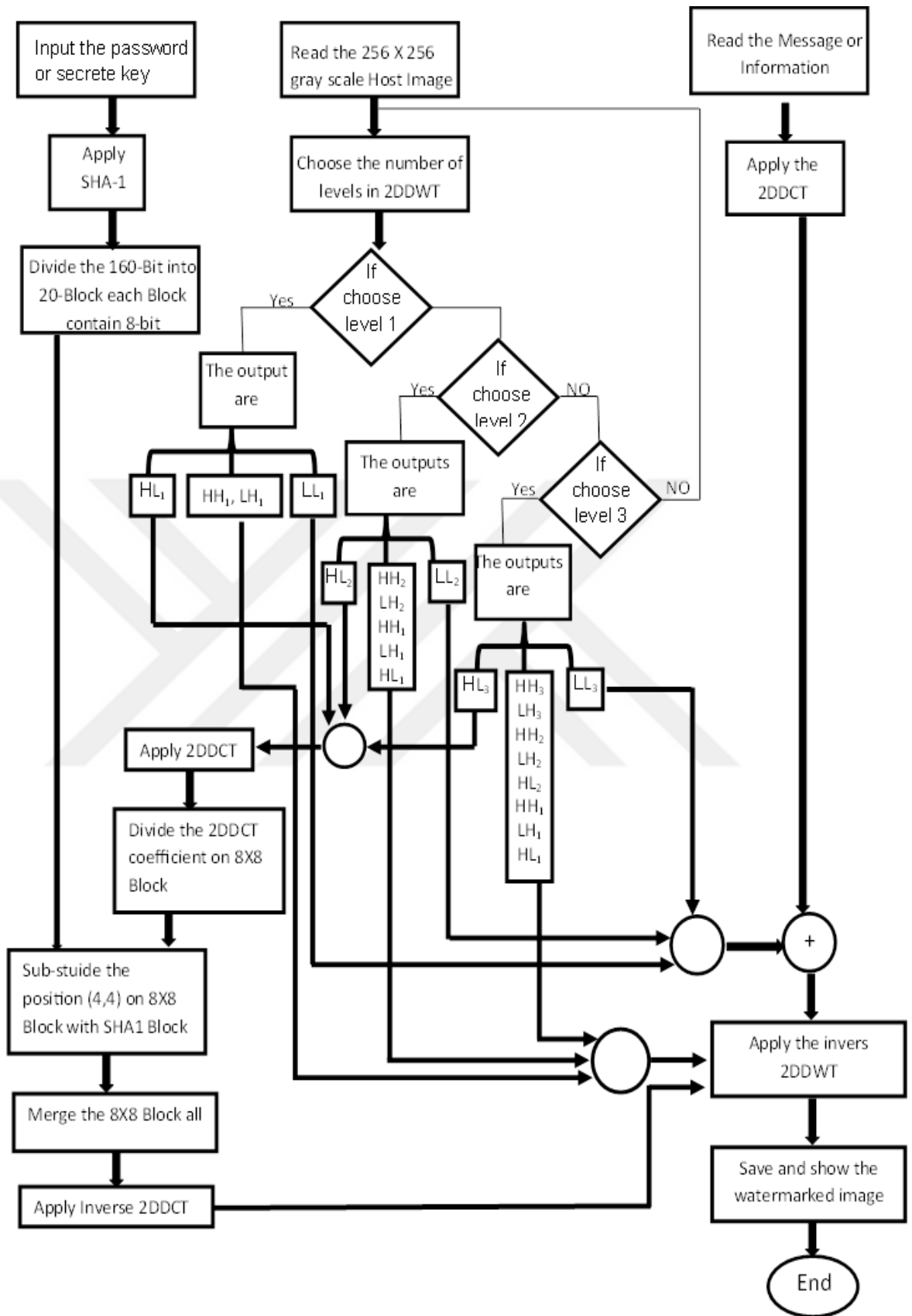
#### Step5: Embedding Processing

- 1- Adding the coefficients of 2D-DCT, which are calculated from step 3 with  $(LL_j)$  of the host image from step1.
- 2- Apply the inverse multi-level 2D-DWT by reading the modified  $(HL_j)$  from step 4 and the other sub-bands image from step1.
- 3- Save and show the watermarked image.

The steps 1, 2, and 3 can be performed in parallel order, after that step 4 and 5 can be done in parallel order together. Thus the timing diagram as explained in (Figure 16). The flow chart of the total our embedding algorithm is clarifying with all details in (Figure 17).



**Figure 16** The time diagram of proposed algorithm.



**Figure 17** The flow chart of the copyright watermarking.

## 4.2. The Suggest Copyright Watermark Extracting (Detection) Algorithm

The extracting algorithm is the same way of the embedded, it depends on two images: the original image and the watermarked image, as shown in (Figure 18). The working of the suggested algorithm include following steps:

**Step1:** Read the original and the watermarked images. Input the secure key and apply the SHA-1 on it.

**Step2:** Choose the number of levels in 2D-DWT, if level one, then applies one level 2D-DWT for the watermarked and the original image, if level two, then apply two levels 2D-DWT for the watermarked and the original image, if level three then apply three level 2D-DWT for the watermarked and the original image.

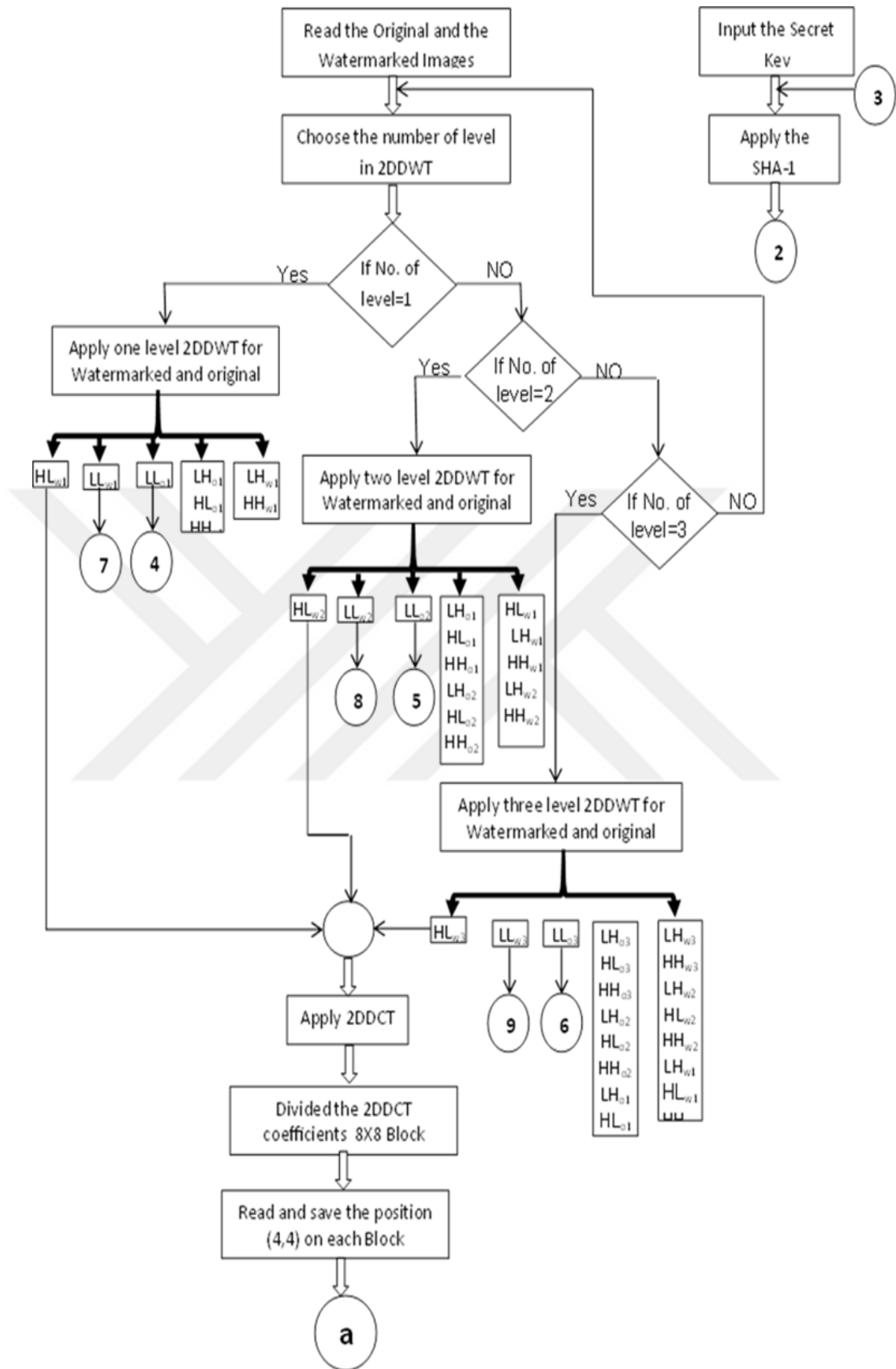
**Step3:** Apply 2D DCT on the coefficients.

**Step4:** Divide the 2D-DCT coefficient in  $8 \times 8$  blocks.

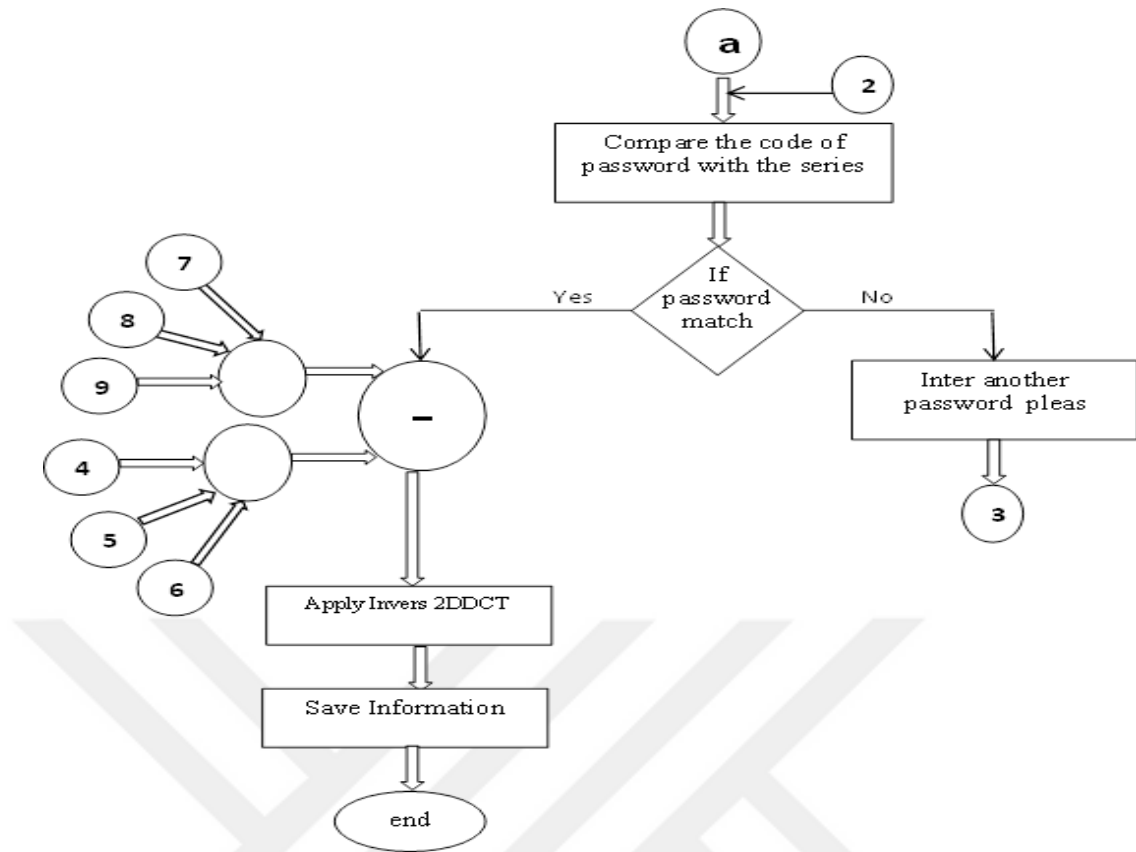
**Step5:** Read and save the position (4,4) on each block.

**Step6:** Compare the code of password with the SHA-1 sereise.

**Step7:** Apply the inverse 2D-DCT and save the information; if a correct password or request inter the new password and repeat the steps.



**Figure 18** The proposed copyright watermark extracting algorithm.



**Figure 18** Complement The proposed copyright watermark extracting algorithm.

### 4.3. Metrics for Quality

There are many measurements of watermarking quality calculated to check the robustness of the used technique such as: PSNR, NCC and NHD, we depend on that measurements because they are commonly used in watermarking, we discussed them below:

#### 4.3.1. Peak Signal to Noise Ratio

The real requirement of digital watermarking systems is to hide a given mark within the coverage data, such that it is undetectable to a human eye. The picture used in the watermarking algorithm uses local properties of the picture to get high invisibility rates. Represent picture in (I) and its watermarked picture (IW), then the standard deviation between (I) and (IW) is represented by the Mean Square Error (MSE):

$$\text{MSE}(\mathbf{I}, \mathbf{I}^W) = \frac{1}{N * M} \sum_{i=1}^N \sum_{j=1}^M ||f(i, j) - f'(i, j)||^2$$

PSNR is used for evaluating the feature of reconstructing in the picture compression techniques. It is defined in the expression of the logarithmic decibel (dB) scale as:

$$\text{PSNR}(\mathbf{I}, \mathbf{I}^W) = 10 \log_{10} \frac{255*255}{MSE} = \text{PSNR}(\mathbf{I}, \mathbf{I}^W) = 20 \log_{10} \frac{255}{\sqrt{MSE}} \text{ dB}$$

It is the proportion between the power of a signal and the power of corrupt noise that effects on that signal. The minimum value of MSE means minimal deformation, thus, the high PSNR amount is better or the watermarked picture is closer to the original picture. Commonly, PSNR higher than 32 dB means invisible visual degradation and a human eye don't recognize both pictures [25].

#### 4.3.2. Normalized Correlation Coefficient (NCC)

To measure the quality of the technique used for watermarking it should find the similarity between the cover picture and the watermarked picture additionally the original watermark and the recovered watermark. Whenever the value of the NCC is high, it shows good technique. NCC is getting this by the equation below [26]:

$$\text{NCC} = \frac{\sum_i \sum_j [ I(i,j) - I_w(i,j) ]}{\sum_i \sum_j [ I(i,j) + I_w(i,j) ]}$$

Where:

$I(i,j)$ : is the original picture pixel value

$I_w(i,j)$ : is the watermarked picture pixel value.

### 4.3.3. Normalized Hamming Distance (NHD)

NHD is used to calculate the degree of closeness among the original watermark and the extracted watermarked image, it is defined as in the equation:

$$\text{NHD}(W, W') = \frac{1}{N_w} \sum_{L=1}^{N_w} W(i) \oplus W'(i)$$

Where (w) the original picture and (W') extracted watermark picture. ( $N_w$ ) is the range of the watermark, and ( $\oplus$ ) is the XOR symbol, that giving the distance ranges around (0 and 1). Generally, the distance between two identical pictures must be nearest to zero [27].

### 4.4. The Graphical User Interface Model (GUI)

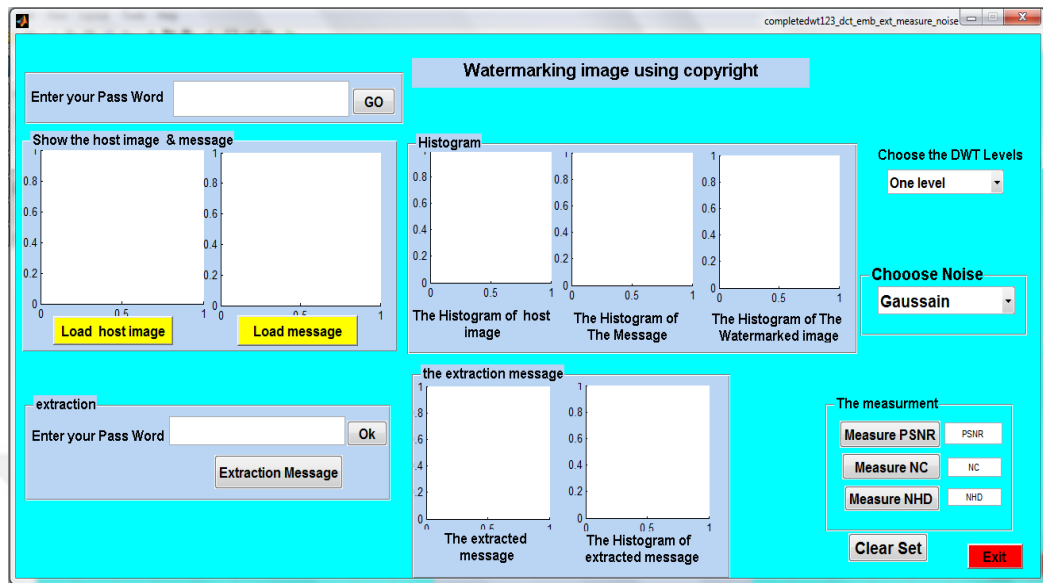
We are using the GUI tools from Matlab2015a to show how the algorithm is done and display the results of this work. The GUI model consists of three parts (the embedding part, the extracting part and the adding noise part which contain the multi type of noise). As shown in (Figure 19).

#### 4.4.1. The Graphical User Interface (GUI) Model of embedding and extracting

In the embedding code, we must choose the host image and the message and then we must enter the password or secret key, so we must perform the following steps:

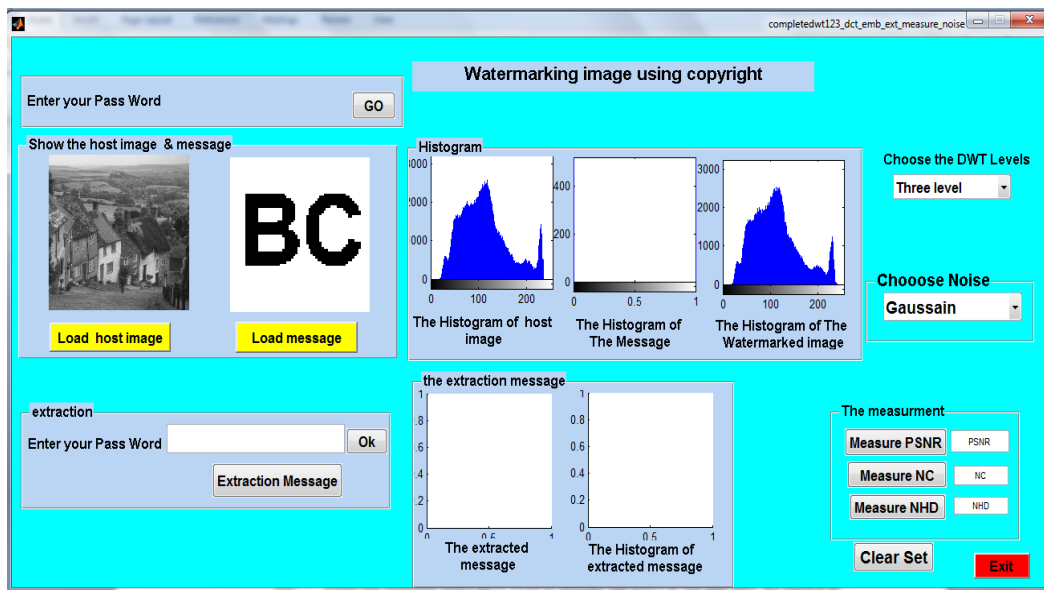
- 1- Enter your password in the edit text and then press "GO" button.
- 2- Choose "Load host image" button to find the host image on your computer and load it.
- 3- Choose "Load message" button to find the message information from your computer and load it into the program. As shown in (Figure 19). After the password was entered and go button was pressed; a password is disappeared to save the

password and increase the security of the algorithm. The host image and the message must display in your GUI windows if your choices are true.



**Figure 19** The graphical user interface of the proposed algorithm.

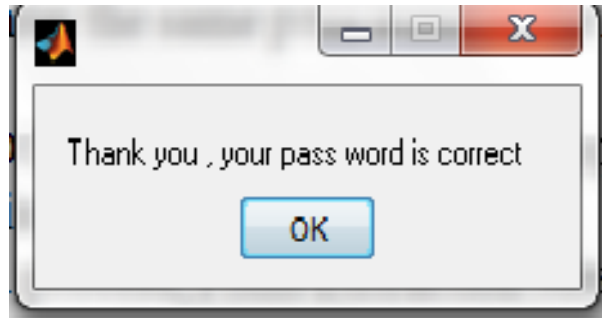
- 4- Choose the number of DWT levels by “Choose the DWT levels” POP-UP menu. At this point, the embedding program is executed and the results histogram image display in histogram panels. As shown in (Figure 20).



**Figure 20** The implementation of step 1, 2, 3 and 4 of our GUI model.

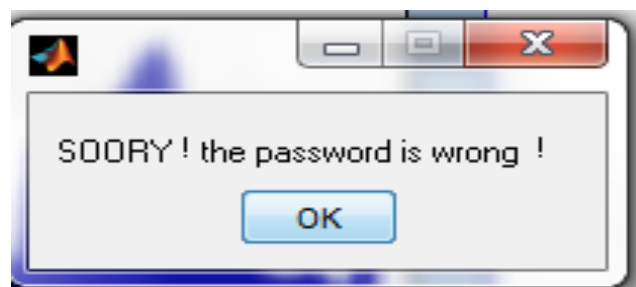


5- In order to execute the second part of the GUI model which can perform the extracting algorithm, we must enter the same password in the edit text of extracting part and then: presses “Ok” button, the password is disappearing to increase the security of our algorithm. As shown in (Figure 21).

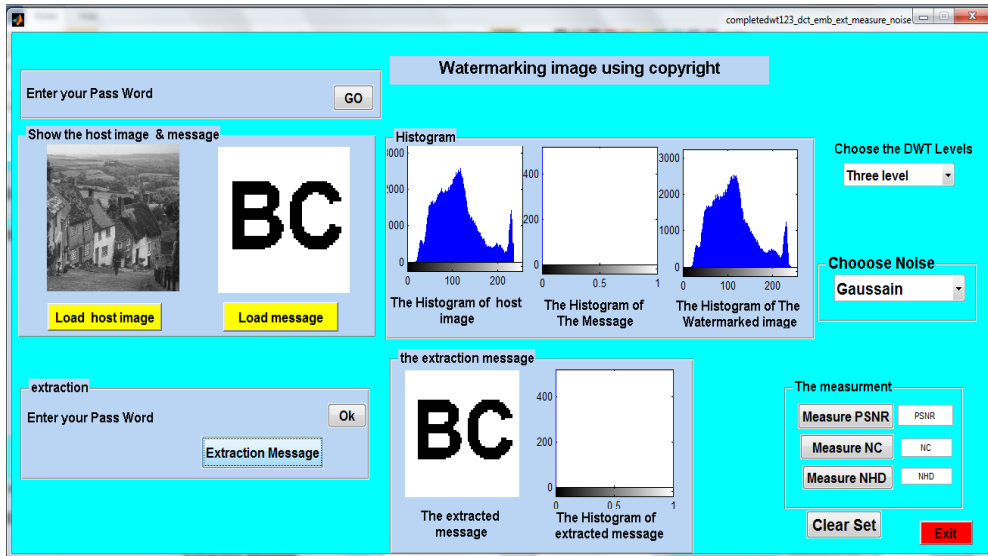


**Figure 21** The message of the correct password.

- 6- To begin the extraction process, press “Extraction Message” button.
- 7- The extraction message panels contain the extraction message and its histogram.
- 8- The first step in The extraction program is comparing the password which entered into the extraction part with the password that coded in the watermarked image by using SHA-1, If your password which entered matches with the password in the watermarked image, the message in (Figure 21). If the two passwords are doesn't match the message in (Figure 22) is shown. The extracting program is done completely and the reconstructing message appears in the extracted message panel as shown in (Figure 23).



**Figure 22** The message of the false password.



**Figure 23** The implementation extracting part our GUI model.

9- To calculate the PSNR, NCC, and NHD of the copyright watermarking algorithm:

- A- Press the “Measure PSNR” button to display the PSNR in the edit text.
- B- Press the “Measure NC” button to display the NC in the edit text.
- C- Press the “Measure NHD” button to display the NHD in the edit text.

As shown in (Table 1), If the host image is” GOLDHILL” and the message is as described in (Figure 24).

The following results for the one, two and three level in Table1. If the host image is “GOLDHILL” image and the message is described in (Figure 24).



(a) Gray scale host image

(b) The message

(c) Watermarked

**Figure 24** Gray scale image before and after watermarking and the message.

**Table 1** The fidelity criteria of the proposed algorithm











<b>GOLDHILL image</b>	<b>One Level</b>	<b>Two Levels</b>	<b>Three Levels</b>
<b>PSNR (dB)</b>	<b>49.0147</b>	<b>47.4382</b>	<b>47.7769</b>
<b>NCC</b>	<b>0.999988</b>	<b>0.99999</b>	<b>0.99991</b>
<b>NHD</b>	<b>0</b>	<b>0</b>	<b>0</b>

Table1 explicate the outcome for 3 levels after using the host image is (GOLDHILL image), the message is (BC image) and the result watermarked image and the measures for PSNR, NCC and NHD.

We use a three level in our work to get the best level for watermark embedding and extracting the most important for information.

In this thesis, the standard images such as (Baboon, Barbara, Boat, Cameraman, and Papers) are used as host images, the results of applying the three levels shown in (Table 2).

**Table 2** The results of applying the three levels on standard images.

Images	Host image (input)	Watermarked image (output)	PSNR (dB)	NCC	NHD
Baboon			46.4291	0.9999	0
Barbara			48.2016	0.9999	0
Boat			48.1494	0.9999	0
Camera			48.2953	1	0
Peppers			48.3515	0.9999	0

The previous results of applying the three levels on five different images show accepted value in PSNR reach to 48 dB, which means that the hidden information (the message) does not effect the large portion of the original image, In other hand the images are virtually indistinguishable by human observers, the value of NCC close to one as shown in previous table and 0 for NHD in all the images means that all the images are identical.

## CHAPTER 5

### THE NOISE EFFECT OF THE COPYRIGHT WATERMARKING ALGORITHM

The robustness of the watermark in the application is a very important issue in watermarking algorithm, thus we apply some type of noise and showing their effects on the proposed algorithm in this thesis. The MATLAB program and its GUI tools have been used to measure and display the fidelity criteria.

#### 5.1. Noise Modelling and Digital Image Filtering

Noise is the undesirable data that it broken dawn image quality. Noise known as an operation ( $n(i, j)$ ), which influence the obtained image ( $f(i, j)$ ) and it is not a part of the site (primary signals  $S(i, j)$ ). This operation is shown in equation (1) [28]:

$$f(i, j) = S(i, j) + n(i, j) \quad \dots\dots 1$$

Numerous variation operators are responsible for the noise representation in the picture. The quantity of noise relies on the amount of pixels oblique in the picture. The fundamental sources of noise in the digital picture are taken after:

- 1- The imaging sensor may be impacted by ecological at picture acquisition.
- 2- Imperfect light grade and sensor warmth may prompt to noise in the picture.
- 3- Interference in the communication channel may also miss the picture.
- 4- The dusts existing on a scanner screen can cause noise in the picture [28].

## 5.2. Noise Types

The noise ( $n(i, j)$ ), can be described by histogram or by probability density function (PDF), which is applied on the PDF of the original image ( $s(i, j)$ ).

Generally, our focus is studying the effect of these types of noise into our proposed algorithm, such as: salt & pepper, adjustment, gaussian, poison, median filter, average filter, gamma correlation and speckle noise [28].

### 5.2.1. Impulse Noise (Salt and Pepper Noise)

In this type of noise, black and white dots seem in the picture, such as salt and pepper.

The source of this noise is the sharp and flashy variation of the picture, likewise dust in the picture source, overheated incorrect components, by malfunction of camera's sensor cells, memory cell inadequacy [29].

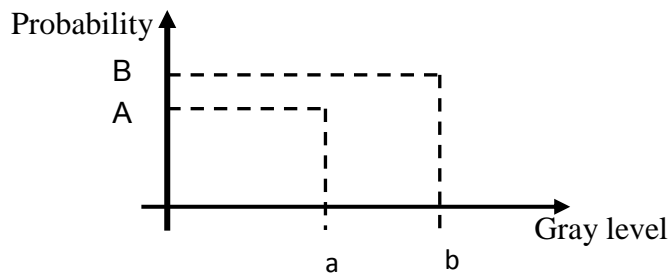
Assume a picture matrices (3x3) (Show Figure 25), consider the middle value is corrupted by pepper noise, consequently the middle value (212) is exchanged with the value zero. In that link, they can see that noise is embedded dead pixels dark or bright. Accordingly, in a salt and pepper noise, gradually brightest pixel values are sitting in dark region and vice versa [30].

254	207	210
97	212	32
632	106	20

254	207	210
97	0	32
632	106	20

**Figure 25** The central pixel value is corrupted by pepper noise.

The salt & pepper noise have two values (a) and (b) and the likelihood of getting each of them under 0.1. For (8 bit/pixel) picture, the intensity value of peppers noise is near to zero and for salt noise is nearly to 255 [28]. The PDF can be shown as in (Figure 26).



**Figure 26** The PDF of salt & pepper noise.

$$PDF_{salt \& pepper} = \begin{cases} A & \text{for gray scale} = a \text{ ("pepper")} \\ B & \text{for gray scale} = b \text{ ("salt")} \end{cases} \dots\dots 2$$

The image is oblique to a tiny range due to noise. (Figure 27) shows the effect of this noise with the different value of the density of salt & pepper [28].



The original image without noise



Image with 10% salt & pepper.



Image with 20% salt & pepper.

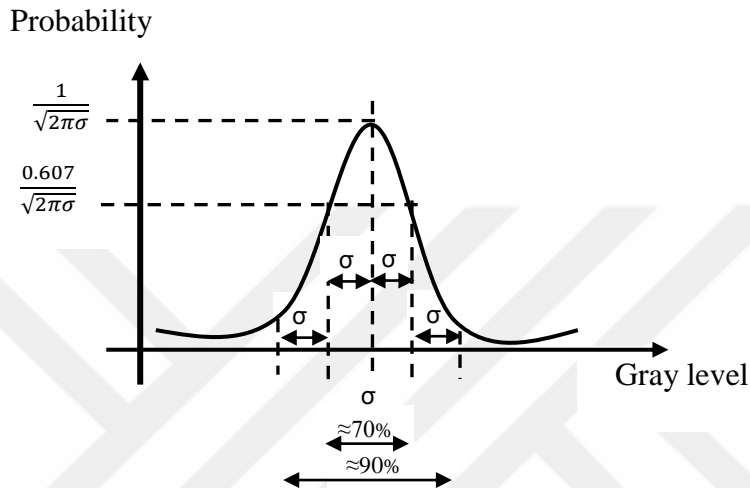


Image with 40% salt & pepper.

**Figure 27** The Salt &Pepper noise with different density of noise.

### 5.2.2. Gaussian Noise (Amplifier Noise)

This noise is additive in nature and follows gaussian distribution form. It implies that every pixel in the noisy picture is the amount of the real pixel. The probability density function (showed in Figure 28) of gaussian random variable is given by equation (3) [28] [30]:



**Figure 28** The probability density function of gaussian noise.

$$PDF_{gaussian} = \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{(g-\mu)^2}{2\sigma^2}} \dots\dots\dots 3$$

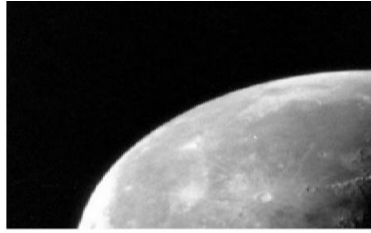
Where:  $g$  = gray level.

$\mu$  = mean value.

$\sigma$  = standard deviation.

Figure 29, displays the effect of applying gaussian noise with zero mean value and different value of standard deviation [29].





The original image without noise

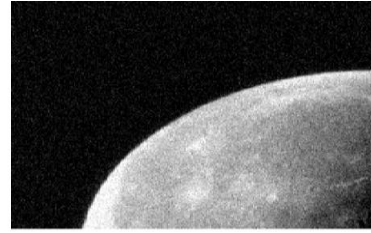


Image with  $\mu = 0$  and  $\sigma = 0.005$

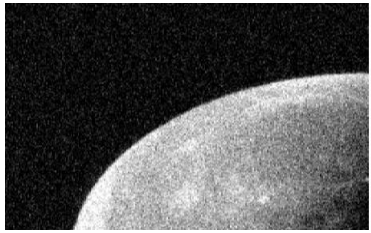


Image with  $\mu = 0$  and  $\sigma = 0.015$

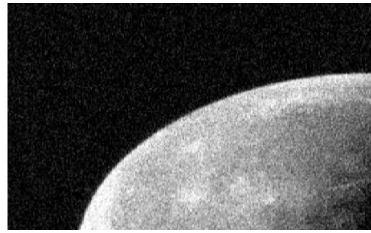


Image with  $\mu = 0$  and  $\sigma = 0.010$

**Figure 29** The effect of gaussian noise.

Approximately 70% of the amount is contained in  $\mu \pm \sigma$  and 90% of the amount is contained in  $\mu \pm 2\sigma$ . Although theoretically speaking, the PDF is non-zero all over between  $-\infty$  to  $+\infty$ , it is usual to suppose the function (0) nearly  $\mu \pm 3\sigma$ . Gaussian noise is good for styling natural processes that introduce noise [28].

### 5.2.3. Poisson Noise

This type of noise occurs when some of the photons sensed by the sensor is not suitable to give noticeable data. This noise has a root mean square value proportional to the square root density of the picture. Various pixels are culminate by separate noise amount. Figure 30 showed the result of adding poisson noise.



The original image without noise



Poisson noise image

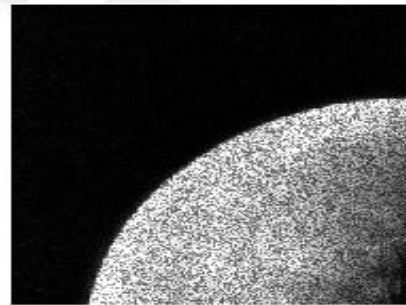
**Figure 30** The effect of poisson noise.

This noise appears depending on the statistical characteristic of electromagnetic waves, as x-rays, gamma rays, and visible lights. The x-ray and gamma ray exporter released the quantity of photons per unit time [29] [31].

#### 5.2.4. Speckle Noise

It is multiplicative noise. Their occurrence has been shown in the coherent imaging systems as in the radar, and in laser. Speckle noise occurs as gaussian noise in the picture. Its probability density function follows the gamma distribution, as shown in Figure 31 and given as in equation (4) [29] [31].

$$F(g) = \frac{g^{\alpha-1} e^{-\frac{g}{a}}}{(\alpha - 1)! a^\alpha} \dots\dots\dots 4$$



The original image without noise

The speckle noise image with  $\sigma = 0.1$

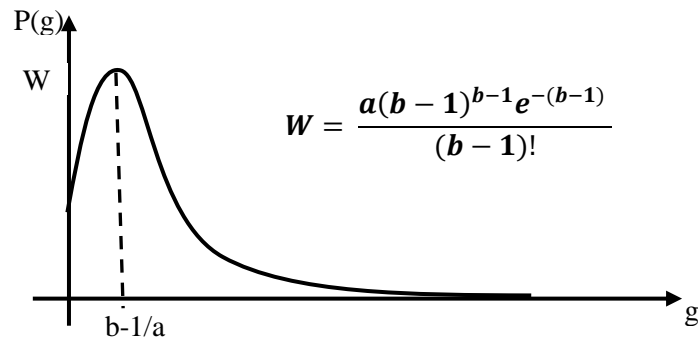
**Figure 31** The effect of speckle noise.

#### 5.2.5. Gamma Noise

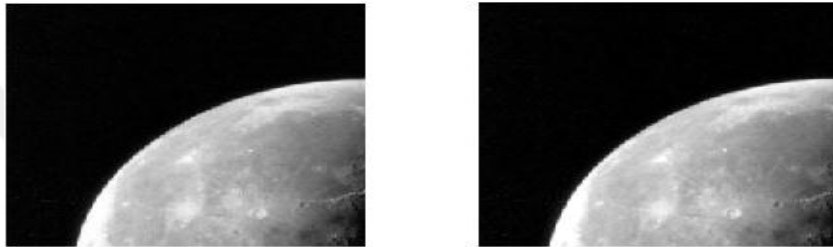
This type is present in the laser-based images. It conforms to the gamma distribution. As shown in the (Figure 32) and an equation given in (5), the effect of gamma noise is shown in (Figure 33) [30]:

$$PDF(g) = \begin{cases} \frac{a^b g^{b-1} e^{-ag}}{(b - 1)!} & \text{for } g \geq 0 \\ 0 & \text{for } g < 0 \end{cases} \dots\dots 5$$

Where mean  $\mu = \frac{b}{a}$  And variance  $\sigma^2 = \frac{b}{a^2}$



**Figure 32** The probability density function of gamma noise.



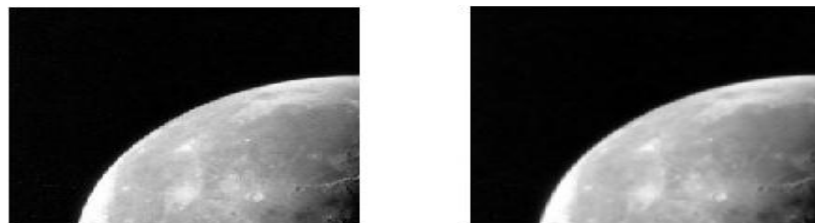
The original image without noise.

The gamma noise image.

**Figure 33** The effect of gamma noise.

### 5.2.6. Mean Filter

The mean filter is an averaging linear filter. It is determining the average amount of the corrupted image in pre-decided region. Then the center pixel intensity is changed by that average value. This operation is duplicated for all pixels in the image. Figure 34 showed the effect of using the mean filter for varying size [30].



The original image without noise

The mean filter with 3X3 filter size

**Figure 34** The effect of of mean filter.

### 5.2.7. Median Filter

It is a non-linear filter, which response is based on the ranking of the pixel amount include in the filter area. The Median filter is common for reducing certain kinds of noise. The center value of the pixel is changed by the median of the pixel mount under the filter area, Figure 35 showed the impact of the median filter [30].



The original image without noise



The median filter image.

**Figure 35** The effect of median filter.

### 5.2.8. Adjustment filter

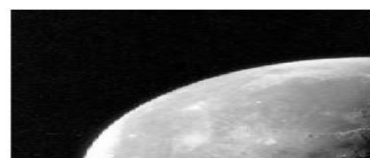
Adjustment density is a mechanism for mapping an image's density amount for new values. The gamma value portrays the form of the curve portraying the relation between the qualities in the new and old image. If gamma is under than one, the mapping is weighted toward higher (brighter) output amount. If gamma is larger than one, the mapping is weighted toward lower (darker) output amount. If deleted the argument, gamma defaults to one (linear mapping) [32]. Figure 36 shows the image adjustment by using multi-value of gamma.



The original image without noise.



The adjustment image with gamma=0.4.



The adjustment image with gamma=0.8.



The adjustment image with gamma=1.5.

**Figure 36** The effect of image adjustment.

### 5.3. The Graphical User Interface Model of Multi Type of Noise

To study the noise effects of the proposed algorithm, we use eight types of noise and filter in this thesis; we built our system in MATLAB program by using the GUI model as shown in (Figure 37).

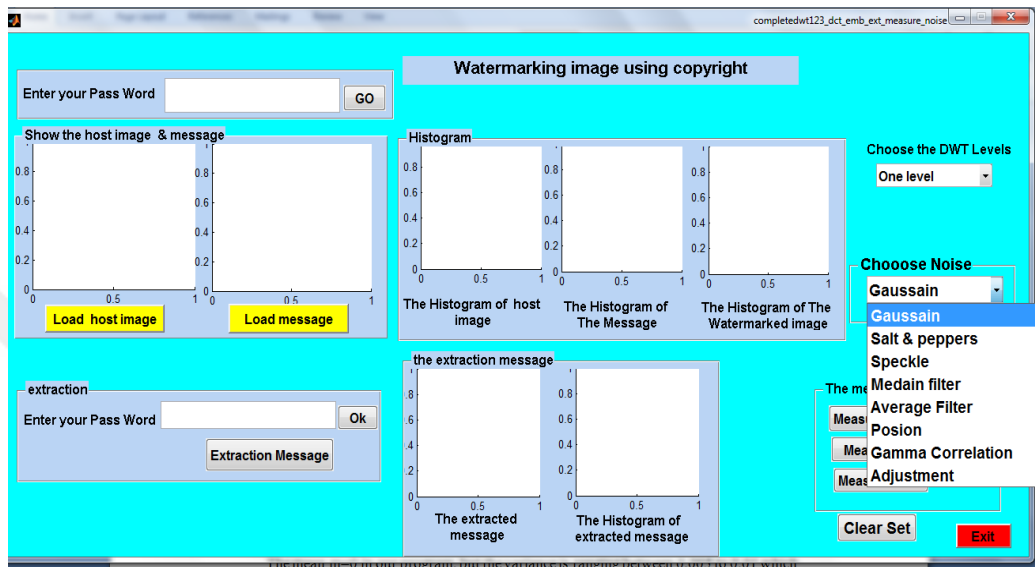


Figure 37 The eight types of noise in GUI model.

The GUI steps are:

- 1- Choose Noise POP-UP menu which contains a multi - type of noise, firstly choose “Gaussian” to adding gaussian white noise of mean ‘m’ and variance ‘var’ to our watermarking algorithm. (Note that the host image is “GOLDHILL” gray scale image). The mean  $m=0$  in our program, but the variance is ranging between 0.005 to 0.01 which display in question message as shown in (Figure 38).

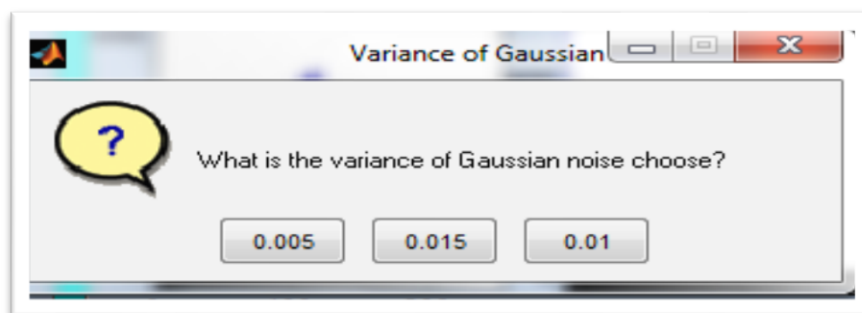





Figure 38 The message of choosing a variance value.

2- Choose one of these three values of variance to find the gaussian effect and the new figure is displayed the original host image, the message and the noisy image, as shown in (Table 3).

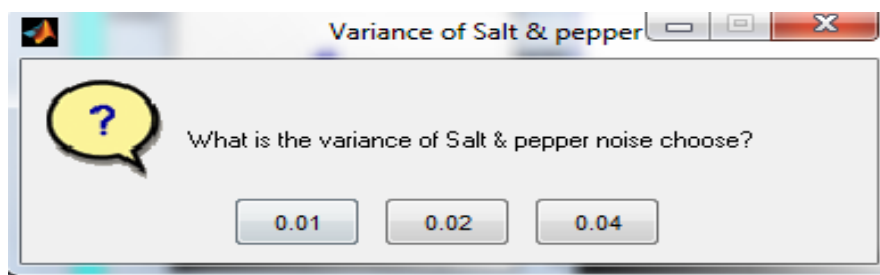
**Table 3** The gaussian noise with  $\sigma = 0.005, 0.015$  and  $0.10$

Variance	Results		The reconstruction message
0.005	PSNR	38.83	
	NCC	0.98769	
	NHD	0.00195	
0.015	PSNR	27.69	
	NCC	0.96	
	NHD	0.069	
0.010	PSNR	28.039	
	NCC	0.972	
	NHD	0.0293	

As we show in the previous table, we use three different random values for variance, these values are most commonly in previous work, and we used those values to show the effect of noise on the image and showing the efficiency of the system.

We are getting the best result for PSNR, NCC and NHD when we used the variance value 0.005




3- Choose the “salt & peppers” in POP\_UP menu, this kind of noise depends on noise density ‘d’. The values of (d) are ranging from 0.01 to 0.04, which can be chosen by question message as shown in (Figure 39).



**Figure 39** The message of salt & pepper density.

Then display the measurements BOTTONs as shown in (Table 4).

**Table 4** The effect of salt and pepper with  $d=0.01, 0.02$  and  $0.04$






Density	The results		The reconstruction message
0.01	PSNR	40.43	
	NCC	0.978	
	NHD	0	
0.02	PSNR	39.42	
	NCC	0.959	
	NHD	0.011	
0.04	PSNR	38.02	
	NCC	0.9188	
	NHD	0.056	

As we show in the previous table, we use three different random density values ( $d$ ), these values are most commonly in previous work, , and we used those values to show the effect of noise on the image and showing the efficiency of the system.

We are getting the best result for PSNR, NCC and NHD when we used the variance value 0.01.

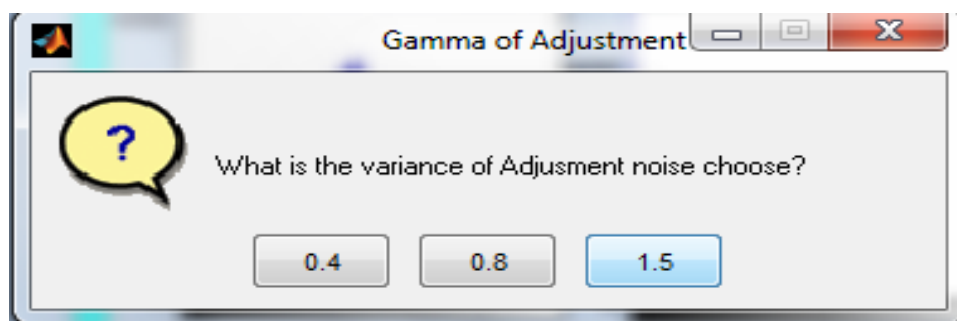
4- The speckle, median, average filter, poisons and gamma correlation noise can be implemented on our algorithm and the measurements can be displayed as shown in (Table 5).

**Table 5** The effect of different types of noises

Noise type	The Results		The reconstruction message
Speckle	PSNR	27.416	
	NCC	0.934	
	NHD	0.084	
Median filter	PSNR	34.73	
	NCC	0.996	
	NHD	0.00097	
Average filter	PSNR	33.77	
	NCC	0.995	
	NHD	0	
Poison	PSNR	31.05	
	NCC	0.995	
	NHD	0	
Gamma correlation	PSNR	41.6579	
	NCC	0.9978	
	NHD	0	

As we see in the results of the previous table, we are getting a very good reconstruction message at: Average filter, Poison and Gamma correlation, and the better results in gamma correlation.

5- The Adjustment noise depends on the gamma value so you must choose this value by click on the specific value of question message shown in (Figure 40).






**Figure 40** The question message of choosing gamma.



Most of the research is used more than the value and this value selected as random values to show the best result and effect this noise on the algorithm.

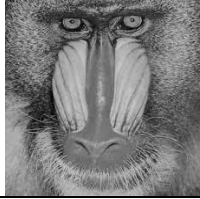




After applying the noise on the image, the measurements can be displayed as shown in (Table 6).

**Table 6** The effect of adjustment noise with gamma=0. 4, 0.8 and 1.5

Gamma	The results		The reconstruction message
0.4	PSNR	10.56	
	NCC	0.9969	
	NHD	0.1846	
0.8	PSNR	21.65	
	NCC	0.997	
	NHD	0.045	
1.5	PSNR	16.86	
	NCC	0.997	
	NHD	0.0878	

The previous results in the table show that the better PSNR,NCC and NHD when used (0.8) as the gamma value.

We use other standard gray scale images such as (Baboon, Barbara, Boat, Cameraman and Peppers), show (Figure 41). Experimentation multiple image to enable a better understanding of the proposed watermark algorithm.

	Baboon
	Barbara
	Boat
	Cameraman
	Pepper

**Figure 41** The gray scale images used to show noise effect.

The Speckle, median, average filter, poison and gamma correlation noise were implemented on previous images and the measurements can be displayed as shown in (Table 7).

**Table 7** The effect of different noise on the used images.

Type of Noise	The measurement	Baboon	Barbara	Boat	Cameraman	Peppers
The Speckle Noise	PSNR	26.27	28.15	28.03	28.60	28.018
	NCC	0.846	0.925	0.866	0.9270	0.951
	NHD	0.1445	0.1357	0.144	0.1504	0.1219
Median Filter	PSNR	36.77	38.69	40.211	40.754	39.295
	NCC	0.999	0.9997	0.9997	0.9974	0.9983
	NHD	0	0	0	0	0
Average Filter	PSNR	35.43	37.66	38.195	38.8	37.909
	NCC	0.9978	0.998	0.997	0.9964	0.9981
	NHD	0.00195	0.00195	0.0059	0.0117	0.00098
Poison	PSNR	29.81	31.66	31.396	31.84	31.478
	NCC	0.994	0.9983	0.9954	0.9963	0.9975
	NHD	0	0	0	0	0
Gamma Correlation	PSNR	41.589	41.86	43.228	42.58	39.816
	NCC	0.999	0.9999	0.999	0.9973	0.9982
	NHD	0	0	0	0	0

As we show in the table above, we are getting the best result for PSNR when we used gamma correlation; it is almost nearly (40), we are getting the NCC values nearly same in the different noise also the NHD values nearly same in the different noise.

After applying, the gaussian noise with  $\sigma = 0.005, 0.015$  and  $0.10$  (it is commonly values used in previous work) on different images we obtained the results as showed in (Table 8).

**Table 8** Effect of gaussian noise for different variance values.

The Variance	The Measurement	Baboon	Barbara	Boat	Cameraman	Peppers
$\sigma=0.005$	PSNR	27.86	29.56	29.57	29.816	29.19
	NCC	0.980	0.992	0.985	0.993	0.9939
	NHD	0.00488	0.0009	0.0078	0.0029	0.0127
$\sigma=0.015$	PSNR	27.064	28.41	28.43	28.71	28.1
	NCC	0.9511	0.9669	0.942	0.954	0.9713
	NHD	0.0292	0.0635	0.075	0.0684	0.0791
$\sigma=0.010$	PSNR	26.94	28.74	28.785	29.02	28.418
	NCC	0.966	0.981	0.964	0.985	0.985
	NHD	0.031	0.0312	0.0429	0.0419	0.0390

The previous results in table, shown that the better PSNR when used (0.005) as the variance value, we getting the NCC values nearly same in the different noise and the best NHD values at (0.005) as the variance value.

Then we are applying the salt & peppers with  $d=0.01, 0.02$  and  $0.04$  on the different images to obtain the results as showed in (Table 9).

**Table 9** Effect of salt & peppers for different density values.

The Density	The Measurement	Baboon	Barbara	Boat	Cameraman	Peppers
D=0.01	PSNR	40.09	40.79	41.805	41.386	39.083
	NCC	0.973	0.97966	0.980	0.981	0.9777
	NHD	0	0	0.0009	0	0.00195
D=0.02	PSNR	38.99	39.88	40.66	40.46	38.422
	NCC	0.948	0.960	0.957	0.964	0.959
	NHD	0.0039	0.00977	0.0117	0.0068	0.0107
D=0.04	PSNR	37.42	38.47	39.05	38.988	37.37
	NCC	0.899	0.921	0.9164	0.929	0.9216
	NHD	0.034	0.0527	0.0625	0.0419	0.05859

As we show in the previous table, we use three different random density values and we used those values to show the effect of noise on the image and showing the efficiency of the system. We are getting the best result for PSNR, NCC and NHD when we used the variance value 0.01.

Finally, we are applying, the adjustable noise with  $\gamma=0.4, 0.8$  and  $1.5$  on the different images to obtain the results as showed in (Table 10).

**Table 10** Effect of adjustment noise for different gamma values

Gamma Values	The Measurement	Baboon	Barbara	Boat	Cameraman	Peppers
0.4	PSNR	9.946	11.668	12.251	12.655	11.064
	NCC	0.999	0.9995	0.9996	0.9962	0.99765
	NHD	0.248	0.2089	0.1982	0.2129	0.2666
0.8	PSNR	20.748	22.74	22.999	23.66	22.312
	NCC	0.999	0.9999	0.9999	0.997	0.9983
	NHD	0.0419	0.0410	0.04589	0.0488	0.0547
1.5	PSNR	15.5	17.828	17.60	18.37	17.597
	NCC	0.9996	0.99964	0.9996	0.996	0.997
	NHD	0.064	0.0937	0.1152	0.0839	0.09668

As we show in the previous table, we use three different gamma values, these values are most commonly in previous work, and we used those values to show the effect of noise on the image and showing the efficiency of the system.

We are getting the best results for PSNR, NCC and NHD when we used gamma value (0.8).

## CAPTER 6

### CONCLUSIONS AND FUTURE WORK

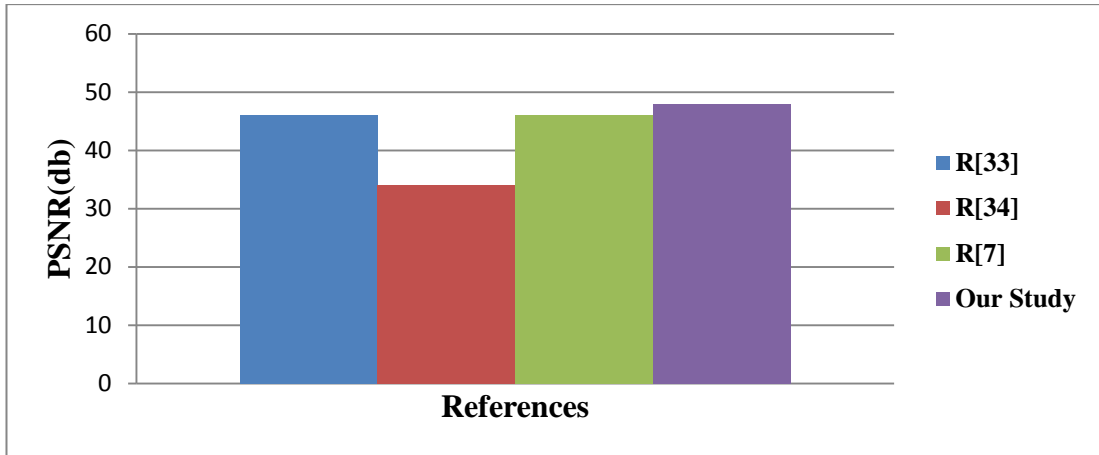
#### 6.1. Conclusions

Through this research, we introduced a novel robust and private watermark method using transform domain techniques. The watermarking image techniques based on a three level discrete wavelet transform. The implementations results shows that the three level DWT provide better performance than one level and two level DWT, as well as the results obtained from the recovered images and the watermark are similar to the original images.

In the beginning, we watermarked the message in the frequency domain. The method employs the combinatorial 2D-DCT with multi-level 2D-DWT to realize the watermark algorithm.

This thesis was implemented firstly without using any type of noise, all the results indicated that the PSNR was reached to 48 dB, which means that the hidden information (the message) does not effect in the large portion of the original image.

We made a comparison between some different researches and our work, when we programmed the proposed watermark algorithm without any type of noise in the (Figure 42).

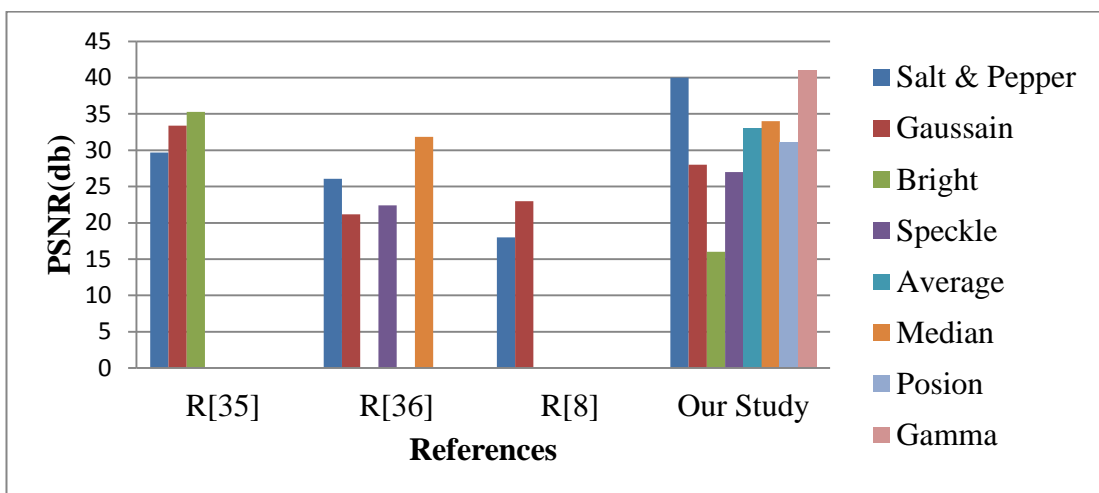


**Figure 42** The PSNR in dB of different references and our study without noise.

As we show in the previous chart, we get the best result for the PSNR (48db) compared with other previous works.

To get better robustness and security of used method, hash scrambling transformation was used, then we are adding a multi type of noise, we got a large amount of robust against salt & peppers with different values of density. This work has an efficient and perfect reconstruction when using median filter, poison and gamma correlation.

The results of this thesis when using some types of noise and compare it with other previous researchers in the chart below:



**Figure 43** The effect of many types of noises in watermarking algorithms.



## 6.2. Future Work

The proposed methods can be extended and improved in the following aspects:

- It is possible to add another mathematics theory, method by employing some better matrix decomposition of SVD and compare the results
- We can be expanding our algorithm by trying other functions of secure hash algorithms.
- We can use techniques such as colour image watermark, it would significantly boost the usage of the image processing, and thus we can develop our work and apply our proposed algorithm for colour images.



## REFERENCES

1. **Mohanty, S. P. (1999).** "Watermarking of digital images", Submitted at Indian Institute of Science Bangalore, 1-3. -560 12.
2. **Mohanpurkar, A. A., & Joshi, M. S. (2011, December).** "Applying watermarking for copyright protection, traitor identification and joint ownership: A review. In *Information and Communication Technologies (WICT)*", 2011 World Congress on (pp. 1014-1019). IEEE.
3. **Jalil, Z. (2010).** "Copyright protection of plain text using digital watermarking", Doctoral dissertation, National University of Computer and Emerging Sciences Islamabad.
4. **Xuehua, J. (2010).** "Digital watermarking and its application in image copyright protection". In *Intelligent Computation Technology and Automation (ICICTA)*, International Conference on (Vol. 2, pp. 114-117). IEEE.
5. **Thawkar, S.(2012).** "Digital Image Watermarking for Copyright Protection", *International Journal of Computer Science and Information Technologies*, 3(2), 3757-3760.
6. **Bhargava, N., Sharma, M. M., Garhwal, A. S., & Mathuria, M. (2012).** "Digital image authentication system based on digital watermarking". In *Radar, Communication and Computing (ICRCC)*, International Conference on (pp. 185-189). IEEE.

7. **Kumar, A., Ghrera, S. P., & Tyagi, V. (2016).** “*Modified buyer seller watermarking protocol based on discrete wavelet transform and principal component analysis*”. Indian Journal of Science and Technology, 8(35).
8. **Furqan, A., & Kumar, M. (2015).** ” *Study and analysis of robust DWT-SVD domain based digital image watermarking technique using MATLAB*”. In Computational Intelligence & Communication Technology (CICT), IEEE International Conference on (pp. 638-644).
9. **Obimbo, C., & Salami, B. (2012).** ”*Using digital watermarking for copyright protection*”. INTECH Open Access Publisher.
10. **Terzija, N. (2006).** “*Robust digital image watermarking algorithms for copyright protection Doctoral dissertation*”, Universität Duisburg-Essen, Fakultät für Ingenieurwissenschaften» Informatik und Angewandte Kognitionswissenschaft» Angewandte Kognitions-und Medienwissenschaft» Allgemeine Psychologie: Kognition.
11. **Abbasfard, M. (2009).** “*Digital image watermarking robustness:A comparative study*”. Delft University of Technology, RERTRE, 74.
12. **Sharma, M., & Shiwani, S. (2013).** “*Noise Attack Analysis on Non Blind DWT Watermarking Algorithm*”. International Journal of Emerging Technology and Advanced Engineering, 3(7), 374-378.
13. **Singh, B. K., & Dua, T.(2015).** ”*Image Authentication Using Digital Watermarking*”, International Journal of Computational Engineering Research.
14. **Dubolia, R., Singh, R., Bhadoria, S. S., & Gupta, R. (2011).** ” *Digital image watermarking by using discrete wavelet transform and discrete cosine transform and comparison based on PSNR*”. In Communication Systems and Network Technologies (CSNT), International Conference on (pp. 593-596). IEEE.
15. **Rawat, K. S., & Tomar, D. S. (2010).** “*Digital watermarking schemes for authorization against copying or piracy of color images*”. Indian Journal of Computer Science and Engineering, 1(4), 295-300.

16. **G. R. Sinha, (2012).** ” *Implementation of Modified DWT and LSB Techniques for Image Watermarking*”.
17. **Watson, A. B. (1994).** “*Image compression using the discrete cosine transform*”, *Mathematica journal*, 4(1), 81.
18. **Chen, H. Y., & Zhu, Y. S. (2012).** “*A robust watermarking algorithm based on QR factorization and DCT using quantization index modulation technique*”, *Journal of Zhejiang University SCIENCE C*, 13(8), 573-584.
19. **Raid, A. M., Khedr, W. M., El-Dosuky, M. A., & Ahmed, W. (2014).**” *JPEG image compression using discrete cosine transform-A Survey*”, arXiv preprint arXiv:1405.6147.
20. **Khayam, S. A. (2003).** “*The discrete cosine transform (DCT): theory and application*”. Michigan State University, 114.
21. **Sharma, P., & Swami, S. (2013).** “*Digital image watermarking using 3 level discrete wavelet transform*”. In *Conference on Advances in Communication and Control Systems* (pp. 129-133).
22. **Docherty, J., & Koelmans, A. (2011, May).** “*A flexible hardware implementation of SHA-1 and SHA-2 Hash Functions. In Circuits and Systems (ISCAS)*”, 2011 IEEE International Symposium on (pp. 1932-1935).
23. **Wen, C. Y., & Yang, K. T. (2006).** “*Image authentication for digital image evidence*”, *Forensic science journal*, 5(1), 1-11.
24. **Watkins, M., & Wallace, K. (2008).**” *Ccna security official exam certification guide (exam 640-553)*”. Cisco Press.

25. **Wang, Z., & Bovik, A. C. (2009).** “*Mean squared error: Love it or leave it , A new look at signal fidelity measures*”. IEEE signal processing magazine, 26(1), 98-117.
  
26. **Dabas, P., & Khanna, K. (2013).** “*A study on spatial and transform domain watermarking techniques*”. International Journal of Computer Applications, 71(14).
  
27. **Bandyopadhyay, T., Bandyopadhyay, B., & Chatterji, B. N. (2012).** “*Image security through SVD based robust watermarking and compression techniques*”. International Journal of Emerging Trends & Technology in Computer Science, 1(3), 160-165.
  
28. **R. C. Gonzales, R. E. Woods (2002).** ” *Digital Image Processing*”, 2-nd Edition.
  
29. **Verma, R., & Ali, J. (2013).** “*A comparative study of various types of image noise and efficient noise removal techniques*”. International Journal of advanced research in computer science and software engineering, 3(10), 617-622.
  
30. **Boyat, A. K., & Joshi, B. K. (2015).** “*A review paper: noise models in digital image processing*”, arXiv preprint arXiv:1505.03489.
  
31. **Patidar, P., Gupta, M., Srivastava, S., & Nagawat, A. K. (2010).** “*Image de-noising by various filters for different noise*”, International Journal of Computer Applications, 9(4).
  
32. **Karspeck, A. R., & Anderson, J. L. (2007).** “*Experimental implementation of an ensemble adjustment filter for an intermediate ENSO model*”, Journal of Climate, 20(18), 4638-4658.
  
33. **TN, S., Ramesha, K., & Raj, C. P.,(2014).**“*A New Technique to Digital Image Watermarking Using DWT for Real Time Applications*”, Journal of

34. **Singh, B., Dhaka, V. S., & Saharan, R. (2014).** " *Blind detection attack resistant image watermarking* ", In Consumer Electronics (GCCE), IEEE 3rd Global Conference on (pp. 289-293).
35. **Kumar, A. (2014).** " *A Novel Watermarking Algorithm for Color Images Based on Discrete Wavelet Transform* ", International Journal of Computer and Electrical Engineering, 6(4), 303.
36. **Yan, H., & Yang, W. (2013).** " *A Watermarking Algorithm Based on Wavelet and Hadamard Transform for Color Image* ", Journal of Software Engineering and Applications, 6(03), 58.
37. **Abdullatif, M., Zeki, A. M., Chebil, J., & Gunawan, T. S. (2013).** " *Properties of digital image watermarking. In Signal Processing and its Applications (CSPA)* ", IEEE 9th International Colloquium on (pp. 235-240).
38. **Krunal, M., & Lokesh, M. (2013).** " *Current classification and introduction of Watermarking Techniques in Digital Images* ", International Journal of Engineering Research and Applications, 3(1), 840-846.
39. **Panah, A. S., Van Schyndel, R., Sellis, T., & Bertino, E. (2016).** " *On the properties of non-media digital watermarking: a review of state of the art techniques* ", IEEE Access, 4, 2670-2704.
40. **Rashid, A. (2016).** " *Digital Watermarking Applications and Techniques: A Brief Review* ", International Journal of Computer Applications Technology and Research Volume 5–Issue 3, 147-150, ISSN:2319–8656.

## APPENDICES A

### CURRICULUM VITAE

#### PERSONAL INFORMATION

Surname, Name: ALLAYLA, Hassan Fakhry  
Nationality: Iraqi  
Date and Place of Birth: 9 Jun 1979, Mosul, Iraq  
Material Status: Married  
Phone: +90 539 259 1284  
Email: [hassan79.allayla@gmail.com](mailto:hassan79.allayla@gmail.com)

#### EDUCATION

Degree	Institution	Year of Graduation
M.Sc.	Çankaya University Computer Engineering	2017
B.Sc.	Mosul Univ. College of Engineering. Computer Engineering Dept.	2003
High School	Omar Bin Alkhattab	1997

#### WORK EXPERIENCE

Year	Place	Enrollment
2004 - present	Mosul Univ. College of Engineering. Computer Eng. Dept.	Laboratories Instructors

#### FOREIGN LANGUAGES

Arabic (mother language), English.

#### HOBBIES

Reading, News, Travelling.