



# **Developing a Robust Digital Image Watermark by Using Frequency and Spatial Domains**

تطوير علامة مائية صلبة للصور الرقمية  
باستخدام المجالين الترددي و المكاني

**By  
Wisam Ahmad Hassan**

**Supervised by  
Prof. Dr. Alaa Al-Hamami**

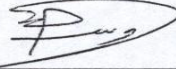
**This thesis is submitted in partial fulfillment of the  
requirements for the degree of Master in computer  
science**

**Department of Computer Science  
College of Computer Sciences and Informatics  
Amman Arab University  
May 2010**

## AUTHORIZATION OF THESIS

I, the undersigned "Wisam Ahmad Hassan" authorize hereby "Amman Arab University for Graduate Studies" to provide copies of this thesis to libraries, institutions, agencies, and other parties upon their request.

Signature \_\_\_\_\_



© Copyright by

AMMAN ARAB UNIVERSITY FOR GRADUATE STUDIES (AAU).

## APPROVAL

**Name:** Wisam Ahmad Hassan

**Degree:** Master of Computer Science

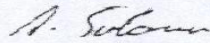
**Title of thesis:** Developing a Robust Digital Image Watermark  
by Using Frequency and Spatial Domains

**Examining Committee:**



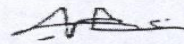
---

**Chair. Dr. Basil Kasasbeh**



---

**Dr. Adnan Rawashdeh, Member**



---

**Prof. Dr. Alaa Al-hamami, Member and Supervisor**

## **Dedication**

**I am pleased to dedicate this work to the people most precious to my heart; my father and my mother, who did not spare any effort in my support throughout the preparatory period for this study.**

**I also do not forget in this place to dedicate this achievement to my wife for her patience, encouragement through all the difficult moments that I passed.**

**Finally I wish to express my thanks to my friends who motivated me to finish my thesis.**

## **Acknowledgment**

**God, without your guidance and help, I would never have reached where I am today. Thank you.**

**I wish to express special thanks to Dr. Alaa Al-Hamami, for his support and guidance during the preparation of this thesis.**

**Special thanks to Dr. Ali Al-Haj, Samer Al-Khateeb, Hussam Al-Khawaldeh, Malek Al-Zoboun, Rodwan Abu-Saif, and Tuqa Al-Manasrah, for their help and support during the preparation of this thesis.**

**Also special thanks to the esteemed chairman and members of the Examination Committee of this thesis.**

## Table of Contents

<b>DEDICATION .....</b>	<b>IV</b>
<b>ACKNOWLEDGMENT .....</b>	<b>V</b>
<b>TABLE OF CONTENTS .....</b>	<b>VI</b>
<b>LIST OF TABLES.....</b>	<b>IX</b>
<b>LIST OF FIGURES .....</b>	<b>X</b>
<b>LIST OF ABBREVIATIONS.....</b>	<b>XVII</b>
<b>ABSTRACT .....</b>	<b>XIX</b>
<b>CHAPTER ONE INTRODUCTION.....</b>	<b>1</b>
1.1 BACKGROUND: .....	1
1.2 CRYPTOGRAPHY:.....	1
1.3 HISTORY OF CRYPTOGRAPHY:.....	3
1.4 STEGANOGRAPHY:.....	5
1.5 HISTORY OF STEGANOGRAPHY:.....	8
1.6 STEGANOGRAPHY VS CRYPTOGRAPHY: .....	10
1.7 WATER MARKING: .....	11
1.8 HISTORY OF WATERMARKING:.....	12
1.8.1 SPATIAL DOMAIN: .....	13
1.8.1.1 LEAST SIGNIFICANT BIT (LSB): .....	14
1.8.2 FREQUENCY DOMAIN: .....	14
1.8.2.1 DISCRETE WAVELET TRANSFORM (DWT): .....	15
1.9 STATEMENT OF THE PROBLEM: .....	15
1.10 CONTRIBUTION: .....	16
1.11 THESIS ORGANIZATION:.....	17
<b>CHAPTER TWO LITERATURE SURVEY .....</b>	<b>18</b>
2.1 WATERMARKING STAGES: .....	18
2.1.1 EMBEDDING STAGE:.....	18
2.1.2 EXTRACTION STAGE:.....	19
2.2 WATERMARKING APPLICATIONS:.....	19
2.2.1 COPYRIGHT PROTECTION AND AUTHENTICATION:.....	20
2.2.2 FINGERPRINTING AND DIGITAL “SIGNATURES”: .....	21
2.2.3 COPY PROTECTION AND DEVICE CONTROL:.....	22
2.2.4 BROADCASTING MONITORING:.....	22



2.2.5 DATA AUTHENTICATION: .....	24
2.3 WATERMARKING REQUIREMENTS: .....	24
2.3.1 PROPERTIES RELATED TO THE EMBEDDING PROCESS: .....	25
2.3.1.1 PERCEPTUAL INVISIBILITY: .....	25
2.3.1.2 STATISTICAL INVISIBILITY: .....	25
2.3.1.3 FIDELITY: .....	25
2.3.1.4 DATA PAYLOAD: .....	26
2.3.1.5 EMBEDDED EFFECTIVENESS: .....	26
2.3.2 PROPERTIES RELATED TO THE DETECTION PROCESS: .....	26
2.3.2.1 ROBUSTNESS: .....	26
2.3.2.2 BLIND/INFORMED DETECTION: .....	27
2.3.2.3 FALSE POSITIVE RATE: .....	28
2.3.3 PROPERTIES RELATED TO BOTH EMBEDDING AND DETECTION: .....	28
2.3.3.1 SECURITY: .....	28
2.3.3.2 COST: .....	29
2.3.3.3 MULTIPLE WATERMARKING: .....	29
2.4 WATERMARKING TECHNIQUES: .....	30
2.5 WATERMARKING ATTACKS: .....	34
2.5.1 INTERFERENCE AND REMOVAL ATTACKS: .....	35
2.5.2 GEOMETRICAL ATTACKS: .....	35
2.5.3 CRYPTOGRAPHIC ATTACKS: .....	36
2.5.4 PROTOCOL ATTACKS: .....	36
2.6 PREVIOUS STUDIES: .....	37
2.6.1 SPATIAL DOMAIN ALGORITHMS: .....	37
2.6.2 FREQUENCY DOMAIN ALGORITHMS: .....	39
2.6.2 DISCUSSION OF SPATIAL DOMAIN ALGORITHMS: .....	45
2.6.3 DISCUSSION OF FREQUENCY DOMAIN ALGORITHMS: .....	45
<b>CHAPTER THREE THE PROPOSED METHOD .....</b>	<b>47</b>
3.1 INTRODUCTION .....	47
3.2 EMBEDDING STAGE: .....	47
3.3 EXTRACTION STAGE: .....	48
3.4 FLOWCHART ILLUSTRATION: .....	49
3.4.1 <i>Embedding Process</i> : .....	49
3.4.2 <i>Extraction process</i> : .....	53
3.5: SUMMARY: .....	56
<b>CHAPTER FOUR EXPERIMENTAL RESULTS .....</b>	<b>58</b>
4.1 PERFORMANCE EVALUATION: .....	58
4.2 ATTACKS ON THE PROPOSED WATERMARKING SYSTEM: .....	64

4.2.1: ADDING NOISE:.....	64
4.2.2 MEDIAN FILTERING:.....	66
4.2.3 REDUCING NOISE: .....	68
4.2.4 JPEG COMPRESSION: .....	70
4.2.5 <i>Image Cropping</i> : .....	72
4.2.6 IMAGE CUTTING:.....	74
4.2.7 IMAGE SHARPENING:.....	76
4.2.8 INK SKETCH: .....	79
4.2.9 IMAGE GLOW:.....	81
4.3 ROBUSTNESS RESULTS VIEWING:.....	83
4.4 IMPERCEPTIBILITY RESULTS VIEWING:.....	84
<b>CHAPTER FIVE CONCLUSIONS AND FUTURE WORKS.....</b>	<b>85</b>
5.1 CONCLUSIONS:.....	85
5.2 FUTURE WORKS: .....	86
<b>REFERENCES .....</b>	<b>87</b>



## List of Tables

Number	Title	Page
1.1	Rotation Scheme outline	5
4.1	The correlation values for each image used in the tests against different attacks	85
4.2	The PSNR values for each image used in the tests	86

## List of Figures

Number	Title	Page
1.1	Cryptography for secure communication	3
1.2	Steganographic system	7
1.3	Steganography	11
1.4	Cryptography	11
1.5	Basic scheme of watermarking	12
1.6	Annual number of papers published on watermarking and Steganography by the IEEE	13
2.1	Digital Watermarking-Embedding	20
2.2	Digital Watermarking -Extraction	21
2.3	Types of Watermarking Techniques	32
2.4	Schematic representation of dual watermarking	34

<b>2.5</b>	Classification of watermarking attacks	<b>36</b>
<b>2.6</b>	Quantization of the middle coefficient	<b>42</b>
<b>3.1</b>	Watermark image transforming to binary form	<b>51</b>
<b>3.2</b>	Representing the watermark image in vector array	<b>51</b>
<b>3.3</b>	Applying DWT function for the host image and its resulted four decompositions	<b>52</b>
<b>3.4</b>	LH <sub>1</sub> coefficients after converting to vector	<b>52</b>
<b>3.5</b>	Converting LH <sub>1</sub> coefficients into binary form	<b>53</b>
<b>3.6</b>	LH <sub>1</sub> after Embedding watermark bits in it	<b>54</b>
<b>3.7</b>	Applying IDWT function for the host image coefficients and its resulted watermarked image	<b>55</b>
<b>3.8</b>	Applying DWT function for the watermarked image and its resulted coefficients	<b>55</b>
<b>3.9</b>	LH <sub>1</sub> coefficients after converting to vector	<b>56</b>
<b>3.10</b>	Selection of the HL <sub>1</sub> coefficients from the vector and converting them into binary	<b>57</b>

<b>3.11</b>	Extracting watermarks' bits from $LH_1$ binary numbers	<b>57</b>
<b>3.12</b>	Converting watermarks' bits extracted from $LH_1$ into watermark image	<b>58</b>
<b>4.1</b>	The watermarked image "Building" with its corresponding extracted watermark	<b>64</b>
<b>4.2</b>	The watermarked image "Clock" with its corresponding extracted watermark	<b>64</b>
<b>4.3</b>	The watermarked image "Field" with its corresponding extracted watermark	<b>65</b>
<b>4.4</b>	The watermarked image "Haram" with its corresponding extracted watermark	<b>65</b>
<b>4.5</b>	The watermarked image "Flowers" with its corresponding extracted watermark	<b>66</b>
<b>3.6</b>	The watermarked image "Nature" with its corresponding extracted watermark	<b>66</b>
<b>4.7</b>	The attacked watermarked image "Building" using added noise (intensity=100, coverage=10) with its corresponding extracted watermark	<b>67</b>
<b>4.8</b>	The attacked watermarked image "Clock" using added noise (intensity=100, coverage=10) with its corresponding extracted watermark	<b>67</b>

<b>4.9</b>	The attacked watermarked image "Field" using added noise (intensity=100, coverage=10) with its corresponding extracted watermark	<b>68</b>
<b>4.10</b>	The attacked watermarked image "Flowers" using added noise (intensity=100, coverage=10) with its corresponding extracted watermark	<b>68</b>
<b>4.11</b>	The attacked watermarked image "Field" using median filter (Radius=1, Percentile=100) with its corresponding extracted watermark	<b>69</b>
<b>4.12</b>	The attacked watermarked image "Building" using median filter (Radius=1, Percentile=100) with its corresponding extracted watermark	<b>69</b>
<b>4.13</b>	The attacked watermarked image "Haram" using median filter (Radius=1, Percentile=100) with its corresponding extracted watermark	<b>70</b>
<b>4.14</b>	The attacked watermarked image "Nature" using median filter (Radius=1, Percentile=100) with its corresponding extracted watermark	<b>70</b>
<b>4.15</b>	The attacked watermarked image "Building" using reducing noise (Radius=100, Strength=0.5) with its corresponding extracted watermark	<b>71</b>
<b>4.16</b>	The attacked watermarked image "Clock" using reducing noise (Radius=100, Strength=0.5) with its corresponding extracted watermark	<b>71</b>

<b>4.17</b>	The attacked watermarked image “Field” using reducing noise (Radius=100, Strength=0.5) with its corresponding extracted watermark	<b>72</b>
<b>4.18</b>	The attacked watermarked image “Haram” using reducing noise (Radius=100, Strength=0.5) with its corresponding extracted watermark	<b>72</b>
<b>4.19</b>	The attacked watermarked image “Building” using JPEG compression (Quality=50) with its corresponding extracted watermark	<b>73</b>
<b>4.20</b>	The attacked watermarked image “ Clock ” using JPEG compression (Quality=50) with its corresponding extracted watermark	<b>73</b>
<b>4.21</b>	The attacked watermarked image “ Field ” using JPEG compression (Quality=50) with its corresponding extracted watermark	<b>74</b>
<b>4.22</b>	The attacked watermarked image “ Flowers ” using JPEG compression (Quality=50) with its corresponding extracted watermark	<b>74</b>
<b>4.23</b>	The attacked watermarked image “Building” after cropping (30.5%) with its corresponding extracted watermark	<b>75</b>
<b>4.24</b>	The attacked watermarked image “Clock” after cropping (30.5%) with its corresponding extracted watermark	<b>75</b>
<b>4.25</b>	The attacked watermarked image “Field” after cropping (30.5%) with its corresponding extracted watermark	<b>76</b>
<b>4.26</b>	The attacked watermarked image “Haram” after cropping (30.5%) with its corresponding extracted watermark	<b>76</b>

<b>4.27</b>	The attacked watermarked image "Building" after cutting 4 squares (0.95×0.93) with its corresponding extracted watermark	<b>77</b>
<b>4.28</b>	The attacked watermarked image "Clock" after cutting 4 squares (0.95×0.93) with its corresponding extracted watermark	<b>77</b>
<b>4.29</b>	The attacked watermarked image "Field" after cutting 4 squares (0.95×0.93) with its corresponding extracted watermark	<b>78</b>
<b>4.30</b>	The attacked watermarked image "Flowers" after cutting 4 squares (0.95×0.93) with its corresponding extracted watermark	<b>78</b>
<b>4.31</b>	The attacked watermarked image "Building" using sharpen (amount=20) with its corresponding extracted watermark	<b>79</b>
<b>4.32</b>	The attacked watermarked image "Clock" using sharpen (amount=20) with its corresponding extracted watermark	<b>79</b>
<b>4.33</b>	The attacked watermarked image "Flowers" using sharpen (amount=20) with its corresponding extracted watermark	<b>80</b>
<b>4.34</b>	The attacked watermarked image "Nature" using sharpen (amount=20) with its corresponding extracted watermark	<b>80</b>
<b>4.35</b>	The attacked watermarked image "Field" using Ink sketch (ink outline=20, coloring=100) with its corresponding extracted watermark	<b>81</b>
<b>4.36</b>	The attacked watermarked image "Clock" using Ink sketch (ink outline=20, coloring=100) with its corresponding extracted watermark	<b>81</b>



<b>4.37</b>	The attacked watermarked image “Nature” using Ink sketch (ink outline=20, coloring=100) with its corresponding extracted watermark	<b>82</b>
<b>4.38</b>	The attacked watermarked image “Building” using Ink sketch (ink outline=20, coloring=100) with its corresponding extracted watermark	<b>82</b>
<b>4.39</b>	The attacked watermarked image “Field” using Image Glow (radius=1, brightness=10, contrast=10) with its corresponding extracted watermark	<b>83</b>
<b>4.40</b>	The attacked watermarked image “Clock” using Image Glow (radius=1, brightness=10, contrast=10) with its corresponding extracted watermark	<b>83</b>
<b>4.41</b>	The attacked watermarked image “Nature” using Image Glow (radius=1, brightness=10, contrast=10) with its corresponding extracted watermark	<b>84</b>
<b>4.42</b>	The attacked watermarked image “Flowers” using Image Glow (radius=1, brightness=10, contrast=10) with its corresponding extracted watermark	<b>84</b>

## List of Abbreviations

Abbreviation	Description	Page
<b>DCT</b>	Discrete Cosine Transform	<b>32</b>
<b>DWT</b>	Discrete Wavelet Transform	<b>15</b>
<b>HAS</b>	Human Audio System	<b>26</b>
<b>HH</b>	High Pass Filtering through Rows followed by High Pass Filtering through Columns	<b>15</b>
<b>HL</b>	High Pass Filtering through Rows followed by Low Pass Filtering through Columns	<b>15</b>
<b>HVS</b>	Human Visual System	<b>26</b>
<b>IDWT</b>	Inverse Discrete Wavelet Transform	<b>55</b>
<b>LH</b>	Low Pass Filtering through Rows followed by High Pass Filtering through Columns	<b>15</b>
<b>LL</b>	Low Pass Filtering through Rows followed by Low Pass Filtering through Columns	<b>15</b>
<b>LSB</b>	Least Significant Bit	<b>14</b>

<b>MSE</b>	Mean Square Error	<b>61</b>
<b>PSNR</b>	Peak Signal To Noise Ratio	<b>61</b>
<b>ROT</b>	Rotation Scheme	<b>4</b>
<b>SAG</b>	Screen Actor's Guild	<b>24</b>

# **Developing a Robust Digital Image Watermark by Using Frequency and Spatial Domains**

**By  
Wisam Ahmad Hassan**

**Supervised by  
Prof. Dr. Alaa Al-Hamami**

## **Abstract**

The rapid growth of the internet, and the speed of file transfers caused the digitalization of media assets, so many illegal copies of images, music titles, and video films appeared. As a countermeasure mechanism; digital watermarking took its role to protect these digital assets and associated rights.

In this thesis a new approach is presented for private digital image watermarking, the meaning of private, here, is the images that could not be found on public resources like Internet. It combines two domains for watermark embedding, the frequency domain particularly Discrete Wavelet Transform (DWT), and the spatial domain particularly Least Significant Bit (LSB).

The proposed watermarking algorithm operates in the Discrete Wavelet Transform (DWT) to separate the image into a lower resolution approximation image (LL1) as well as Horizontal (HL1), Vertical (LH1) and Diagonal (HH1) detail components. The process can then be repeated to compute multiple “scale” wavelet decomposition.

Specific coefficients from the vertical detail components are selected and transformed to binary code then the system picks one of the least significant bits for each number according to the number of ones in the most significant part and replace it with one bit from the watermark message. Then the Inverse Discrete Wavelet Transform (IDWT) is applied to the transformed image to obtain the watermarked image.

This algorithm has been tried against many attacks like lossy compression, noise addition, cropping, and some other attacks against its robustness. It achieved a high success of increasing robustness of the proposed watermark, with little or no additional impact on image quality.

## تطوير علامة مائية صلدة للصور الرقمية باستخدام المجالين الترددي و المكاني

### الملخص

كان التطور المتسارع في الانترنت، و السرعة في نقل الملفات سببا في تحويل الوسائط المتوافرة إلى النظام الرقمي، و لهذا فإن العديد من النسخ غير القانونية من الصور و المقاطع الموسيقية و أفلام الفيديو بدأت بالظهور. و كإجراء مضاد لهذا الأمر أخذت تقنية العلامة المائية دورها في حماية هذه الموجودات الرقمية و الحقوق المرتبطة بها.

تقدم هذه الرسالة خوارزمية خاصة بالعلامة المائية للصور الرقمية ذات الاستخدام الخاص\_ أي أنها متعلقة بالصور ذات الاستعمال الخاص\_ و ليس ذلك النوع من الصور التي تجدها على شبكة الانترنت. حيث تدمج هذه الخوارزمية مجالين مختلفين للعلامة المائية: المجال الترددي؛ تحديدا تحويل المويجات المنفصلة مع المجال المكاني؛ و تحديدا البت الأقل أهمية.

تعمل الخوارزمية المقترحة بداية في نطاق المجال الترددي و هذا يؤدي إلى تحليل الصورة المراد حمايتها إلى أربع صور أقل في الوضوح و هي (LL<sub>1</sub>) و (HL<sub>1</sub>) و (LH<sub>1</sub>) و (HH<sub>1</sub>)، و هذه العملية يمكن تكرارها أكثر من مرة لتكوين تدرجات أصغر من الصورة. بعد ذلك يتم اختيار مجموعة من النقاط التابعة للجزء (LH<sub>1</sub>) بناء على عدد البتات الخاصة بالعلامة المائية التي سيتم إدراجها داخل هذه الصورة و تحول إلى النظام الثنائي حتى تسهل عملية استبدال بت من العلامة المائية ببت آخر من كل بايت تم اختياره. في النهاية يتم إخضاع الأجزاء الأربعة من الصورة المراد إخفاء العلامة المائية بداخلها لعملية عكسية تؤدي من جديد لتجميعها و تكوينها للصورة السابقة و لكن بعد أن تم إخفاء العلامة المائية بداخلها.

أظهرت هذه الخوارزمية فعالية عالية فيما يتعلق بصلادة العلامة المائية، حيث تم تجربتها من خلال إخضاعها لهجمات مختلفة مثل عمليات إضافة التشويش و تقليله و الضغط ذو فقدان و القص و القطع و غير ذلك من الهجمات و تم استرداد العلامة المائية المخفية بدرجات متفاوتة من الصلادة، كما أنها أظهرت قدرة جيدة على إخفاء العلامة المائية دون التأثير على الصورة الحاملة بشكل ملحوظ .



# Chapter One

## Introduction

### 1.1 Background:

In the last two decades the Internet has become user friendly with the introduction of Mosaic web browser and it quickly became clear that people wanted to download pictures, music, and videos. The Internet is an excellent distribution system for digital media because it is inexpensive, eliminates warehousing and stock, and delivery is almost instantaneous. However, content owners also see a high risk of piracy. Thus, they eagerly seek technologies that promise to protect their rights [8].

### 1.2 Cryptography:

The first technology content owners turn to is cryptography. It is probably the most common method of protecting digital content and certainly one of the best developed as a science [8]. Cryptography means “secret writing”. Another definition Cryptography is the process of sending indistinct form of messages, so that only the intended recipient can understand the secret message [25].

In cryptography the message to be sent before encryption is called a plain text, and then it is encrypted to become a cipher text prior to delivery. It is decrypted by the end receiver using a key provided at the destination. The process of converting the plain text to cipher text is called encryption or enciphering, and the reverse process is called decryption or deciphering [13], this is shown in Figure 1.1 [33]:

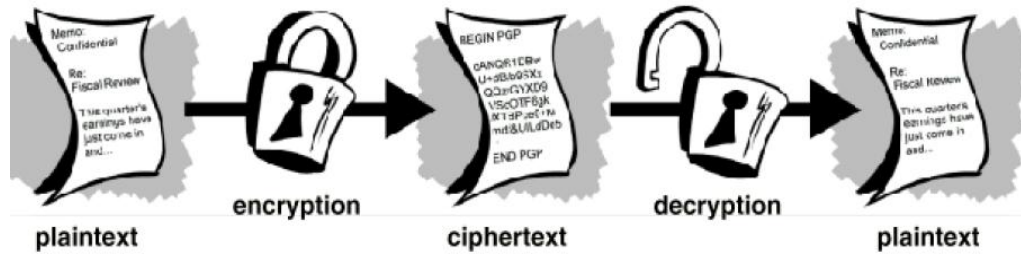


Figure 1.1: Cryptography for secure communication

Throughout history, crypto has been used for a variety of purposes, both ethical and not so ethical. As with any technology, cryptography can be used both legitimately and by those who have illegal or immoral secrets to hide [4].

Cryptography has been used to protect the following [4]:

- ■ Launch codes of nuclear weapons.
- ■ The location of military troops.
- ■ Names of suspected criminals.
- ■ The formula for a new product.
- ■ A new research idea.

But it has also been used to do the following [4]:

- ■ Convey stolen industrial secrets.
- ■ Send directives to terrorists.
- ■ Plan criminal activities.

### 1.3 History of Cryptography:

Cryptography was in use long before computers ever arrived on the scene. In fact, one of the earliest uses of crypto dates back to Julius Caesar. Julius Caesar utilized a basic level of encryption, often referred to as a Caesar cipher, to communicate his political and military secrets. The Caesar cipher is also referred to as a ROT or rotation scheme. Caesar or ROT ciphers simply rotate a character a certain number of places in the alphabet. Say that you are using ROT 3 scheme with the English language; in that case, each letter would be rotated three spaces in the alphabet [4].

The word “cat” would become “fdw” by rotating the letters three places forward— letter “c” rotated three places to the letter “f”, and so on.

This table shows ROT 1 scheme where each letter moves one letter to the right:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a

To encrypt a message with ROT 1 scheme you find the letter on the top row and replace it with the letter on the bottom row. In this case “cat” would become “dbu”. To translate “dbu” back into the original message, you find the letter in the bottom row and replace it with the letter in the top row.

Here's an ROT 2 table, which works the same way with a two-letter shift:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
c d e f g h i j k l m n o p q r s t u v w x y z a b
```

Even though ROT is a very basic scheme, it illustrates at a fundamental level how cryptography works. The following table shows how a couple of different words are translated into unreadable text using the two rotation schemes outlined here. Try taking each scrambled message and use the preceding tables to translate it back to the original message [4].

Table 1.1: Rotation Scheme outline

ROTATION NUMBER	TEXT 1	TEXT 2	TEXT 3	TEXT 4
	<b>Cat</b>	<b>Hello</b>	<b>this is a test</b>	<b>Hello</b>
ROT 1	dbu	ifmmp	N/A	N/A
ROT 2	ecv	jgnnq	N/A	N/A

Notice that the last two rows in the table, “This is a test” and “Hello,” could not be translated precisely, because this scheme does not account for spaces or uppercase letters. It is important even in basic cryptography schemes to account for all characters that may appear in your input text.

Cryptography played a major role during World War II. Both sides spent a lot of time and money trying to crack the cryptography schemes of the other. In fact, throughout most of the major (and minor) wars in history, cryptography has played a critical role [4].

More recently, in the last 10 years, a lot of public attention has focused on cryptography. Several critical events elicited this attention, but two are particularly worth noting. The United States government launched a big effort in the 1990s to acquire the escrow of all encryption keys. This would essentially lead to a country where there was no way to protect secure information. Law enforcement would have to go through a legal process, but in the end these agencies could essentially read any messages they wanted to. This resulted in such a public uproar that the proposal was quickly put on the back burner, and the government stopped pursuing it. During this time there was heightened interest in Steganography because people realized that the only way to keep information secure might be by keeping it hidden [4].

Encryption protects the content during transmission of the data from the sender to the receiver. However after decrypting the message by the end receiver, the data is no longer protected [25], thus there is a strong need for an alternative or complement to cryptography; a technology that can protect content even after it is decrypted.

#### **1.4 Steganography:**

Steganography is complement to cryptography, Steganography is derived from the Greek word steganos, meaning covered or secret, and graphy (writing or drawing). On the simplest level, Steganography is hidden writing whether it consists of invisible ink on paper or copyright information hidden in an audio file [4].

While cryptography is about protecting the content of the messages, Steganography is about concealing their very existence [29].

Examples can be thought of as messages are exchanged between drug dealers via emails in encrypted forms, or messages exchanged by spies in covert communication. Steganography hides the fact that the communication has ever occurred as shown in Figure 1.2.

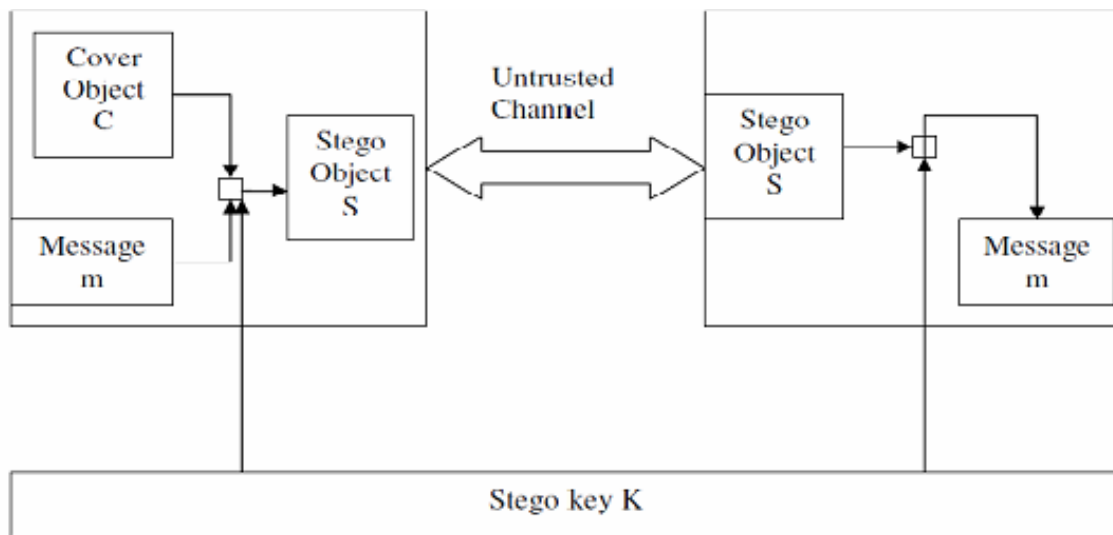


Figure 1.2: Steganographic system

Let us consider that Alice, who wants to share a secret message  $m$  with Bob, selects randomly a harmless message or a cover object  $C$ . The message to be shared is then embedded into  $C$ , by using key  $K$  (called stego-key), and the cover object  $C$  is transformed to stego object  $S$ . This stego “object” can be transmitted to Bob without raising any suspicion. This should be done in such a way that a third party knowing only the apparently harmless message  $S$  cannot detect the existence of

the secret. The cover object could be any data such as image files, written text or digital sound. In a perfect system, a normal cover object should not be distinguishable from the stego object, neither by a human nor by a computer looking for statistical patterns [20].

Alice transmits the stego object  $S$  to Bob over an insecure channel. Bob can reconstruct the message  $m$  by using the same key  $K$  as used by Alice during embedding the message in the cover object. The extraction process should not need any knowledge of the cover object [20].

Any person watching the communication should not be able to decide whether the sender is sending covers with messages embedded into them. In other words, a person with a number of cover objects  $C_1, C_2, \dots, C_n$  should not be able to tell which cover object  $C_i$  has the message embedded in it, and the security of invisible communication lies in the inability to distinguish cover objects from the stego objects [20, 29].

However, not all the cover objects can be used to hide the data for covert communication, since the modifications done after the data is hidden, they should not be visible to anyone not involved in the communication. The cover object needs to have sufficient redundant data, which can be replaced by secret information [20].



## 1.5 History of Steganography:

Although information hiding seems a new science, yet it is one of the oldest known techniques used in secret communications. One of the most famous classical examples is found in Histories of Herodotus, father of history of the ancient Greek times. The story tells us that Histiaeus wishes to inform his allies to revolt against the Persian king. But the problem was how to inform these allies of his planned revolt without letting the Persian king know about the plan. So Histiaeus shaved the head of one of his trustworthy servants, and tattooed the message on the servant's scalp. When the slave's hair grew back, Histiaeus sent his servant through the Persian territory to his allies [6].

Upon the arrival of the servant, he reported to the leader of Histiaeus's allies, and indicated that his hair should be shaved to reveal the message. In this scenario, the message is the primary value to Histiaeus and the servant is the carrier of the message [6].

Some of the hieroglyphics on the monuments of the Egyptians contain secret writing. The artist would describe the life of his master but would put in some hidden meaning. It became a kind of a contest where a person was recognized as being more important if his life story contained more of this secret information. In order to put in the secret information, the writing became so complex that nobody but the writer could understand the story. Therefore the practice began to die out [10].

In 1499 Trithemius published Steganographia, one of the first books about steganography. Techniques such as writing between the lines of a document with invisible ink created from juice or milk, which show only when heated, were used as far back as ancient Rome. In World War II, Germany used microdots to hide large amounts of data on printed documents, masquerading as dots of punctuation [4].

A more recent and quite ingenious use of steganography helped Commander Jeremiah Denton convey the truth about his North Vietnamese captors. When paraded in front of the news media as part of staged propaganda, Denton blinked his eyes in Morse code spelling out T-O-R-T-U-R-E [7].

The boom of Steganography coincides with the appearance of the Internet. The rapid spread of computer networks and shift to digitization of media created a very favorable environment for covert Steganographic communication. Recently, Steganography has been suspected as a possible means of information exchange and planning of terrorist attacks. It is only natural that such technology by its very nature could be used for planning criminal activities [7].

Steganography is considered broken even when the mere presence of the secret message is detected. Indeed, the fact that we know that certain parties are communicating secretly is often a very important piece of information [7].

## 1.6 Steganography Vs Cryptography:

The term Steganography meaning “cover writing”, whereas cryptography means “secret writing”. Cryptography is the process of sending indistinct form of messages, so that only the intended recipient can understand the secret message [25].

Encryption protects the content during transmission of the data from the sender to the receiver. However after decrypting the message by the end receiver the data is no longer protected [25]. Whereas steganography does not encrypt the message to be sent, it is embedded as it is, and does not require secret transmission, in other words Steganography hides messages in plain sight rather than encrypting the message; it is embedded in innocent cover. The following two figures illustrate block diagrams of steganography and cryptography respectively [25] as in Figures 1.3 and 1.4.

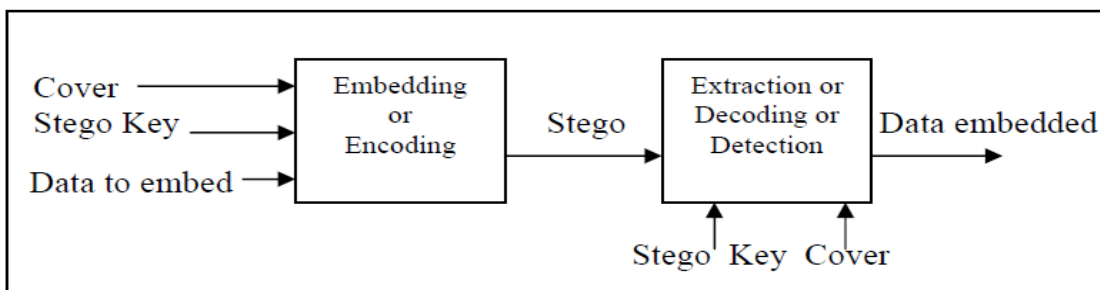


Figure 1.3: Steganography

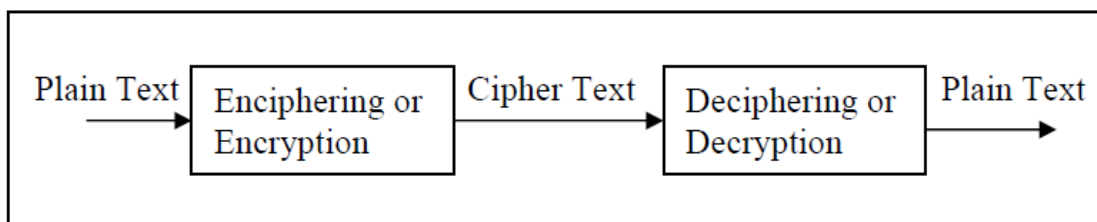


Figure 1.4: cryptography

## 1.7 Water marking:

Watermarking has the potential to fulfill the strong need for an alternative or complement to cryptography because it places information within the content where it is never removed during normal usage.

There are a lot of definitions for the term "digital watermarking" for instance it means embedding information into digital material in such a way that it is imperceptible to a human observer but easily detected by computer algorithm [20].

A digital watermark is a transparent, invisible information pattern that is inserted into a suitable component of the data source by using a specific computer algorithm [20].

Digital watermarks are signals added to digital data (audio, video, or still images) that can be detected or extracted later to make an assertion about the data [28].

Figure 1.5 shows a basic scheme of watermarking [14]:

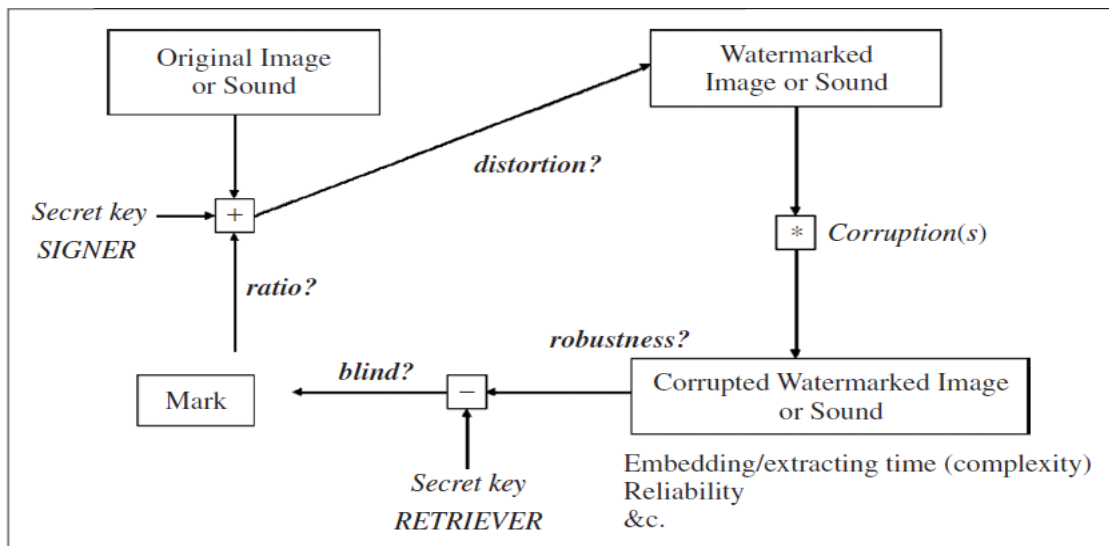


Figure 1.5: Basic scheme of watermarking

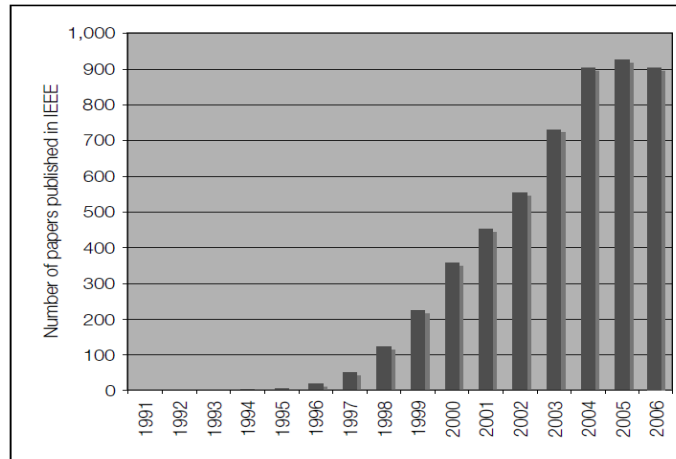
## 1.8 History of Watermarking:

Although the art of papermaking was invented in China over one thousand years earlier, paper watermarks did not appear until about 1282, in Italy. The marks were made by adding thin wire patterns to the paper molds. The paper would be slightly thinner where the wire was and hence more transparent [7].

By the eighteenth century, watermarks on paper made in Europe and America had become more clearly utilitarian. They were used as trademarks, to record the date the paper was manufactured, and to indicate the sizes of original sheets. It was also about this time that watermarks began to be used as anti-counterfeiting measures on money and other documents [7].

It is difficult to determine when digital watermarking was first discussed. In 1979, Szepanski described a machine-detectable pattern that could be placed on documents for anti-counterfeiting purposes. Nine years later, Holt et al. described a method for embedding an identification code in an audio signal. However, it was Komatsu and Tominaga, in 1988, which appear to have first used the term digital watermark. Still, it was probably not until the early 1990s that the term digital watermarking really came into vogue [7].

About 1995, interest in digital watermarking began to mushroom. Figure 1.6 is a histogram of the number of papers published on the topic [7].



**Figure 1.6: Annual number of papers published on watermarking and steganography by the IEEE.**

Digital watermarking has gained a lot of attention and has evolved very fast, and while there are a lot of topics open for further research, practical working methods and systems have been developed.

Since this thesis uses two kinds of watermarking domains; here is an explanation about these domains:

### **1.8.1 Spatial Domain:**

Spatial domain watermarking schemes are simple and usually do not need the original image to extract watermark. However they suffer a major drawback: as they are not robust to common signal processing operations, the watermark is not spread all over the image. Thus common signal processing operations can easily erase the embedded watermark without affecting the quality of the watermarked image [13]; LSB is an example of spatial domain techniques.

### **1.8.1.1 Least Significant Bit (LSB):**

LSB watermarking describes a straightforward and basic way to integrate watermark information in digital documents. Considering a basic grayscale image, the pixel and its values can be sliced up into significant and irrelevant levels. Because the significant levels merely represent a digital noise pattern, it could be easily used for digital watermarking. However, such technique is very insecure because the watermark can be easily destroyed. On the other hand, such technique can be useful in copy control and authenticity applications [28].

### **1.8.2 Frequency Domain:**

In this domain the document has to be transformed into its frequency components using any kind of discrete transformations like discrete cosine, discrete wavelet, discrete Fourier, the watermark appears to be very resistant to the usual attacks. Furthermore, integrating watermarks in the most important frequency components improve security and resistance, because every change significantly reduces the quality of the image. Therefore, it is important to identify the coefficients of the transformation that are less infected by the attack method. In most cases digital watermarks are integrated into the mid-band frequencies. Research has determined a specific sensibility of high-band frequencies against filter operations, lossy compression, and noise insertion whereas manipulating low frequencies seems to produce visible artifacts anytime [16]. DWT is an example of frequency domain techniques.

### **1.8.2.1 Discrete Wavelet Transform (DWT):**

Wavelets are special functions which in a form analogous to sines and cosines in Fourier analysis, are used as basal functions for representing signals. For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub-bands LL, LH, HL and HH. The sub-band LL represents the coarse-scale DWT coefficients while the sub-bands LH, HL and HH represent the fine-scale of DWT coefficients. To obtain the next coarser scale of wavelet coefficients, the sub-band LL is further processed until some final scale N is reached, Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively [1].

### **1.9 Statement of the problem:**

With the rapid development of the current information technology, electronic publishing, such as the distribution of digitized images/videos, is becoming more and more popular. An important issue for electronic publishing is copyright protection. Watermarking is one of the current copyright protection methods that have recently received considerable attention. Basically, "invisible" watermarking for digital images consists of signing an image with a signature or copyright message such that the message is secretly embedded in the image and there is negligible visible difference between the original and the signed images [34].



Watermarks should be robust against standard data manipulations. Security is a special concern, and watermarks should resist even attempted attacks by knowledgeable individuals. On the other hand, watermarks should be imperceptible and convey as much information as possible. In general, watermark embedding and retrieval should have low complexity because for various applications, real-time watermarking is desirable.

So we are interested to give a new watermarking method for digital images. The method is based on the Discrete Wavelet Transform (DWT) and Least Significant Bit (LSB). It will be tested by using special attacks such as lossy compression, noise addition, and cropping. It is predicted that it will achieve all watermark requirements especially the robustness and imperceptible assessments.

### **1.10 Contribution:**

The aim of this research is to present a new algorithm for image watermarking; it is characterized by simplicity and clarity. Since it combines the Discrete Wavelet Transform (DWT) that is proved to be highly resistant to both compression and noise, with minimal amounts of visual degradation, with least Significant Bit (LSB). It is predicted that it will achieve high immunity against several attacks for image watermarking such as lossy compression, noise addition, and cropping. It will be the first time of using DWT with LSB in this manner for image watermarking, so it is worthy to know what the results are.

### **1.11 Thesis Organization:**

The major objective of this thesis is to present a new technique for digital image watermarking, this will be accomplished by combining two domains for watermark embedding and extraction; the frequency domain particularly Discrete Wavelet Transform (DWT), and the spatial domain particularly Least Significant Bit (LSB). The focus of the study is on invisible watermarks. The watermarking terminology and its application will be discussed later in chapter 2, also previous literature studies will be included, in chapter 3 the proposed algorithm steps will be explained in details with suitable figures, chapter 4 is for experimental works; the algorithm will be tried by implementing it using different attacks then the watermark will be extracted to measure its robustness. The imperceptibility of the watermark will be calculated also, after that a fair evaluation of the technique will be applied using suitable tools.

Finally in chapter 5, the primary results of this investigation will be reviewed as a conclusion. In conclusion, recommendations will be made for future research efforts in this area.

## Chapter Two Literature Survey

### 2.1 Watermarking Stages:

An ideal watermarking system, however, would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. As a side effect of these different requirements, a watermarking system will often trade capacity and perhaps even some security for additional robustness [19].

A watermarking system is made up of a watermark embedding system and a watermark recovery system. The system also has a key which could be either a public or a secret key. The key is used to enforce security, which is prevention of unauthorized parties from manipulating or recovering the watermark [32, 24].

#### 2.1.1 Embedding Stage:

Watermark embedding is the process of superposition of a digital signal into the original image [25]; in this case, secret or public keys and other parameters can be used to extend the watermarking encoder.

Figure 2.1, illustrates the Embedding stage [32].

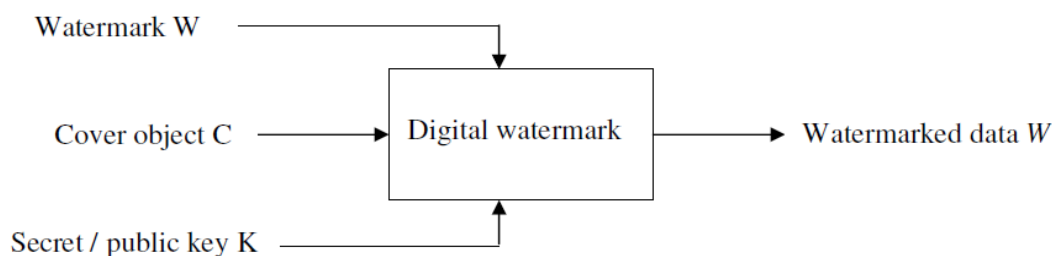


Figure 2.1: Digital Watermarking -Embedding

For the embedding process the inputs are the watermark, cover object and the secret or the public key. The watermark used can be text, numbers or an image. The resulting final data received is the watermarked data  $W$ .

### 2.1.2 Extraction Stage:

The watermark is extracted using a decoder function. In this case, the decoder  $D$  loads the watermarked, normal or corrupted image  $I'$ , and extracts the hidden signature  $S$ .

Figure 2.2, illustrates the extraction stage [32].

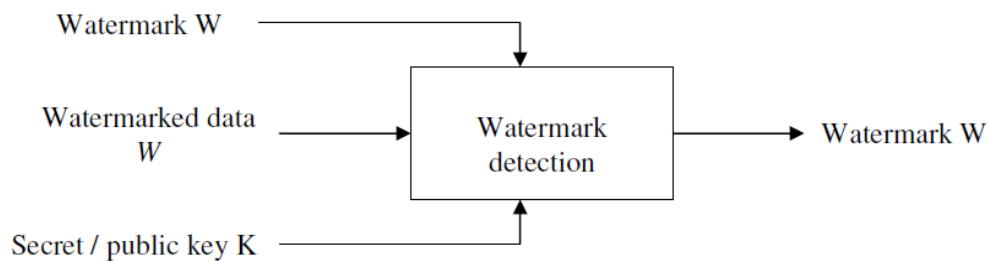


Figure 2.2: Digital Watermarking –Extraction

The inputs during the decoding process are the watermark or the original data, the watermarked data and the secret or the public key. The output is the recovered watermark  $W$ .

## 2.2 Watermarking Applications:

Watermarking can be used in a wide variety of applications. In general, if it is useful to associate some additional information with a Work, this metadata can be embedded as a watermark. Of course, there are other ways to associate information with a Work, such as placing it in the header of a digital file, encoding it in a visible bar code on an image,

or speaking it aloud as an introduction to an audio clip [7].

Watermarking is distinguished from other techniques in three important ways [7]:

1) Watermarks are imperceptible. Unlike bar codes, they do not detract from the aesthetics of an image.

2) Watermarks are inseparable from the Works in which they are embedded. Unlike header fields, they do not get removed when the Works are displayed or converted to other file formats.

3) Watermarks undergo the same transformations as the Works. This means that it is sometimes possible to learn something about those transformations by looking at the resulting watermarks.

It is these three attributes that make watermarking invaluable for certain applications, here are brief descriptions of such applications:

### **2.2.1 Copyright Protection and Authentication:**

In this case, the author or originator integrates a watermark containing his/her own intellectual property signature into the original document and delivers it as usual. By doing this, he/she can proof his/her intellectual creation later on [28].

Copyright protection is probably the most prominent application of watermarking today. The objective is to embed information about the source, and thus typically the copyright owner of the data in order to prevent other parties from claiming the copyright on the data. Thus, the watermarks are used to resolve rightful ownership, and this application requires a very high level of robustness. The driving force for this application is the Web which contains millions of freely available images that the rightful owners want to protect. Additional issues besides robustness have to be considered. For example, the watermark must be unambiguous and still resolve rightful ownership if other parties embed additional watermarks. Hence, additional design requirements besides mere robustness apply [20].

### **2.2.2 Fingerprinting and Digital “Signatures”:**

To identify those who make illegal copies or redistribute them, an automated agent scanning system can be used to track down the traitor [28].

There are other applications where the objective is to convey information about the legal recipient rather than the source of digital data, mainly in order to identify single distributed copies of the data. This is useful to monitor or trace back illegally produced copies of the data that may circulate, and is very similar to serial numbers of software products [20].

### **2.2.3 Copy Protection and Device Control:**

Digital watermarks can be used to enable copy control devices. In this combination, the recording device scans the digital data stream for an existing watermark and enables or disables the recording action for a specific movie or stream. Such technology could extend the pay-per-view concept and close the gap between the applied cryptographic approach and its usability. However, the implementation in consumer devices seems to be possible in using the same procedures applied when inserting the Macro Vision and CSS DVD copy mechanisms. By limiting available DVDs to CSS-compliant DVD players, manufacturers had to integrate new encoders that are secured by patent law regulations in their devices to maintain market position [28].

### **2.2.4 Broadcasting Monitoring:**

In this case, digital watermarking can enable technical frameworks, which automatically monitor broadcasting streams at satellite nodes all over the world and identify illegally broadcast material [28].

There are several types of organizations and individuals interested in broadcasting monitoring. Advertisers, of course, want to ensure that they receive all of the air time they purchase from broadcasters, such as the Japanese television stations caught in the 1997 scandal. Performers, in turn, want to ensure that they get the royalties due to them from advertising firms. A 1999 spot check by the Screen Actor's Guild (SAG)

found an average of \$1,000 in underpaid per hour of U.S. television programming. In addition, owners of copyrighted Works want to ensure that their property is not illegally rebroadcast by pirate stations [7].

A low-tech method of broadcasting monitoring is to have human observers watch the broadcasts and record what they see or hear. This method is costly and error prone. It is therefore highly desirable to replace it with some form of automated monitoring. Techniques for doing this can be broadly broken down into two categories. Passive monitoring systems try to directly recognize the content being broadcast, in effect simulating human observers (though more reliable and at lower cost) [7].

Active monitoring systems rely on associated information that is broadcast along with the content.

A passive system consists of a computer that monitors broadcasts and compares the received signals with a database of known Works. When the comparison locates a match, the song, film, TV program, or commercial being aired can be identified. This is the most direct and least intrusive method of automated broadcasting monitoring. It does not require the introduction of any associated information into the broadcast, and therefore does not require changes to advertisers' workflow. In fact, it does not require any cooperation with the advertisers or broadcasters [7].



### **2.2.5 Data Authentication:**

Digital watermarking is often used to prove the authenticity of a specific digital document. The digital watermark contains information that can be used to prove that the content has not been changed. Any such operation on the file destroys or changes the integrated watermark. If the watermark information can be extracted without errors, the authenticity can be proved. In order to design an effective watermarking algorithm, the watermarking data or procedure can be linked to the content of the digital document. Such watermarks are called fragile watermarks or vapor marks [8].

### **2.3 Watermarking Requirements:**

An ideal watermarking scheme must satisfy a set of constraints of very various natures. Most intervening techniques are related to the fields of signal transmission cryptography and human perception psychological phenomena. The design is complicated by the conflicting interdependence of the different constraints. It makes it difficult to study all aspects simultaneously but it appears also hard to successfully isolate the different constraints.

The main requirements which should be fulfilled by a watermarking scheme are imperceptibility, security and robustness [12]. Digital watermarks must have a set of properties; these properties can be categorized as follows:

## **2.3.1 Properties Related to the Embedding Process:**

### **2.3.1.1 Perceptual Invisibility:**

It is important to recognize whether the brought bit sample of the watermark produces perceptible changes acoustically or optically. A perfect nonperceptible bit sample is present if data material marked with watermark and the original cannot be distinguished from each other. This classifier is based on the idea and properties of the human visual system (HVS) and human audio system (HAS). The watermark is nonperceptible or invisible if a normal human being is unable to distinguish between the original and the carrier [28].

### **2.3.1.2 Statistical Invisibility:**

The watermark should not be detected by an unauthorized person by means of statistical methods. For example, the availability of a great number of digital works watermarked with the same code should not allow extracting the embedded mark by applying statistically based attacks. A possible solution consists of using content dependent watermarks [15].

### **2.3.1.3 Fidelity:**

Fidelity (transparency) refers to the perceptual similarity between the original watermarked image and the watermarked image [6]. A watermark is said to have a high fidelity if the degradation it causes is very difficult for the viewer to perceive [26].

### **2.3.1.4 Data Payload:**

Data payload refers to the number of bits a watermark encodes within a unit of time or within a Work. For a photograph, the data payload would refer to the number of bits encoded within the image. For audio, data payload refers to the number of embedded bits per second that are transmitted. For video, the data payload may refer to either the number of bits per field (or frame) or the number of bits per second. A watermark that encodes  $N$  bits is referred to as an  $N$ -bit watermark. Such a system can be used to embed any one of  $2^N$  different messages [7].

### **2.3.1.5 Embedded Effectiveness:**

With this definition of watermarked Works, the effectiveness of a watermarking system is the probability that the output of the embedder will be watermarked. In other words, the effectiveness is the probability of detection immediately after embedding. This definition implies that a watermarking system might have an effectiveness of less than 100% [7].

## **2.3.2 Properties Related to the Detection Process:**

### **2.3.2.1 Robustness:**

Robustness refers to the ability to detect the watermark after common signal processing operations [7]. Robustness also means the resistance ability of the watermark information changes and modifications made to the original file [28].

Examples of common operations on images include spatial filtering, lossy compression, printing and scanning, and geometric distortions (rotation, translation, scaling, and so on). Video watermarks may need to be robust to many of the same transformations, as well as to recording on video tape and changes in frame rate, among other influences. Audio watermarks may need to be robust to such processes as temporal filtering, recording on audio tape, and variations in playback speed that result in wow and flutter [7].

### **2.3.2.2 Blind/Informed Detection:**

In some applications, the original, unwatermarked Work is available during detection. For example, in a transaction-tracking application, it is usually the owner of the original Work who runs the detector, in order to discover who illegally distributed a given copy. The owner, of course, should still have an unwatermarked version of the Work and can thus provide it to the detector along with the illegal copy. This often substantially improves detector performance, in that the original can be subtracted from the watermarked copy to obtain the watermark pattern alone. The original can also be used for registration, to counteract any temporal or geometric distortions that might have been applied to the watermarked copy [7].

In other applications, detection must be performed without access to the original Work. Consider a copy control application. Here, the detector must be distributed in every consumer recording device.

Having to distribute the unwater marked content to every detector would not only be impractical, it would defeat the very purpose of the watermarking system [7].

We refer to a detector that requires access to the original, unwatermarked Work as an informed detector. Conversely, detectors that do not require any information related to the original are referred to as blind detectors [7].

In the watermarking literature, systems that use informed detection are often called private watermarking systems, whereas those that use blind detection are called public watermarking systems [7].

### **2.3.2.3 False Positive Rate:**

A false positive is the detection of a watermark in a Work that does not actually contain one. When we talk of the false positive rate, we refer to the number of false positives we expect to occur in a given number of runs of the detector [7].

## **2.3.3 Properties Related to Both Embedding and Detection:**

### **2.3.3.1 Security:**

The security of a watermark refers to its ability to resist hostile attacks. A hostile attack is any process specifically intended to thwart the watermark's purpose. The types of attacks we might be concerned about fall into three broad categories:

- \_ Unauthorized removal
- \_ Unauthorized embedding
- \_ Unauthorized detection

Unauthorized removal and embedding are referred to as active attacks because these attacks modify the cover Work. Unauthorized detection does not modify the cover Work and is therefore referred to as a passive attack [7].

### **2.3.3.2 Cost:**

The cost of implementing watermark embedders and detectors can be very complicated and depends on the business models involved [11]. There are three principals of concern:

- 1) The speed with which embedding and detection must be performed
- 2) The number of embedders and detectors that must be installed.
- 3) Whether the detectors and embedders are to be implemented as special-purpose hardware devices or as software applications or plug-ins.

### **2.3.3.3 Multiple Watermarking:**

An alternative to altering the existing watermark is to embed a second watermark. The presence of both watermarks can then be used to denote the copy-no-more state. Conversely, the initial copy-once state can be denoted by two watermarks, the primary and secondary.

The secondary watermark could be a relatively fragile watermark compared to the primary one, and its removal would denote copy-no-more. These two methods appear at first sight to be equivalent but in fact have very different false positive behaviors. Their implementation also raises technical challenges, such as the need to embed watermarks in compressed media without changing the bit rate [17].

An example of the need for multiple watermarks to coexist in a Work arises in the area of transactional watermarks. Content distribution often includes a number of intermediaries before reaching the end user. Thus, a record label might first want to include a watermark identifying itself as the copyright owner. The Work might then be sent to a number of music web sites. Each copy of the Work might have a unique watermark embedded in it to identify each distributor. Finally, each web site might embed a unique watermark in each Work it sells for the purpose of uniquely identifying each purchaser [7].

## **2.4 Watermarking Techniques:**

Digital watermarks and their techniques can be subdivided and segmented into various categories; for example, they can be classified according to the application, source type (image watermarks, video watermarks, audio watermarks, text watermarks), human perception, and technique used. As watermarks can be applied in the spatial or frequency domain, different concepts, such as Discrete Fourier (DFT), discrete cosine (DCT), and wavelet transformation, or additionally

, manipulations in the color domain and noise adding can be mentioned. Furthermore, digital watermarks can be subdivided on the basis of human perception. Digital watermarks can be invisible or visible [28].

Figure 2.3, illustrates the different types of watermarking techniques [25]:

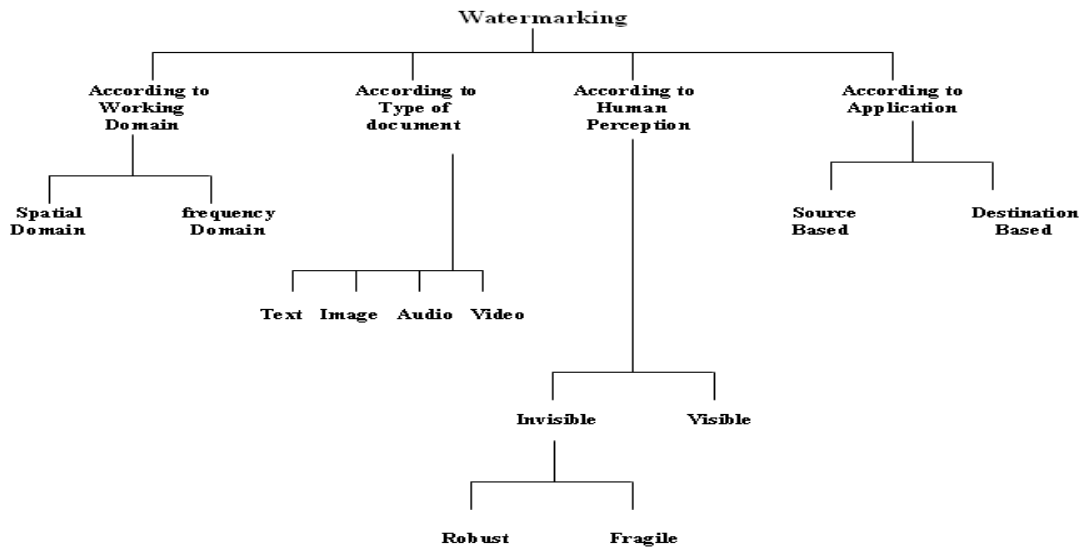


Figure 2.3: Types of Watermarking Techniques

Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows.

- \_ Image Watermarking
- \_ Video Watermarking
- \_ Audio Watermarking
- \_ Text Watermarking



According to the human perception, the digital watermarks can be divided into three different types as follows:

- \_ Visible watermark
- \_ Invisible-Robust watermark
- \_ Invisible-Fragile watermark
- \_ Dual watermark

Visible watermark is a secondary translucent overlaid into the primary image. The watermark appears visible to a casual viewer on a careful inspection. The invisible-robust watermark is embedded in such a way that an alternation made to the pixel value is perceptually not noticed and it can be recovered only with appropriate decoding mechanism. The invisible-fragile watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark. Dual watermark is a combination of a visible and an invisible watermark. In this type of watermark an invisible watermark is used as a back up for the visible watermark as clear from the following diagram [25]:

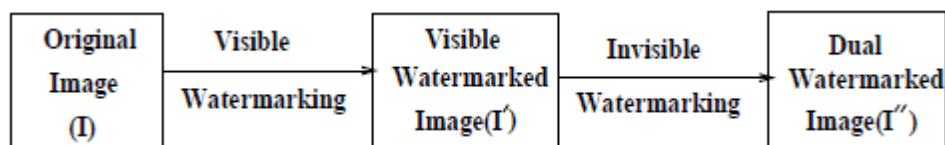


Figure 2.4: Schematic representation of dual watermarking

An invisible robust private watermarking scheme requires the original or reference image for watermark detection; whereas the public watermarks do not.

From the application point of view the digital watermark could be as follows:

- \_ Source based
- \_ Destination based

Source-based watermarks are desirable for ownership identification or authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed. A source-based watermark could be used for authentication and to determine whether a received image or other electronic data has been tampered with. The watermark could also be destination based where each distributed copy gets a unique watermark identifying the particular buyer. The destination -based watermark could be used to trace the buyer in the case of illegal Reselling [25].

According to the working domain a watermark may be spatial or frequency. Spatial domain watermarking schemes are simple and usually do not need the original image to extract watermark. However they suffer a major drawback: as they are not robust to common signal processing operations, as the watermark is not spread all over the image. Thus common signal processing operations can easily erase the embedded watermark without affecting the quality of the watermarked image [13].

In frequency domain the document has to be transformed into its frequency components using any kind of discrete transformations like discrete cosine, discrete wavelet, discrete Fourier, the watermark

appears to be very resistant to the usual attacks. Furthermore, integrating watermarks in the most important frequency components improve security and resistance, because every change significantly reduces the quality of the image, therefore, it is important to identify the coefficients of the transformation that are less infected by the attack method. In most cases digital watermarks are integrated into the mid-band frequencies. Research has determined a specific sensibility of high-band frequencies against filter operations, lossy compression, and noise insertion whereas manipulating low frequencies seems to produce visible artifacts anytime [16].

## 2.5 Watermarking Attacks:

Watermarking research has produced a wide range of watermarking techniques that can be subdivided into various methodological complexity levels. Each of these methods tries to reduce vulnerability in various attack scenarios. There are a lot of categories for these attacks such as friendly and malicious categories, but the most comprehensive one is shown in Figure 2.5:

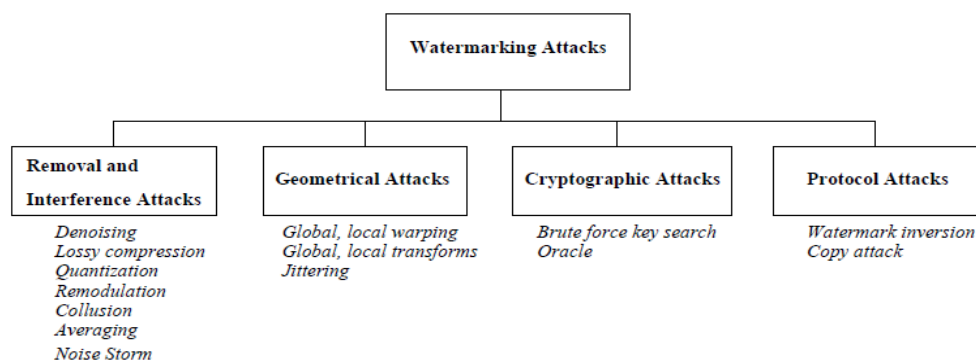


Figure 2.5: Classification of watermarking attacks

### **2.5.1 Interference and Removal Attacks:**

The main idea consists of assuming that the watermark is additive noise relative to the original image. The interference attacks are those which further add noise to the watermarked image. This noise may have any of a number of different statistical distributions such as Gaussian or Laplacian. The removal attacks exploit the linear additive model in order to derive optimal estimators used for denoising and consequently removing of the watermark. In other cases both the removal attacks and the interference attacks can be combined such as in the denoising with perceptual remodulation attacks [27].

### **2.5.2 Geometrical attacks:**

In contrast to the removal attacks, geometrical attacks intend not to remove the embedded watermark itself, but to distort it through spatial alterations of the stego data. The attacks are usually such that the watermark detector loses synchronization with the embedded information. The most well known integrated software versions of these attacks are Unzign and Stirmark [27].

The global distortions are rotation, scaling, change of aspect ratio; translation and shearing that belong to the class of general affine transformations. The line/column removal and cropping/translation are also integrated in Stirmark. Most recent watermarking methods survive after these attacks due to the usage of special synchronization techniques [27].

### **2.5.3 Cryptographic attacks:**

Cryptographic attacks are very similar to the attacks used in cryptography. There are the brute force attacks which aim at finding secret information through an exhaustive search. Since many watermarking schemes use a secret key it is very important to use keys with a secure length. Another attack in this category is the so called Oracle attack which can be used to create a non-watermarked image when a watermark detector device is available [27].

### **2.5.4 Protocol attacks:**

The protocol attacks aim at attacking the concept of the watermarking application. The first protocol attack was proposed by Craver et al [9]. They introduce the framework of invertible watermark and show that for copyright protection applications watermarks need to be non-invertible. The idea of inversion consists of the fact that an attacker who has a copy of the stego data can claim that the data contains also the attacker's watermark by subtracting his own watermark. This can create a situation of ambiguity with respect to the real ownership of the data. The requirement of non-invertibility on the watermarking technology implies that it should not be possible to extract a watermark from non-watermarked image. As a solution to this problem, the authors propose to make watermarks signal-dependent by using a one-way function [27].

## 2.6 Previous Studies:

### 2.6.1 Spatial Domain Algorithms:

An algorithm has been developed by Martin Kutter, Frederic Jordan and Frank Bossen [22]. The host image is not needed for extracting the watermark. The Watermark used is a string of bits. It is made more redundant by repeating each bit  $c_r$  times. Two leading bits are added to the mark: a zero and a one bit. These two bits form a mini-template that will be used in the extraction process.

This algorithm manipulates the values of the blue channel at single pixels. This gives  $XY$  possible sites. The pixels are visited in a zig-zag path to get a sequence. A bit  $S_i$  of the watermark is embedded at a given location  $(x, y)$  by modifying the blue channel  $b$  at this location by a fraction of the luminance.

$$l(x, y) = 0.299r(x, y) + 0.587g(x, y) + 0.114b(x, y) \quad \text{----- 2.1}$$

A parameter  $\alpha$  is used to control the strength of the embedding.

$$b'(x, y) = \begin{cases} b(x, y) + \alpha l(x, y) & \text{if } s_i = 0 \\ b(x, y) - \alpha l(x, y) & \text{if } s_i = 1 \end{cases} \quad \text{----- 2.2}$$

**Where:**

**$(x, y)$  :** a given location

**$S_i$  :** a bit of the watermark

**$\alpha$  :** a strength parameter

**$b(x, y)$  :** blue channel for location  $(x, y)$

**$b'(x, y)$  :** watermarked data

The detector tries to extract a reconstructed watermark  $S''$  from a possibly Marked image  $I''$ . Now we can use common methods to compare the reconstructed  $S''$  to the original watermark  $S$ .

An algorithm has been developed by P.M.J. Rongen, M.J.J.J.B. Maes and C.W.A.M. van Overveld [23]. The host image is not needed to detect the watermark.

The watermark is black and white image of the same size as the host image, with an about equal number of black and white pixels. A pixel in the host image that corresponds to a white pixel in the watermark is said to be on the watermark, a pixel in the host image that corresponds to a black pixel in the watermark is said to be off the watermark.

The  $K$  most salient points of the image (as defined by a saliency function  $S_{x,y}$ ) are the possible sites. (Where  $k \approx (X \times Y) / 100$ ) The saliency measure is a local property, i.e. it is determined by small neighborhood of a point. Furthermore, it should be preserved as much as possible under image processing operations such as smoothing, JPEG/MPEG compression.

The aim of embedding is to have a large percentage of the salient points lie on the watermark. The authors propose two methods to archive this:

1. Move the salient points by introducing small, local, geometrical changes to the image ("wrapping").

2. Decrease the second method 2K most salient points are considered during embedding. Those on the watermark have their salience increased; those off the watermark have their salience decreased. During detection only the K most salient points will be considered.

**Where:**

<b><math>K</math></b>	<b>: The most salient points of the image</b>
<b><math>S_{x,y}</math></b>	<b>: a saliency function</b>
<b>on the watermark</b>	<b>: A pixel in the host image that corresponds to a white pixel in the watermark</b>
<b>off the watermark</b>	<b>: A pixel in the host image that corresponds to a white pixel in the watermark</b>

To detect the watermark the positions of the K most salient points with respect to the watermark are considered. For a non watermarked image we expect to find about half of them on the off the watermark. The authors compute a detection threshold for a given false alarm probability.

## **2.6.2 Frequency Domain Algorithms:**

### **(1) Discrete wavelet Transform (DWT) Algorithm:**

Wang [32]: an algorithm has been developed by Houngh-Jyh Mike Wang, Po-Chyi Su and C.-C. Jay Kuo [31]. The original image is needed for watermark extraction. The sites are all the DWT coefficients, one signature value can be embedded per coefficient. Only the N the most



“significant” ones are selected and manipulated. No form of random site selection is done. The selection of the sites is iterative. For the actual embedding the following formula is used:

$$f'_{k,l}(i) = f_{k,l}(i) + \alpha\beta_{k,l}T_{sj} \quad \text{----- 2.3}$$

Where:

- $T_{sj}$  : computed threshold
- $\alpha$  : embedding strength
- $B_{k,l}$  : parameter for sub-band
- $F_{k,l}(i)$  : unmarked coefficients
- $F'_{k,l}(i)$  : watermarked coefficients

$$s''_j = f''_{k,l}(i) - f_{k,l}(i) \quad \text{----- 2.4}$$

The extraction follows the embedding algorithm. The coefficients of the host image are subtracted to get the potential watermark:

Now we can use common methods to compare the reconstructed  $S''$  to the original watermark  $S$ . The selection of the coefficients is completely deterministic. If we used the same algorithm to embed a second watermark into the image  $S'$  this second watermark would interfere with the first watermark.

An algorithm has been developed by Deepa Kundur and Demetrios Hatzinakos [21]. The host image is not needed for watermark extraction, the watermark consists of a string of bits  $\{-1, 1\}$ .

The watermark is embedded into the coefficients of the entire detail image up to level L. One bit can be encoded in a triple of coefficients. Random site is used. If a triple  $f_{1,l}(x,y)$ ,  $f_{2,l}(x,y)$ ,  $f_{3,l}(x,y)$  has been selected for embedding, sort the three coefficients in ascending order:

$$F_{k_1,l}(x,y) \leq f_{k_2,l}(x,y) \leq f_{k_3,l}(x,y)$$

The range of values between  $F_{k_1,l}(x,y)$  and  $f_{k_3,l}(x,y)$  is divided into bins of width

$$\Delta = \frac{f_{k_3,l}(x,y) - f_{k_1,l}(x,y)}{2Q - 1} \quad \text{----- 2.5}$$

Where:

$F_{k_1,l}(x,y)$ : coefficient

$f_{k_2,l}(x,y)$  : coefficient

$f_{k_3,l}(x,y)$  : coefficient

Q : is a parameter of the algorithm.

To embed a bit, the coefficient  $f_{k_2,l}(x,y)$  is quantized to either one of the even numbered or one of the odd numbered hashes shown in Figure 2.6:

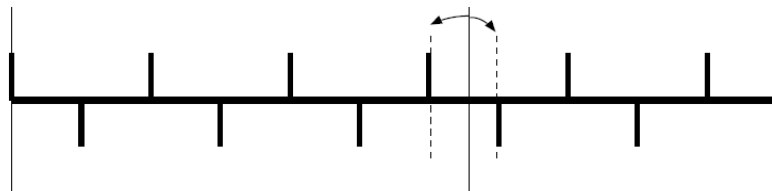


Figure 2.6: Quantization of the middle coefficient

The extraction follows the embedding algorithm step by step, the position of  $f_{2,l}(x,y)$  between  $f_{1,l}(x,y)$  and  $f_{3,l}(x,y)$  and the knowledge of  $Q$  alone is enough to read out a bit. The authors use correlation to compare  $S''$  to  $S$ .

## (2) Discrete Cosine Transform (DCT) Algorithm:

An algorithm has been developed by Ingemar J. Cox, Joe Kilian, Tom Leighton and Talal Shamoon [5]. The host image is needed to detect the watermark.

The watermark consists of a sequence of  $n$  real numbers, where each value  $s_i$  is chosen independently according to the normal distribution with mean 0 and variance 1. The  $n$  highest magnitude AC coefficients are used to embed the watermark. Three different formulas for embedding a bit  $s_i$  into a coefficient  $c_i$  are:

$$c'_i = c_i + \alpha s_i \quad \text{----- 2.6}$$

$$c'_i = c_i(e^{\alpha s_i}) \quad \text{----- 2.7}$$

$$c'_i = c_i(1 + \alpha s_i) \quad \text{----- 2.8}$$

Where:

$s_i$  : watermark value

$\alpha$  : embedding strength

$c_i$  : high magnitude coefficient

$c'_i$ : watermarked data

The extraction follows the embedding algorithm. The DCT of  $I''$  is computed, and for the  $n$  highest magnitude AC coefficients of  $I$  the difference to the corresponding coefficients of  $I''$  is computed. Thus  $S''$  is constructed.  $S''$  can now be compared to  $S$  with common methods. The authors show very promising results regarding the robustness of the watermark.

An Algorithm has been proposed by Ibrahim Zaki Al-Oqily [3]. Al-Oqily proposed two algorithms; the host image is needed to detect the watermark in one of them, while another algorithm needn't.

The watermark  $W = w_1, w_2, \dots, w_m$  consists of a pseudo random sequence of length  $M$ ; each value  $w_i$  is a random real number with a normal distribution having zero mean and unity variance.

The set of coefficients from  $(k+1)$ th to  $(k+m)$ th will be used to embed the watermark after ordering the Full frame DCT coefficient into a zig-zag sequence.

The watermark embedding will be done according to the following equation:

$$I'_j = I_j + \alpha W_j S_j \text{ ----- 2.9}$$

Or

$$I' = I + \alpha WS \text{ ----- 2.10}$$

Where:

- $I_j$  : original DCT coefficient
- $I'_j$  : the marked coefficients
- $\alpha$  : embedding strength
- $W$  : watermark sample
- $S$  : slacks

The DCT coefficients are reordered into a zigzag scan, and the coefficients from the (k + 1)th to (k + m)th are selected to generate a vector  $I'$ . Second, the full frame perceptual model is applied to the corrupted image; the slacks are reordered into a zigzag scan, and the slacks from the (k + 1)th to (k + m)th are selected to generate a vector  $S'$ . Third the seed (key) is used to regenerate the watermark  $W$ . And finally we compute an approximation for the embedded watermark using the following equation:

$$W' = S' w \text{ ----- 2.11}$$

Where:

- $S'$  : slacks vector
- $w$  : generated watermark
- $W'$  : embedded watermark

## **2.6.2 Discussion of Spatial Domain Algorithms:**

Kutter's algorithm is for the color images. The strength of the watermark is dependent on the luminance of the host image. The algorithm manipulates only the value of the blue channel [18].

Norgen's Algorithm; the authors show very promising results for the second embedding method. Both algorithms do not need the original image for extracting the watermark. Both of them add high frequency noise in one form or the other to the image. This makes them vulnerable to lossy image compression [18].

## **2.6.3 Discussion of Frequency Domain Algorithms:**

### **(1) Discussion of Discrete Wavelet Transform Domain Algorithms:**

Wang's algorithm: As the selection of the coefficients is image dependent a manipulation of the image might have changed the coefficients in such a way that the selection algorithm chooses them in a different order; the authors do not address this problem [18].

The selection of the coefficients is completely deterministic. If we used the same algorithm to embed a second watermark into the image S' this second watermark would interfere with the first watermark [18].

Kundur's algorithm: is a blind algorithm (do not need the original image for watermark detection). The authors embed the watermark repeatedly at different resolutions [18].

## **(2) Discussion of Discrete Cosine Transform Domain Algorithms:**

Cox's algorithm: use the  $X \times Y$  DCT of the whole image. This is computationally more expensive, but gives impressive results [18].

The algorithm can extract a reliable copy of the watermark from images that have been significantly degraded through several common geometric distortions and signal processing techniques, scaling by 75% of image size, JPEG compression with quality factor 5%, dithering, clipping, photocopying, rescanning and scaling. Robustness against geometric deformation is also achieved by the use of the original image in the detection step [3].

Al-Oqaily's algorithm: The proposed blind watermarking algorithm is weak against cropping attack, the detector was only able to detect watermarks in cropped images if the cropping doesn't exceed 31% of the total size of the image [3].

The proposed informed watermarking algorithm is weak against the resizing attack, but this weakness can be avoided completely if the attacked image resized back to its original size. In the cropping attack the missing parts of the cropped image was replaced from the original image to get a positive detection [3].

## Chapter Three the Proposed Method

### 3.1 Introduction

The proposed watermarking approach consists of two domains; frequency domain and spatial domain. These two domains are combined in a way that makes the watermark more robust against several attacks.

These are the steps of the proposed algorithm:

### 3.2 Embedding Stage:

1. The host image used is a Grayscale Image, or any color image transformed in Grayscale.
2. The watermark is monochrome image (white & black).
3. By using the Discrete Wavelet Transform (DWT) the host image (I) is separated into a lower resolution approximation image (LL1) as well as horizontal (HL1), vertical (LH1) and diagonal (HH1) detail components.
4. The watermark (W) should be transformed into binary form to get a specific array, after that this array should be transformed to a vector array.
5. All the float numbers resulting from the DWT transformation, should be converted into binary digits (8 bits).
6. Now selected pixels from the vertical decomposition are chosen equal to the number of the Watermark's bits; to embed one bit from the watermark into single pixel from the vertical decomposition.



7. For each selected number the following process is done; the number of one's in the most significant part for each binary number will be computed to determine which bit from the least significant part will be converted by one bit from the watermark (W)\_this process is repeated according to the number of the watermark's bits.
8. After embedding all bits of the watermark (W), then the inverse discrete wavelet transform is applied to the Transformed image to get the watermarked image (I').

### **3.3 Extraction Stage:**

1. Apply Discrete Wavelet Transform (DWT) for the watermarked image ( I').
2. Select a specific number of Pixels from the vertical (LH) detail components, depending on the number of the watermark bits (N).
3. For each selected pixel, the real number resulting from the DWT transformation should be converted into binary digits (8 bits).
4. Now the number of one's in the most significant part for each binary number will be computed to determine which bit from the least significant part is a watermark bit.

- After collecting all the bits, a converting process is applied for all collected binary digits to get the watermark (W).

### 3.4 Flowchart Illustration:

A flowchart example for the proposed algorithm is given below:

#### 3.4.1 Embedding Process:

- Converting watermark image to binary form:

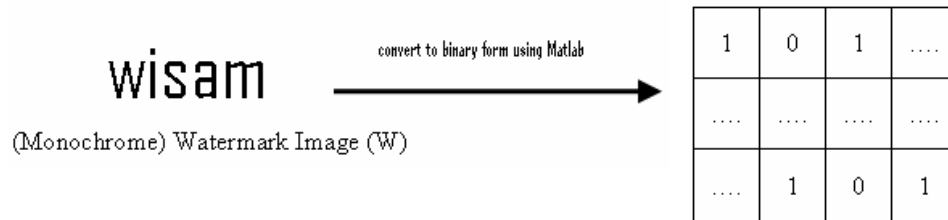


Figure 3.1: watermark image transforming to binary form

- Converting watermark binary form to vector array:

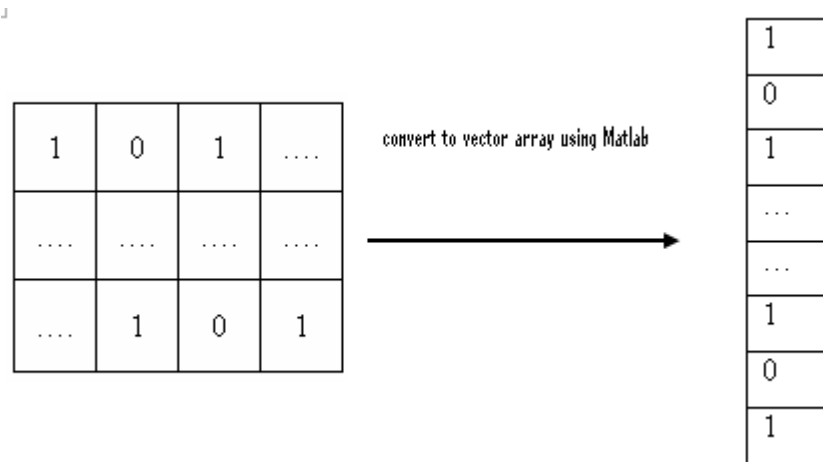


Figure 3.2: representing the watermark image in vector array

### 3. Applying DWT function to the host image:

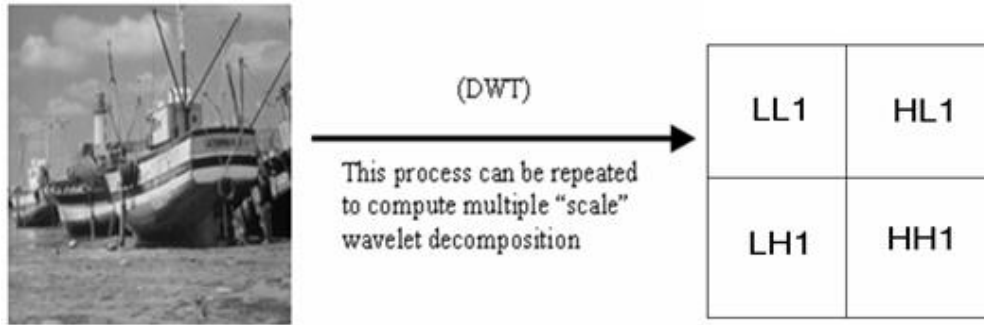


Figure 3.3: Applying DWT function for the host image and its resulting four decompositions

### 4. Convert the $LH_1$ matrix into vector array:

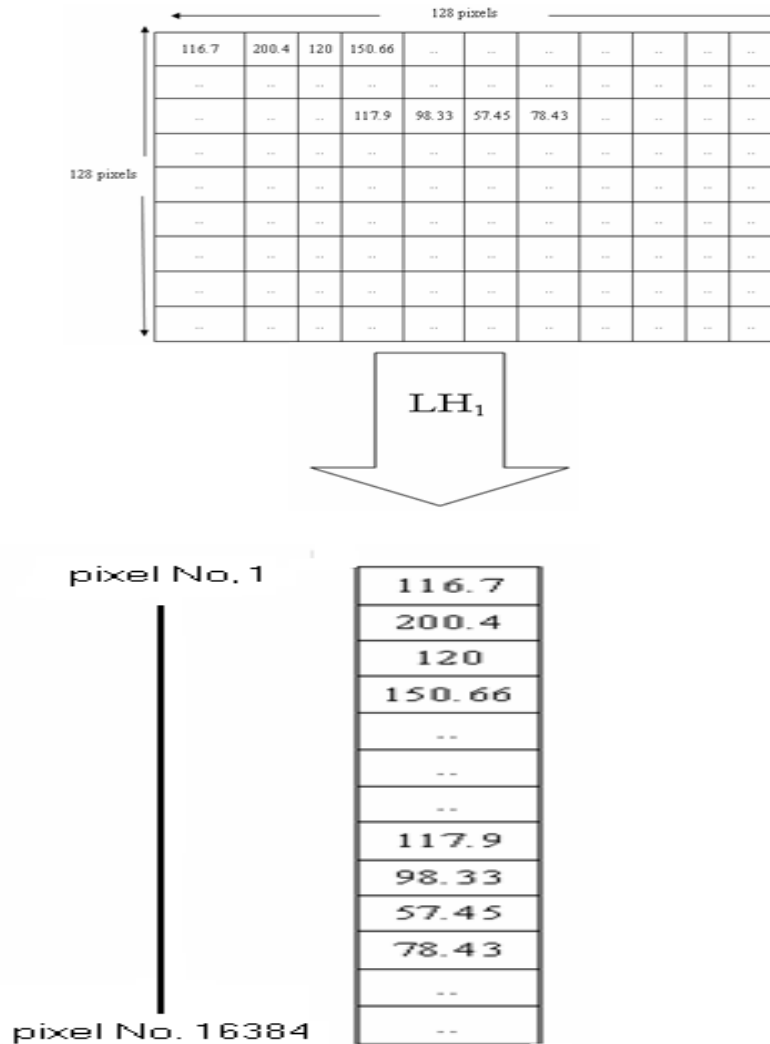


Figure 3.4:  $LH_1$  coefficients after converting to vector

5. Convert the  $LH_1$  coefficients into binary code:

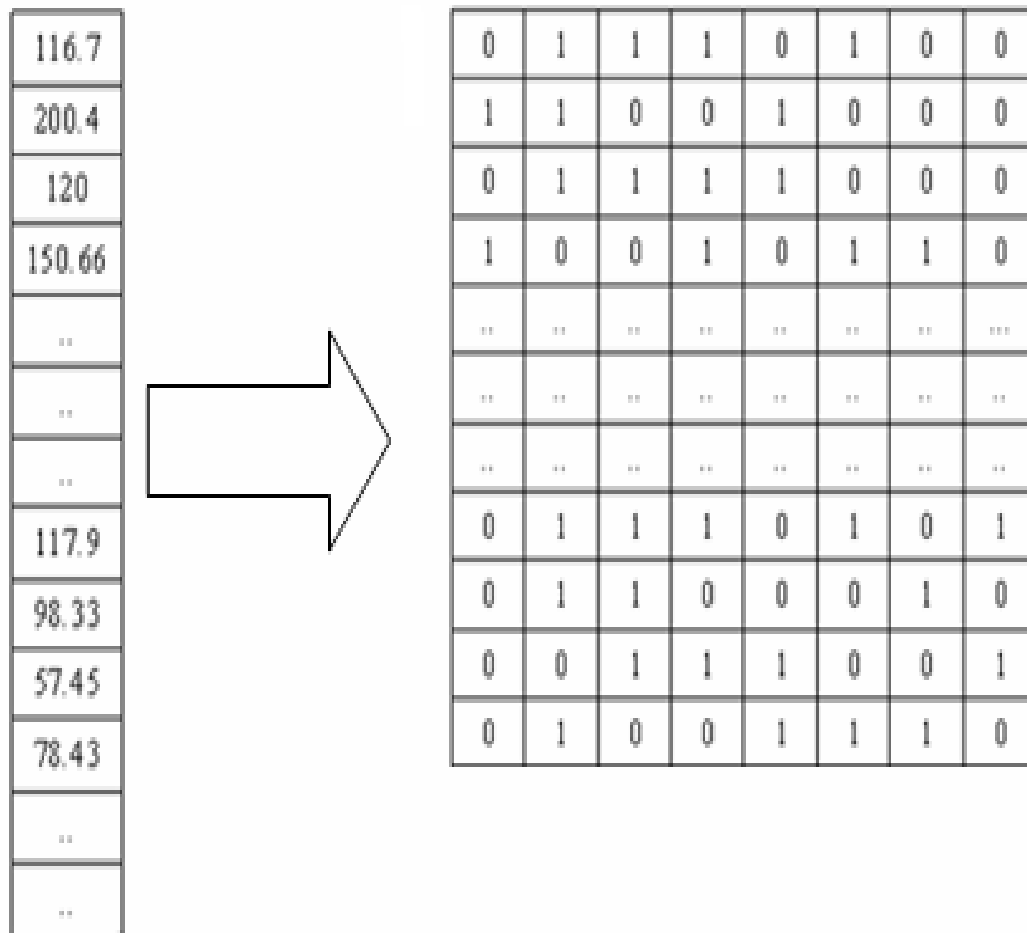


Figure 3.5: converting  $LH_1$  coefficients into binary form

6. Embedding one bit from the watermark image into one byte from LH<sub>1</sub>:

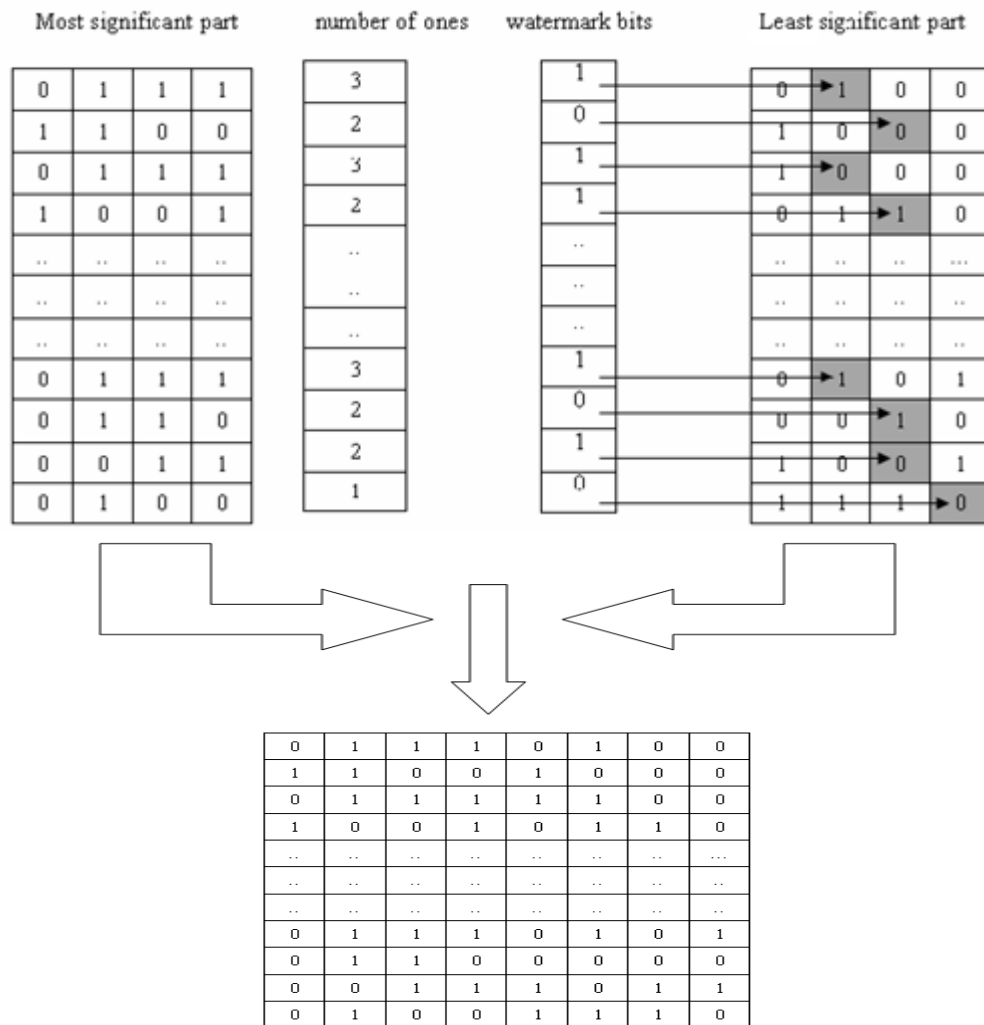


Figure 3.6: LH<sub>1</sub> after Embedding watermark bits in it

7. After embedding the watermark into the  $LH_1$  coefficients, the (IDWT) function is applied to the approximation and the details coefficients to get the watermarked image ( $I'$ ):

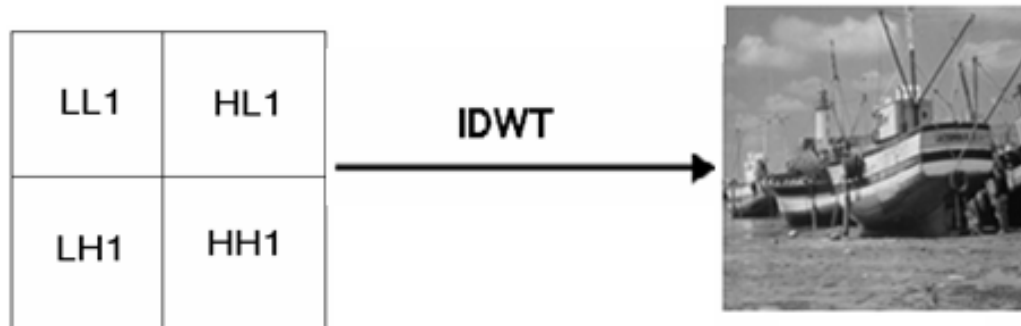
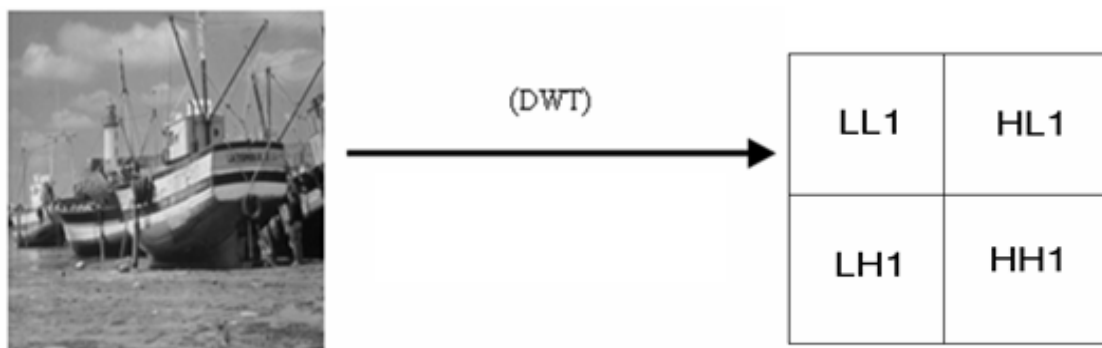


Figure 3.7: Applying IDWT function for the host image coefficients and its resulted watermarked image

### 3.4.2 Extraction process:

1. The DWT function is applied to the watermarked image ( $I'$ ):



watermarked image ( $I'$ )

Figure 3.8: Applying DWT function to the watermarked image and its resulting coefficients

2. Convert the  $LH_1$  matrix into vector array:

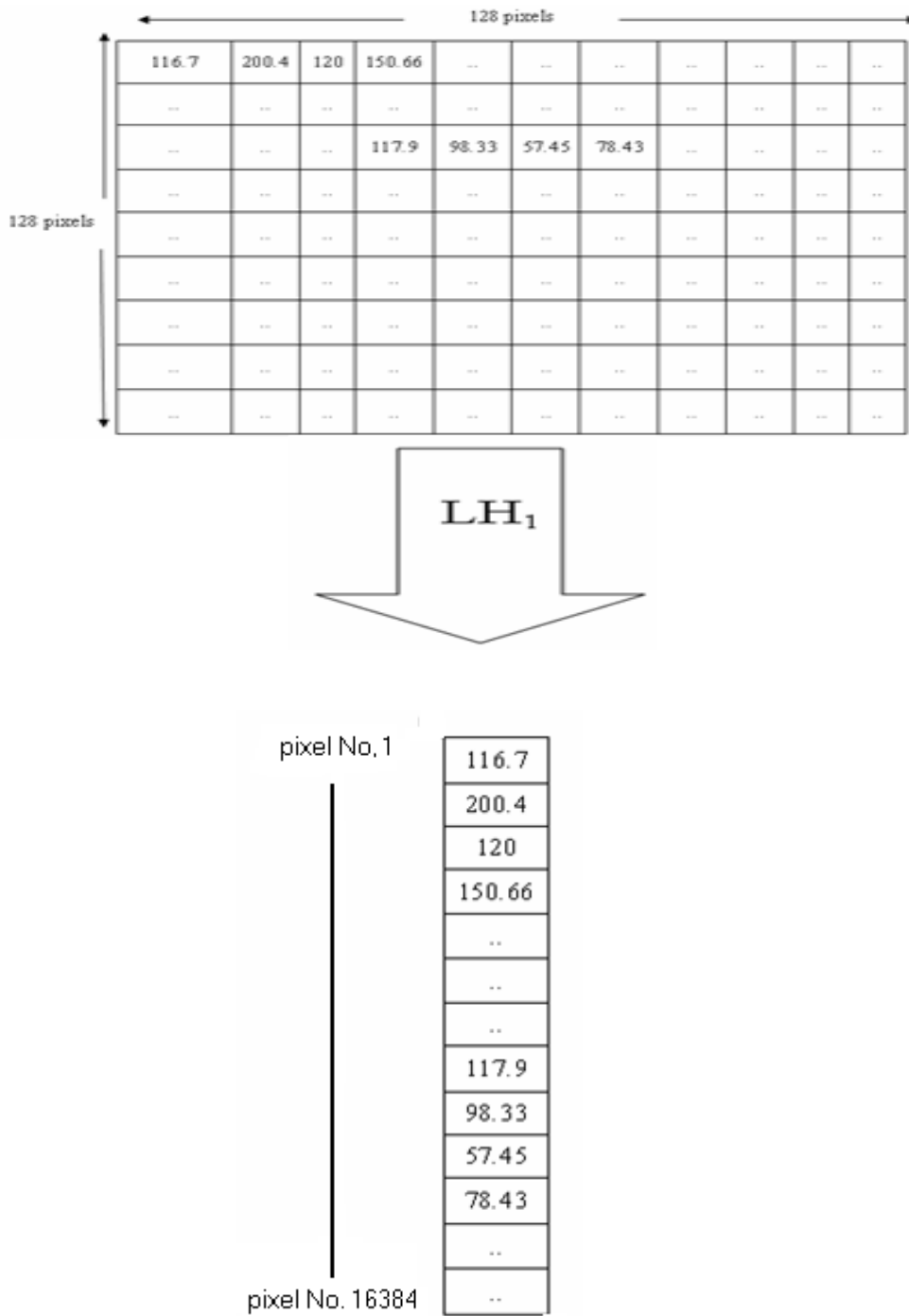


Figure 3.9:  $LH_1$  coefficients after converting to vector

3. Convert coefficients from  $LH_1$  into binary code:

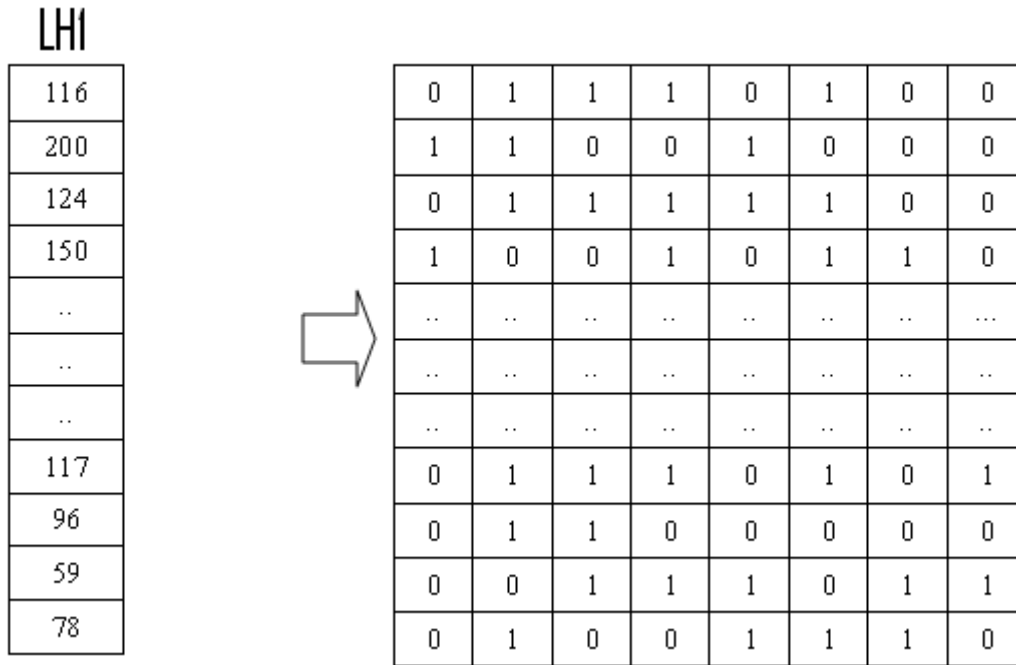


Figure 3.10: Selection of the  $LH_1$  coefficients from the vector and converting them into binary

4. Extracting one bit of watermark image from each byte from  $LH_1$  :

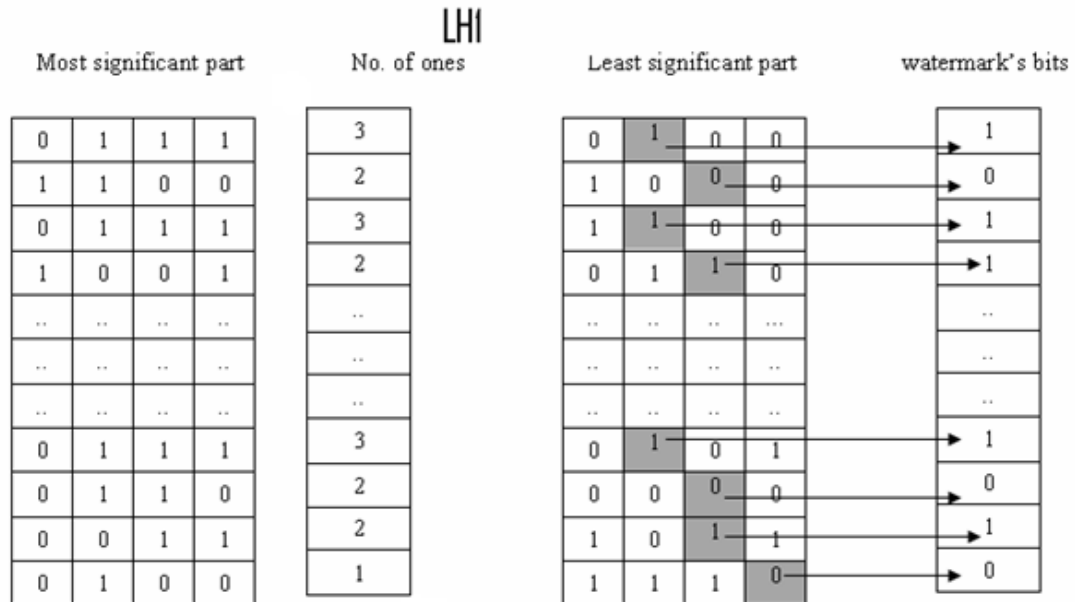


Figure 3.11: Extracting watermarks' bits from  $LH_1$  binary numbers



## 5. Converting Watermark's bits into original image using Matlab:

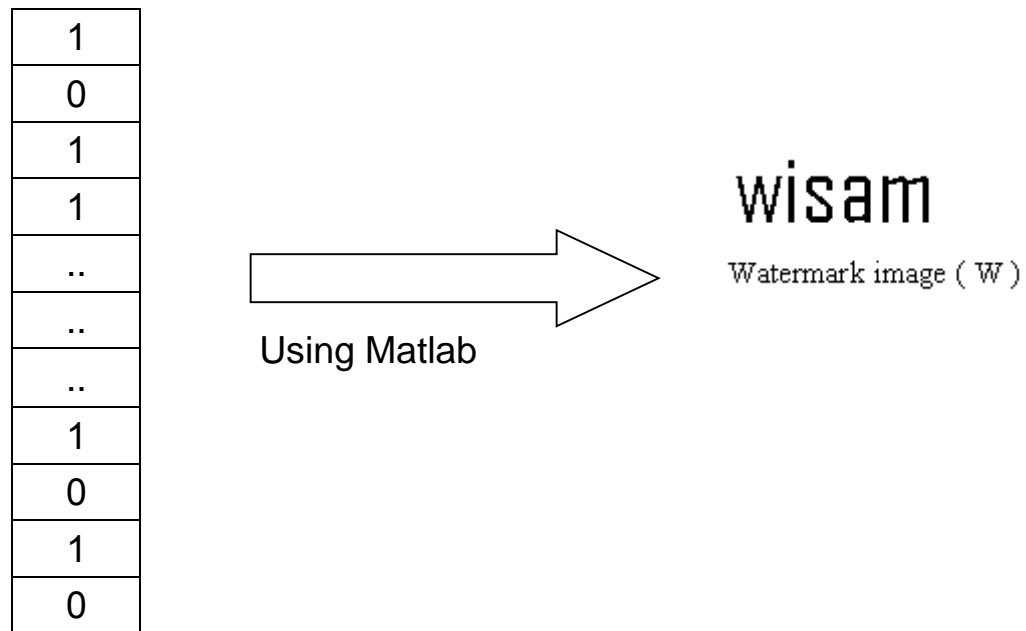


Figure 3.12: Converting watermarks' bits extracted from  $LH_1$  into watermark image

### 3.5: Summary:

In this chapter the proposed algorithm was presented using two ways; the theoretical steps and the flowchart illustration. In order to embed a watermark into an image many steps should be taken; firstly the host image should be an 8-bit depth or transformed to 8-bit depth for implementation facilitation after that the DWT function is applied to that image to get four coefficients matrices, our work focuses on the vertical coefficients matrix, a selected coefficients from this matrix will be picked for binary conversion and then bits embedding according to the number of one's in the most significant part as before discussed .

In the extraction stage the same steps will be taken to get the bits from the watermarked image and then they are transformed again to get the watermark image.

This algorithm combines two different ways for image watermarking; frequency domain and spatial domain, an advantage of the spatial techniques is that they can be easily applied to any image regardless of subsequent processing. An advantage of the frequency techniques is that they improve both the robustness and quality of the watermark because they exploit the properties of the cover image (hide watermarking information in noisy regions and edges of images, rather than in smoother regions). So it is predicted to be a promising technique; that what will be tested in the next chapter.

## Chapter four Experimental results

### 4.1 performance evaluation:

This chapter discusses the results of the experiments carried out to test the performance of the proposed watermarking system. First, the robustness against various attacks of the algorithm for grayscale images is tested. Second, the imperceptibility of the watermarking system is presented.

Watermarking algorithms are usually evaluated with respect to two metrics; imperceptibility and robustness. The two metrics are described below:

#### Imperceptibility:

Imperceptibility means that the perceived quality of the host image should not be distorted by the presence of the watermark [2]. As a measure of the quality of a watermarked image, the peak signal to noise ratio (PSNR) is typically used. PSNR in decibels (dB) is given below in equation 4.1[2]:

$$\begin{aligned} \text{PSNR}_{\text{dB}} &= 10 \cdot \log_{10} \left( \frac{\text{MAX}_I^2}{\text{MSE}} \right) \\ &= 20 \cdot \log_{10} \left( \frac{\text{MAX}_I}{\sqrt{\text{MSE}}} \right) \end{aligned} \quad \text{----- 4.1}$$

Where:

**Max:** the maximum value for the pixels

**MSE:** the mean Square Error

## Robustness:

Robustness is a measure of the immunity of the watermark against attempts to remove or degrade it, intentionally or unintentionally, by different types of digital signal processing attacks [30]. The obtained robustness results will be reported for ten major digital signal processing operations (attacks): adding noise, reducing noise, median noise, image compression, image cropping, image cutting, image sharpening, crystallize, Glow, and ink sketch. The similarity between the original watermark and the watermark extracted from the attacked image were measured using the correlation factor  $\rho$  given below in equation 4.2 [2]:

$$\rho(w, \hat{w}) = \frac{\sum_{i=1}^N w_i \hat{w}_i}{\sqrt{\sum_{i=1}^N w_i^2} \sqrt{\sum_{i=1}^N \hat{w}_i^2}} \quad \text{----- 4.2}$$

Where:

**N:** number of pixels in the watermark

**W:** original watermark

**$\hat{W}$ :** extracted watermark

Six different host images were used for testing, these are:



**Building Image**



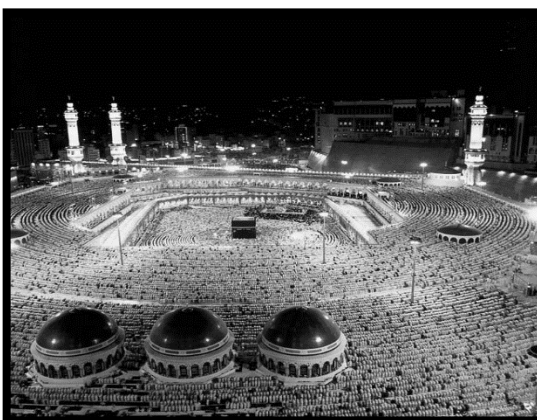
**Clock Image**



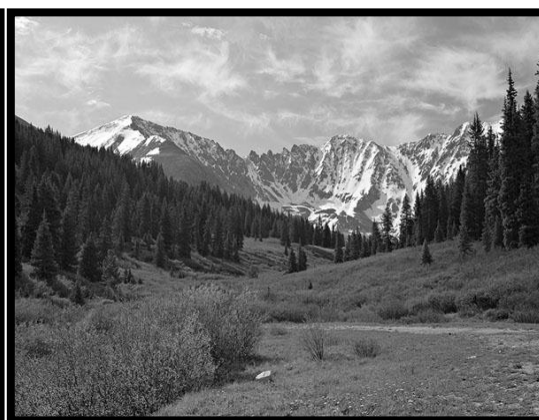
**Field Image**



**Flowers Image**



**Haram Image**



**Nature Image**

One watermark image is used, here it is:

**WISAM**

Here are the six watermarked images with their corresponding extracted watermarks:



Figure 4.1: The watermarked image “Building” with its corresponding extracted watermark

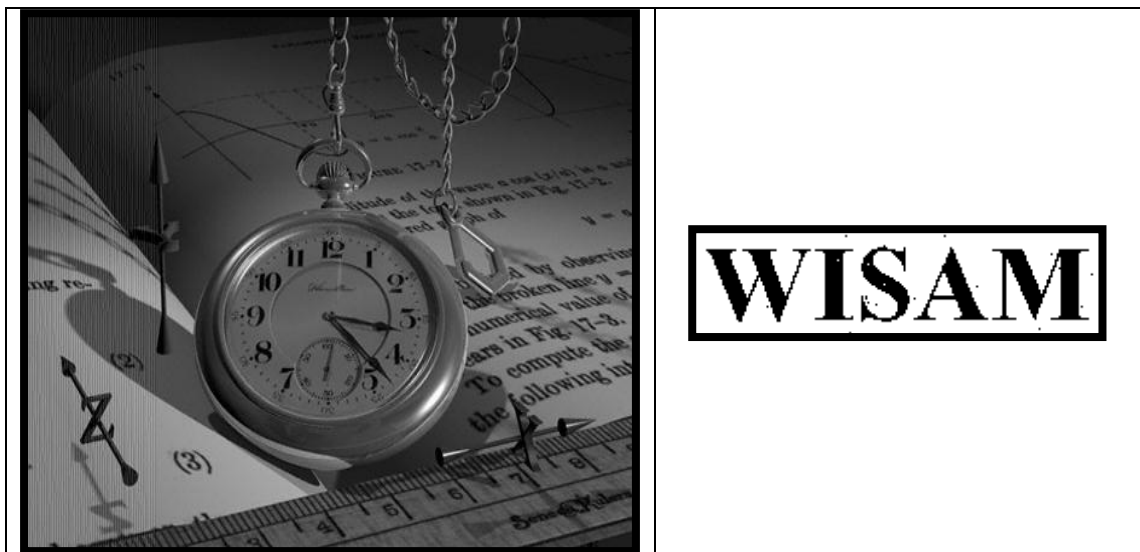


Figure 4.2: The watermarked image “Clock” with its corresponding extracted watermark



	The correlation factor = 0.9984
--	------------------------------------

	
	The correlation factor = 100%

Figure 4.3: The watermarked image “Field” with its corresponding extracted watermark

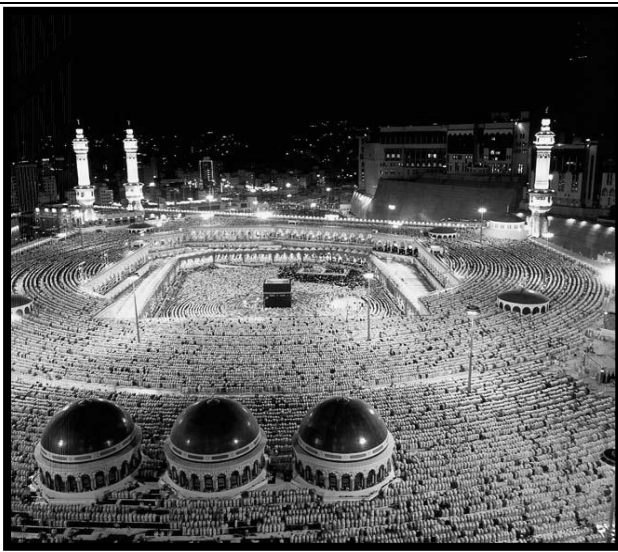

	
	The correlation factor = 0.9468

Figure 4.4: The watermarked image “Haram” with its corresponding extracted watermark

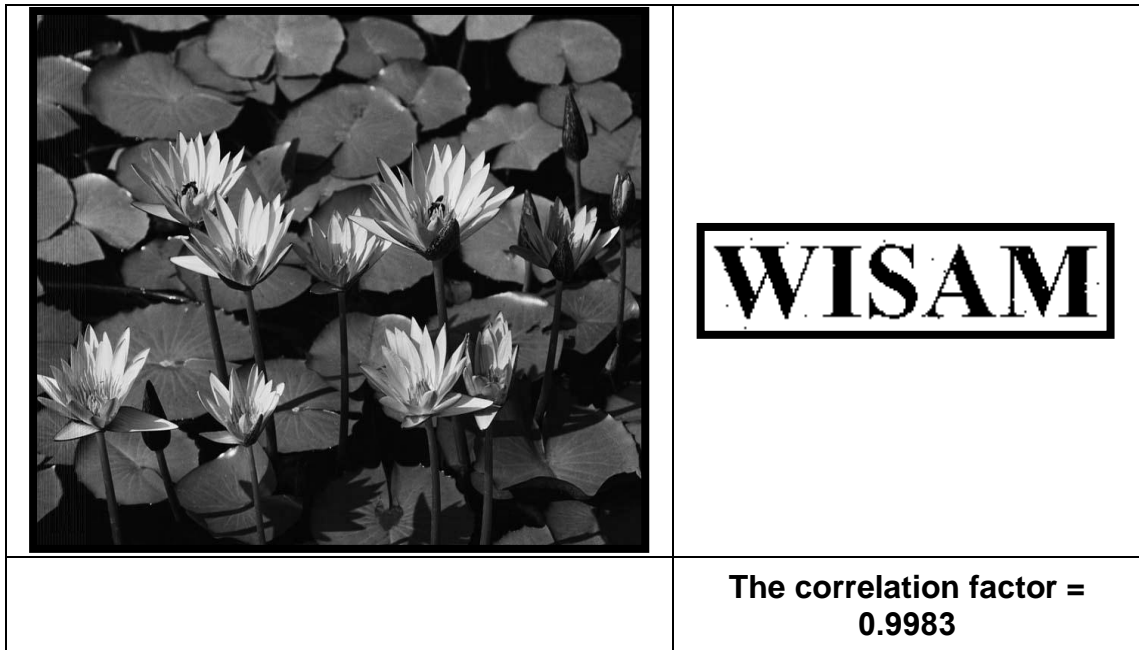


Figure 4.5: The watermarked image “Flowers” with its corresponding extracted watermark

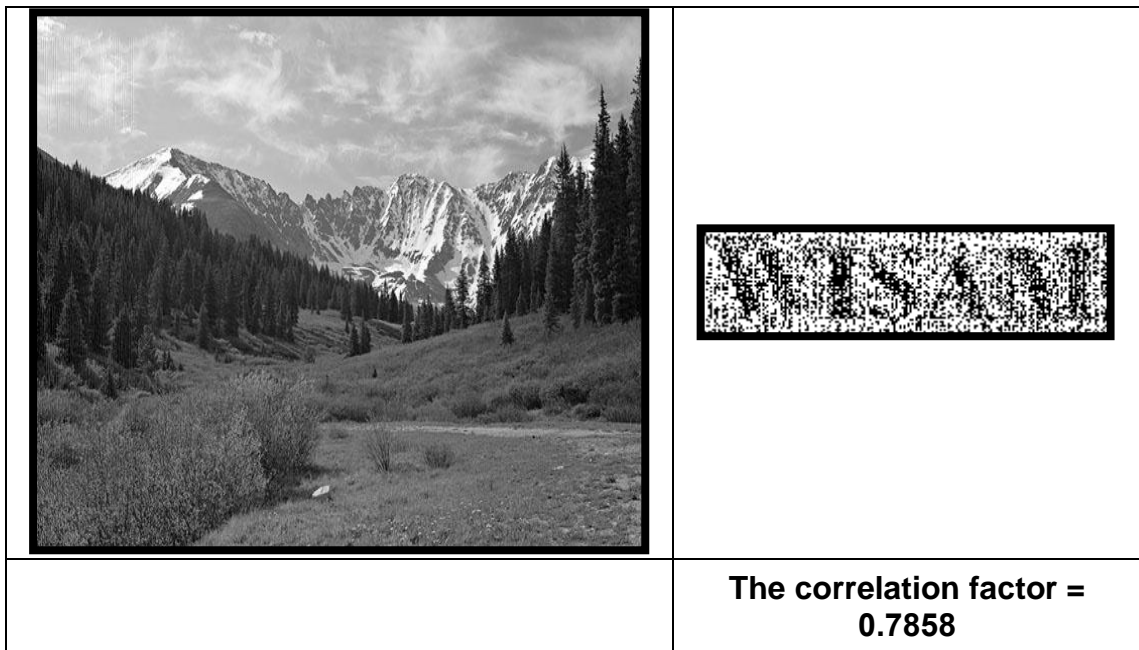


Figure 4.6: The watermarked image “Nature” with its corresponding extracted watermark



## 4.2 Attacks on the Proposed Watermarking System:

### 4.2.1: Adding Noise:

Where all pixels in an image are affected, resulting in an observed highly degraded image quality

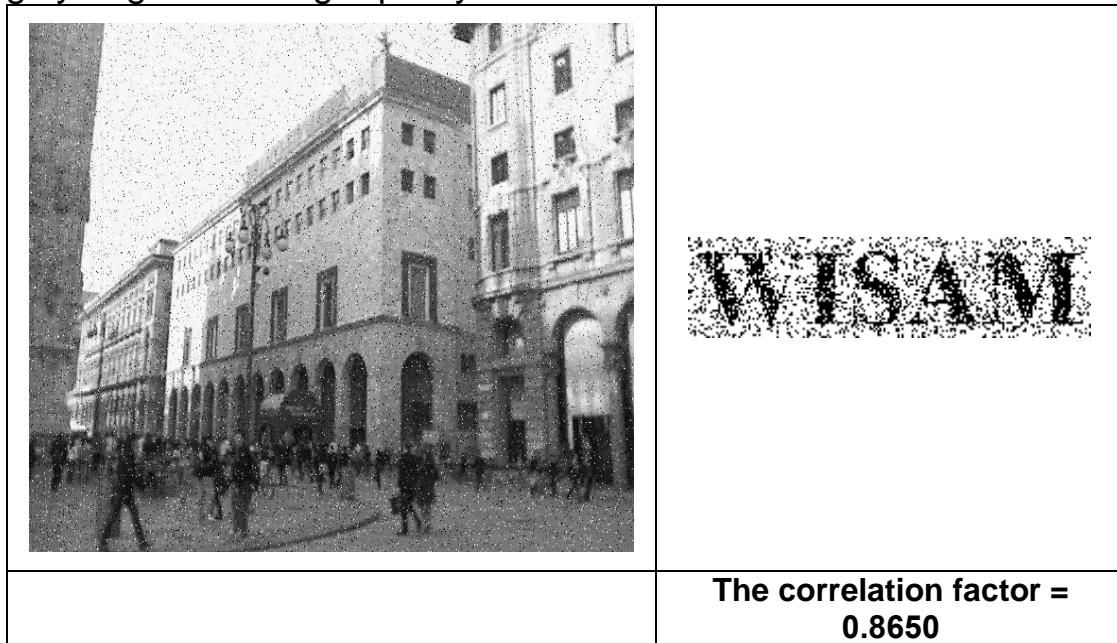


Figure 4.7: The attacked watermarked image “Building” using added noise (intensity=100, coverage=10) with its corresponding extracted watermark

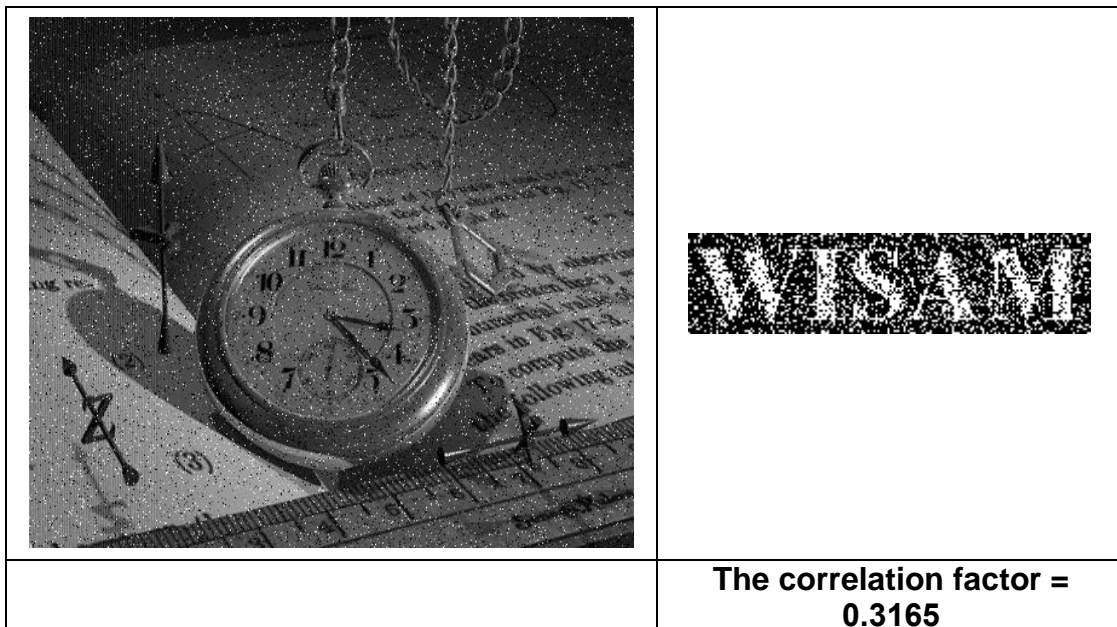


Figure 4.8: The attacked watermarked image “Clock” using added noise (intensity=100, coverage=10) with its corresponding extracted watermark



	
	<p>The correlation factor = <b>0.8754</b></p>

Figure 4.9: The attacked watermarked image “Field” using added noise (intensity=100, coverage=10) with its corresponding extracted watermark



	
	<p>The correlation factor = <b>0.7618</b></p>

Figure 4.10: The attacked watermarked image “Flowers” using added noise (intensity=100, coverage=10) with its corresponding extracted watermark

### 4.2.2 Median Filtering:

Median filter, as its name implies replaces the value of the pixel by the median of the gray levels in the neighboring pixels.



Figure 4.11: The attacked watermarked image “Field” using median filter (Radius=1, Percentile=100) with its corresponding extracted watermark

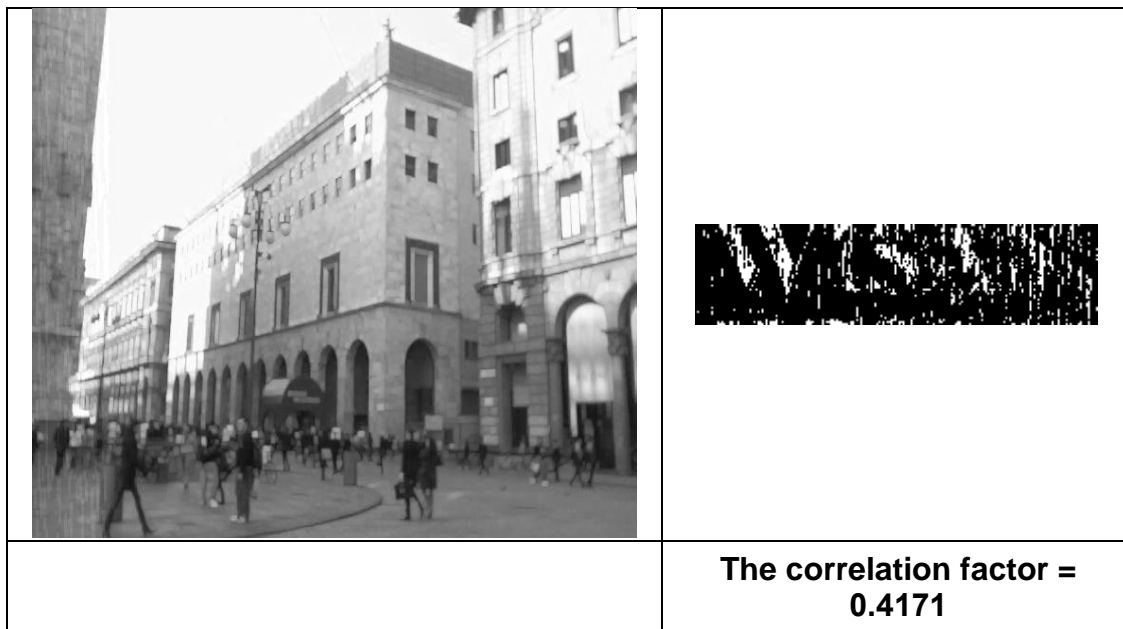


Figure 4.12: The attacked watermarked image “Building” using median filter (Radius=1, Percentile=100) with its corresponding extracted watermark



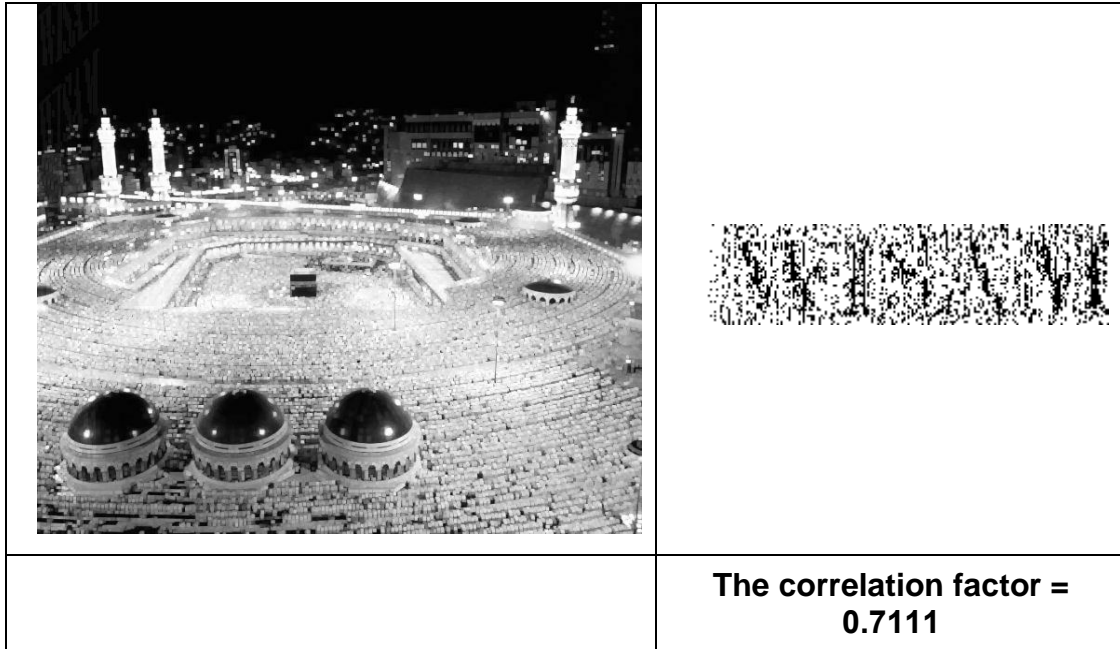


Figure 4.13: The attacked watermarked image “Haram” using median filter (Radius=1, Percentile=100) with its corresponding extracted watermark

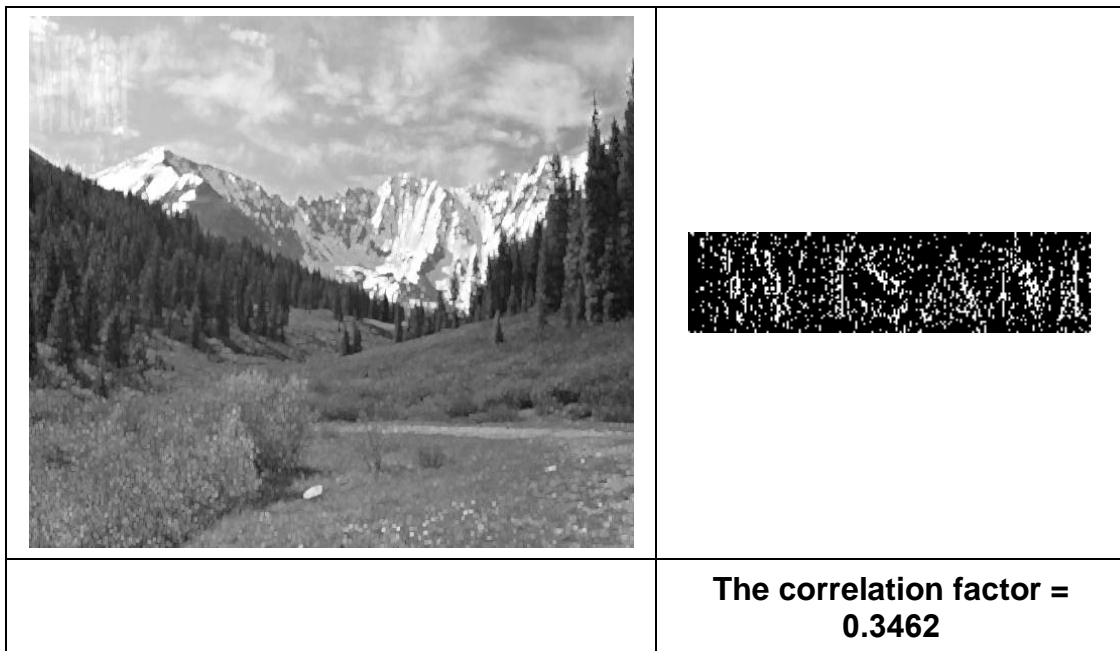


Figure 4.14: The attacked watermarked image “Nature” using median filter (Radius=1, Percentile=100) with its corresponding extracted watermark

### 4.2.3 Reducing Noise:

All attempts to determine whether differences in pixel values constitute noise or real photographic detail, and average out the former.

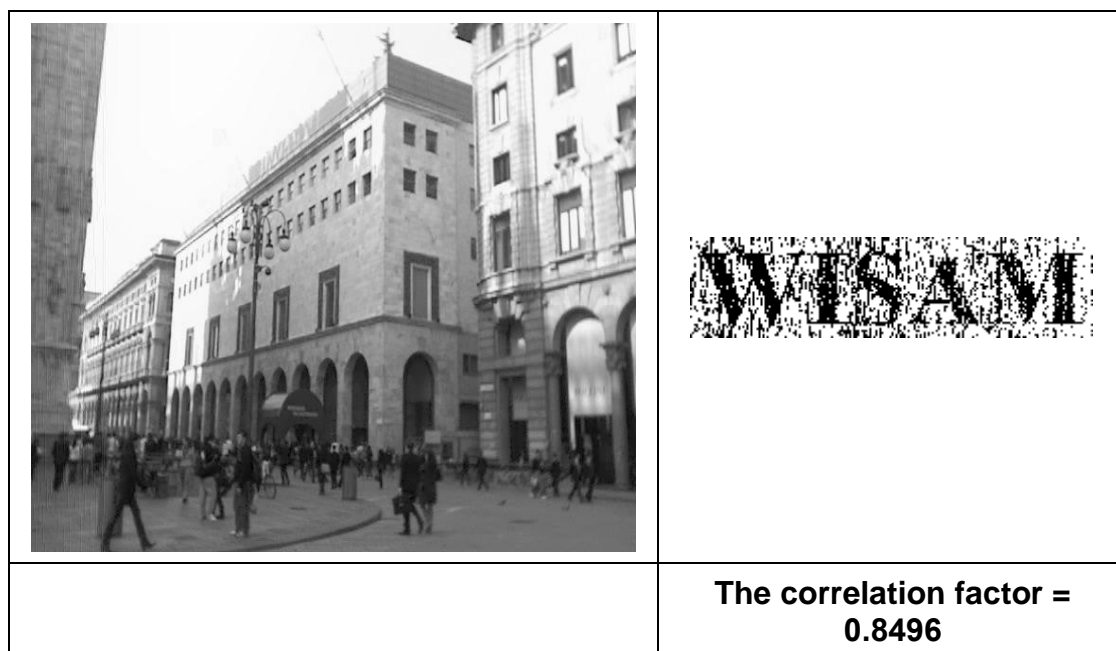


Figure 4.15: The attacked watermarked image “Building” using reducing noise (Radius=100, Strength=0.5) with its corresponding extracted watermark

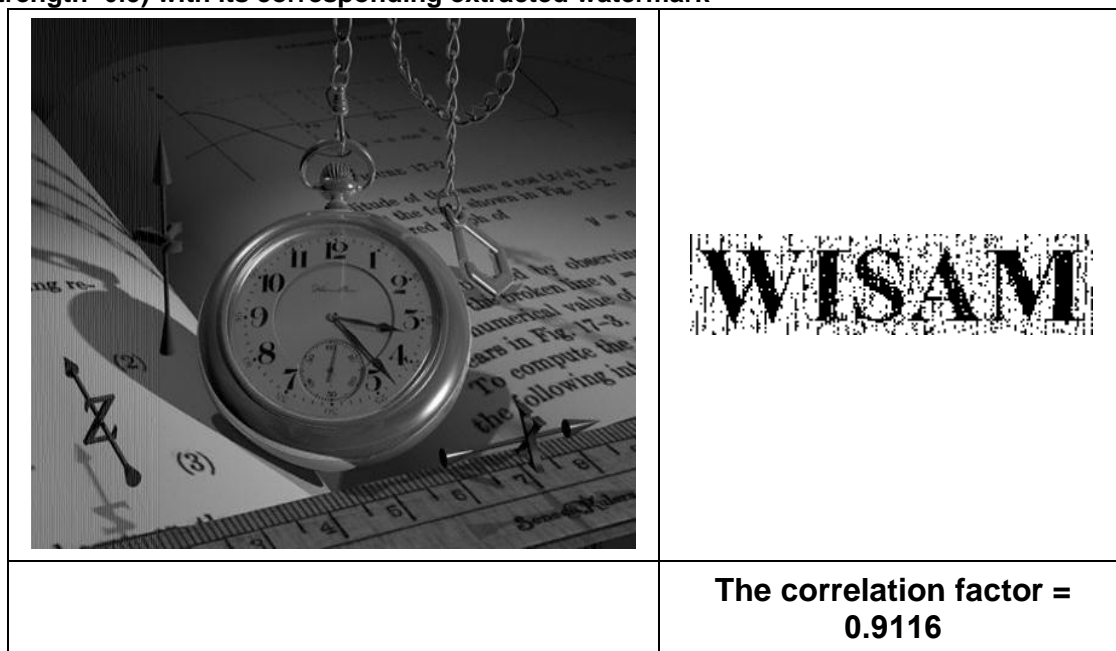
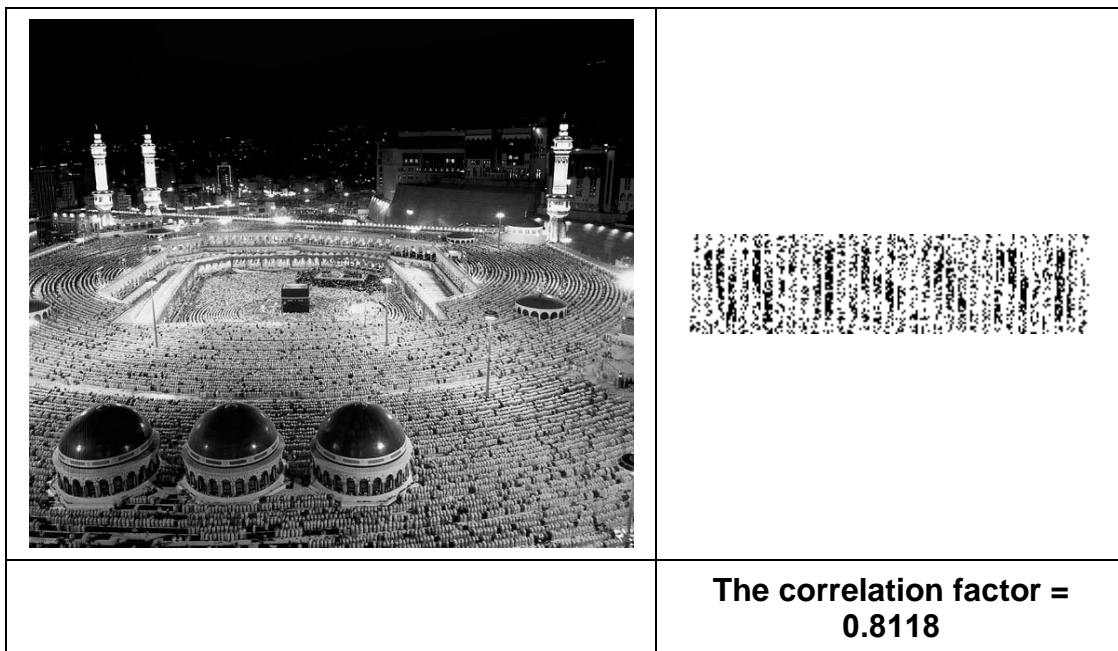


Figure 4.16: The attacked watermarked image “Clock” using reducing noise (Radius=100, Strength =0.5) with its corresponding extracted watermark



**Figure 4.17: The attacked watermarked image “Field” using reducing noise (Radius=100, Strength =0.5) with its corresponding extracted watermark**



**Figure 4.18: The attacked watermarked image “Haram” using reducing noise (Radius=100, Strength =0.5) with its corresponding extracted watermark**

#### 4.2.4 JPEG Compression:

JPEG compression is designed for compressing, varies with the degrees of looseness, depending on a compression parameter, such as the quality parameter.

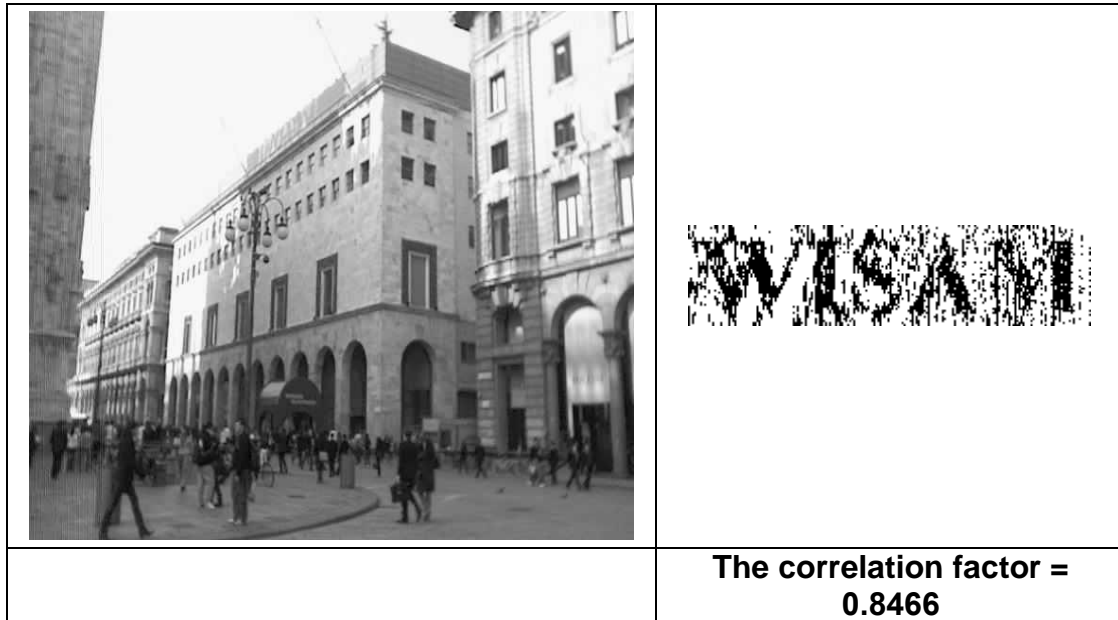


Figure 4.19: The attacked watermarked image “Building” using JPEG compression (Quality=50) with its corresponding extracted watermark

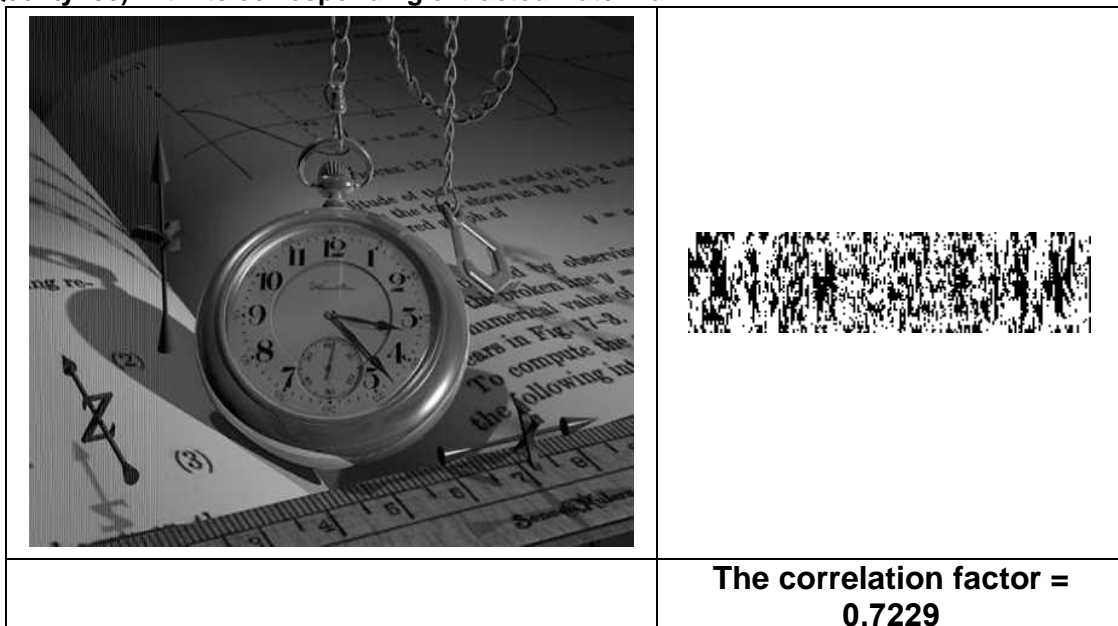




Figure 4.20: The attacked watermarked image “Clock” using JPEG compression (Quality=50) with its corresponding extracted watermark

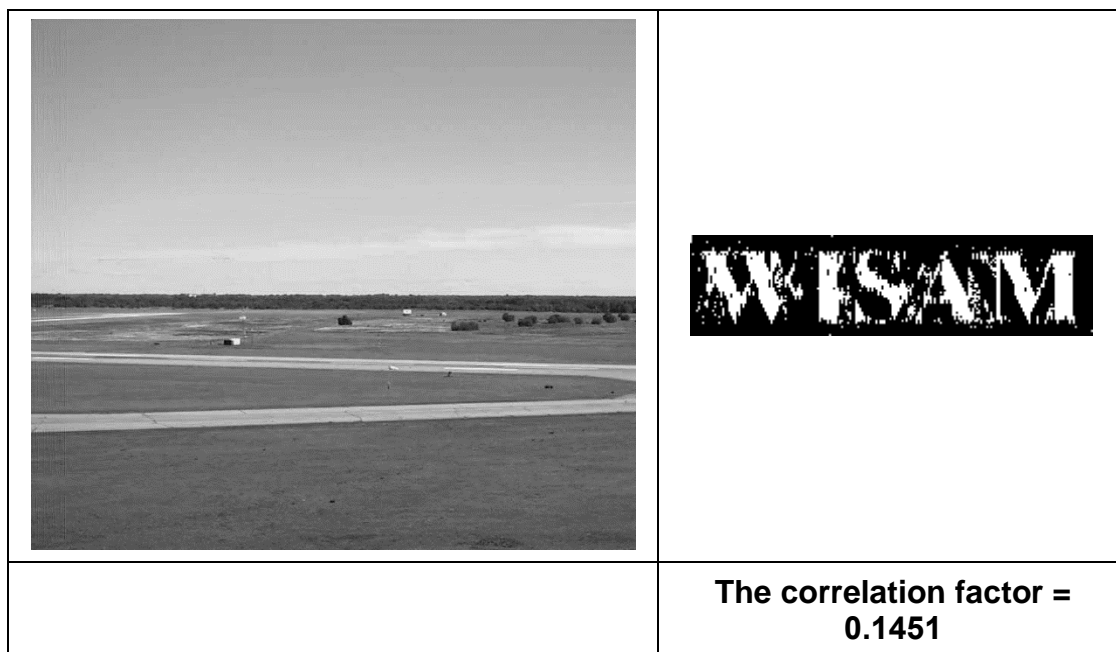


Figure 4.21: The attacked watermarked image “Field” using JPEG compression (Quality=50) with its corresponding extracted watermark

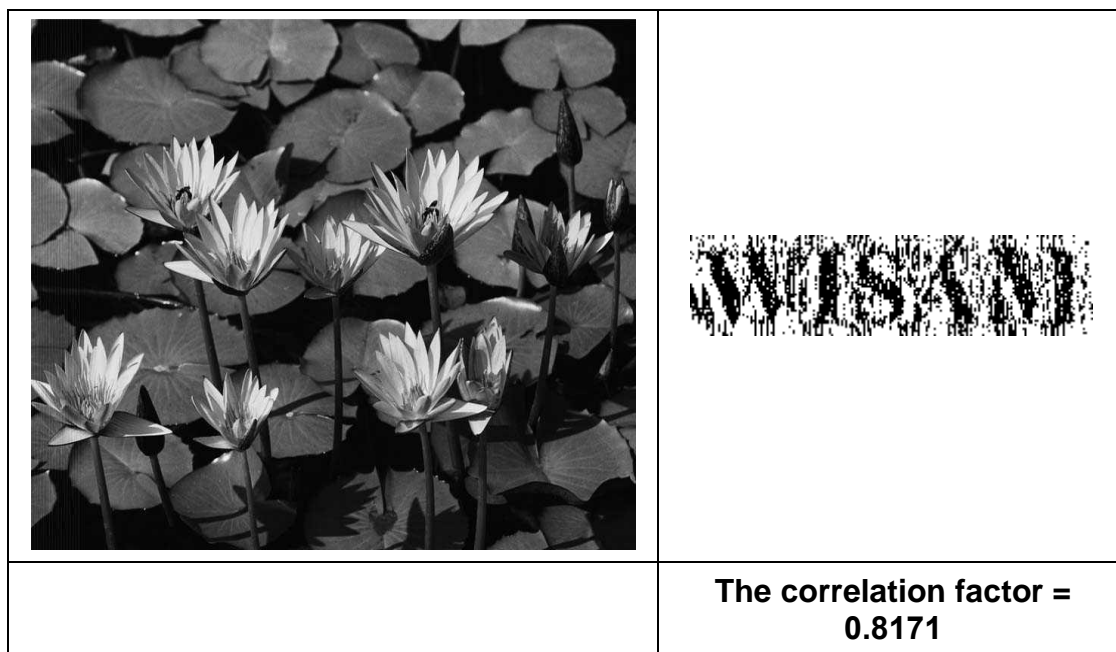


Figure 4.22: The attacked watermarked image “Flowers” using JPEG compression (Quality=50) with its corresponding extracted watermark



#### 4.2.5 Image Cropping:

Causes the image to be replaced with only the area that was selected.



Figure 4.23: The attacked watermarked image “Building” after cropping (30.5%) with its corresponding extracted watermark



Figure 4.24: The attacked watermarked image “Clock” after cropping (51%) with its corresponding extracted watermark



Figure 4.25: The attacked watermarked image “Field” after cropping (50%) with its corresponding extracted watermark

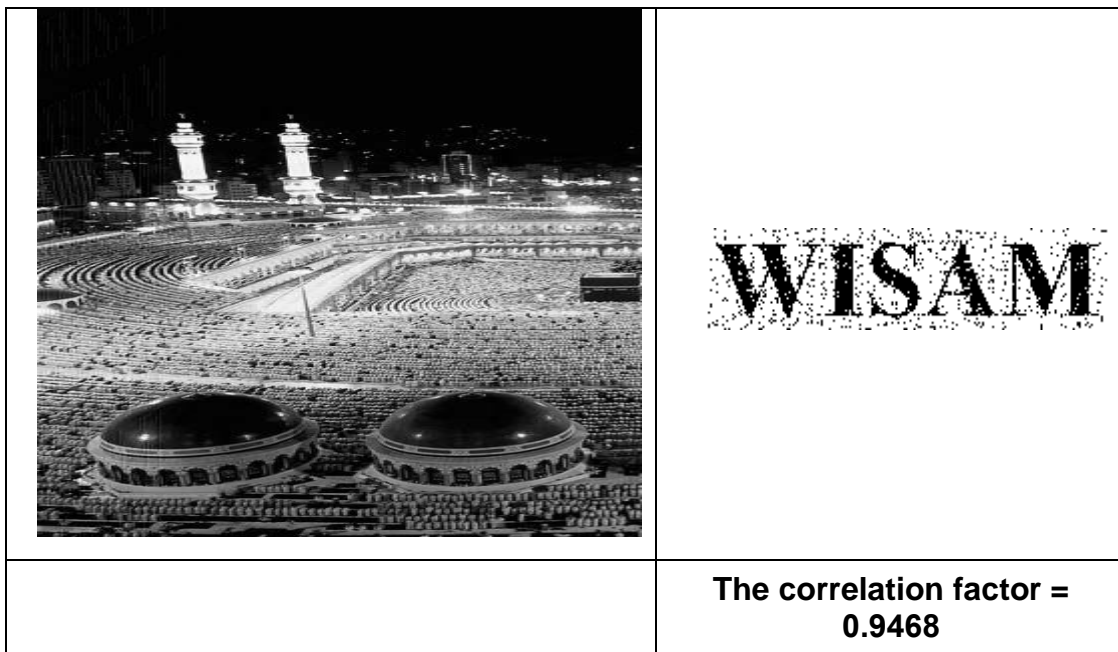


Figure 4.26: The attacked watermarked image “Haram” after cropping (53.5%) with its corresponding extracted watermark

## 4.2.6 Image Cutting:

Removing a selected portion of the active layer, and replacing it with transparent pixels. The current selection outline is also removed.



Figure 4.27: The attacked watermarked image “Building” after cutting 4 squares (0.95×0.93) with its corresponding extracted watermark

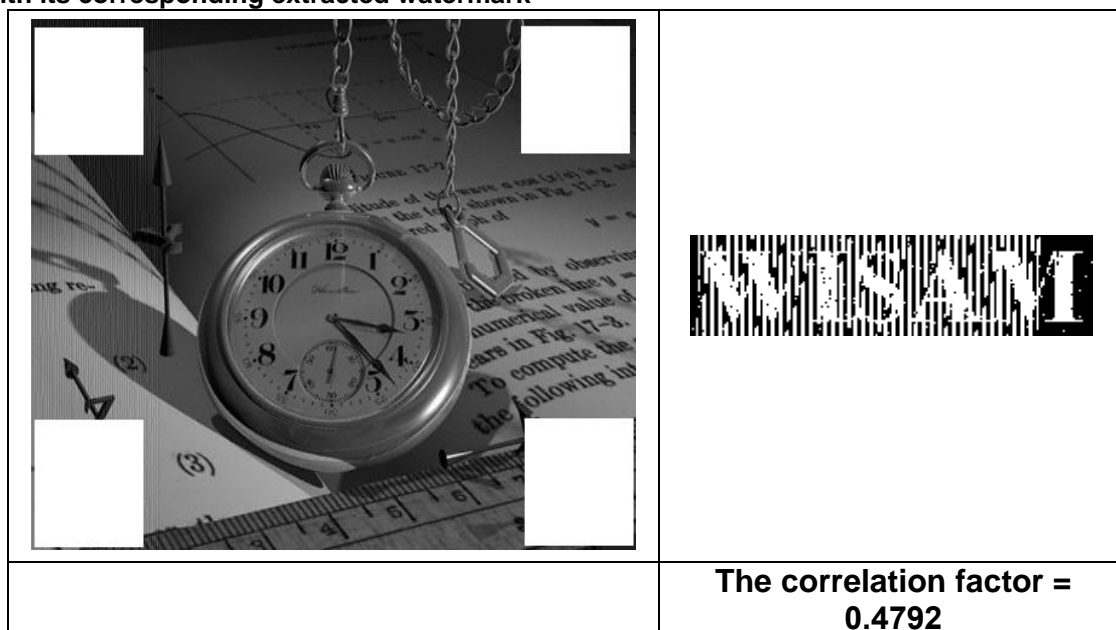


Figure 4.28: The attacked watermarked image “Clock” after cutting 4 squares (0.95×0.93) with its corresponding extracted watermark

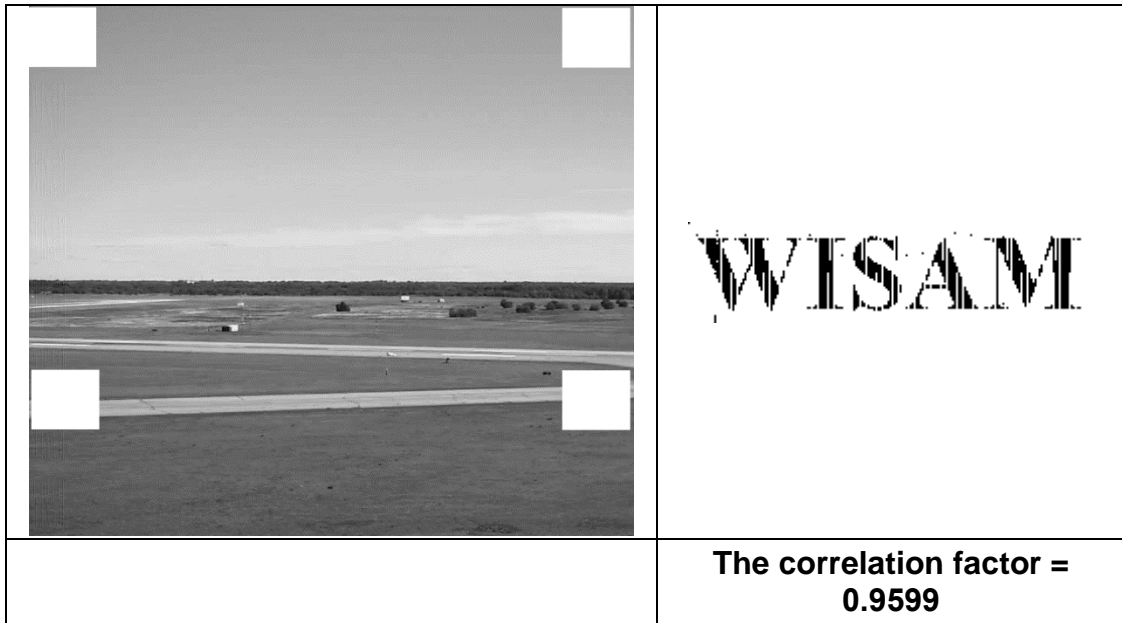


Figure 4.29: The attacked watermarked image “Field” after cutting 4 squares (0.95×0.93) with its corresponding extracted watermark

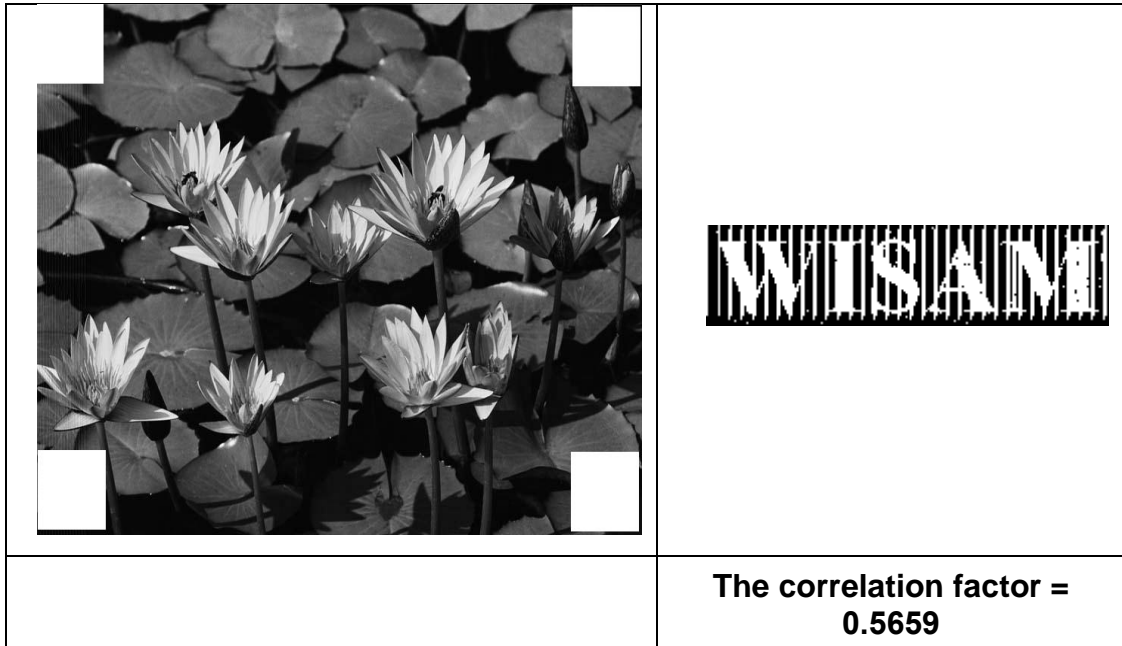


Figure 4.30: The attacked watermarked image “Flowers” after cutting 4 squares (0.95×0.93) with its corresponding extracted watermark

### 4.2.7 Image Sharpening:

Sharpening the edges, if an image has an appearance that is too soft.

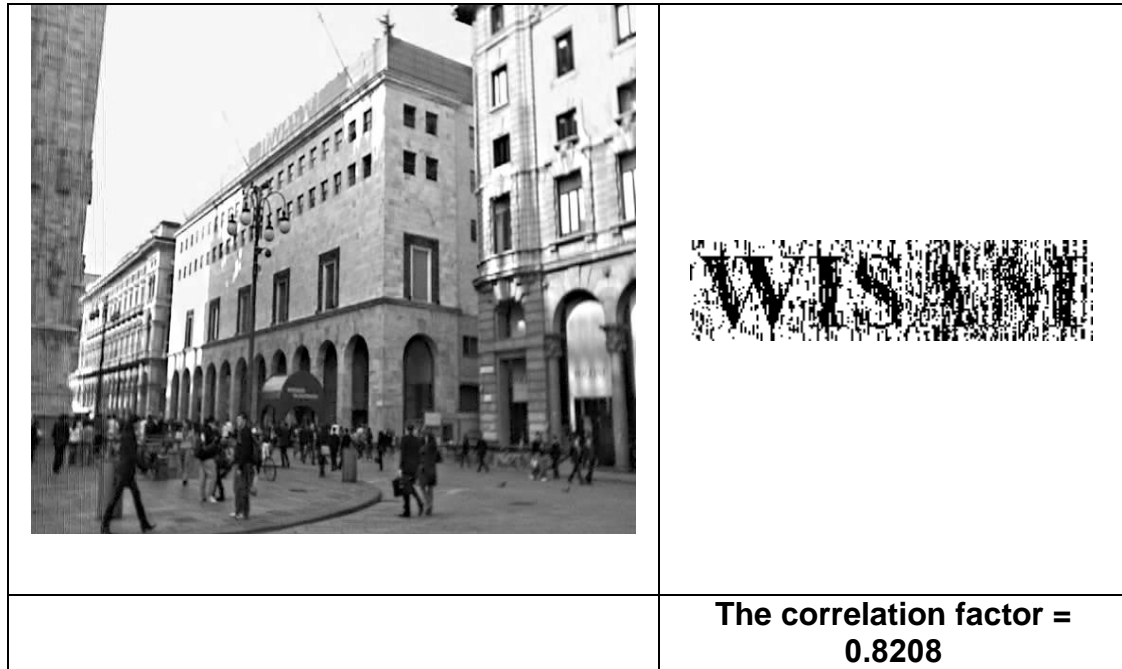


Figure 4.31: The attacked watermarked image “Building” using 'Sharpen' (amount=20) with its corresponding extracted watermark



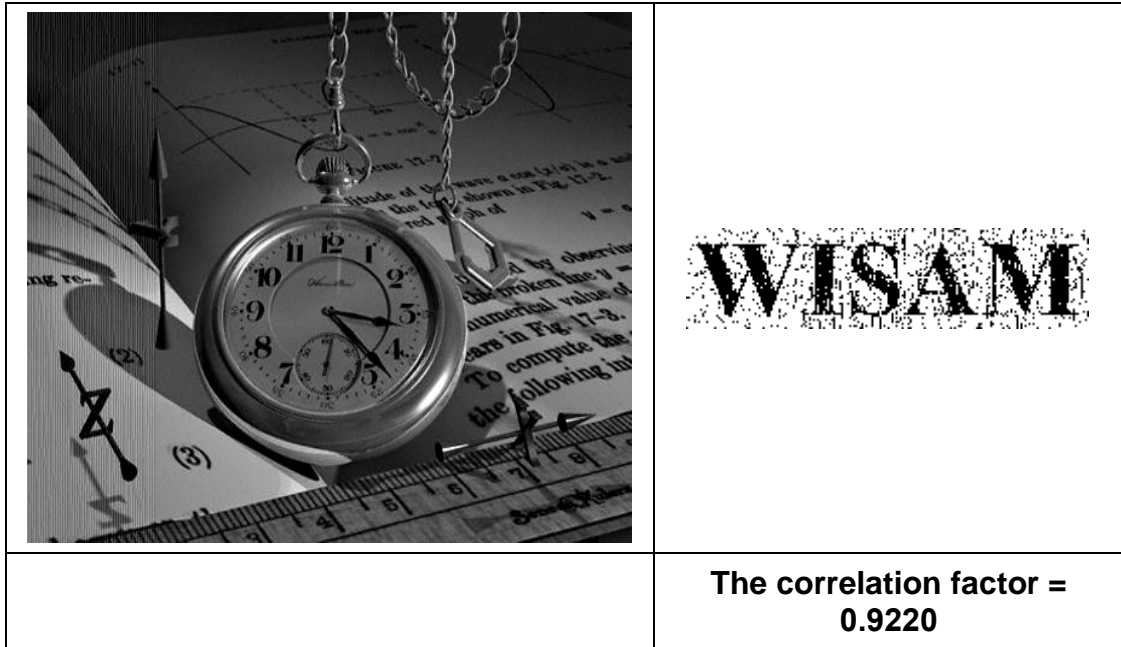
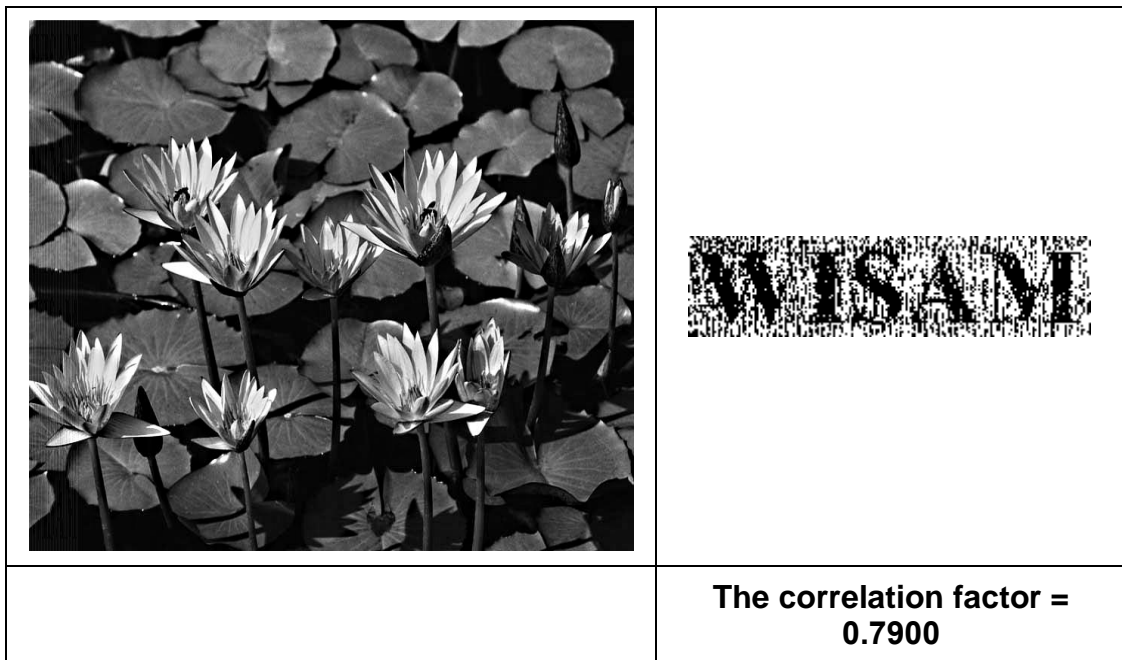
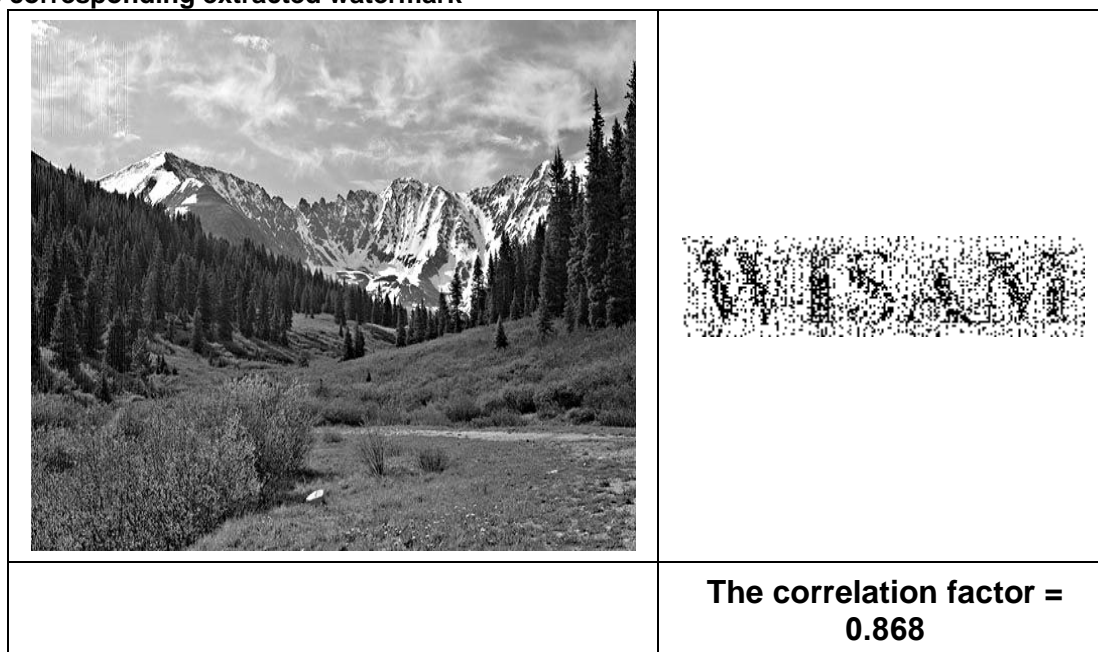


Figure 4.32: The attacked watermarked image “Clock” using 'Sharpen' (amount=20) with its corresponding extracted watermark



**Figure 4.33: The attacked watermarked image “Flowers” using 'Sharpen' (amount=20) with its corresponding extracted watermark**



**Figure 4.34: The attacked watermarked image “Nature” using 'Sharpen' (amount=20) with its corresponding extracted watermark**

### 4.2.8 Ink Sketch:

Making an image appears like it may have been drawn using an ink pen.

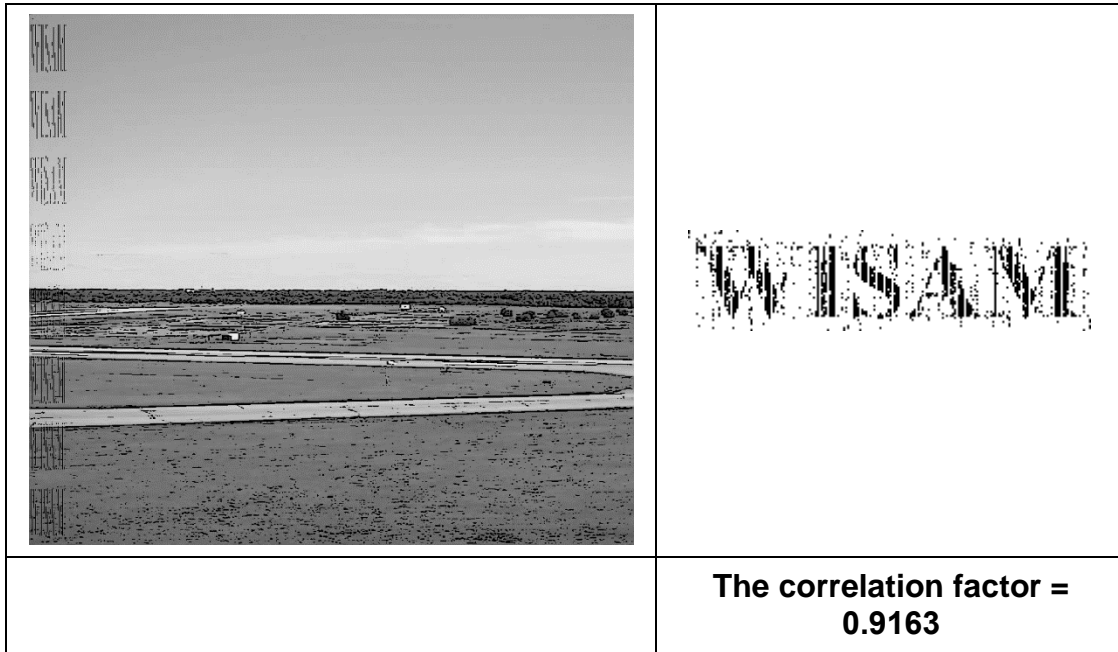


Figure 4.35: The attacked watermarked image “Field” using 'Ink sketch' (ink outline=20, coloring= 100) with its corresponding extracted watermark

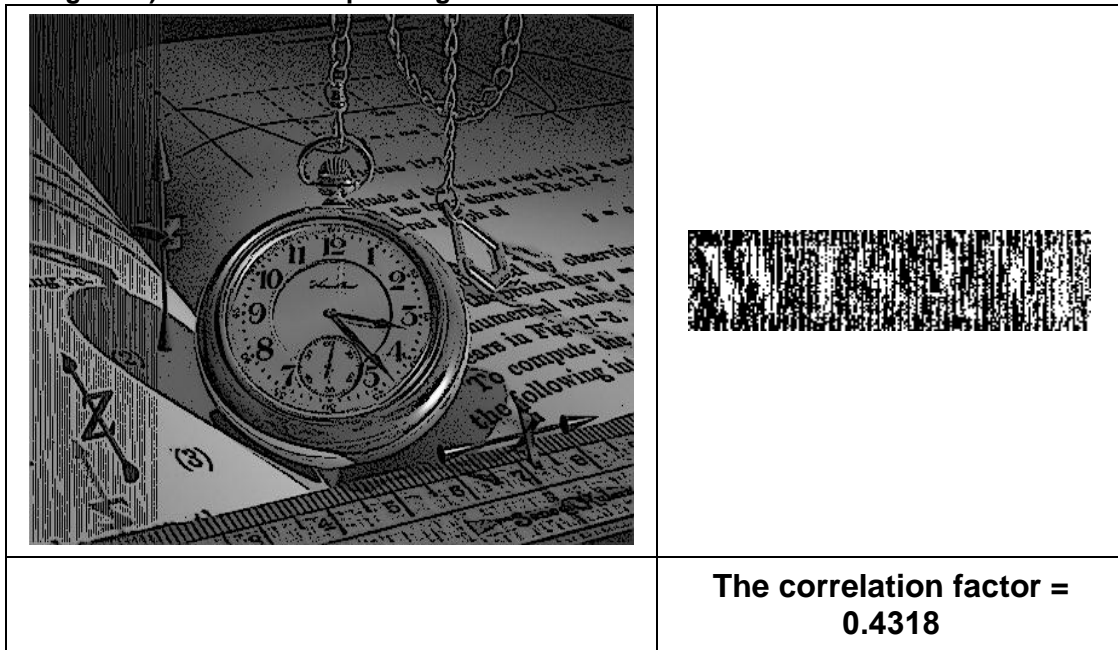


Figure 4.36: The attacked watermarked image “Clock” using 'Ink sketch' (ink outline=20, coloring= 100) with its corresponding extracted watermark



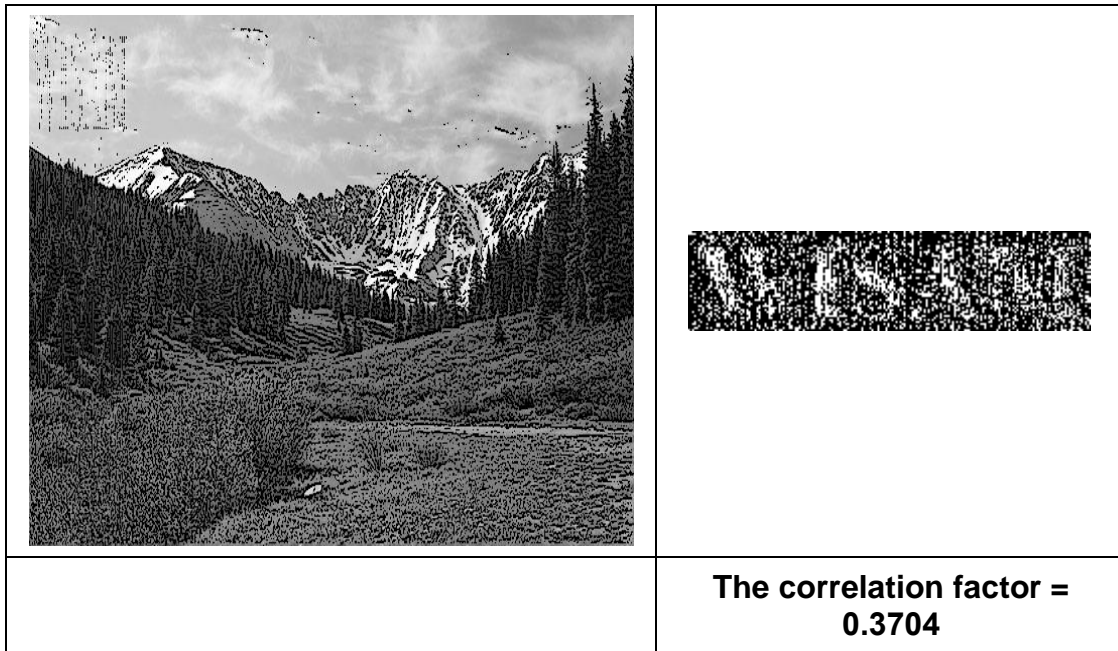


Figure 4.37: The attacked watermarked image “Nature” using 'Ink sketch' (ink outline=20, coloring= 100) with its corresponding extracted watermark

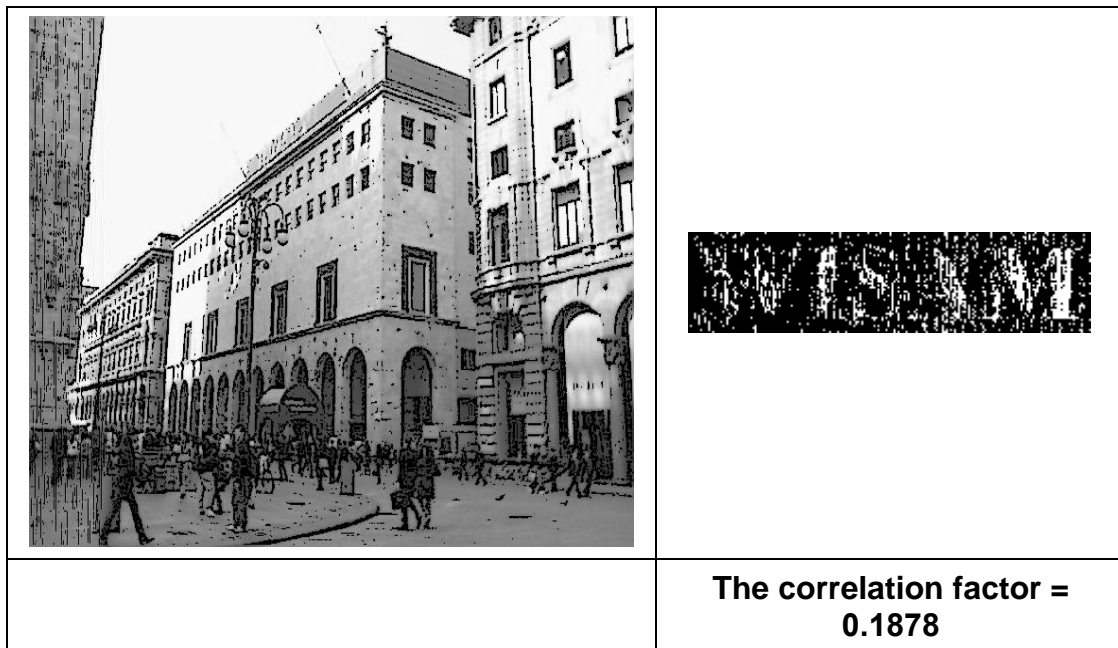


Figure 4.38: The attacked watermarked image “Building” using 'Ink sketch' (ink outline=20, coloring= 100) with its corresponding extracted watermark

### 4.2.9 Image Glow:

Giving the image a glowing effect, by controlling the brightness and contrast of the resulting image.



Figure 4.39: The attacked watermarked image “Field” using 'Image Glow' (radius=1, brightness= 10, contrast=10) with its corresponding extracted watermark



Figure 4.40: The attacked watermarked image “Clock” using 'Image Glow' (radius=1, brightness= 10, contrast=10) with its corresponding extracted watermark

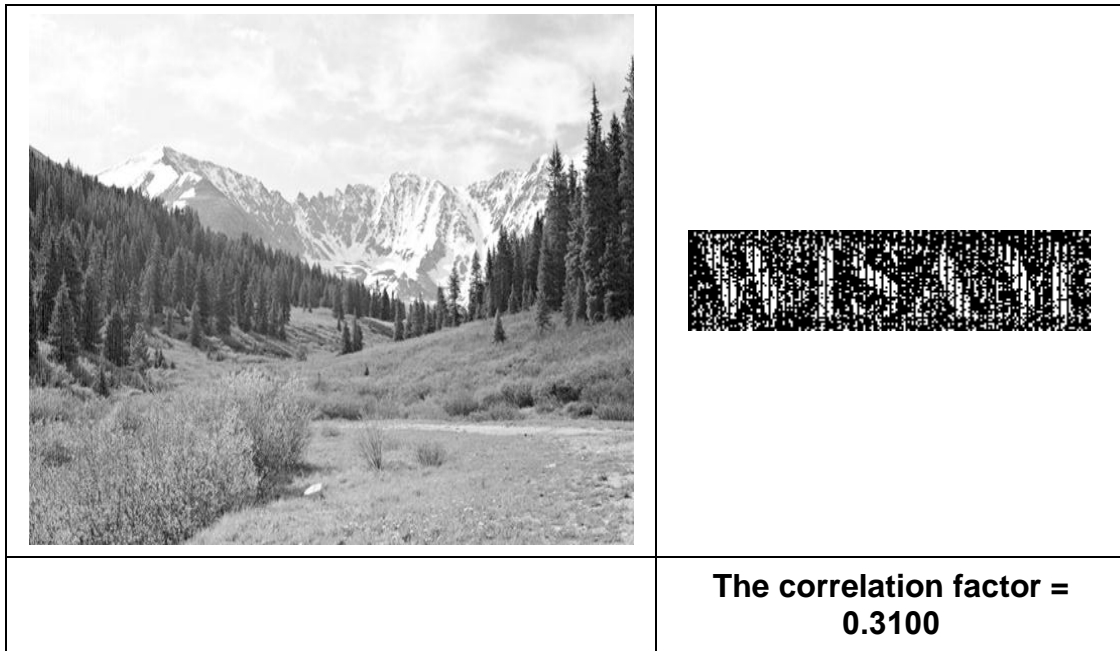


Figure 4.41: The attacked watermarked image “Nature” using 'Image Glow' (radius=1, brightness= 10, contrast=10) with its corresponding extracted watermark

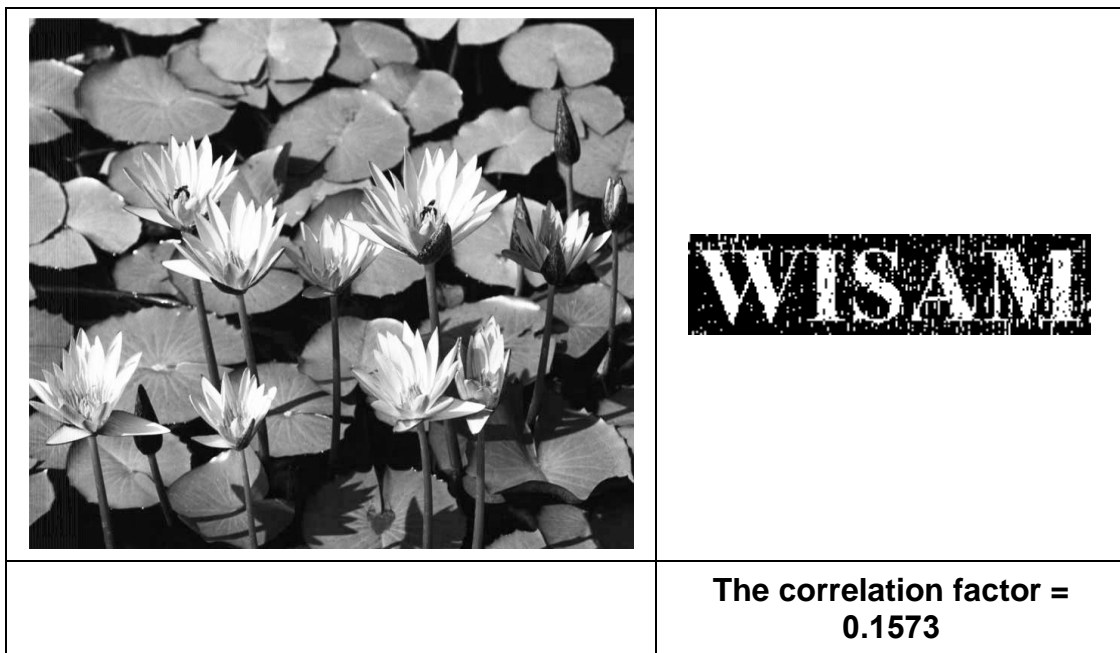


Figure 4.42: The attacked watermarked image “Flowers” using 'Image Glow' (radius=1, brightness= 10, contrast=10) with its corresponding extracted watermark

### 4.3 Robustness Results Viewing:

In this section the previous robustness results of the proposed watermarking system will be summarized in the following table for the sake of discussion in the next chapter.

		<b>Correlation Value between original and extracted watermark</b>					
<i>Name of Image</i>	<i>Name of Attack</i>	<i>Field</i>	<i>Clock</i>	<i>Building</i>	<i>Haram</i>	<i>Flowers</i>	<i>Nature</i>
	<b>Adding Noise</b>	88%	32%	87%	30%	76%	32%
	<b>Median Filter</b>	75%	13%	42%	71%	85%	35%
	<b>Reducing Noise</b>	99%	91%	85%	81%	88%	81%
	<b>JPEG Compression</b>	15%	72%	85%	66%	82%	70%
	<b>Image Cropping</b>	1%	95%	100%	95%	22%	79%
	<b>Image Cutting</b>	96%	48%	89%	36%	37%	57%
	<b>Image Sharpening</b>	87%	92%	82%	77%	79%	85%
	<b>Ink Sketch</b>	92%	43%	19%	45%	52%	37%
	<b>Image Glow</b>	95%	8%	70%	35%	16%	31%

Table 4.1: The correlation values for each image used in the tests against different attacks

#### 4.4 Imperceptibility Results Viewing:

In the following table, the Imperceptibility of the proposed watermarking system will be viewed for each image used in the tests, for the sake of discussion in the next chapter.

<i>Name of Image</i>	<i>PSNR Value</i>
<i>Field</i>	<b>38.74</b>
<i>Clock</i>	<b>33.97</b>
<i>Building</i>	<b>40.01</b>
<i>Haram</i>	<b>39.91</b>
<i>Flowers</i>	<b>38.47</b>
<i>Nature</i>	<b>37.80</b>

Table 4.2: The PSNR values for each image used in the tests

## Chapter Five

### Conclusions and Future Works

#### 5.1 Conclusions:

In this thesis an image watermarking system using spatial and frequency domains was proposed. The Least Significant Bit (LSB) approach lacks immunity and robustness against many image attacks, on the other hand Discrete Wavelet Transform (DWT) approach is not sufficient to achieve robust watermarking system, so the two approaches were combined together in order to produce a new robust watermarking system.

Based on the results that have been illustrated in the previous chapter, and after subjecting the proposed algorithm to many different attacks, it is noticed that this algorithm achieved a high degree in robustness since the values of correlation between the original watermark and the extracted watermark were very promising in all used attacks (see table 4.1).

With regard to the second criteria (i.e. imperceptibility), the Peak Signal to Noise Ratio (PSNR) was used for evaluation, in general a processed image is acceptable to human eyes if its PSNR is greater than 30 dB to 45 dB which has been achieved as shown in table 4.2.

Other requirements were realized such as the increase of data payload, since the used watermark had relatively big resolution (200×50).



The security of the watermark is considered to be high, since the ability to resist hostile attacks. The watermarking system is blind because the original image is not needed in the extraction phase.

Finally all the results of the experiments that was carried out to test the performance of the proposed watermarking algorithm confirmed the effectiveness of the proposed algorithm with respect to the watermark imperceptibility and its robustness against large set of possible attacks.

## **5.2 Future Works:**

LH1 decomposition was used to embed the watermark's bits; the system can be extended to use other decompositions for the sake of scattering watermark's bits in order to enhance both robustness and imperceptibility. Another suggestion is to try embedding a colored watermark instead of a monochromatic one.

In addition, it is possible to use some kinds of encryption for the watermark before the embedding process in order to increase security.

## References

- [1] Al-Haj, A., **Cmbined DWT-DCT Digital Image Watermarking**. Journal of Computer Science Vol. 3, PP. 740-746. (2007).
- [2] Al-Haj, A., Manasrah, T., **SVD-Based Image Water marking**, Journal of Digital Information Management, Volume 7, Number 2, April, (2009).
- [3] Al-Oqaily, I., **A Robust Discrete Cosine Transformation-Based Watermarking Algorithm for Digital Images**. Master Thesis, University of Jordan, Amman, Jordan, (2003).
- [4] Cole, E., Krutz, R., **Hiding in Plain Sight: Steganography and the Art of Covert Communication**, Wiley Publishing, (2003).
- [5] Cox, I., Kilian, J., Leighton, T., and Shamoon, T., **A secure, robust watermark for multimedia**. Information Hiding: First International Workshop, Cambridge, UK, volume 1174 of Lecture Notes in Computer Science, PP. 183-206, (1996).
- [6] Cox, I., Miller, M., & Bloom, J., **Digital Watermarking**. (1st edition) SanFrancisco, Morgan Kaufmann (2002).



- [7] Cox, I., Miller, M., Bloom, J., Fridrich, J., & Talker, T., **Digital Watermarking and Steganography**. (2<sup>nd</sup> edition), Morgan Kaufmann, (2008).
- [8] Cox, I., Miller, M., Linnartz, J., & Kalker, T., **A review of watermarking principles and practices**. In K. Parhi & T. Nishitani (Eds.), Digital signal processing in multimedia systems, PP. 461-485, (1999).
- [9] Craver, S., Memon, N., Yeo, B. and Yeung, M., **Can invisible watermark resolve rightful ownerships?** In Fifth Conference on Storage and Retrieval for Image and Video Database, volume 3022, PP. 310-321, San Jose, USA, February (1997).
- [10] Davern, P., and Scott, M., **Steganography its history and its application to Computer based data files**, computer application, Ca-0759, Dublin city university, Ireland (2000).
- [11] Decker, S., **Engineering Considerations in Commercial Watermarking**, IEEE Communications Magazine. 0163-6804/1, PP. 128-133, (2001).
- [12] Delannay, D., **Digital Watermarking Algorithms Robust Against Loss of Synchronization**. Thesis submitted for obtaining the rank of Doctor in Applied Sciences, Catholic University of Leuven, Belgium, (2004).
- [13] Dogramacy, M., **Digital watermarking in Transformed Domain**. Master Thesis, University of Jordan, Amman, Jordan, (2005).
- [14] Dugelay, J., Baskurt, A., and Daoudi, M., **3D Object Processing, Compression, Indexing and Watermarking**, John Wiley & Sons, Ltd, (2008).

- [15] Fridrich, J., Goljan, M., **Comparing Robustness of Watermarking Techniques**, SPIE Security and Watermarking of Multimedia Content, San Jose, CA, Jan, (1999).
- [16] Hanjalic, A., Langelaar, G., van Roosmalen, P., Biemond, J., & Langendijk, R., **Image and video databases: Restoration, watermarking and retrieval**. Amsterdam: Elsevier, (2000).
- [17] Hartung, F., and Girod, B., **Watermarking of uncompressed and compressed video**. Signal Processing, 66(3), PP. 283–301, (1998).
- [18] Jellinek, B., **Invisible Watermarking of Digital Images for Copyright Protection**, Thesis to obtain the academic degree graduate at the Faculty of Science, University of Salzburg, 21 January, (2000).
- [19] Johnson, N., Jajodia, S., and Duric, Z., **Information hiding: Steganography and watermarking attacks and countermeasures**, Kluwer academic Publishers, (2000).
- [20] Katzenbeisser, S., and Petitcolas, F., **Information Hiding: Techniques for steganography and digital watermarking**. Boston, MA: Artech House, (2000).
- [21] Kundur, D., and Hatzinakos, D., **Digital watermarking using multiresolution wavelet decomposition**. Proceedings of the IEEE International Conference on Acoustics, Volume 5, PP. 2969-2972, Washington, (1998).

- [22] Kutter, M., Jordan, F., and Bossen, F., **Digital signature of color images using amplitude modulation**. Proceedings of the SPIE Storage and Retrieval for Image and Video Databases V, vol. 3022, PP. 518-526 (1997).
- [23] Maes, M., Rongen, P., and van Overveld, C., **Digital image watermarking by salient modification practical results**. Conference on Security and Watermarking of Multimedia Contents, number 3657, PP. 273-282, California, USA, (1999).
- [24] Mandhani, N., **WATERMARKING USING DECIMAL SEQUENCES**. Master Thesis, Louisiana State University and Agricultural and Mechanical College, USA, August, (2004).
- [25] Mohanty, S., **Digital Watermarking: A Tutorial Review**. Master Project Report, Dept. of Electrical Engineering, India, Institute of Science, DANGALORE, - 560 012, India, (1999).
- [26] Oliveira, S., Nascimento M., and Zaiane O., **Digital Watermarking: Status, Limitations and Prospects**. Technical Report TR 02-01, University Of Alberta, January, (2002).
- [27] Pereira, S., Voloshynovskiy, S., Madueno, M., Marchand-Maillet, S., and Pun, T., **Second Generation Benchmarking and Application Oriented Evaluation**, Lecture Notes In Computer Science; Vol. 2137, Proceedings of the 4th International Workshop on Information Hiding, Springer-Verlag, London, UK, PP. 340-353, (2001).

- [28] Seitz, J., **Digital Watermarking for Digital Media**. (1st edition). Information Science Publishing, (2005).
- [29] Shoemaker, C., **Hidden bits: A survey of techniques for digital watermarking**, Independent study, EER 290, (2002).
- [30] Voloshynovskiy, S., Pereira, S., Iquise, V., and Pun, T., **Attack modelling: Towards a second generation watermarking benchmark**. Signal Processing, (2001).
- [31] Wang, H., and Kuo, C., **Wavelet based digital image watermarking**. In Optics Express Focus Issue: Digital Watermarking, vol. 3, (1998).
- [32] Wang, Y., Doherty, J., and Van Dyck, R., **A watermarking algorithm for fingerprinting intelligence images**, Conference on Information Science and Systems, the John Hopkins University, (2001).
- [33] [www.pgi.org/doc/pgintro](http://www.pgi.org/doc/pgintro), The Pyrotechnics Guild International, Inc., on Feb, 2010.
- [34] Xia, X., Boncelet, C., and Arce, G., **Wavelet transform based watermark for digital images**, Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716, OPTICS EXPRESS vol. 3, NO. 12, (1998).

