



University of Bradford eThesis

This thesis is hosted in [Bradford Scholars](#) – The University of Bradford Open Access repository. Visit the repository for full metadata or to contact the repository team



© University of Bradford. This work is licenced for reuse under a [Creative Commons Licence](#).

**COMBINED ROBUST AND FRAGILE
WATERMARKING ALGORITHMS FOR STILL
IMAGES**

Taha Dawood Jassim

Ph.D.

2014

COMBINED ROBUST AND FRAGILE WATERMARKING ALGORITHMS FOR STILL IMAGES

Design and evaluation of combined blind discrete wavelet transform-based robust watermarking algorithms for copyright protection using mobile phone numbers and fragile watermarking algorithms for content authentication of digital still images using hash functions

Taha Dawood Jassim

B.Eng., M.Sc.

Submitted for the Degree of

Doctor of Philosophy

School of Engineering, Design and Technology

University of Bradford

2014

Abstract

COMBINED ROBUST AND FRAGILE WATERMARKING ALGORITHMS FOR STILL IMAGES

Design and evaluation of combined blind discrete wavelet transform-based robust watermarking algorithms for copyright protection using mobile phone numbers and fragile watermarking algorithms for content authentication of digital still images using hash functions.

Keywords

Image processing; Watermarking; Still image; Discrete wavelet transform (DWT); Hash function; MD5; Authentication; Copyright; PSNR; SSIM;

This thesis deals with copyright protection and content authentication for still images. New blind transform domain block based algorithms using one-level and two-level Discrete Wavelet Transform (DWT) were developed for copyright protection. The mobile number with international code is used as the watermarking data. The robust algorithms used the Low-Low frequency coefficients of the DWT to embed the watermarking information. The watermarking information is embedded in the green channel of the RGB colour image and Y channel of the YCbCr images. The watermarking information is scrambled by using a secret key to increase the security of the algorithms. Due to the small size of the watermarking information comparing to the host image size, the embedding process is repeated several times which resulted in increasing the robustness of the algorithms. Shuffling process is implemented during the multi embedding process in order to avoid spatial correlation between the host image and the watermarking information. The effects of using one-level and two-level of DWT on the robustness and image quality have been studied. The Peak Signal to Noise Ratio (PSNR), the Structural Similarity Index Measure (SSIM) and Normalized Correlation Coefficient (NCC) are used to evaluate the fidelity of the images. Several grey and still colour images are used to test the new robust algorithms. The new algorithms offered better results in the robustness against different attacks such as JPEG compression, scaling, salt and pepper noise, Gaussian noise, filters and other image processing compared to DCT based algorithms.

The authenticity of the images were assessed by using a fragile watermarking algorithm by using hash function (MD5) as watermarking information embedded in the spatial domain. The new algorithm showed high sensitivity against any tampering on the watermarked images. The combined fragile and robust watermarking caused minimal distortion to the images. The combined scheme achieved both the copyright protection and content authentication.

Table of Contents

CHAPTER 1	1
1.1 Motivation.....	1
1.2 Overview of Digital Watermarking.....	2
1.3 Aims.....	3
1.4 Achievements and Contributions.....	4
1.5 Overview of the thesis.....	6
1.6 References	7
CHAPTER 2.....	9
2.1 Overview	9
2.2 Definition of Digital Image Processing.....	9
2.3 Sampling and Quantization.....	11
2.4 Spatial Domain	12
2.4.1 Grey Level Images.....	12
2.4.2 Colour Images.....	14
2.4.2.1 RGB (Red Green Blue).....	14
2.4.2.2 YCbCr.....	14
2.5 Transforming the Domain.....	15
2.5.1 Discrete Fourier Transform.....	16
2.5.2 Discrete Cosine Transform (DCT).....	17
2.5.3 Discrete Wavelet Transform (DWT).....	19
2.6 Two Dimensional Filtering.....	23
2.6.1 Averaging Filters.....	23
2.6.2 Gaussian Low-pass Filter.....	24
2.6.3 Median Filter.....	25
2.7 Image Compression.....	27
2.7.1 JPEG Lossy Algorithm Steps.....	27
2.8 Hash Code.....	32
2.8.1 MD5 (Message-Digest algorithm 5)	33
2.8.2 SHA-1(Secure Hash Algorithm).....	34
2.9 References.....	34

CHAPTER 3	36
3.1 Introduction.....	36
3.2 Basic Concepts.....	36
3.3 Application.....	37
3.3.1 Copyright protection.....	37
3.3.2 Content Authentication.....	38
3.4 Requirements.....	38
3.4.1 Imperceptibility.....	38
3.4.2 Security.....	39
3.4.3 Robustness.....	39
3.4.4 Capacity.....	40
3.5 Watermark Classifications.....	40
3.5.1 Spatial and Transform Domain.....	40
3.5.1.1 Spatial Domain.....	40
3.5.1.2 Transform (Frequency) Domain.....	42
3.5.2 Non-Blind and Blind Watermarking Techniques.....	42
3.5.2.1 Non-Blind Watermarking Technique.....	42
3.5.2.2 Blind Watermarking Technique.....	42
3.5.3 Robust and Fragile Watermarking Techniques.....	43
3.5.3.1 Robust Watermarking.....	43
3.5.3.2 Fragile Watermarking.....	43
3.6 Evaluation and Benchmarking.....	43
3.6.1 Peak Signal to Noise Ratio (PSNR).....	43
3.6.2 The Structural Similarity Index Measurement (SSIM).....	44
3.6.3 The Normalized cross Correlation (NCC).....	46
3.7 Attacks.....	46
3.7.1 JPEG Compression Attack.....	47
3.7.2 Image Enhancement Attack.....	48
3.7.3 Removal Attack.....	48
3.7.4 Cropping Attack.....	49
3.7.5 Resize Attack.....	50
3.7.6 Additive Noise.....	50
3.7.7 Filtering.....	51

3.8	Literature Survey of Watermarking Techniques.....	52
3.8.1	Robust.....	52
3.8.2	Fragile.....	59
3.9	Final Remarks.....	63
3.9.1	Robust remarks.....	63
3.9.2	Fragile remarks.....	64
3.10	References.....	66
CHAPTER 4	72
4.1	Introduction.....	72
4.2	Host Images and Watermarks	72
4.3	DWT Embedding for Grey Images.....	74
4.3.1	Proposed DWT Robust Image Watermark Algorithm.....	75
4.3.2	The Embedding Process.....	75
4.3.3	The Extraction Process.....	82
4.3.4	Results.....	84
4.4	DWT Embedding for Colour Images.....	89
4.4.1	Embedding and Extraction for Green Channel.....	90
4.4.2	Result of Green Channel Algorithm.....	93
4.4.3	Y Channel Embedding and Extraction.....	99
4.4.4	Result of Y Channel Algorithm.....	102
4.5	Comparison with previous work.....	108
4.6	Final Remarks.....	110
4.7	References.....	110
CHAPTER 5.....	112
5.1	Introduction.....	112
5.2	Two-level DWT Watermarking Scheme for Grey Images.....	112
5.2.1	Proposed 2-levels DWT Robust Grey Image Watermark Algorithm.....	113
5.2.2	The Embedding Process.....	114
5.2.3	The Extraction Process.....	116
5.2.4	Results.....	118

5.3	Two-level DWT Watermarking Scheme for Colour Images.....	123
5.3.1	The Embedding Process.....	123
5.3.2	The Extraction Process.....	125
5.3.3	Results.....	125
5.4	Comparison with previous work.....	133
5.5	Final Remarks.....	134
5.6	References.....	135
CHAPTER 6.....		136
6.1	Introduction.....	136
6.2	Fragile Watermarking Scheme for Grey Level images.....	136
6.2.1	The Embedding and Extraction Process for Grey Images....	137
6.2.2	Results.....	139
6.3	Fragile Watermarking Scheme for RGB Images.....	141
6.3.1	Embedding and Extraction Process for RGB Images.....	141
6.3.2	Results.....	145
6.4	Combined Watermarking.....	148
6.4.1	Combined the one-level DWT robust algorithm with the fragile algorithm.....	148
6.4.2	The embedding process and the extraction process.....	149
6.4.3	Results.....	153
6.4.4	Combined the two-level DWT robust algorithm with the Fragile algorithm.....	157
6.4.5	The embedding process and the extraction process.....	159
6.4.6	Results.....	163
6.5	Comparison with Previous Work.....	167
6.6	Final Remarks.....	170
6.7	References.....	170
CHAPTER 7.....		172
7.1	Overview.....	172
7.2	Work Summary.....	172
7.3	Conclusions.....	174

7.4 Recommendation for Further Work.....	176
Appendix A (Author's Publication Record).....	177
Appendix B (List of Programmes).....	198

Acknowledgments

I would like to express my deepest appreciation my supervisors, *Prof. Raed A. Abd-Alhameed* and *Prof. Hussain Al Ahmed*. Their advice, assistance, help, guidance, encouragement and continuous support during my research journey were highly appreciated. Without their supervision and constant help this thesis would not have been possible.

I would like to express my appreciation to all those who provided me the possibility to complete my research. A special gratitude I give to Dr. Ahmed Al Gindy whose contribution, feedback and suggestions helped me a great deal. Special thanks to my colleagues Miss Julie Porter and Dr. William Pedley who supported me in writing my thesis.

Most importantly, I would like to express my deepest appreciation to my beloved wife Dalia who has had many sleepless nights and was always a great support in the moments when there was no one to answer my queries. Also special thanks to my lovely children Maab, Noor and Rawan for their patience with me during my studies. At the end, a special thanks to my family. Words cannot express how grateful I am to my mother; your prayers for me were what sustained me thus far. I would also like to thank all brothers and sisters who supported and encouraged me during my journey.

List of Abbreviations

2D IDWT	2D Inverse Discrete Wavelet
2DDWT	2D Discrete Wavelet
B	Blue
BBCW	Block Based Checksum Watermarking
BCD	Binary Coded Decimal
Cb	Blue minus luma ($B - Y$)
Cr	Red minus luma ($R - Y$)
DCT	Discrete Cosine Transform
DE	Different Expansion Algorithm
DFT	Discrete Fourier Transform
DSWC	Discrete Selective Wavelet Coefficient
DWPT	Discrete Wavelet Packet Transform
DWT	Discrete Wavelet Transform
G	Green
GA	Genetic Algorithm
HH	High High
HL	High Low
HVS	Human Visual System
IDWT	Inverse Discrete Wavelet Transform
ITU	International Telecommunication Union
JPEG	Joint Photographic Experts Group
LH	Low High
LL	Low Low
LSB	Least Significant Bit Coding
MD5	Message-Digest algorithm 5
MSB	Most Significant Bit
MSE	Mean Squared Error MSE
NCC	Normalized Correlation Coefficient
NIST	National Institute of Standard and Technology

PN	pseudo random
PSNR	Peak Signal to Noise Ratio
R	Red
SHA-1	Secure Hash Algorithm
SSIM	Structural Similarity Index Measure
VQ	Vector Quantisation VQ
VW2D	Variable-Watermark Two-Dimensional algorithm
VW2D	Variable-Watermark Two-Dimensional algorithm
Y	Luma

List of Variables

b	blue channel
C	Contrast
Δ	watermark embedding strength
e	extracted watermark
g	green channel
i	original image
ib	b blue component of the original image
ig	green component of the original image
ir	red component of the original image
L	luminance
N_{HB}	sub-blocks of the host image
r	red channel
S	Structure
w	watermarked image
wb	blue component of the watermarked image
wg	green component of the watermarked image
wr	red component of the watermarked image
x	x-coordinates of image pixel
y	y-coordinates of image pixel
δ	dct coefficients

List of Tables

Table 2.1: DCT coefficients matrix after quantization.....	28
Table 2.2: DCT coefficients matrix after quantization	29
Table 2.3: DCT coefficients matrix after quantization.....	30
Table 2.4: DCT coefficients matrix after quantization.....	30
Table 2.5: DCT coefficients matrix after quantization.....	30
Table 3.1: ITU-R quality and impairment scales.....	44
Table 4.1: PSNR with different grey images.....	85
Table 4.2: SSIM with different grey images.....	85
Table 4.3: NCC for Lena image with different attacks, at $\Delta=16$	87
Table 4.4: PSNR with different colour images (green channel embedding).....	94
Table 4.5: SSIM with different colour images (green channel embedding).....	95
Table 4.6: NCC for Colour Lena image with different attacks (green channel), at $\Delta=24$	95
Table 4.7: High resolution colour images examined by the proposed algorithm for green channel.....	98
Table 4.8: PSNR with different colour images (Y channel embedding).....	103
Table 4.9: SSIM with different colour images (Y channel embedding)	103
Table 4.10: NCC for Colour Lena image with different attacks (Y-channel), at $\Delta=24$	104
Table 4.11: High resolution colour images examined by the proposed algorithm for Y- channel.....	107

Table 4.12: The Normalized Correlation Coefficient for Lena colour image at $\Delta=24$	109
Table 4.13: The PSNR for Lena colour image with different Δ	109
Table 4.14: The SSIM for Lena colour image with different Δ	109
Table 5.1: PSNR with different grey images.....	119
Table 5.2: SSIM with different grey images.....	119
Table 5.3: NCC for Lena image with different attacks, at $\Delta=16$	121
Table 5.4: PSNR with different colour images (green channel embedding).....	128
Table 5.5: SSIM with different colour images (green channel embedding).....	129
Table 5.6: NCC for Lena image with different attacks at $\Delta=16$	129
Table 5.7: High resolution colour images examined by the proposed algorithm for green channel.....	132
Table 5.8: The PSNR for Lena colour image with different Δ	133
Table 5.9: The SSIM for Lena colour image with different Δ	134
Table 6.1: MD5 Hash code Calculation.....	141
Table 6.2: MD5 Hash code Calculation for Editing Colour Images.....	146
Table 6.3: MD5 Hash code calculations for editing different channels.....	147
Table 6.4: PSNR with different colour images for the combined algorithm.....	154
Table 6.5: SSIM with different colour images for the combined algorithm.....	154
Table 6.6: NCC for Colour Lena image with different attacks at $\Delta=24$	155
Table 6.7: MD5 Hash code Calculation for Editing Colour Images.....	157
Table 6.8: PSNR with different colour images for the combined algorithm.....	164
Table 6.9: SSIM with different colour images for the combined algorithm.....	164
Table 6.10: NCC for Colour Lena image with different attacks at $\Delta=24$	165

Table 6.11:MD5 Hash code Calculation for Editing Colour Images.....	167
Table 6.12: The PSNR for Lena colour image with different Δ	168
Table 6.13: The SSIM for Lena colour image with different Δ	169
Table 6.14: The NCC for Lena colour image with different types of attacks.....	169

List of Figures

Figure 2.1: Examples of grey images.....	10
Figure 2.2: Colour image and RGB components.....	10
Figure 2.3: Lena sampled 16 by 16 sampling rate.....	11
Figure 2.4: Grey images with different grey levels.....	11
Figure 2.5: A 256×256 , 8-bit image with different subsample sizes images.....	13
Figure 2.6: Lena with different subsampling but same size.....	13
Figure 2.7: RGB Lena standard image.....	14
Figure 2.8: The YCbCr image with Y, Cb and Cr channels.....	15
Figure 2.9: Lena in spatial and frequency domain by using DFT.....	17
Figure 2.10: Lena in spatial and frequency domain by using DCT.....	19
Figure 2.11: The concept of DWT.....	20
Figure 2.12: Block diagram of 2DWT.....	21
Figure 2.13: DWT transformed image after one-level of decomposition.....	22
Figure 2.14: A block diagram of the 2D IDWT.....	22
Figure 2.15: 3×3 mask.....	23
Figure 2.16: Averaging mask filter.....	24
Figure 2.17: Averaging smooth filter examples.....	24
Figure 2.18: Gaussian mask filter.....	25
Figure 2.19: Gaussian filter examples.....	25
Figure 2.20: Median filter.....	26
Figure 2.21: A block diagram of JPEG lossy algorithm.....	27
Figure 2.22: The zigzag pattern	31
Figure 2.23: Different compression ratios for Lena's still grey image.....	32
Figure 2.24: MD5 flow chart.....	33
Figure 3.1: Digital image watermarking scheme.....	37
Figure 3.2: Original Lena and watermarked Lena with different PSNR values.....	45
Figure 3.3: JPEG compression attacks.....	47
Figure 3.4: Contrast adjustment attack.....	48

Figure 3.5: Removal attack.....	48
Figure 3.6: Cropping attack.....	49
Figure 3.7: Examples of resizing attacks.....	50
Figure 3.8: Additive noise attacks.....	51
Figure 3.9: Filtering attack.....	51
Figure 4.1: Host colour images.....	73
Figure 4.2: Host grey-scale images.....	74
Figure 4.3: DWCS process.....	77
Figure 4.4: Flow chart of the embedding process.....	81
Figure 4.5: Flow chart of the extraction process.....	83
Figure 4.6: Original Lena and watermarked Lena images with different strengths..	86
Figure 4.7: several attacks for watermarked image.....	88
Figure 4.8: Original and watermarked images with high resolution.....	89
Figure 4.9: A flow chart of the embedding in the green channel.....	91
Figure 4.10: A flow chart of the extraction process.....	92
Figure 4.11: Original Lena with different watermark strength (green channel).....	96
Figure 4.12: Several attacks for colour watermarked image (green channel).....	97
Figure 4.13: A flow chart of the embedding Y channel process.....	100
Figure 4.14: A flow chart of the extraction process.....	101
Figure 4.15: Original Lena with different watermark strength (Y- channel).....	115
Figure 4.16: Several attacks for colour watermarked image (Y- channel).....	116
Figure 5.1: Embedding process.....	115
Figure 5.2: The extraction process.....	117
Figure 5.3: Original Lena and watermarked Lena images with different strength...	120
Figure 5.4: Several attacks for watermarked image.....	122
Figure 5.5: Original and watermarked images with high resolution.....	123
Figure 5.6: The Embedding process.....	124
Figure 5.7: The extraction process.....	127
Figure 5.8: Original Lena with different watermark strength (green channel).....	130
Figure 5.9: several attacks for colour watermarked image (green channel).....	131
Figure 6.1: The embedding process.....	138
Figure 6.2: The extraction process.....	139
Figure 6.3: Different examples of image editing.....	140

Figure 6.4: The embedding process.....	143
Figure 6.5: The extraction process.....	144
Figure 6.6: Different examples of colour image editing.....	146
Figure 6.7: Different examples of image editing in different channels.....	147
Figure 6.8: The embedding process combined algorithm of one-level DWT robust and fragile algorithms.....	151
Figure 6.9: The extraction process combined algorithm of one-level DWT robust and fragile algorithms.....	152
Figure 6.10: Different examples of colour image editing.....	156
Figure 6.11: Embedding Process Combined Algorithm of two-level DWT robust and fragile algorithms.....	160
Figure 6.12: Embedding Process Combined Algorithm of two-level DWT robust and fragile algorithms.....	162
Figure 6.13: Different examples of colour image editing.....	166

CHAPTER 1

INTRODUCTION

1.1 Motivation

In the last decades, the rapid developments in the internet and telecommunications areas are beyond expectations. The dramatic increment of the bandwidth and the speed of the transmitting data via the internet make accessing and sharing information an easy task for anybody. However, the ownership and the copyright of the multimedia data are becoming a big concern.

Nowadays, more than 38% of the populations of the world are using the internet [1] and the on-line commerce and services become an urgent need due to huge number of potential customers. The on-line market advantages are plentiful. On the other hand the security of the payment is one of the challenges that the companies and user are to deal with. In the normal commerce they used to have hard copy documents and the copyright issue is solved. While, the type of the documents which have been used in the on-line commerce are digital ones. Therefore, when digital documents are transmitted via the internet they can be copied several times by anybody who received these documents in a just of few clicks. Efficient ways of overcoming poor behaviour, from malicious users, are through methods of copyright and ownership

The right tool to enable content protection is the digital watermarking. The watermarking process is the process which embeds digital information into the digital document format such as digital image without considerably degrading its visual quality. The watermarked image can be sent via the internet. At the receiver side, the extracted watermark from the watermarked image can be used for copyright protection purposes and authentication of the content.

The digital watermarking technology is adapted commercially by several companies such as Digimarc Company [2].

1.2 Overview of Digital Watermarking

A digital watermark is any digital signal which can be embedded imperceptibly into data such as audio, video and images for different reasons including copyright protection, owner authentication and captioning [3]. There are some certain features that a watermark should have. The following features are follows:

- Difficult to notice. The embedded watermark information should not be noticeable to the viewer and adding the watermark information into the host image should not degrade the quality of the content of the host image. It is difficult to differentiate between the watermarked image data and the host image data [3].
- Robustness. The watermark should be robust to survive against common image processing, geometric distortion such as cropping, scaling and other types of image attacks. Any attempt to remove or amend the watermark will lead to appropriate degradation of the perceptual quality of the original data [4].

- **Security.** It is the capability of the watermarking algorithm to survive against aggressive attacks. The techniques which are used in the watermarking security could be understood in the same way as the encryption's security technique [5]. The watermarking techniques could be defined as a secured system if an unauthorized party know the exact algorithms (embedding and extraction) but still cannot remove or detect the watermarking information. A secret key or secret keys can be used to achieve that [5].
- **Payload.** The size of the encoded information that can be encoded in a watermark called payload. The size of the watermark depends on the application. For instant, one bit is needed for copy control application, while it required more bits if the application is relative to the protection of intellectual property rights [6].
- **Trustworthiness.** The watermark technique should assure that the fake watermark is impossible to generate and supply trustworthy evidence to safeguard the rightful ownership [7].

1.3 Aims

Recently, digital watermarking has become a substantial area of research. There are several areas has been covered by many researches such as: watermarking techniques, applications, analysis and attacks. However, digital watermarking challenges are still not enclosed for example: robustness, requirements, design considerations for the embedding-extraction system which will not affect the quality of the image, tradeoffs, security, dealing with different file formats, dealing with different sizes of images.

The aims of this research are to design and develop image watermarking techniques. The first watermarking techniques are used for copyright protection of still colour images. The second watermarking techniques are deal with the tamper detection and authentication. The last watermarking techniques are the combination of the robust and fragile watermarking techniques in order to create multi-purpose watermarking techniques which can be used for copyright protection, tamper detection and content authentication.

1.4 Achievements and Contributions

The major achievements of this research are:

- The development of robust watermarking algorithms.
- The development of fragile watermarking algorithms.
- The development of combined robust and fragile algorithms.

The developed robust watermarking algorithm in this research utilised the Discrete Wavelet Transform. The image is divided into blocks in the spatial domain. The DWT has been used to convert the host image into frequency domain. The watermarking information is the mobile number with international code. The watermarking information is scrambled by using a secret key. The embedding process area is the Low-Low sub-bands in each converted block. The Discrete Selective Wavelet Coefficient algorithm (DSWC) has been used in order to get the highest magnitude coefficient in the Low-Low sub-band which will use for embedding process. The embedding process is repeated several times due to the small size of the watermark information compared to the size of the host image. The shuffling process is applied on the watermarking

copies. The extraction process does not need the original image in the receiver side. The averaging for the sum of extraction watermarking copies is been used.

The developed fragile watermarking has used the special domain. The hash function (MD5) is used as a watermarking information. The hash function is calculated for the host image itself. The embedding process used the frame of the host image for embedding the hash function. The selective pixels for the embedding are located on the frame of the host image.

The developed combined algorithms are combining the robust algorithms and fragile algorithms. The copyright protection and the content authentication are integrated by using the combined algorithms. The combined algorithms does not affect on the quality of the watermarked image.

The following points can summarize the proposed techniques:

1. Observably distinguishable extraction – The results can be evaluated subjectively and objectively by the viewer. The watermarking information is either mobile number or Hash function rather than the traditional pseudo random numbers.
2. Hiddenness or transparency – the robust and fragile watermarks are invisible in the images underneath typical viewing conditions.
3. Robustness against attacks – the robust watermark has survived against different attacks and geometric distortions. The watermarked image will be affected severely if any attacker tries to remove the watermark.

4. Sensitivity for any image tampering – the fragile watermark is destroyed for any image manipulating.
5. Security – the scrambling for the robust watermarking by using secret key and the selective DWT coefficients will increase the security of the robust algorithms.
6. Blind – the robust and fragile watermarks can be extracted without need to the original image.
7. Error decline - the process of error reduction is implemented after the reconstruction of the robust watermark.
8. Easy to use (do-able) – the watermarking algorithms can be used for different type of file images and different sizes.
9. Integrity – the combined watermarking algorithms can be used for copyright protection and content authentications.

1.5 Overview of the thesis

The remaining chapters of this thesis are structured as follows. Chapter two provides the basic information of the digital signal processing. It also describes the common transforms which are used in watermarking techniques. Two dimensional filter, image compression and hash function are also described in chapter two. Chapter three describes and investigates the digital watermarking. The basic concepts, application, requirements and different types of digital watermarking are explained also. The state of the art assessment tools which are used to evaluate and assess the watermarking techniques (PSNR and SSIM) are also explained in chapter three. Following that, a survey and literature review for the previous research about the robust and fragile

watermarking techniques. Chapter four deals with and explores the robust watermarking techniques for grey-scale and still colour images by using one-level Discrete Wavelet Transform (DWT). The green channel colour robust watermarking techniques and Y channel colour robust watermarking techniques are discussed also in chapter four. In chapter five, two-level DWT robust watermarking techniques for grey-scale and still colour images are investigated. This chapter also deals the green channel and Y channel embedding types for robust watermarking techniques. Chapter six discusses the combined robust watermarking and fragile watermarking techniques. It also investigates the combined algorithm of the fragile and robust watermarking techniques. Chapter seven represents the conclusion and a plan for future work. The list of the publications which produced from this works is listed in Appendix A and Appendix B is the list of the programmes.

1.6 References

- [1] " *Global Digital Statistics 2014* " report, 2014 edition.
- [2] "Digimarc Corporation " in <https://www.digimarc.com/solutions/images/>.
- [3] J. Cox, "Digital watermarking and steganography", *Morgan Kaufmann, Burlington, MA, USA*, 2008
- [4] M. Kutter and F. A. P. Petitcolas, "A Fair benchmark for image watermarking systems", *Electronic Imaging '99. Security and Watermarking of Multimedia Contents, Theinternational Society for optical Engineering*, , Sans Jose, USA, 1999.
- [5] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, " Watermarking Digital Image and VideoData," *IEEE Signal processing magazine*, Vol. 17, Issue 5, pp. 20-46, August2000.

- [6] M. Kutter and F. A. P. Petitcolas, "A Fair benchmark for image watermarking systems ", *Electronic Imaging '99. Security and Watermarking of Multimedia Content, The International Society for Optical Engineering*, Sans Jose, USA, 1999.
- [7] R. Liu and T. Tan, "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership," in *IEEE Transactions on Multimedia*, 2002, pp. 121 -128.

CHAPTER 2

Digital Image Processing

2.1 Overview

Digital image processing is an important research topic. This chapter introduces the basic concepts in digital image processing such as: image processing system components, image sampling and quantization. Also, it covers spatial domain for grey level and colour images, transform domain, two dimensional filtering, image compression and hash function.

2.2 Definition of Digital Image Processing

Digital image processing is a technology of implementing a group of computer algorithms to process digital images. The result of this process could be images or image properties or some representative characteristics. The image processing applications can be found in many areas such as robotics/intelligence systems, medical imaging, remote sensing, photography, data security and image copyrighting (watermarking) [1].

A function with two dimensions $f(x,y)$ could be used to represent the image, where x, y are the coordinates and f represents the amplitude of the function at any couple of x, y . The amplitude f is called the image intensity at that location. An image can be called a digital image because of the amplitude values of f are all finite. A digital image comprises a collection with a set number of elements, where every element has a certain

location and value. These elements are represented as a picture element, or as an image element called pixels. Pixel is the term most widely used to represent the elements of a digital image. The pixels have spatial coordinates that indicate the position of the points in the image, and intensity (grey level) values [1].

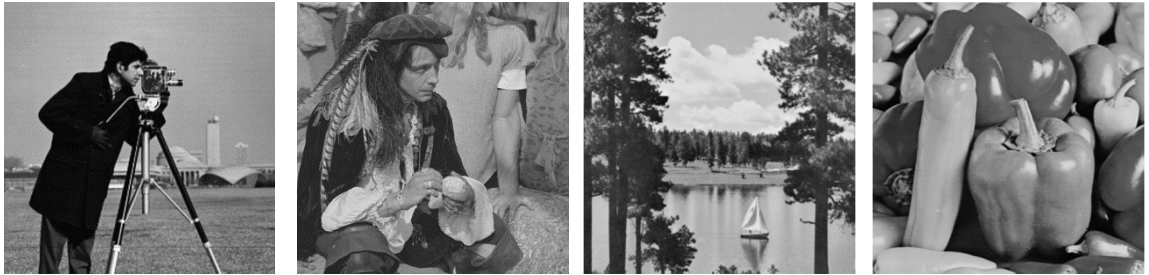


Figure 2.1: Examples of grey images.

A colour image contains greater dimensional information than a grey image. Red (R), Green (G) and Blue (B) are the components of the colour image. There are different combinations which produce the colour image in the real world. The RGB is one of the colour combinations which are based on human perception and Y, Cb and Cr planes is another combination which can also produce colour images. The Y component corresponds to the luminance information while the colour information of the colour images are represented by Cb and Cr components. Figure 2.2 presents the RGB components and the colour image which is created from the aforementioned components [2].



Figure 2.2: Colour image and RGB components

2.3 Sampling and Quantization

The computer processor cannot deal with continuous data unless this data is converted to digital form. Therefore, the image function $f(x,y)$ should be digitized - both coordinates and amplitudes. In general the camera plays the role of digitizing an image. The digitizer in the camera is used to quantize and sample the analogue signal and store it in the frame buffer. The quality of the digital image depends on the sampling rate (pixel) and the quantization level. Figure 2.3 illustrates an image divided into 256 levels in both coordinates [1].

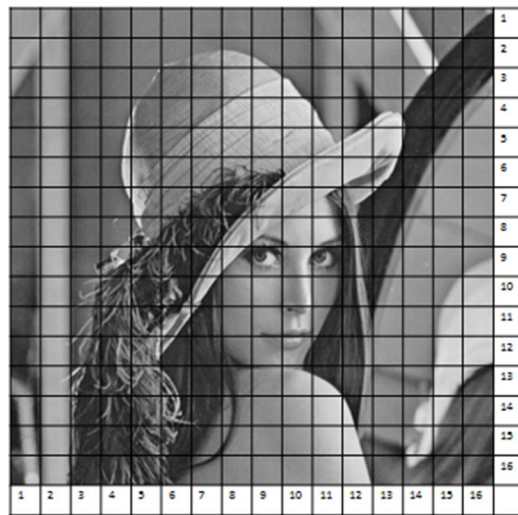


Figure 2.3: Lena sampled 16 by 16 sampling rate.

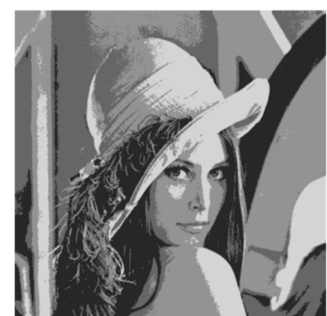
Figure 2.4 shows different grey quantization levels. Photographic quality can be achieved by using 256 levels.



a. 128 grey levels



b. 8 grey levels



c. 4 grey levels

Figure 2.4: Grey images with different grey levels.

2.4 Spatial Domain

The spatial domain means the plane of the image itself. In that domain the cumulative pixels are creating the image. It operates directly through these pixels. The spatial domain can be categorized into two types; Grey level images category and Colour images category.

2.4.1 Grey Level Images

Any small noticeable change in the grey level is referred to as the grey-level resolution. Determining visible changes in the grey level is a very subjective manner. There is no colour information. However, it contains grey-level information. The different grey levels depend on the number of bits which are used for each pixel. The grey level number is commonly an integer to the power of 2. The most public number is 8 bits (256 grey levels). However, this resolution is not always enough. For instance, 16 bits are used for medical applications or satellite applications. Figure 2.5 shows an 8 bits image (256 grey levels) which has 256×256 pixels size. The other images are subsample of the 256×256 image. The sub-sampling was achieved by removing the appropriate number of columns and rows from the original. For instance, the 128×128 image was generated by erasing every other row and column in the 256×256 image and so on. However, the number of grey levels was kept at 256. The effects from size reduction are difficult to diagnose because of the size differences. In order to compare these effects, the simplest way is to enlarge the entire subsampled images to the same size 256×256 pixels as shown in figure 2.6 [1].



Figure 2.5: A 256×256 , 8-bit image with different subsample sizes images

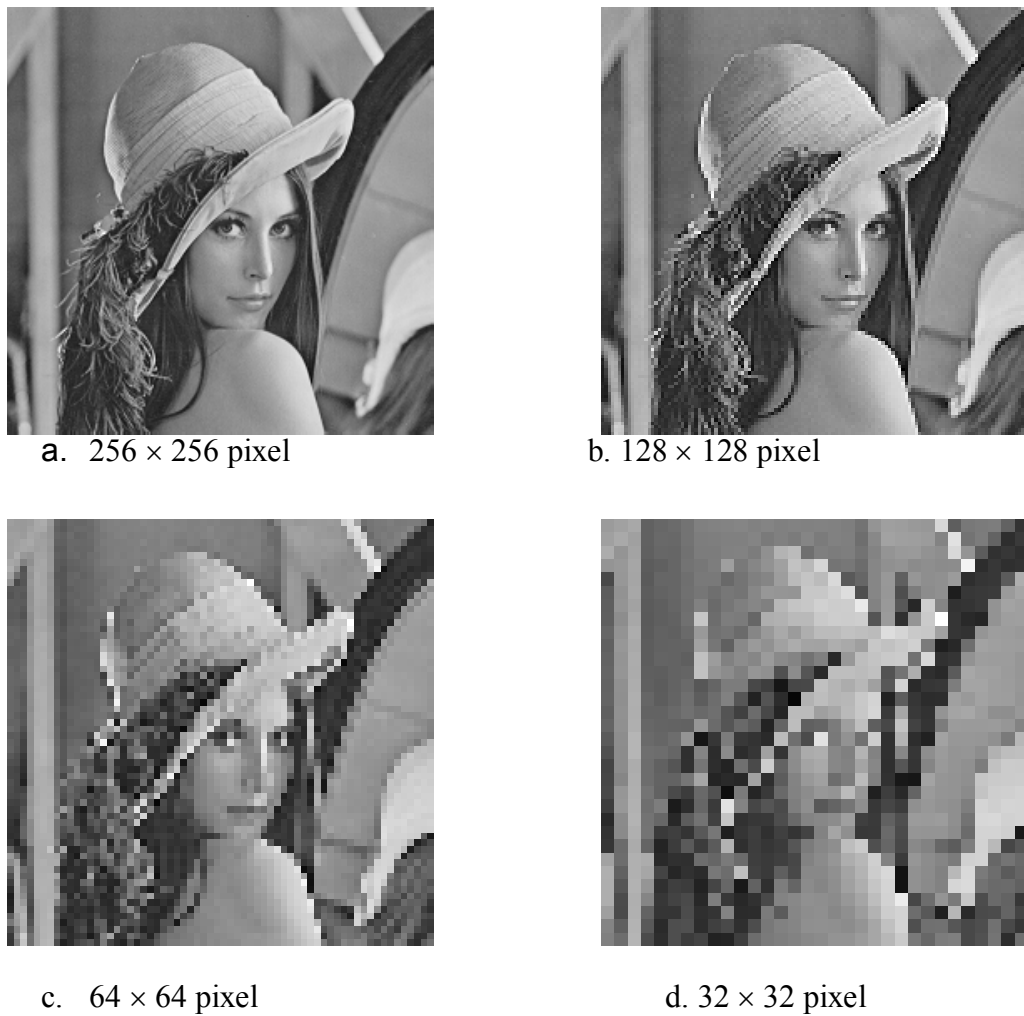


Figure 2.6: Lena with different subsampling but same size.

2.4.2 Colour Images

As humans, the colour image can be defined by its attributes of brightness, hue and colourfulness. However, the computer can describe a colour image by using the amount of red, green and blue light emissions which are required to match a colour [3].

2.4.2.1 RGB (Red Green Blue)

The RGB is an additive system based on tri-chromatic theory [3]. It is a very common colour implementing system used in computer systems, TVs, videos etc. Figure 2.7 illustrates an RGB colour image with 512×512 pixels.



Figure 2.7: RGB Lena standard image.

2.4.2.2 YCbCr

Y Cb Cr is another way of representing colour images. The brightness of the image (luma) is presented by Y, while Cb is blue minus luma ($B - Y$) and finally Cr is red minus luma ($R - Y$). Figure 2.8 shows the Y channel, Cb channel, Cr channel and the

YCbCr image. The Y-channel can be used as an image in greyscale, while the Cb and Cr channels have much less contrast.



Figure 2.8: The YCbCr image with Y, Cb and Cr channels.

2.5 Transforming the Domain

It may be a very complicated computational process to perform some processes on an image in the spatial domain. However, these processes can be made much easier to perform after transforming an image to a different domain. One of the common domains is the frequency domain. The frequency domain can be used for image filtering to apply or remove noise, to sharpen or extract features.

2.5.1 Discrete Fourier Transformation

The Fourier Transformation is an important image processing tool which can be used to decompose an image in the spatial domain into sine and cosine components in the frequency domain [2]. However, the suitable transformation tool for the digital images is the discrete Fourier transform (DFT). If the Fourier transform has been sampled then it will become a DFT, then it will not cover all frequencies which represent an image. However, the groups of samples are big enough to fully designate the spatial domain image. The image in the spatial and frequency domain has the same size, because the number of frequencies relate to the number of the pixels in the spatial domain.

For a digital image which has $M \times N$ size, the DFT can be calculated by the following equation [3]:

$$F(u, v) = \frac{1}{MN} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} f(x, y) e^{-j2\pi(\frac{ux}{M} + \frac{vy}{N})} \dots \dots \dots (2.1)$$

where:

$$u = 0, 1, 2, \dots, M - 1$$

$$v = 0, 1, 2, \dots, N - 1$$

Similarly, given $F(u, v)$, the $f(x, y)$ can be obtained by the inverse Fourier Transform, as shown below:

$$f(x, y) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} F(u, v) e^{j2\pi(\frac{ux}{M} + \frac{vy}{N})} \dots \dots \dots (2.2)$$

where:

$$x = 0, 1, 2, \dots, M - 1$$

$$y = 0, 1, 2, \dots, N - 1$$

The image in the frequency domain is a complex valued image which is contained in magnitude and phase. However, the magnitude in the frequency domain will cover most

of the geometric structure information. Figure 2.9 shows Lena in the spatial and frequency domain and the log transform of the frequency domain.

It is clearly shown in figure 2.9 that the DC value ($F(0,0)$) in the spatial domain is represented by the brightest spot of the image and the rest of frequency coefficients appeared dark because their values are too large to be displayed. However, in order to enhance the darker values in comparison to the brighter values, a log scale can be used to bring out the detail as shown in Figure 2.9 c.

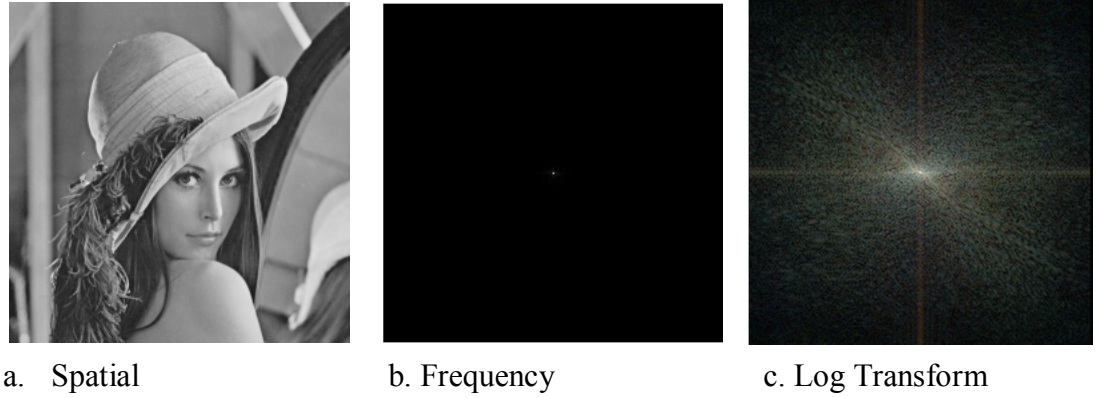


Figure 2.9: Lena in spatial and frequency domain by using DFT.

2.5.2 Discrete Cosine Transform (DCT)

One of the drawbacks of the DFT is that the data in the frequency domain has complex values even for the real input data. The discrete cosine transform resolves this problem. The DCT is not the real part of DFT however, it is a separate transform. The image in the frequency domain can be represented as a addition of cosines of variable amounts of magnitudes and frequencies. The 2-D DCT equation for image ($N \times N$) is given by [4]:

$$C(u, v) = \delta(u)\delta(v) \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} f(x, y) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right] \dots \dots (2.3)$$

where:

$$u, v = 0, 1, 2, \dots \dots \dots, N-1$$

$$\delta(u) = \begin{cases} \sqrt{\frac{1}{N}} & \text{For } u = 0 \\ \sqrt{\frac{2}{N}} & \text{For } u \neq 0 \end{cases} \dots \dots (2.4)$$

$$\delta(v) = \begin{cases} \sqrt{\frac{1}{N}} & \text{For } v = 0 \\ \sqrt{\frac{2}{N}} & \text{For } v \neq 0 \end{cases} \dots \dots (2.5)$$

If u and $v = 0$, then the coefficient will be a DC coefficient. The rest of the coefficients are AC coefficients. The inverse transform of DCT is defined as:

$$f(x, y) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \alpha(u)\alpha(v)C(x, y) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right] \dots \dots (2.6)$$

where:

$$x, y = 0, 1, 2, \dots \dots \dots, N-1$$

Figure 2.10 shows Lena in the spatial domain and in the frequency domain.



a. Spatial domain

b. Frequency domain

Figure 2.10: Lena in spatial and frequency domain by using DCT.

2.5.3 Discrete Wavelet Transform (DWT)

The discrete wavelet transform (DWT) can be used instead of the discrete cosine transform (DCT) in many image processing applications such as image compression because of the following advantages [5]:

- a. The wavelet decomposes an input signal with multi-resolution representation because it has a great facility of sub-band coding.
- b. The DWT offers a good compromise between frequency and spatial resolution of the signal.

The DWT transform uses small waves of limited extent and of varying frequency. However, the DCT and DFT are using sinusoidal waves as basis functions. These small waves (wavelet) can be scaled and shifted which makes the analysis process for contents of the spatial frequency of an image at different resolution and positions an achievable task. Therefore, the wavelet can be considered as an effective tool in multi-resolution analysis of images. Moreover, wavelets can obtain detailed analyses at any specified location in space which is known as space-frequency localization. It is like

using a magnifier over an image to discover the details about a specific location. This magnifier can be moved up, down, left and right to explore more locations [6].

The discrete wavelet transform's concept is shown in figure 2.11.

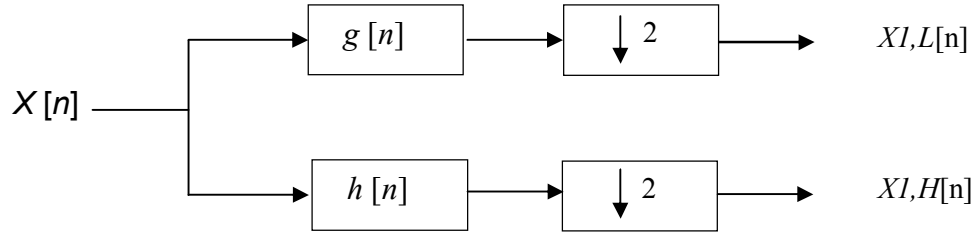


Figure 2.11: The concept of DWT.

where:

$X[n]$: input,

$h[n]$: high pass filter,

$g[n]$: low pass filter,

↓2: down – sampling by the factor of 2,

$X1, L[n]$: the low pass filter output,

$X1, H[n]$: the high pass filters output.

The 2D DWT is a combination of 1D wavelet transform. Figure 2.12 illustrates a block diagram of 2D wavelet transform [6].

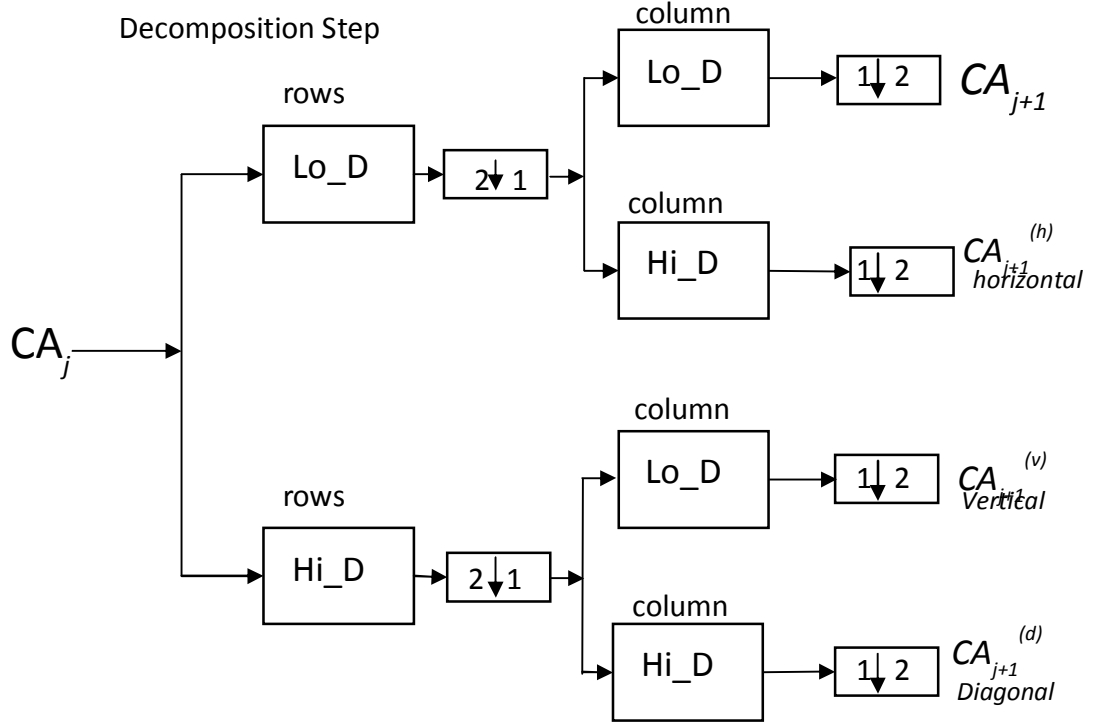


Figure 2.12: Block diagram of 2DWT

where:

Initialization $CA_0 = s$ for the decomposition initialization,

Lo_D : low pass filter,

Hi_D : High pass filter,

$\downarrow 2$: down – sampling by the factor of 2.

If the 2-D block diagram, shown in figure 2.13 is applied on the digital image (Lena for example), the result is a Discrete Wavelet Transformed (DWT) image with first level of decomposition, as shown in Figure 2.14. The first part is the approximation of the image, the second part is the vertical details, the third one shows the horizontal details and the last one shows the diagonal details.



Figure 2.13: DWT transformed image after one-level of decomposition.

The reconstructed image can be obtained by using 2D Inverse Discrete Wavelet Transform (2D IDWT). Figure 2.17 illustrates the block diagram of the 2D IDWT.

Reconstruction Step

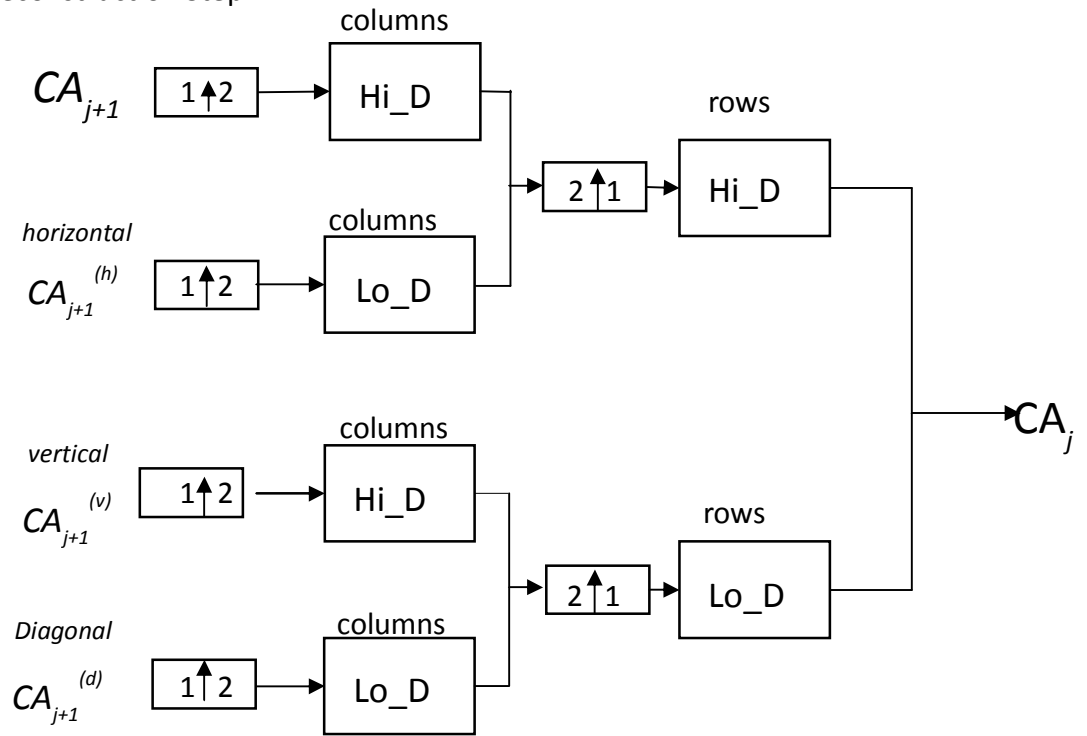


Figure 2.14: A block diagram of the 2D IDWT.

2.6 Two Dimensional Filtering

The filtering process in the spatial domain is a direct convolution between the input image and a mask (window) of size $w \times w$, where w is an odd integer (for example 3, 5 and 7). Figure 2.15 explains the 3×3 mask; the modified pixel is located in the centre of the window ($w5$) [2].

$w1$	$w2$	$w3$
$w4$	$w5$	$w6$
$w7$	$w8$	$w9$

Figure 2.15: 3×3 mask

The convolution process is multiplying point-by-point the mask with the image in an area of 3×3 if the mask is 3×3 . Then summed up and the result value will be used to replace the centre pixel of that window of the image. Then the filter mask will be moved by one pixel to the left and the same procedure will be repeated till the end of the row in the image. Next, the mask will be shifted down to the next row and the same scenario will be repeated for the second row. That means if we have a 3×3 mask filter, the process will continue until it arrives at the last pixel of the image. The shifting process is from left to right and from top to bottom is known as the 2-D convolution process.

2.6.1 Averaging Filters

The cells value of the averaging filter is constant value of 1's. The scaling factor is $1/9$ to make sure that the result of the convolution process will not run off the allowable dynamic range of the intensity level. For instance, for the 8 bit image, the scaling factor will guarantee that the convolution results will not exceed 255. Figure 2.16 shows the mask filter for the averaging filter [2].

1/9	1	1	1
	1	1	1
	1	1	1

Figure 2.16: Averaging mask filter

The main objective of the averaging filter is to reduce the uniform type of noise as well as Gaussian noise. However, increasing the filter size will cause the filtered image to be blurred and the significant information for instance edges will be less sharp. Figure 2.17 shows the salt pepper noise (intensity = 0.01) added to Lena image in (a), while (b) is a smoothed Lena by using a 5×5 smooth averaging filter.



a. Lena Image with salt and pepper noise (intensity = 0.01)



b. Lena with 5×5 mask filter

Figure 2.17: Averaging smooth filter examples.

2.6.2 Gaussian Low-pass Filter

The Gaussian filter is considered to be more powerful than an averaging filter; it is used to overcome many types of noise. The kernel of the Gaussian filter is designed mainly following experimental analysis and based on observation rather than being

mathematically analysed. However, the centre value should be higher and positive in value compared to its neighbour values. One of the possible choices would be as shown in figure 2. 18 [2].

1/16	1	2	1
	2	4	2
	1	2	1

Figure 2.18: Gaussian mask filter

Once again, the scaling factor is 1/16 to make sure that the allowable dynamic ranges of the given image are more than the resulting pixel value. The normal size of Gaussian filter is 3x3, 5x5, and 7x7. Figure 2.19 shows examples for a 3x3 Gaussian filter.



a. Noisy Lena

b. Lena with 3×3 mask filter

Figure 2.19: Gaussian filter examples.

2.6.3 Median Filter

The Median filter is considered as being underneath the group of a nonlinear statistical filter. The median filter mask is wxw window and the centre value is the

median value ($\frac{w^2+1}{2}$) of $w \times w$ pixels. In order to explain this, assume that the 3×3 window has the following value of pixels [2].

20	15	19
33	60	25
22	20	19

The ascending order for the pixel values will be:

[15, 19, 19, 20, 20, 22, 25, 33, 60].

The median will be the 5th value which is 20 for this example. Therefore the pixel value of 60 will be replaced by the value 20. The median filter works effectively with the speckle (also called salt and pepper). Figure 2.20 illustrates the median filter effect on Lena's image affected by salt and pepper noise.



a. Lena with salt and pepper noise



b. Lena after median filter

Figure 2.20: Median filter.

2.7 Image Compression

One of the international effective compression standards of still digital images is the Joint Photographic Experts Group (JPEG). JPEG consists of specifications for both lossless and lossy compression algorithms. The main objective of the lossy standard is aimed to minimize the high frequency elements of the image frame that will be difficult to detect by the human eye. The JPEG standard seems to be more efficient for colour images than for grey images because the human eye cannot sense slight changes in the colour space while it can simply detects minor change in intensity (light to dark or vice versa) [7].

2.7.1 JPEG Lossy Algorithm Steps

The block diagram shown in figure 2.21 explains the steps of JPEG lossy algorithms.

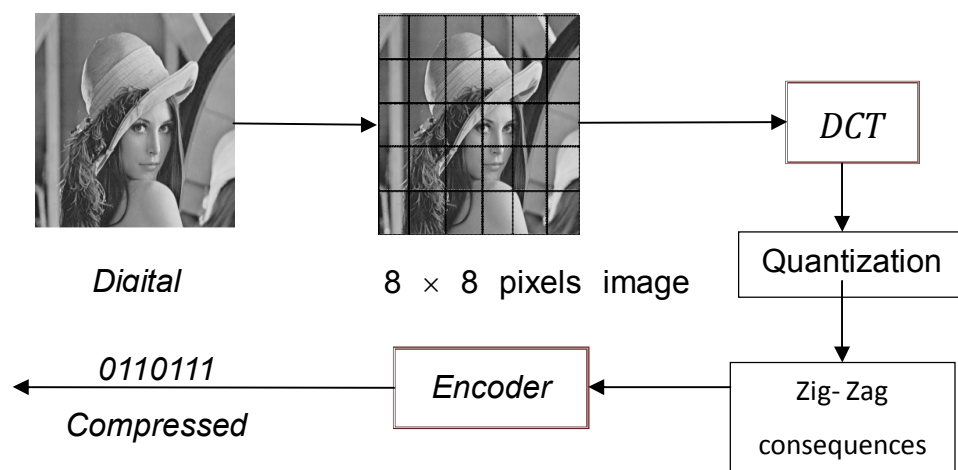


Figure 2.21: A block diagram of JPEG lossy algorithm

The first step in the JPEG lossy algorithm is to divide the digital image into blocks, each block is 8×8 pixel, then the discrete cosine transform (DCT) is implemented to each block. The frequency domain coefficients are divided by the quantization table and rounded to integers. This stage allows for large compression. However, it produces the lossy nature of JPEG. A variable length code on these coefficients has been used in JPEG's compression technique, and the compressed data stream is written to an output file (*.jpg).

The 8×8 pixel block images are transformed from spatial domain to the frequency domain by using DCT. The inputs of the DCT are 8×8 array integers. For example, an 8 bits grey image has levels from 0(Black) to 255(White). The output of the DCT transform is an 8×8 integers array of DCT coefficients; the coefficients range is from -1024 to 1023. The first coefficient in the output array ([1, 1] coefficient) has zero frequency which is the DC coefficient, while the remaining 63 coefficients are AC coefficients. The signal energy of most images lies at low frequencies. These coefficients are allocated in the upper left corner of the DCT array. However, the lower coefficients appear in the lower right corner of the DCT array, and are almost small enough to be neglected with little visible distortion. Tables 2.1 and 2.2 show an example of an 8×8 input block from a grey still image and the output block after DCT transform respectively.

Table 2.1: 8×8 block sample from grey image

140	144	147	140	140	155	179	175
144	152	140	147	140	148	167	179
152	155	136	167	163	162	152	172
168	145	156	160	152	155	136	160
162	148	156	148	140	136	147	162
147	167	140	155	155	140	136	162
136	156	123	167	162	144	140	147
148	155	136	155	152	147	147	136

Table 2.2: DCT coefficients

186	-18	15	-9	23	-9	-14	19
21	-34	26	-9	-11	11	14	7
-10	-24	-2	6	-18	3	-20	-1
-8	-5	14	-15	-8	-3	-3	8
-3	10	8	1	-11	18	18	15
4	-2	-18	8	8	-4	1	-7
9	1	-3	4	-1	-7	-1	-2
0	-8	-2	2	1	4	-6	0

Initially, each of the DCT coefficients is divided by a quantization coefficient value. Then, the resulting value is rounded to an integer. Increasing quantization coefficient values yield more compressed data. On the other hand the quality of the image reduces because the DCT are represented less accurately. In general, the quantized high frequency coefficients are more compact than the quantized low frequency coefficients and the contribution of the quantized high frequency coefficients have little representation of the graphical image and cannot be observed by the human eye.

The main source of loss of information in the JPEG compression is the quantization process. The excellent compression ratios can be achieved by using larger quantum coefficient values. However, the de-quantization will produce a poor image quality due to the higher probability of errors in the DCT output. On the other hand, low quantization values yield good image quality. This diversity gives the JPEG users extreme flexibility in choosing the image quality based on storage capacity and imaging requirements. For example, table 2.3 shows a quantization matrix and the input DCT coefficients matrix before the quantization is shown in table 2.4 while the output matrix quantization is illustrated in table 2.5.

Table 2.3: Example of quantization coefficients matrix

3	5	7	9	11	13	15	17
5	7	9	11	13	15	17	19
7	9	11	13	15	17	19	21
9	11	13	15	17	19	21	23
11	13	15	17	19	21	23	25
13	15	17	19	21	23	25	27
15	17	19	21	23	25	27	29
17	19	21	23	25	27	29	31

Table 2.4: DCT coefficients matrix before quantization

92	3	-9	-7	3	-1	0	2
-39	-58	12	17	-2	2	4	2
-84	62	1	-18	3	4	-5	5
-52	-36	-10	14	-10	4	-2	0
-86	-40	49	-7	17	-6	-2	5
-62	65	-12	-2	3	-8	-2	0
-17	14	-36	17	-11	3	3	-1
-54	32	-9	-9	22	0	1	3

Table 2.5: DCT coefficients matrix after quantization

90	0	-7	0	0	0	0	0
-35	-56	-9	11	0	0	0	0
-84	54	0	-13	0	0	0	0
-45	-33	0	0	0	0	0	0
-77	-39	45	0	0	0	0	0
-52	60	0	0	0	0	0	0
-15	0	-19	0	0	0	0	0
-51	19	0	0	0	0	0	0

After quantization, it is clearly shown in table 2.5 that more than half of the DCT coefficients are equal to zero. To take advantage of this the run-length coding is integrated with JPEG. For every non – zero DCT coefficient, the number of zeroes that preceded the number is recorded by JPEG, the number of bits are needed to represent the number's amplitude and the amplitude itself. To associate the runs of zeroes, the zigzag pattern is processed with the DCT quantized coefficients. The following figure 2.22 explains the zigzag pattern.

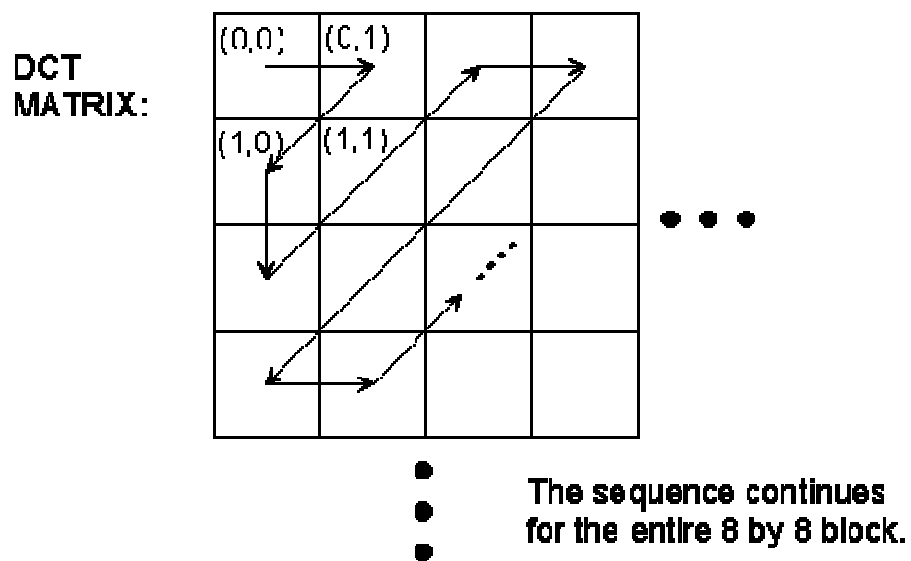


Figure 2.22: The zigzag pattern

Huffman, Shannon-Fano or Arithmetic coding are examples of codes which have been used in JPEG compression algorithms. The variable length code depends on the type of the coding which has been used in JPEG algorithms. To create a pair which has its own code word, the number of previous zeroes and the bits needed for the current number's amplitude form a pair. In the JPEG output there are the code words of the pair and the code words for the coefficient's amplitude. It is necessary that jpeg writes a unique end-of-clock sequence to the output stream after each block, then the same process will be repeated for the next block. Once the process has been completed for all blocks, JPEG writes the end-of-file marker. Figure 2.23 show different compression ratios for Lena's still grey image.



a. Lena original



b. JPEG-compressed Lena at a compression ratio of 20:1



c. JPEG-compressed Lena at a compression ratio of 12:1



d. JPEG-compressed Lena at a compression ratio of 32:1

Figure 2.23: Different compression ratios for Lena's still grey image.

2.8 Hash Code

The function that converts a data string (data base, digital file, digital images, etc.) into a numeric string output of a fixed length is called Hash algorithm. Usually, the output string is much smaller than the original data. The Hash code is a unique code per each input data. Therefore, any tampering in the content of the data input can be easily figured out. The following minimum properties for the hash algorithms which can be defined as a function h [7]:

1. h maps a finite input of length x to a fixed output, $h(x)$ of length n .
2. $h(x)$ is easy to compute.

The MD5 (Message-Digest algorithm 5) and the SHA-1 (Secure Hash Algorithm) are the two most common Hash algorithms.

2.8.1 MD5 (Message-Digest Algorithm 5)

The hash algorithm named MD and its revised version MD5 have been successively proposed by Ronald L. Rivest in 1991. MD5 hash function with a 128-bit hash value as output is widely used in cryptography. For the 32-bit machines, the MD5 algorithm is considered to be quite fast. Moreover, large substitution tables are not required; hence it can be coded pretty compactly. However, MD5 is slightly more complex and slower than MD, but the security level design has been improved. For example, the input data for the MD5 algorithm will produce as output a 128-bit message digest of the input. Figure 2.24 shows the standard protected hash function. [8]:

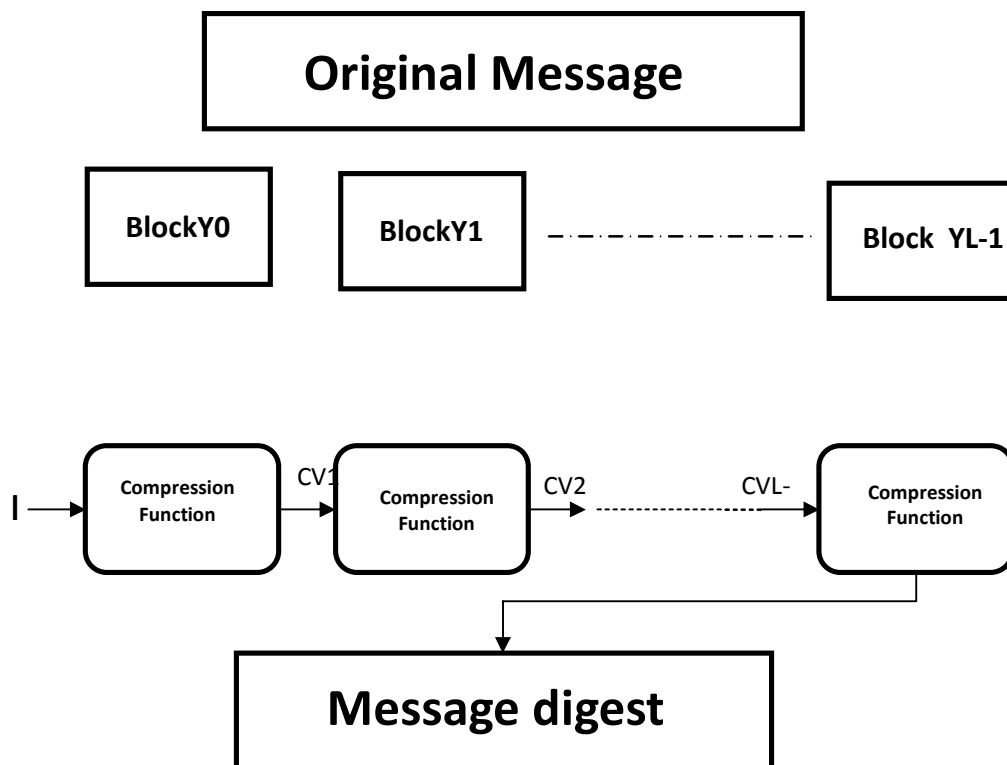


Figure 2.24 General Structure of Secure Hash Code

where:

Y_0, Y_1, \dots, Y_{L-1} are 512-bit blocks.

IV and CV represent initial value and chaining variable respectively.

2.8.2 SHA-1 (Secure Hash Algorithm)

The National Institute of Standard and Technology (NIST) have produced the secure hash algorithm (SHA). In 1993, the first member of SHA (SHA-0) was published. While, SHA-1 is the improved version of SHA-0 was published 1995. Moreover, NIST has issued four different designs with increased output ranges: SHA-224, SHA-256, SHA-384, and SHA-512 [8].

The SHA-1 algorithm has been set up on principle similar to MD message digest algorithm. It will produce a 160-bit digest when it operates on message blocks of 512 bits. The SHA-1 code has 2 bits longer than MD5 code which can be considerably stronger than MD5 against attacks. SHA-1 requires 160-bit buffer while 128-bit buffer is produced by MD5. Therefore, SHA-1 is slower than MD5.

2.9 References

- [1] R. S. Gonzalez and R. E Woods, *Digital Image Processing*, New Jersey, Prentice-Hall, INCC. 2002.
- [2] "Digital Image Processing: Part I" in <https://www.bookboon.com>.
- [3] "Colour Space Conversions" in <http://www.poynton.com/PDFs/coloureq.pdf>.
- [4] N. Ahmed, T. Natarajan, and K. R. Rao, "Discrete cosine transform," *IEEE Transactions on Computers*, vol. C-32, pp. 90-93, Jan. 1974.
- [5] P. J. Fleet, *Discrete Wavelet Transformation*, New Jersey, A John Wiley & Sons, INCC, 2007.
- [6] "Multi-Resolution Analysis", in <http://book.idea2.org/version-2-ee-iit-kharagpur-2-147.html>.

- [7] V. Dwivedi, "JPEG Image Compression And Decompression With Modeling Of DCT Coefficients On The Texas Instrument Video Processing Board TMS320DM6437," in *Department of Electronic Engineering*. vol. M.Sc. Gujarat University, India, 2006, p. 109.
- [8] C. Wen and K. Yang, "Image authentication for digital image evidence," *Forensic Science Journal*, vol. 5, pp. 1-11, 2006.

CHAPTER 3

Digital Image Watermarking

3.1 Introduction

This chapter presents digital image watermarking characteristics, and measurements. It also covers a literature survey of robust and fragile watermarking techniques, together with an analysis of the constraints and knowledge gaps in the latest research.

3.2 Basic Concepts

Digital image watermarking is defined as embedding digital data called a watermark (such as: digital signature, logo, text and digital image) into a digital image. The watermarked image can be stored in the receiver side or transmitted via a communication channel (internet, intranet, etc.), and could be modified or corrupted. On the receiver side, digital watermark information is to be detected or extracted from the possibly watermarked image to identify the owner. Figure 3.1 explains the concept of the digital image watermarking technique [1].

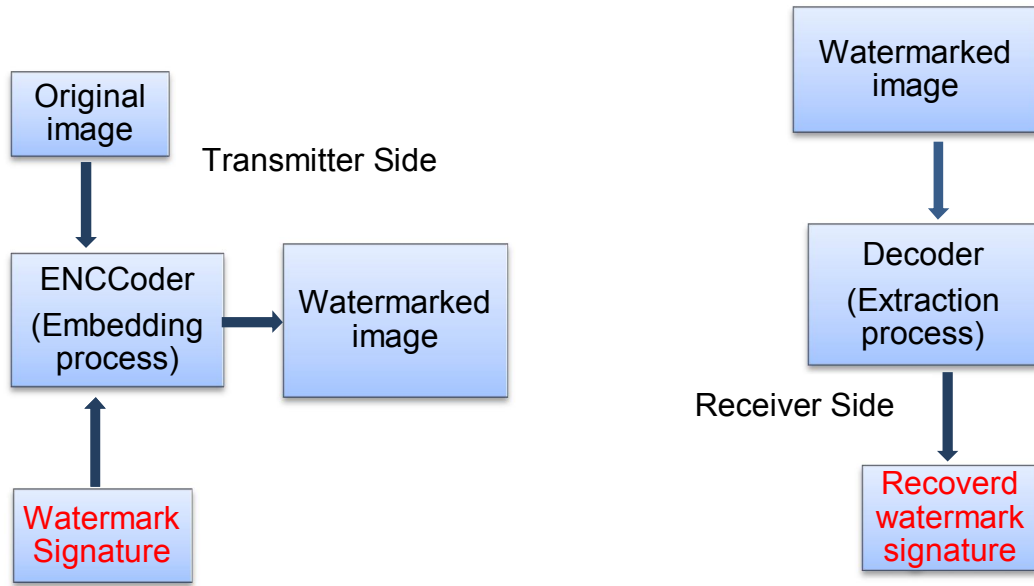


Figure 3.1: Digital image watermarking scheme.

3.3 Application

There are many application areas in which digital image watermarking is used, such as: copyright protection, copy protection, content authentication, tamper detection and localisation, transaction tracking (figure printing) and broadcast monitoring [1]. However, in this thesis the emphasis will be on copyright protection and content authentication applications only.

3.3.1 Copyright protection

One of the important applications of digital image watermarking is copyright protection. The watermarking process empowers the identification of the copyright holder and consequently protects the rights in content distribution. To achieve high level owner rights protection, robust watermarks are needed to be embedded into an image. Common image processing techniques could be applied on the watermarked image to destroy the watermark; however the robust watermark should survive these attacks [2].

3.3.2 Content Authentication

Content authentication is considered as one of the main applications of digital image watermarking. Unlike other types of application such as copyright protection, the main objective of content authentication is to confirm the integrity of the image. The image can only be considered authentic if it has not been manipulated or tampered with [2].

Content authentication requires a fragile watermark. Any attempt to modify the watermarked image will destroy the fragile watermark and the image will be considered as non-authentic. This feature is a vital requirement for many important situations, for example when the image is being used as evidence in a criminal investigation changing anything in the image such as a car number plate may lead to an incorrect or improper conviction [3].

3.4 Requirements

The requirements of digital image watermarking depend upon the specific circumstances for which it is needed. All of these requirements are inter-connected. Some of these requirements are described as follows [4]:

3.4.1 Imperceptibility

Imperceptibility is connected to the perceptual transparency of the watermark [5]. In an ideal world, there is no perceptible difference between the watermarked and the original image. Therefore, the embedded watermark is considered imperceptible if the human eye cannot differentiate between the original image and the watermarked image [3.4].

3.4.2 Security

Watermarking security implies the ability of a watermark to resist malicious attack. The watermark used for security requirements should be difficult to remove or to be changed without damaging the host image. Moreover, the watermarking system can be considered as secure, despite the possibility that the unauthorised person with knowledge of the embedding and the extracting of algorithms should not be able to remove or destroy the watermark; this is can be accomplished by using one or more secret keys [4].

3.4.3 Robustness

Robustness refers to the capability of the watermark to survive common processing operations and image manipulations. Common image processing such as compression might cause a problem for the detection of a watermark. Therefore, it is necessary to design a watermark that can survive those operations. For example, lossy compression usually discards perceptually insignificant data and keeps the perceptual significant part. Therefore, it will be a good tactic to embed the watermark into the perceptually significant part. This approach will produce a robust watermark which can survive lossy compression processing. However, since the perceptually significant part is more sensitive to modifications watermarking could create a noticeable distortion in the host image.

The main function of the watermark is to be robust enough to survive both specific attacks and also the image processing operations that will take place during the transmitting process via a communication channel [5].

3.4.4 Capacity

The watermarking capacity is one of the important digital image watermarking requirements. This is the amount of information that can be embedded into the host image. In general, this capacity requirement is usually constrained by two important requirements: imperceptibility and robustness. The higher capacity typically affects either robustness or imperceptibility, or both [5].

3.5 Watermark Classifications

The watermarking techniques for digital images can be classified into different categories; for example according to the working domain it can be classified into spatial domain and transform domain, or sometimes it can be classified based on the watermarking extraction process. If a host image is needed at the decoder it is non blind watermarking, otherwise it is blind watermarking. Finally, it can be classified based on the robustness of the watermark, so there is a robust watermark and a fragile watermark.

3.5.1 Spatial and Transform Domain

3.5.1.1 Spatial Domain

Spatial domain watermarking can be achieved by directly modifying the pixel values of the host image. The low-order bit of each pixel might be flipped during the modification process. Several spatial domain techniques are as follows [6]:

a. Least Significant Bit Coding (LSB)

The LSBs of the subset of pixel values are used for embedding in a sequence like a secret key. Least significant bit coding is a very easy technique. However, the LSB is not robust against simple attacks such as adding noise.

b. Predictive Coding Schemes

The predictive Coding Scheme for grey scale images was proposed by Matsui and Tanaka [7]. There is a certain area for embedding the watermarking into a set of pixels and the differences between the adjacent pixels are replacing the alternate pixels. This scheme is considered more robust than the LSB coding system.

c. Correlation-Based Techniques

This method used a pseudo random (PN) noise with a pattern $W(x, y)$ which is added to the host image. However, the correlation between the random noise and the image itself can be discovered at the decoder side [8].

d. Patchwork Techniques

This method divides the host image into two subsets. The embedding process is applied by increasing one sub-set by a factor K while the other sub-set will be decreased by the same amount [9]. The spatial domain watermarking is still not trustworthy because it cannot survive any digital processing operation for instant filtering or lossy compression.

3.5.1.2 Transform (Frequency) Domain

In contrast to spatial domain methods, the frequency domain uses part of the lower or middle frequency coefficients of the host image to embed the watermarking information. The high frequency is not used for embedding because it could be suppressed by compression. The challenge in this technique is choosing the best frequency positions of the host image in order to be used for the embedding process. There are several frequency domain techniques, which are as follows [7]: Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

3.5.2 Non-Blind and Blind Watermarking Techniques.

Digital watermarking techniques can also be categorized into two schemes:

3.5.2.1 Non-Blind Watermarking Technique

This technique at the decoder side needs at least the host image for watermarking extraction. The Non-Blind technique uses the original image as a hint in order to find where the watermark could be, especially as the watermarked image will be distorted by some attacks [10].

3.5.2.2 Blind Watermarking Technique

This type of technique is a challenging one as it does not require the host image or the embedded watermark information to recover the watermarking information. Therefore, the receiver side (Decoding) and the transmitter side (Encoding) can work independently and there is no need to share any information [11].

3.5.3 Robust and Fragile Watermarking Techniques

3.5.3.1 Robust Watermarking

Generally speaking, robust watermark are ones that cannot be broken easily as they survive against many image processing attacks. Removing a robust watermark will badly affect the quality of the image [6]. The attacker who tries to counterfeit the copyright of the digital image by removing a robust watermark will face difficulty because it will destroy the watermarked image [7].

3.5.3.2 Fragile Watermarking

A watermark is considered as a fragile watermark if the watermark is destroyed whenever the watermarked image has been manipulated. On the other hand, the image is considered authentic (not tampered with) as long as the fragile watermark can be extracted [5].

The main purpose of fragile watermarking is for authentication and proof of integrity. A problem however arises because the fragile watermark can easily be disturbed, because of its fragility [5].

3.6 Evaluation and Benchmarking

The main objective quality assessment parameters which are used to evaluate the watermarked image quality are the Peak Signal to Noise Ratio (PSNR). The Structural Similarity Index Measure (SSIM) [12] and The Normalized cross Correlation coefficients (NCC). These benchmark metrics have been usually used to measure the amount of visual quality degradation between original and watermarked images [12]. However, the subjective assessment of the quality of watermarked image could be used ITU-R 500 [13]. This method of evaluations depends on the judgments of the observers

who will compare between the watermarked image and the host image. The Table below shows the grading of ITU –R 500 standard [13].

Table 3.1: ITU-R quality and impairment scales.

Five-grade scale			
Quality		Impairment	
5	Excellent	5	Imperceptible
4	Good	4	Perceptible, but not annoying
3	Fair	3	Slightly annoying
2	Poor	2	Annoying
1	Bad	1	Very annoying

3.6.1 Peak Signal to Noise Ratio (PSNR)

The PSNR can be defined as a ratio between the maximum power of the original image and the power of the corrupting noise that affects the trustworthiness of its representation [12]. The PSNR has been used to evaluate the quality of the watermarked image. It is easy to calculate the PSNR via the Mean Squared Error (MSE) which compares two images (the original image and the watermarked image) on a pixel-by-pixel basis. The MSE is defined in equation (3.1) and the PSNR is defined in equation (3.2) as follows [14]:

$$\text{For grey – scale images: } MSE_{grey} = \frac{1}{xy} \sum_{x,y} (i_{x,y} - w_{x,y})^2$$

$$\text{For colour images:} \quad (3.1)$$

$$MSE_{colour} = \frac{1}{3xy} \sum_{x,y} (ir_{x,y} - wr_{x,y})^2 + (ig_{x,y} - wg_{x,y})^2 + (ib_{x,y} - wb_{x,y})^2$$

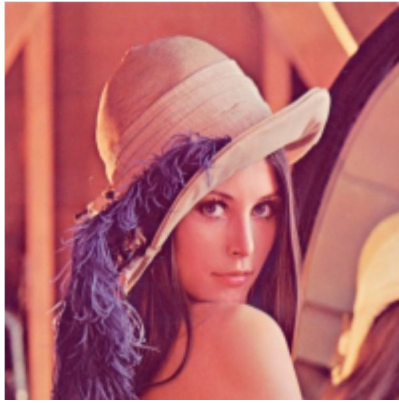
where:

i is the original image and *w* is the watermarked image, *x* and *y* are the image pixels

r is the red channel, *g* is the green channel and *b* is the blue channel.

$$PSNR = 10 \cdot \log_{10} \left(255^2 / MSE \right) \quad (3.2)$$

If the MSE is increased the level of degradation in the watermarked image increases, while the PSNR value will become infinite if the two images (original and watermarked) are exactly the same. Figure 3.2 shows the original Lena host image and watermarked Lena images. The R, G and B channels have been used to embed the watermark separately [12].



a. Original Lena



b. Watermarked image
PSNR = 40 dB



c. Watermarked image
PSNR = 80 dB



d. watermarked image
PSNR = 100 dB

Figure 3.2: Original Lena and watermarked Lena with different PSNR values.

3.6.2 The Structural Similarity Index Measurement (SSIM)

The similarity between two images can be measured by SSIM. The SSIM is used to develop traditional methods like PSNR and MSE which have been verified to be unreliable by human eye perception. The SSIM value is between -1 and 1. The SSIM will be 1 if and only if the two images are identical. The SSIM can be found as follows [12]:

$$SSIM = [L(i, w)]^\alpha \cdot [C(i, w)]^\beta \cdot [S(i, w)]^\gamma \quad 3.3$$

where: i is the original image and w is the watermarked image,

L, C and S are representing luminance, contrast and structure,

α, β and γ are parameters which are used to adjust the luminance,

contrast and structure components.

3.6.3 The Normalized Correlation Coefficients (NCC)

Finally, NCC is another benchmark for the digital image watermarking scheme, and it can be calculated as follows [12]:

$$NC = \sum_{x,y} i_{x,y} e_{x,y} / \sum_{x,y} e_{x,y}^2 \quad 3.4$$

where: i is the original watermark and e is the extracted watermark.

3.7 Attacks

The main value of any watermarking scheme lies in its robustness against attacks. The concept of robustness is naturally obvious: a watermark is considered robust if it cannot be impaired without also rendering the attacked data useless. There are some well known attacks that are carried out on watermarking systems [15]. However for research purposes and evaluating watermarking algorithms, there are also powerful tools such as Stirmark and inZign which are used to generate attacks. Some attacks are explained below:

3.7.1 JPEG Compression Attack

If the watermarked image is not in JPEG format, the first step for the attacker is to convert the watermarked image into JPEG format and changing the “quality factor” of JPEG compression to as low as the attacker can before the features they need on the image deteriorate. Even though the watermarked image is in JPEG format, the attacker tries to reduce the quality factor. The quality factor range is between 0 and 100. The JPEG attack does not need complicated image software. Many image viewers which are available online are able to save JPEG files using different quality factors. This type of attack is therefore treated as the most dangerous one. The objective of the watermarking algorithms is to extract the watermark even though the watermarked image is compressed [16]. Figure 3.3 shows the Lena image (watermarked) and compressed Lena with different quality rates.



Figure 3.3: JPEG compression attacks.

3.7.2 Image Enhancement Attack

Nowadays many digital cameras are used to capture images in digital format and are supplied with enhancement processors. For example contrast enhancement can be adjusted to enhance the subjective quality of the digital image. This process might destroy the watermark. The attacker might use this facility to damage the watermark in the watermarked image. In figure 3.4, the image quality resulting from different contrast enhancement is illustrated.

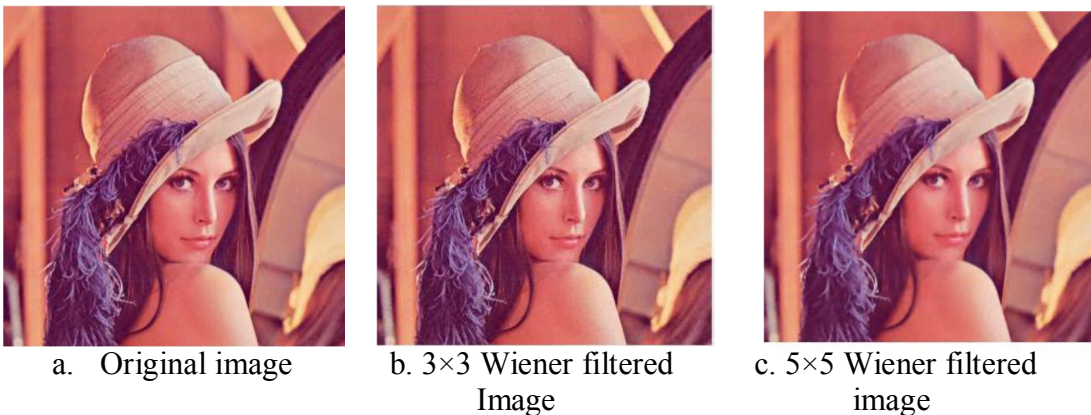


a. Original Lena Image b. Contrast adjustment c. Contrast adjustment

Figure 3.4: Contrast adjustment attack

3.7.3 Removal Attack

The purpose of the removal attack is to remove the watermark information from the watermarked image. The attacker here tries not to affect the quality of the embedded watermark during the process of removing the watermark. Figure 3.5 shows how Wiener filters can be used to maintain the quality of the attacked image.



a. Original image

b. 3×3 Wiener filtered
Image

c. 5×5 Wiener filtered
image

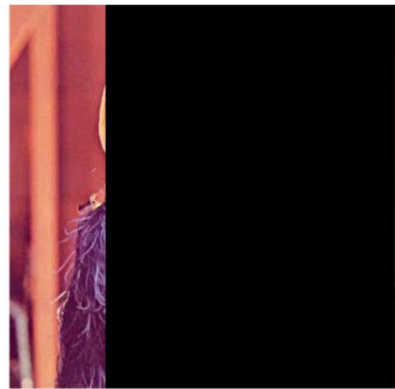
Figure 3.5: Removal attack.

3.7.4 Cropping Attack

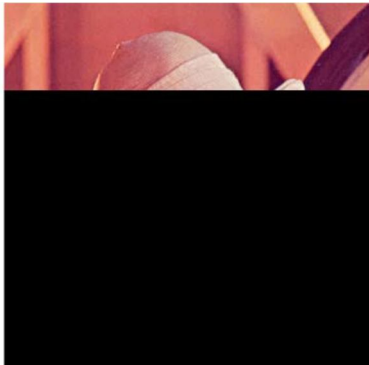
A cropping attack is the cutting or removing of some pixels from the watermarked image. It produces a large distortion in a mean square error (MSE). However, it does not cause any perceptual distortion. For example, this can be done by cutting a small frame from the watermarked image and leaving the rest unchanged [17]. The watermark algorithm should be designed to survive cropping, where the spatial information is discarded. Figure 3.6 illustrates some examples of cropping attacks.



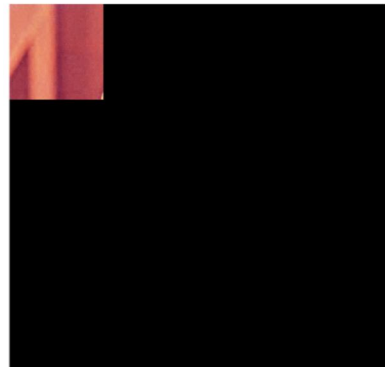
a. Un-cropped image



b. Cropped side to 75% vertically



c. Cropped side to 75% horizontally



d. Cropped both sides to 75%

Figure 3.6: Cropping attack

3.7.5 Resize Attack

The aim of the geometric attack is not to remove the watermark information, but to change the synchronization of the embedded watermark information. Therefore, the extraction process for the watermark in a geometrically modified image is a difficult mission [3.15]. The embedded watermarked information could be extracted if the synchronization in the decoder is regained. For example, figure 3.7 explains some resize attacks: to examine the robustness of the watermark algorithm, the image should first be restored to its original dimension and then the watermark extracted.



Figure 3.7: Examples of resizing attacks.

3.7.6 Additive Noise

During the transmission process of the watermarked image from the Encoder (Transmitter) to the Decoder (Receiver), the watermarked image might face this kind of attack. The aim of the copyright watermarking technique is to survive this attack [18]. Figure 3.8 explains an example of additive noise attack.

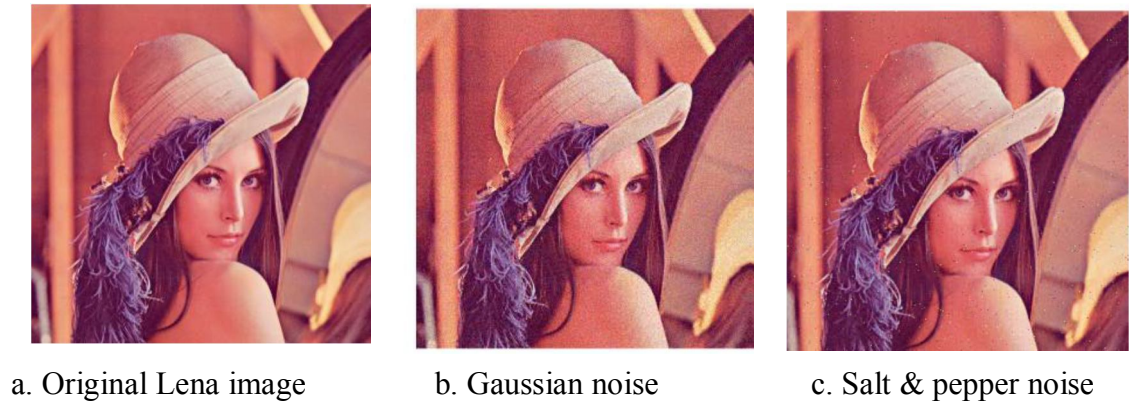


Figure 3.8: Additive noise attacks

3.7.7 Filtering

Another challenge for the watermarking algorithm is to be robust enough to survive if the low-pass filter and median filter are applied to the watermarked image. In general, the filter levels are 3×3 mask size. However, by increasing the filter levels to 5×5 or 7×7 mask size the watermarked image will be severely degraded and the watermark might be destroyed. Figure 3.9 shows examples of such types of filtering attack.



Figure 3.9: Filtering attack

3.8 Literature Survey of Watermarking Techniques

This section will focus on the Transform domain technique. Although, the digital watermarking can be divided into two basic categories: Spatial domain technique and Transform (Frequency) domain technique [3.19].

Usually transformed domain techniques are more robust than spatial domain ones. Watermarking transform techniques based on robustness can be further divided into two categories; robust watermarking and fragile watermarking [20]. While the robust watermarking schemes are used for proving ownership claims, the fragile watermarking schemes are deployed to authenticate multimedia content. The robust watermarking will survive a multiplicity of attacks such as: cropping, scaling, filtering, additive noise and JPEG compression. The aim of using fragile watermarks is to identify and report every possible tampering of watermarked digital media [21].

3.8.1 Robust

Many robust watermarking methods will be introduced in this section. Discrete Cosine Transform (DCT) is one of the well known transformations which have been used for embedding robust watermarks in the host image [22]. Another well known transformation which has been used in robust watermarking is the discrete wavelet transformation (DWT) [5]. In addition to that, a combined DWT-DCT may be used [23].

In 1997 Kundur and Hatzinakos [24], proposed a watermark algorithm by using wavelet domain. The robust watermark was evaluated by the contrast sensitivity of the host image. The algorithm showed resistance to JPEG compression, additive noise and linear filtering. However, the original host image was required in order to extract the watermark.

In the same year Cox et al. [25] tried to design a robust watermark against attacks by using a perceptually significant area of the image to embed the watermark. The DCT transform has been used for this purpose and 1000 random samples were taken and added to the highest magnitude of the DCT 1000 coefficients. The proposed algorithm was robust to dithering, cropping, image scaling, JPEG coding, and rescanning. The extraction process needs the original image and the exact frequency location of the watermark samples. Moreover, the correlation coefficients should be large enough to detect the watermark.

In 1998, Xia et al. [26] proposed a multi-resolution watermark of digital images. Discrete wavelet transform (DWT) was used as a watermarking scheme. The Pseudo-random codes were used as a watermark. The watermark was added to large coefficients at the middle and high frequency bands of the host image. The proposed method showed the DCT method to be more robust [25]. However, the decoding process still needed the original watermark for correlation. Moreover, a watermark cannot be detected if the cross-correlation magnitude is higher than the threshold.

In the same year, Kundar and Hatzinakos [27] proposed a new technique based on the concept of multi-resolution wavelet fusion for the digital watermarking of still images. The extraction process did not require the original image (blind algorithm). The algorithm showed robustness to common image distortion. On the other hand, the length of the watermark was not enough to reduce the probability of detection error.

In 2000, Kaewkamnerd and Rao [28] offered a new image watermark method based on discrete wavelet transform (DWT). In order to increase the robustness and perceptual invisibility, the algorithm was combined with the quantisation model based on the human visual system (HVS). The algorithm showed robustness against the high compression environments. But the authors did not test the algorithm against common attacks such as filtering, cropping, etc.

In 2000, Fotopoulos and Skodras [29] proposed a sub-band DCT approach for image watermarking. The one-level with four bands (sub-band) was achieved by using one-level DWT. The coefficients in each band were rearranged in a vector. Many coefficients in all four bands were being used. However, each band gave a different detection output. The result was found by taking the average detection from all four bands. The proposed algorithm was not tested against watermarking colour images.

In 2001, Cao et al. [30] presented an image adaptive watermarking technique based on a redundant wavelet transform. The host image was not required to extract the watermark from the watermarked image at the receiver side (blind algorithm). A direct production of the wavelet coefficients at different scales was used. The watermark was embedded into salient features of the image in order to check the robustness to subsequent image processing which might be used to attack the watermark. The algorithm was examined through general image processing for instant, low-pass filter, JPEG compression, but it was not tested against cropping, resize, Gaussian filters and scaling attacks.

In 2001, Barni et al. [31] proposed a watermarking algorithm based on wavelet domain. The watermark contained a pseudo random sequence. Modified DWT coefficients of

the image were used to embed the watermark. The algorithm proved that it survived against image cropping. However, the algorithm only works for 50:1 JPEG compression.

In 2004, Shiuh et al. [32] proposed a genetic algorithm (GA) in the transform domain by using Discrete Cosine Transform (DCT). The proposed algorithm showed robustness against watermarking attacks. It also examined both robustness and invisibility. The quality of the watermarked image was improved with the aid of the GA. The authors compared their algorithm with the existing algorithms and showed that the GA algorithm was better in robustness.

In 2004, Tao and Eskicioglu [33] embedded a binary pattern in the form of a binary image in all the four band coefficients at the first and second level of discrete wavelet transform (DWT) host images. It showed that the proposed algorithm was robust resistant to many attacks without badly reducing the quality of the image. The algorithm did not examine the PSNR ratio of the watermarked image. The embedding in many *bands* of the DWT will affect the quality of the image and NCC will be of low value.

In 2005, Kaewkamnerd and Rao [34] presented an image adaptive watermark based on Discrete Wavelet Transform (DWT). In order to increase the watermark robustness and perceptual invisibility, the authors worked on a combination between the algorithm and the quantization model depending on the human visual system (HVS). The factors that affect directly on HVS such as: background luminance, edge, frequency band and texture masking were taken into consideration. The proposed algorithm could extract the watermark from the decoder side both with and without the need for the host image

(blind and non blind). The algorithm showed robustness to the compression attack and other image processing operation such as filtering. However, it was not tested against geometric attack.

In 2005, Golikeri and Nasio [35] proposed a watermarking algorithm based on DCT transform. They divided an image into blocks and calculated the amount of DCT energy in each block. The blocks which contained significant energy represented an area of significant information. These blocks were chosen to embed a Gaussian pseudorandom watermark. The proposed algorithm demonstrated robustness against cropping, scaling, compression and multiple attacks.

In 2006, Wei et al. [36] proposed a genetic algorithm (GA) based on Discrete Cosine Transform (DCT). The watermark was embedded in the modified AC coefficients of the host image in the DCT domain. The insertion and extraction processes were engaged to speed up the genetic watermarking and to avoid loss of the watermark. The proposed GA was designed to be a robust and invisible algorithm. It showed good robustness against watermark attacks and high reliability.

In 2007, Al-Haj [37] presented a combined DWT-DCT algorithm for digital image watermarking. The watermark was embedded in the first and second levels of DWT sub-bands of the host image. The DCT transform was used on the selected DWT sub-bands. The results showed improvements when it was compared to the DWT only. The proposed algorithm demonstrated robustness against several attacks. However, the time

needed to complete the embedding and extraction process was very high if it is compared with DCT algorithm.

In 2008, Al Gindy et al. [38] presented a DCT algorithm for colour digital image watermarking. The green channel was chosen for embedding the watermark. The proposed algorithm showed robustness to JPEG compression, cropping, scaling, low-pass, median and removal attack. Moreover, the algorithm achieved more than 65 dB of average PSNR. However, NCC recorded around 0.7929 for salt and pepper $d=0.02$ attack.

In 2009, Al Gindy et al. [39] proposed an adaptive DCT algorithm for still colour-image watermarking. The image was divided into 8 by 8 blocks before the DCT implementation. It used the green channel for the embedding process. The perceptual capacity for each coefficient inside each DCT block was taken into consideration before the embedding process was started. Thus all the 63 coefficients were scanned (except the DC value) in order to select the highest magnitude for embedding. The algorithm did not require the host image to extract the watermark (Blind Algorithm). It demonstrated robustness to several attacks such as: JPEG compression, additive noise, cropping, scaling, low-pass and median filtering.

In 2010, Mostafa et al. [40] proposed the Discrete Wavelet Packet Transform (DWPT) algorithm for inserting patient information (as a watermark) into medical images. The algorithm did not need the host image to extract the watermark (Blind). The algorithm showed no visible difference between the watermarked image and the original image. Furthermore, it proved to be robust against several attacks such as: Gaussian noise

addition, gamma correction, contrast adjustment, and sharpen filter and rotation. However, recorded PSNR values were very low.

In 2011, Mohammed and Sidqi [41] presented a multi-band wavelets algorithm for an image watermarking scheme. Three criteria were used for the proposed algorithm. The first one used one band for the embedding process, while the second one used two bands. The last criterion used three bands. The proposed algorithm was non-blind. Therefore the host image was required to extract the watermark. It proved to be robust against the JPEG compression ($QF = 25$). However, the PSNR was low (24 dB). Moreover, a large number of wavelets were involved in the embedding process which affected the quality of the watermarked image.

In 2012, Kashyap and G.R. [42] proposed multi resolution digital image watermarking based on 2-level Discrete Wavelet Transform (DWT) and alpha bending techniques. The proposed algorithm compared with the 1-level DWT by using the parameters of a peak signal to noise ratio (PSNR) and the mean square error (MSE). Despite the results of the proposed algorithm being better than the 1-level DWT, from the perspective of PSNR the PSNR recorded was low.

In 2013, Totla and Bapat [43] proposed two algorithms for digital image watermarking; Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) algorithms. The authors compared both algorithms in imperceptibility and robustness to some attacks such as resizing, rotation and cropping. It showed that the DWT algorithm was more robust against attacks such as cropping and resizing as compared to DCT.

Moreover, the PSNR values on several occasions in the DWT were higher than with DCT.

3.8.2 Fragile

In 1998, Bhattacharjee and Kutter [44] presented an authentication scheme for the visual content of digital images. The proposed scheme was robust to noise of the compression. However, it detected the manipulation of the host image. The extraction of feature points from the host image used scaled interaction based on Wavelet (Mexican-Hat type). The lossy compression was unaffected on the feature point of the host image. In order to generate the digital signature of the host image, public key encryption was used to encrypt the feature points from the host image. The authentication was achieved by comparing the feature points in the host image with the feature points in the watermarked image. But the authors did not justify why the Mexican hat wavelet was selected in the first place. Moreover, the JPEG was only 80 % which is a low compression ratio.

In 1999, Wolfgang and Delp [45] proposed two fragile watermark algorithms. The first one used a hash function to obtain a digest of the image. The hash function of the watermarked image was calculated and compared with the hash function of the host image. If the result was not zero it meant that the watermarked image had been manipulated. Moreover, any changes in the hashed image would be spatially localized. The second proposed fragile algorithm used the Variable-Watermark Two-Dimensional algorithm (VW2D). The image in the second algorithm was considered to be authentic even though the watermarked image had some minor changes. Therefore the second algorithm could be considered as a semi fragile watermark algorithm. It showed that the

second algorithm may be preferred over the first one in applications which need adjustment for the sensitivity of a fragile watermarking technique.

In 2001, Celik et al. [46] proposed a hierarchical fragile watermarking scheme based on the public key watermark. The algorithm divided the host image into blocks in a multi level hierarchy and following this, the block signature in this hierarchy was calculated. In the lowest levels of the hierarchy the signatures of small blocks guaranteed greater accuracy of tamper localisation, while high level block signatures offered an increased ability to survive vector quantisation (VQ) attacks.

In 2003, Paquet et al. [47] presented a wavelet digital watermarking scheme for the authentication of digital images. A secret identification key was embedded in the wavelet coefficients by their selective quantization in order to protect the host image. The human visual system characteristics were used to maximize the insertion weights whilst good perceptual transparency was kept. The multi-resolution discrete wavelet decomposition nature permitted the frequency and spatial localisation of image tampering.

In 2004, Alomari and Al-Jaber [48] proposed a secure fragile watermarking algorithm. The proposed algorithm used the binary image data hiding technique to insert an authentication signature into the first bit plane. The hash function (MD5) was used as an authentication signature. It showed that any tampering of a watermarked image could be detected and also gave an indication of how much alteration had occurred and where it was located. However, the MSE recorded was quite high.

In 2006, He et al. [49] proposed a wavelet based watermarking algorithm for secure image authentication. Discrete wavelet coefficients were used for embedding the watermark signature. The watermark signature was scrambled before the embedding into the least significant part of the transformed host image. The proposed algorithm showed excellent tampering localisation properties and offered more security against many attacks. Moreover, it indicated whether the manipulation had occurred in the content watermarked image or in the embedded watermark itself. However, neither the PSNR nor the MSE values were calculated.

In 2007, Kitanovski et al. [50] proposed a combined hashing and watermarking algorithm for image authentication. A watermark was inserted into the quantised index modulation of DCT coefficients. The extraction process did not need the original watermark (Blind algorithm). A robust image hash was used as a watermarking signature in order to increase security. It showed that the proposed algorithm verified the effectiveness in term of robustness and fragility. The PSNR recorded good values.

In 2008, Zhang and Wang [51] proposed a fragile watermarking scheme which could be used to recover the original image from its tampered image. A lossless data hiding method was used to embed the watermark into the host image. The watermark is a tailor-made type which consists of reference bits and check bits as well. The check bits derived from the hash of blocks were embedded into the entire image by using a lossless Different Expansion Algorithm (DE) embedding technique. On the receiver side, it compared between the extracted and calculated check bits in order to identify the manipulated image-blocks. From the other blocks, the reliable reference bits were

extracted and used to exactly reconstruct the original image. However, the PSNR recorded low values.

In 2009, Devi et al. [52] presented a fragile image authentication algorithm with localisation by using Discrete Wavelet Transform (DWT). A logo was used as the secret data. The logo image was repeated many times (watermark) until it matched the size of the High-High sub-band of integer wavelet transform. Moreover, the watermark was scrambled to increase the security level. Odd-Even mapping was used to insert the watermark into the wavelet coefficients. The proposed algorithm detected and localised tampering at pixel level. However, the MSE recorded quite high values.

In 2009, Kung et al. [53] proposed yet another watermarking algorithm scheme. It contained two parts; one for robust watermarking and other for image authentication. The robust scheme used the frequency domain. However, the fragile scheme used the spatial domain. The fragile signature produced from the edge properties which were extracted from the host image. The fragile watermark was removed or was damaged if the watermarked image was tampered with something such as by lossy compression.

In 2012, Sumalatha et al. [54] proposed an algorithm for image authentication and tamper localisation. They used a simple block based checksum watermarking (BBCW) method. The proposed BBCW is a hierarchical method. The image is divided into 4×4 blocks. Then each block is hierarchically divided into 4 sub-blocks. Each sub-block is divided into 2×2 blocks. Tampering with any sub-block or even tampering at pixel level is identified if the block checksum does not match the extracted bit sequence. This

algorithm showed a high quality embedded image. The authors compared their proposed method with several other methods such as the method which is mentioned in ref. 3.49.

In 2013, Mishra et al. [55] presented a fragile watermarking algorithm for medical images. The proposed algorithm used selective bit planes of the integer DWT. The hash value was calculated from the Most Significant Bit (MSB). The watermark signature (Hash function) was inserted into integer wavelet transform. The proposed algorithm detected a tampered area of the image. The presented algorithm supported all data formats such as JPEG, TIFF, GIF, etc. The PSNR recorded high values. However, the MSE also recorded quite high values.

3.9 Final Remarks

3.9.1 Robust remarks

- Pseudo-random sequences or text images are used in many current watermarking techniques. However, mobile phone numbers is rarely used.
- Scrambling the watermark is uncommon in most watermarking algorithms.
- Some current watermarking algorithms use DCT, while others use DWT. However, few current watermarking algorithms combine both.
- Most current watermarking algorithms cannot survive all forms of attack.
- A comparison between DCT and DWT shows that DWT is more robust than DCT against attacks such as cropping and resizing.
- A lot of watermarking methods require the original image before they can extract the watermark on the receiver end (non-blind).
- Very few current watermarking algorithms use multi-embedding for watermark information.

3.9.2 Fragile remarks

- Most current watermarking algorithms use dependent fragile watermarks on the host image itself.
- It is very difficult to differentiate between malicious and non-malicious attacks.
- Some algorithms use spatial domain, while other algorithms use frequency domain.
- The hash function is heavily used as a fragile watermark.
- Some current watermarking algorithms use embedding check-sums in LSB techniques. One of the disadvantages of this technique is the swap possibility between blocks if two watermarked images (fragile) are protected with the same key.
- Others use self-embedding techniques. However, the major drawback for this technique is that the recovery data might be destroyed if the watermarked image has been attacked in several areas.

Based on the aforementioned remarks, the direction of the proposed algorithms in this thesis will be applied to minimise the weakness in some previous algorithms. One of the crucial challenges of digital image watermarking is to design a complete system (robust and fragile) in the transmitter (encoder) side and the receiver (decoder) side that preserves the quality of the image whilst at the same time satisfying the demands of security, robustness, authenticity and capacity. The proposed work in the next chapter (chapter four) will be directed to design a more robust watermark technique with high transparency, robustness and a high capacity for grey and colour still images.

The human Visual System (HVS) is a big concern for digital watermarking techniques. In addition to that, many watermarking techniques cannot survive against high

compression ratio. Thus, Discrete Wavelet Transform will be chosen (robust watermarking) to overcome the aforementioned challenges. DWT has also a multi-resolution description of image features which can provide a multi-resolution explanation of images which explain the resolution at different levels from low to high resolution. To design algorithm can deal friendly with different file formats, different image sizes is another challenge which need to deal with in this thesis. The data capacity for any digital watermarking system is another challenge. The additional data size required has to be calculated without affecting the quality of the image. The robust watermarking technique needs to balance the data amount required for watermarking robustness against the quality of the image. The watermark extraction process which needs the original image is a non-blind watermarking algorithm. In this kind of watermarking algorithms require memory to store the host image for extraction. Therefore, in this thesis blind techniques will be used. If the embedding watermark is embedded one time and not scrambled, this leads to the possibility of not being able to recover the watermark. Thus in this thesis the watermark will be scrambled and multi embedding and multi extraction will be used.

3.10 References

- [1] M. Arnold, S Wolthuson and M. Martin, " *Echniques and Applications of Digital Watermarking and Content* ". Norwood, Artech House, INCC. 2003.
- [2] C. Woo, "Digital Image Watermarking Methods for Copyright Protection and Authentication," in Department of Computer Science. vol. PH. D. Queensland: Queensland University of Technology, 2007, p. 223.
- [3] S. Alomari, A. Al-Jaber, " A Fragile Watermarking Algorithm for Content Authentication", *International Journal of Computing and Information Sciennce*, Vol. 2, No. 1, pp. 27-38, April. 2004.
- [4] A. Al Gindy, " *Design and Analysis of Discrete Cosine Transform-Based Watermarking Algorithms for Digital Images* ", In Department of Electronic Imaging and Media Communication, Vol. PH D. Uk, University of Bradford, 2010.
- [5] M. El-Gayyar, J. Gathen, "Watermarking Techniques Spatial Domain", *Digital right Seminar C. Media Informatic*, Germany, University of Bonn, May, 2006.
- [6] S. Mishra, A. Mahaptra, and P. Mishra, "A Survey on Digital Watermarking Techniques", *International Journal of Computer Science and Information Techniques*, Vol. 4, pp. 451-456, March, 2013.
- [7] T. C. Lin and C. M. Lin, "Wavelet based copyright protection scheme for digital images based on local features", *Information Sciences: an International Journal*, Vol. 179, Sept. 2009.
- [8] R. Thanki, et..al, "Robustness of Correlation Based Watermarking Techniques Using WGN against Different Order Statistics Filters", *International Journal of computer Science and Telecommunication*, Vol. 2, Issue 4, pp. 45-50, July, 2011
- [9] R. Ravula, " *Audio Watermarking Using Transfomation Techniques* ", In Department of Electrical and Computer Engineering, Vol. M. Sc., India, Osmania university, 2006.
- [10] W. Lin, et..al, "A Blind Watermarking Method Using Maximum Wavelet Coefficient Quantization", *Expert Systems with Application Juornal*, Vol. 36, pp. 11509-11516, 2009.

- [11] T. Minamoto, K. Aoki, "A Blind Digital Image Watermarking Method Using Interval Wavelet Decomposition", *International Journal of Signal Processing, Image Processing and Pattern Recognition*, Vol. 3, No. 2, pp. 59-72, June, 2010.
- [12] M. Kutter, F. Petitcolas, "A Fair Benchmark for Image Watermarking Systems", *Electronic Imaging '99. Security and Watermarking of Multimedia Contents*, Vol. 3657, pp. 1-14, January, 1999.
- [13] "Methodology for the subjective assessment of the quality of television pictures", *International Telecommunication Union, Recommendation ITU-R BT.2021*, 2012.
- [14] A. Bamatraf, et.al, "A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB)", *Journal of Computing*, Vol. 3, Issue 4, pp. 1-8, April, 2011.
- [15] S. Voloshynovskiy, S. Pereira, and T. Pun, "Attacks on Digital Watermarks: Classification, Estimation-Based Attack, and Benchmarks", *IEEE Communication Magazine*, Vol. 3, No. 4, pp. 2-11, August, 2001.
- [16] "Analysis of Attacks on Common Watermarking Techniques", in <http://www.ece.ubc.ca/>.
- [17] P. Comesana, F. Gonzalez, "The Impact of The Cropping attack on Scalar STDM data hiding", *IEEE Signal Processing Letters*, Vol. 13, Issue 6, pp. 353-356, June, 2006.
- [18] D. Kirovski and A. Fabien A. Petitcolas, "Blind Pattern Matching Attack on Watermarking Systems," *IEEE Trans. on Signal Processing*, vol. 51, no. 4, pp. 1045–1053, April 2003.
- [19] N. Kashyap, and G. Sinha, "Image Watermarking Using 2-Level DWT", *Advances in Computational Research*, Vol. 4, Issue 1, pp.-42-45, 2012.
- [20] S. P. Mohanty, N. Ranganathan, and R. K. Namballa, "VLSI Implementation of Invisible Digital Watermarking Algorithms Towards the Development of a Secure. JPEG Encoder," *IEEE Workshop on Signal Processing Systems (SIPS)*, pp. 183-188, 2003.

- [21] S. Radharani, M.L. Valarmathi, "A Study on Watermarking Schemes for Image Authentication", *International Journal of Computer Applications*, Vol. 2, No.4, pp 24-32, June, 2010.
- [22] N. Ahmed, T. Natarajan, and K. R. Rao, "Discrete cosine transform," *IEEE Transactions on Computers*, vol. C-32, pp. 90-93, Jan. 1974.
- [23] A. Al-Haj, "Combined DWT-DCT Digital Image Watermarking", *Journal of Computer Science*, pp. 740-746, 2007.
- [24] D. Kundar, D. Hatzinakos, "A Robust Digital Image Watermarking Method Using Wavelet-Based Fusion", *Proceedings of the 1997 International Conference on Parallel Processing (ICPP'97)*, pp.544-548, 1997.
- [25] I. Cox, J. Kilian, F. Leighton, T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Transactions on Image Processing*, Vol. 6, No. 12, December, 1997.
- [26] X. Xia, C. Boncelet, and A. Gonzalo, "Wavelet Transform Based Watermark for Digital Images", *Optics Express* 497, Vol. 3, No.12, December, 1998.
- [27] D. Kundar, D. Hatzinakos, "Digital Watermarking Using Multiresolution Wavelet Decomposition", *Acoustics, Speech and Signal Processing, 1998. Proceedings of the 1998 IEEE International Conference on*, pp. 2969-2972, 1998.
- [28] N. Kaewamnerd, N. K. Rao, "Wavelet Based Image Adaptive Watermarking", *IET Journals and Magazines*, Vol. 36, Issue 4, pp. 312-313, 2000.
- [29] "A Subband DCT Approach To Image Watermarking", in <http://www.docstoc.com/docs/32528211>.
- [30] J. Cao, J. Fowler, N. Younan, "An Image-Adaptive Watermark Based on A Redundant Wavelet Transform", *Proceeding of the IEEE International Conference on Image Processing*, Greece, pp. 277-280, October 2001.
- [31] M. Barni, F. Bartolini, A. Piva, "Improved Wavelet-Based Watermarking Through Pixel-Wise Masking", *IEEE Transactions on Image Processing*, Vol. 10, No. 5, pp. 783-792, May, 2001.

- [32] C. Shieh, et.al, “Genetic Watermarking Based on Transform-Domain techniques”, *Pattern Recognition*, Vol. 37, Issue 3, pp. 555-565, March, 2004.
- [33] T. Peining, M. Ahmet, Eskicioglu, “A robust multiple watermarking scheme in the discrete wavelet transform domain”, *Proceedings of the SPIE*, Vol. 5601, pp. 133-144, 2004.
- [34] “Multiresolution based image adaptive watermarking scheme”, in www.ee.uta.edu/dip/paper/EUSIPCO_water.pdf.
- [35] “A Robust DCT Energy Based Watermarking Scheme For Images”, in http://www.ece.ubc.ca/~adarshg/DCT_Watermark.pdf.
- [36] Z. Wei , J. Dai , J. Li, “Genetic Watermarking Based on DCT Domain Techniques”, *Electrical and Computer Engineering, 2006. CCECE '06. Canadian Conference on*, Canada, pp. 2365 – 2368, May, 2006.
- [37] A. Al-Haj, “Combined DWT-DCT Digital Image Watermarking”, *Journal of Computer Science* Vol. 3, No. 9, pp. 740-746, 2007.
- [38] A. Al-Gindya, H. Al-Ahmad, R. Qahwaji and A. Tawfik, “A Novel Blind Image Watermarking Technique for Colour RGB Images in the DCT Domain Using Green Channel”, *Communications, Computer Applications, 2008. MIC-CCA 2008. Mosharaka International Conference on*, Jordan, pp. 26-31, August, 2008.
- [39] A. Al-Gindya, H. Al-Ahmad, R. Qahwaji and A. Tawfik, “A Frequency Domain Adaptive Watermarking Algorithm for Still Colour Images”, *Advances in Computational Tools for Engineering Applications, 2009. ACTEA '09. International Conference on*, Lebanon, pp. 186-191, July, 2009.
- [40] S. Mostafa, et.al , “ Wavelet Packets-Based Blind Watermarking for Medical Image Management”, *The Open Biomedical Engineering Journal*, Vol. 4, pp. 93- 98, 2010.
- [41] A.Mohammed, H. Sidqi , “ Robust Image Watermarking Scheme Based on Wavelet Technique”, *International Journal of Computer Science and Security (IJCSS)*, Vol. 5, Issue 4, 2011.

- [42] "Image Watermarking Using 2-Level DWT", in [http:// www. bioinfo.in/ contents. php?id=33](http://www.bioinfo.in/contents.php?id=33).
- [43] R. Totla, K. Bapat " Comparative Analysis of watermarking in Digital Images Using DCT & DWT", *International Journal of Scientific and Research Publications*, Vol.3, Issue 2, pp. 1-5, February 2013.
- [44] S. Bhattacharjee, M. Kutter, "Compression tolerant image authentication", *Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on*, Vol. 1, USA, pp. 435-439, October, 1998.
- [45] H. Inoue, T. Katsura, "Wavelet-based watermarking for tamper proofing of still images ", *Image Processing, 2000. Proceedings. 2000 International Conference on*, Vol.2, Canada, pp. 88-91, September, 2000.
- [46] M. Celik , G. Sharma, E. Saber, and A. Tekalp, "A Hierarchical Image Authentication Watermark with Improved Localization and security", *Proceedings IEEE International Conference on Image Processing*, Vol. 2, pp. 502-505. Oct 2001.
- [47] A. Paquet, R. Ward, I. Pitas, "Wavelet packets-based digital watermarking for image verification and authentication", *Journal Signal Processing - Special Section: Security of Data Hiding Technologies*, Vol. 83 Issue 10, pp. 2117 - 2132 , October 2003.
- [48] R. Alomari, A. Al-Jaber, "A Fragile Watermarking Algorithm for content Authentication", *International journal of Computing & Information Science*, Vol. 2, No. 1, pp. 27-39, April, 2004.
- [49] H. He, J. Zhang, H. Tai, "A Wavelet-Based Fragile Watermarking Scheme for Secure Image Authentication", *Digital Watermarking Lecture Notes in Computer Science Volume 4283*, pp 422-432, 2006.
- [50] V. Kitanovski, D. Taskovski, and S. Bogdanova "Combined Hashing/Watermarking Method for Image Authentication", *World Academy of Science, Engineering and Technology*, pp. 422-433, June, 2007.
- [51] X. Zhang , S. Wang, "Fragile Watermarking With Error-Free Restoration Capability", *IEEE Transactions on Multimedia* , Vol.10, No.8, December, 2008.

- [52] P. MeenakshiDevi, M. Venkatesan, K. Duraiswamy, "A Fragile Watermarking Scheme for Image Authentication with TamperLocalization Using Integer Wavelet Transform", *Journal of Computer Science*, Vol. 5, No.11, pp. 831-837, 2009.
- [53] Chih-Ming Kung, et..al, "A Robust Watermarking and Image Authentication Scheme used for Digital ContantApplication", *Journal of Multimedia*, Vol. 4, No. 3,pp. 112-120, June, 2009.
- [54] L. Sumalatha, G. Kumari, V.V Kumar, "A Simple Block Based Content Watermarking Scheme for Image Authentication and TamperDetection", *International Journal of Soft Computing and Engineering (IJSCE)*, Vol.2, Issue4, pp. 113-118, September , 2012.
- [55] S. Mishra, A. Mahapatra, P. Mishra, "A Survey on Digital Watermarking Techniques", (*IJCSIT*) *International Journal of Computer Science and Information Technologies*, Vol. 4 , pp. 451-456, 2013.

CHAPTER 4

One-level DWT Robust Watermarking

4.1 Introduction

This chapter commences by presenting numerous host images and different types of binary watermarks. A new robust watermarking algorithm for still grey scale images will be introduced next. The algorithms work in the frequency domain by using the Discrete Wavelet Transform (DWT). Then the new algorithm will be extended so that it can be used for still colour images. It will use the green channel and Y channels for the embedding process. The aim for the aforementioned robust algorithms is to verify the legal ownership for the digital grey and colour images. In addition to that, is to fulfil the different watermarking requirements for example robustness, quality, capacity and security. Finally, the proposed new algorithms will be tested and compared with previous DCT based algorithms.

4.2 Host Images and Watermarks

For the current and the following chapters, several colour and grey still test images were used. The USC-SIPI image data sheets [1] contain standard images. Some of these images are very common images in digital image processing for example Lena, Baboon,

and Peppers. In addition to that the Kodak images [2] are another source for the standard images which were used throughout this research. Finally, non-standard images taken by a digital camera have also been used. Figure 4.1 shows 45 colour images (24 bits/pixel) and grey scale images (8 bits/pixel). The size of the images are 512×512 pixels. On the other hand, the watermarking information used is the mobile numbers including the international code which are shown in Figure 4.2.

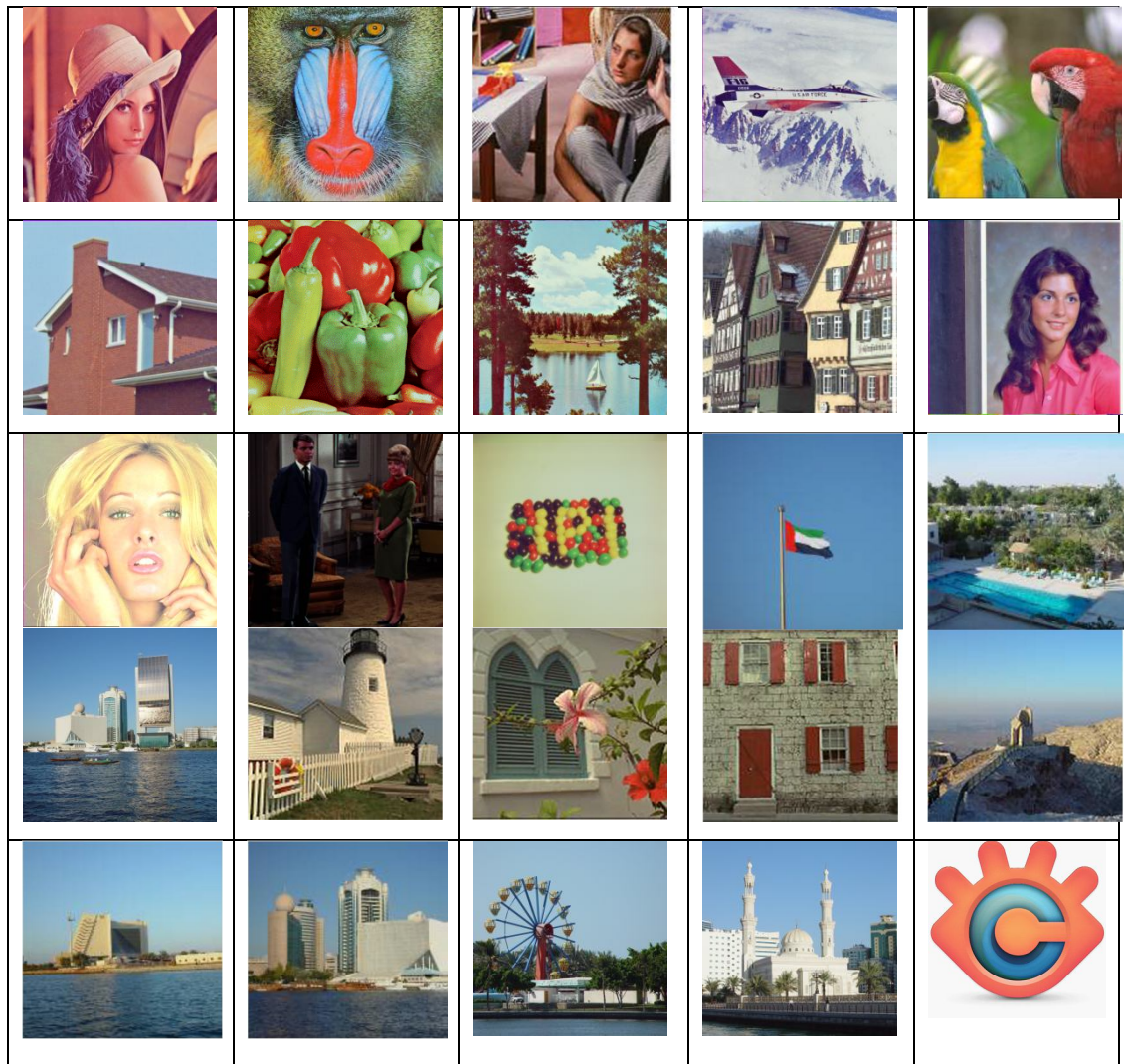


Figure 4.1: Host colour images



Figure 4.2: Host grey-scale images

4.3 DWT Embedding for Grey Images

The proposed embedding algorithm does not need the original host image in order to extract the watermark because it is blind. The binary watermark information is embedded in the LL (Low Low frequency) sub-band coefficients of the DWT-domain. The rationale behind choosing the LL area for the embedding process is because other areas might be affected or discarded in some image processing such as JPEG compression. Moreover, if these coefficients have been manipulated it will lead to severe image degradation before the watermark will be destroyed. In order to increase the robustness of the watermark the multi embedding process is done for many copies of the binary watermark information in the host image. The binary watermark information is converted to a vector format. The shuffle process is implemented on each copy of the watermark information before being embedded by shifting the vector of the binary

watermark information. The shuffle process is required to minimize the spatial correlation between the watermark and the host image. The mobile number with its international code is used as watermark information since it is a unique number.

4.3.1 Proposed DWT Robust Image Watermark Algorithm

The proposed watermarking scheme uses a block based wavelet algorithm to embed the binary watermark into the colour host image. The wavelet transformation is applied and divides the components into four parts LL (low low frequencies), LH (low high frequency), HL (high low frequencies) and HH (high high frequencies). Since small high frequency components may be discarded in some image processing operation such as JPEG compression, the very low frequency components of the grey host image will be utilized during the watermark embedding. Only one coefficient will be used in each 8×8 block for embedding.

4.3.2 The Embedding Process

The embedding process can be described as follows:

1. The host image will be divided into 8×8 blocks in the spatial domain then each block will be converted into the DWT domain. This will result in 4 sub blocks, each block has a 4×4 coefficients. These sub blocks are: Low Low frequency coefficients (LL), Low High coefficients (LH), High Low coefficients (HL) and High High coefficients (HH). Assume that $f(i,j)$ represents the pixel of the grey-scale image and [3]:

$$F_k(u, v) = \text{DWT}\{f_k(i, j)\}, \quad 1 \leq k \leq N_{HB} \quad (4.1)$$

where:

N_{HB} is 8 bits per block.

2. The watermarking information used is the mobile number including the international code. The mobile number across the world would be a unique number if we add the international code to it. The sums of the 14 digits (2 digits) were added at the end of the mobile number making it 16 digits. The 2 decimal digits will be used as a checking parameter for the correct number after extracting it at the receiver side.
3. The watermarking information need to be in binary forms. Therefore, each decimal number is converted into 4 bits using BCD code. Therefore the watermarking information will be 64 bits.
4. A secret key has been used to scramble the binary watermark digits randomly. The scramble process is important to reduce the correlation between the host image and the embedded watermark.
5. Each bit of the watermarking information is embedded into one of the LL sub bands coefficients (16 coefficients) of the transformed host image. A Discrete Wavelet Coefficient Selection (DWCS) process is applied in order to increase the invisibility qualities. The aim of this process is to find the coefficients with the maximum magnitude among the LL sub band coefficients. A flow chart of the DWCS process is explained in figure 4.3. The advantages of using DWCS

process are to increase the security and decrease the visual changes on the watermarked images.

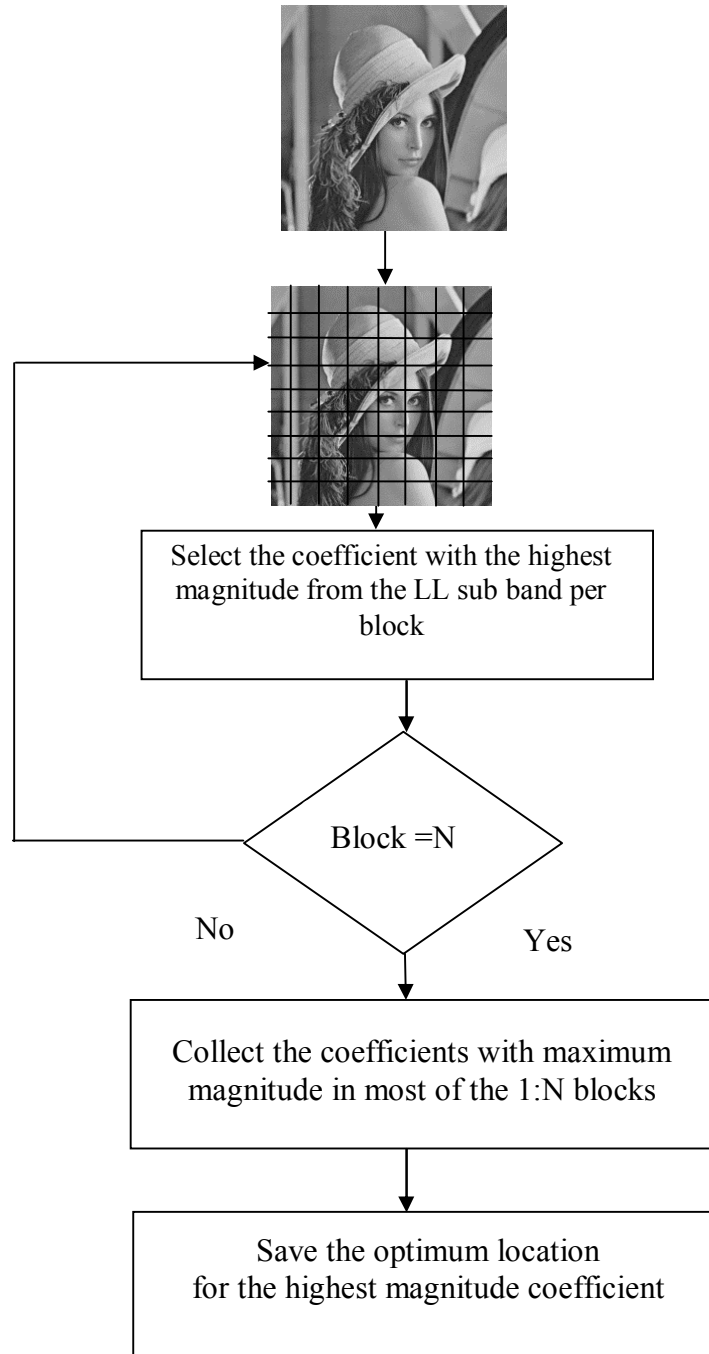
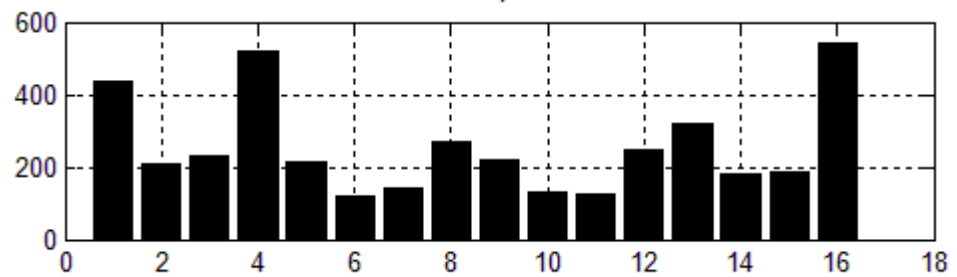
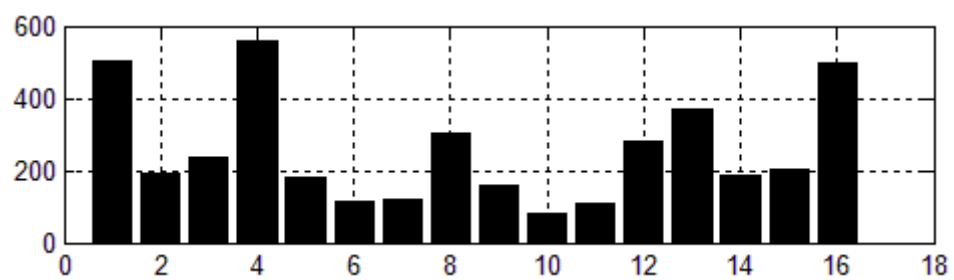


Figure 4.3: DWCS process

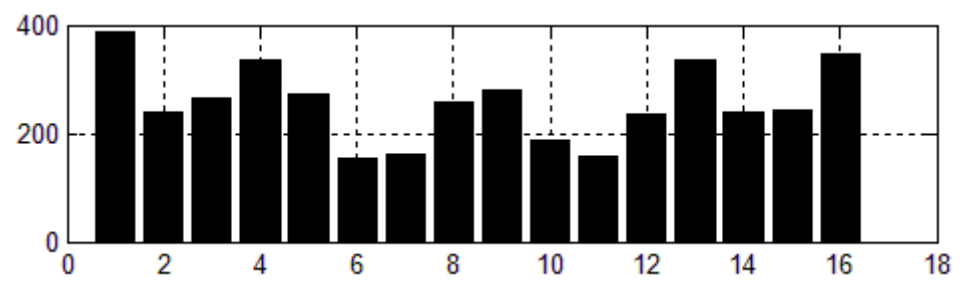
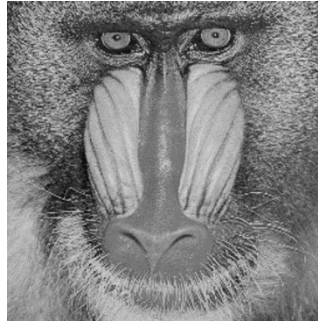
The DWCS is tested by different grey images. The following charts explain the process of DWCS for different images.



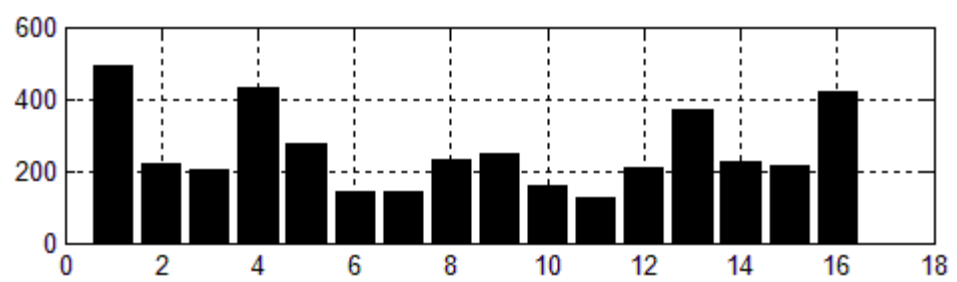
a. Lena grey chart (the highest coefficient is 16 (4,4)).



b. Pepper grey chart (the highest coefficient is 4 (1,4)).



c. Baboon grey chart (the highest coefficient is 1(1,1))



d. Pirate grey chart (the highest coefficient is 1(1,1))

6. The watermarking information will be repeated several times because the size of the image is much bigger than the 64 bits watermark. This process increased the robustness of the proposed algorithm. The bit embedding equation can be defined as follows :

$$\begin{aligned}
 & \text{if}(u,v) = 1 \quad \text{then} \\
 & \quad F_k = \begin{pmatrix} \Delta Q_e\left(\frac{F_k(u,v)}{\Delta}\right) & x,y \in H_k & 1 \leq k \leq N_{HB} \\ F_k(u,v) & x,y \notin H_k & 1 \leq k \leq N_{HB} \end{pmatrix} \quad (4.2) \\
 & \text{if}(u,v) = 0 \quad \text{then}
 \end{aligned}$$

$$Fk = \begin{pmatrix} \Delta Q_o\left(\frac{F_k(u,v)}{\Delta}\right) & x,y \in H_k & 1 \leq k \leq N_{HB} \\ F_k(u,v) & x,y \notin H_k & 1 \leq k \leq N_{HB} \end{pmatrix} \quad (4.3)$$

where

Q_e is the quantization to the nearest even number

Q_o is the quantization to the nearest odd number

Δ is a scaling quantity and it is also the quantization step used to quantize either to an even or odd number.

7. The shuffling process will be used [1] to improve the robustness against vertical cropping.
8. The watermarked host image is produced by using the inverse DWT transformation.

$$f_k(i,j) = IDWT\{Fk(u,v)\}, \quad 1 \leq k \leq N_{HB} \quad (4.4)$$

The embedding process is shown in figure 4.4.

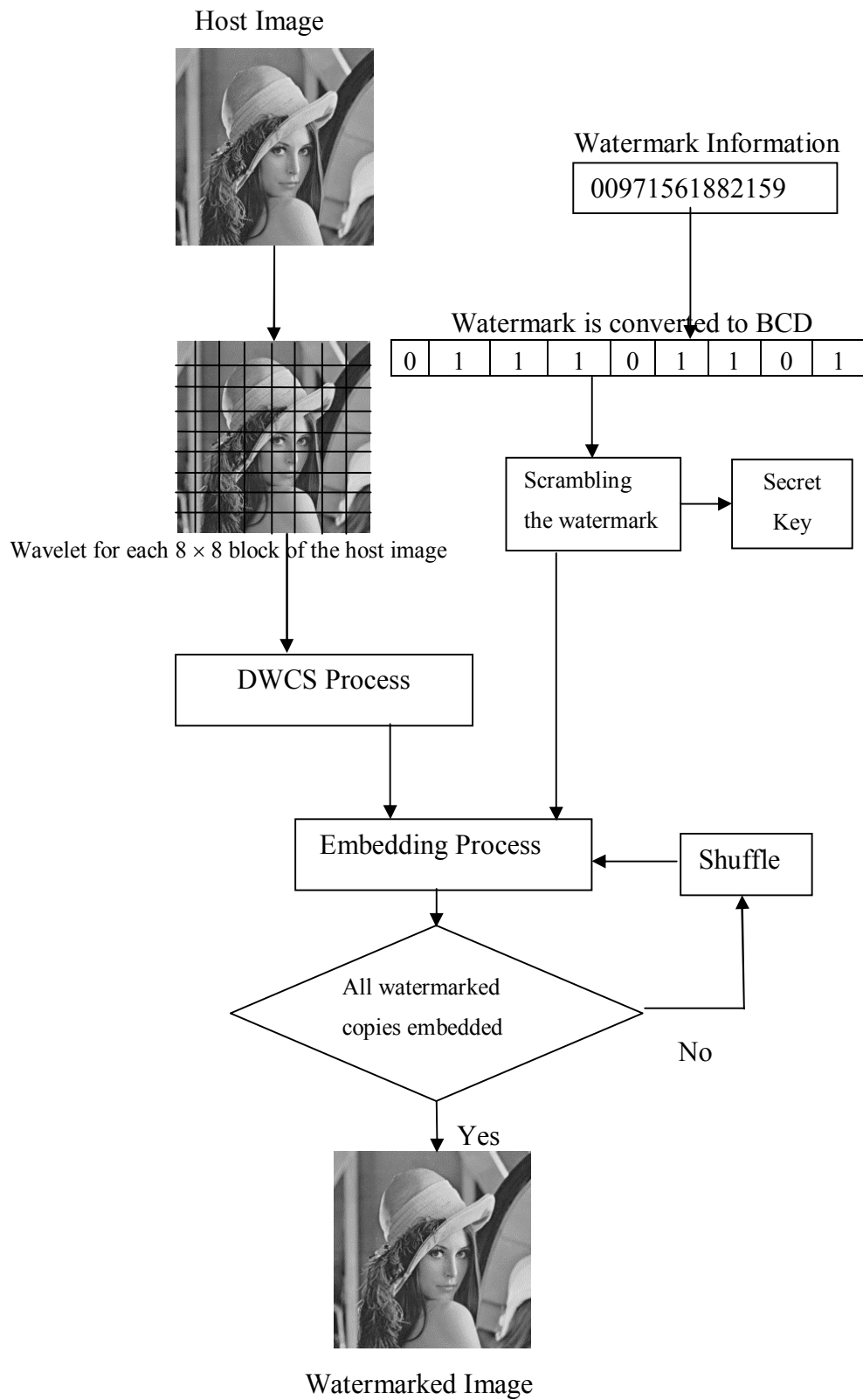


Figure 4.4: Flow chart of the embedding process.

4.3.3 The Extraction Process

At the receiver side, the watermarked image is divided into 8x8 blocks. Each block is converted into the DWT domain. The recovery process is the inverse of the embedding process. Each predefined frequency coefficient is quantized by Δ and rounded to the nearest integer. The formula which is used for extracting the embedded bits is defined as follows:

$$\begin{aligned} \text{If } Q\left(\frac{F_k(x,y)}{\Delta}\right) \text{ odd then } w(i,j) &= 0 \\ \text{If } Q\left(\frac{F_k(x,y)}{\Delta}\right) \text{ even then } w(i,j) &= 1 \end{aligned} \quad (4.5)$$

where:

Q is rounded to the nearest integer

Δ is the same parameter which has been used in the embedding process.

A flow chart of the extraction process is shown in Figure 4.5.

Each coefficient of the image that carries one bit of the embedded watermarks can be extracted by using the above method. These extracted bits will create the embedded watermarks information $w(i,j)$. The watermarking can be obtained by implementing the reverse shuffling process. The same secret key used in the initial scrambling operation will be used. The scrambled watermarks are descrambled to obtain the original watermarks. In the extraction process there is no need for the original image. The check sum will be used to discard the wrong extracted numbers. The recovered mobile number with the correct check sum is averaged (explain about averaging)? to get the resultant extracted watermark.

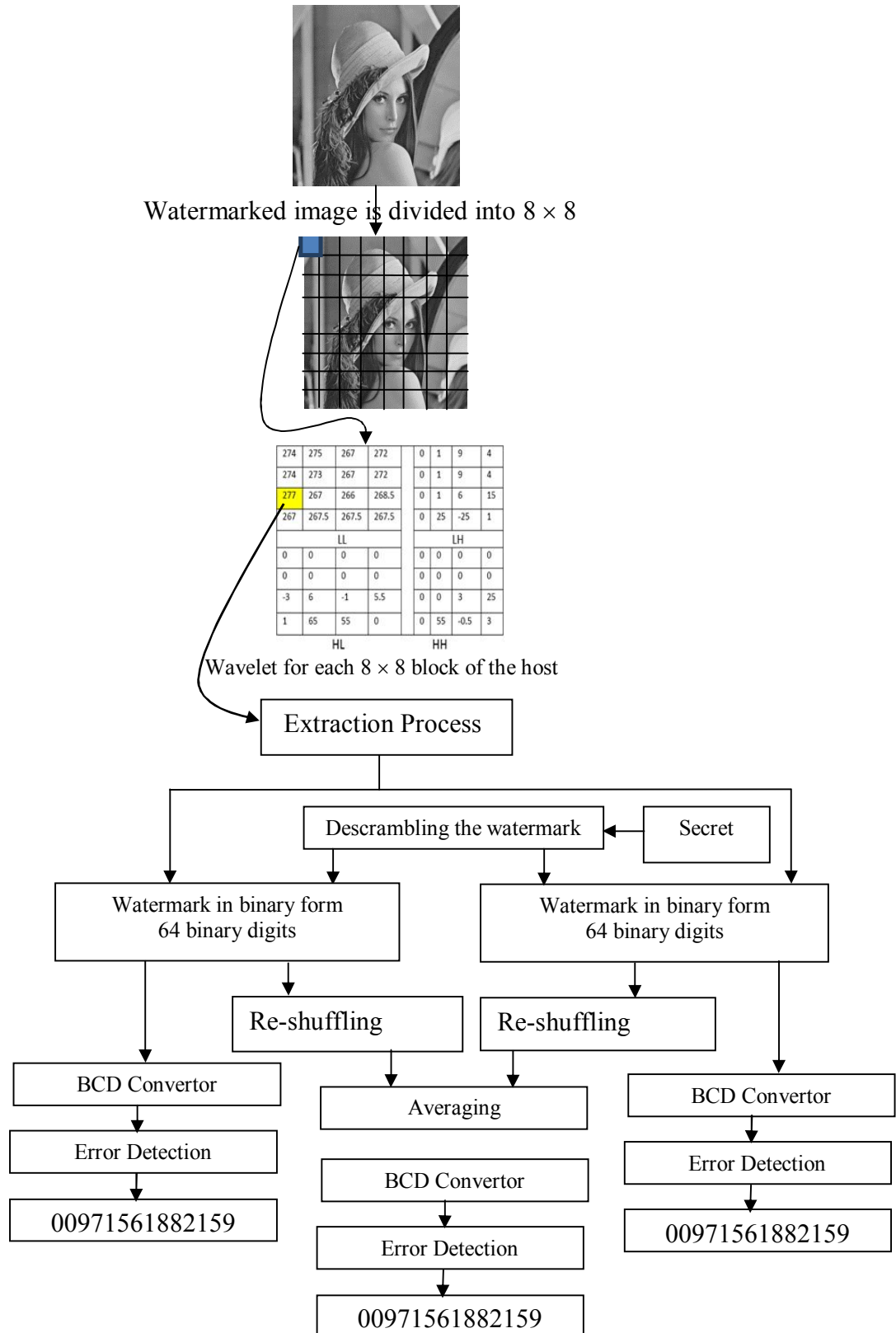


Figure 4.5: Flow chart of the extraction process.

4.3.4 Results

This algorithm is tested using different grey images of size 512×512 with 8 bits per pixel and different watermarking information (different mobile numbers). Test grey images are “Lena”, “Pepper” and “Baboon”. The watermarking information is a mobile number with international code. The techniques that are used to evaluate the perceptual invisibility of the watermarked image are PSNR and SSIM [4]. Stirmark software package is used to apply several attacks on the watermarked image to assess the robustness of the algorithm.

Table 4.1 illustrates the perceptual invisibility of the host image and the watermarked image at different embedding strengths. The PSNR values between the watermarked and original images using the phone number as the watermark information are varied between 53 dB and 39 dB for watermarking strengths $\Delta = 8$ and $\Delta = 40$ respectively. It is clear that the distortion caused to the images is imperceptible even with high values of Δ .

The SSIM is another technique which is used to evaluate the distortion caused to the image by the watermarking process [4]. Table 4.2 shows the SSIM between the host image and the watermarked image. The higher the SSIM percentage is, the larger the similarity between the compared images. The SSIM is very good and values higher the 0.985 were achieved when the Δ is around 20.

In order to assess the robustness of the proposed algorithm, various common signal processing and geometric attacks by using StirMark software package are applied to the

watermarked image. The similarity between the original and extracted watermark can be measured by using Normalized Correlation Coefficient (NCC) as shown in Table 4.3 and. The algorithm survived 3x3 and 5x5 low-pass, 3x3 wiener, 3x3 median filtering, cropping up to 80 % vertically and 48 % horizontally, high JPEG compression up to 20 and Gaussian and salt and pepper noise, scale 0.4 and 2 .

Table 4.1: PSNR with different grey images

Image	Lena	Pepper	Baboon
PSNR at $\Delta = 8$	52.722	52.815	52.838
PSNR at $\Delta = 14$	48.125	48.088	47.962
PSNR at $\Delta = 16$	46.844	46.900	46.761
PSNR at $\Delta = 20$	44.902	45.090	44.910
PSNR at $\Delta = 24$	43.267	43.438	43.324
PSNR at $\Delta = 30$	41.381	41.400	41.361
PSNR at $\Delta = 34$	40.373	40.213	40.357
PSNR at $\Delta = 40$	38.974	38.948	38.975

Table 4.2: SSIM with different grey images

Image	Lena	Pepper	Baboon
SSIM at $\Delta = 8$	0.997	0.998	0.999
SSIM at $\Delta = 14$	0.993	0.993	0.997
SSIM at $\Delta = 16$	0.991	0.991	0.996
SSIM at $\Delta = 20$	0.986	0.987	0.994
SSIM at $\Delta = 24$	0.980	0.981	0.991
SSIM at $\Delta = 30$	0.970	0.971	0.986
SSIM at $\Delta = 34$	0.963	0.962	0.984
SSIM at $\Delta = 40$	0.952	0.952	0.979

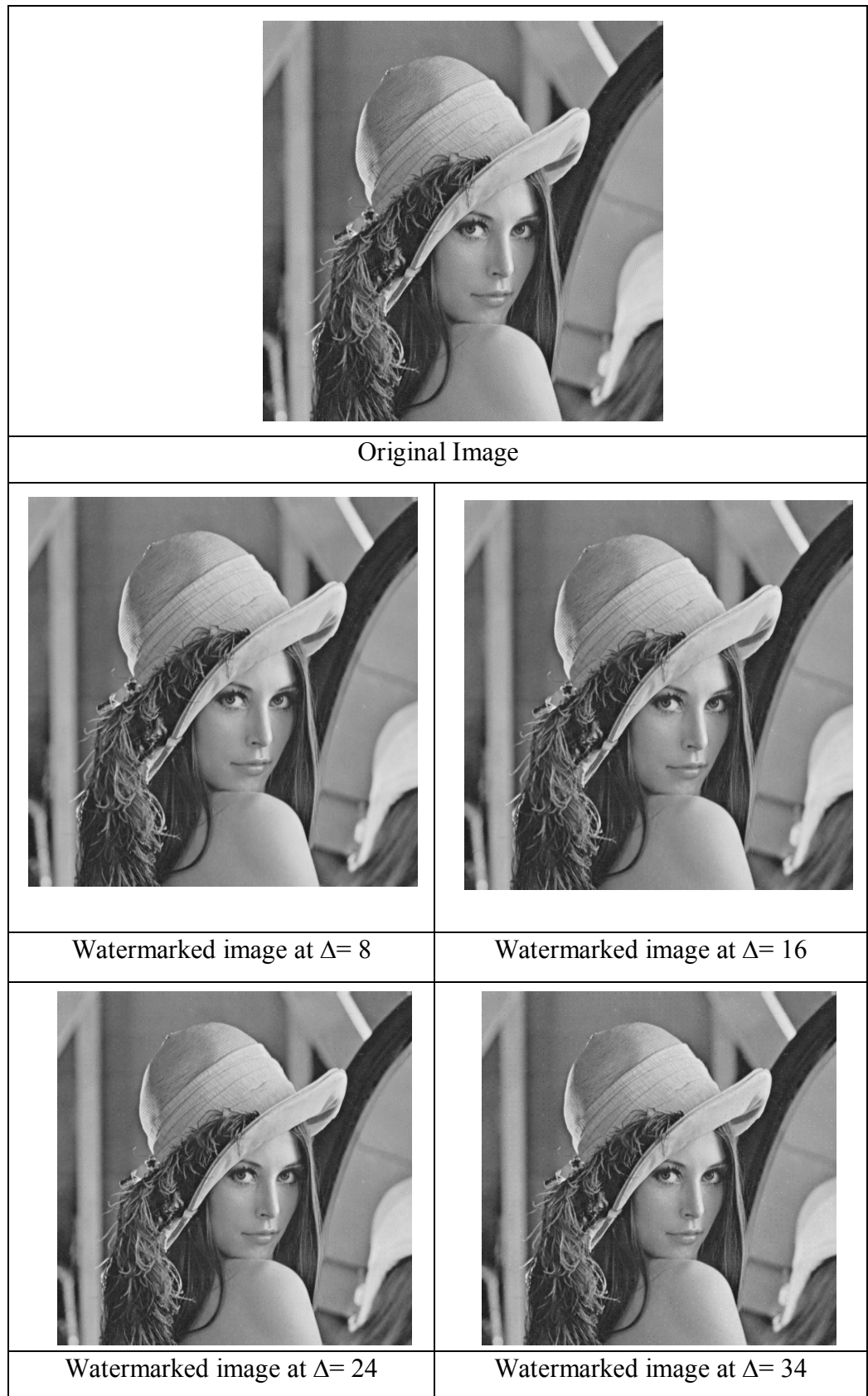


Figure 4.6: Original Lena and watermarked Lena images with different strengths

Table 4.3: The Normalized Correlation Coefficient (NCC) for Lena image with different attacks, at $\Delta=16$

Attacks	NCC	Attacks	NCC
Cropping 50% V	1	Low pass 3×3	1
Cropping 70% V	1	Low pass 5×5	1
Cropping 50% H	1	Wiener 3×3	1
Cropping 70% H	1	Wiener 5×5	1
Gaussian noise m=0, v=0.002	1	Median 3×3	1
Gaussian noise m=0, v=0.003	1	Median 5×5	0
S&P noise, d=0.02+ Median 3×3	1	JPEG 50	1
S&P noise, d=0.05+ Median 3×3	1	JPEG 25	1
Scale 2	1	Scale 0.4	1
Stirmark_AFFINE_3	1	Stirmark_CONV_1	0
Stirmark_AFFINE_8	0	Stirmark_RML_10	1
Stirmark_ROTSCALE_0.25	1	Stirmark_RML_50	1
Stirmark_ROT_-0.25	1	Stirmark_RML_100	1
Stirmark_ROTSCALE_-0.5	0	Stirmark_SS_1	1
Stirmark_ROT_0.25	1	Stirmark_SS_2	1
Stirmark_ROT_-0.5	0	Stirmark_SS_3	1
Stirmark_ROTROP_-0.5	0	Stirmark_ROTROP_0.25	1

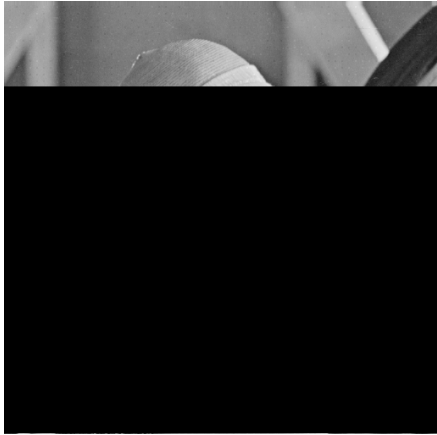





	
Cropping attack80 % H	Gaussian noise $m=0$, $v=0.003$
	
S&P noise attack, $d=0.02+$ Median 3×3	Contrast enhancements attack intensity=0.3, 0.9
	
JPEG 20 attack	Wiener filter attack 5×5

Figure 4.7: several attacks for watermarked image

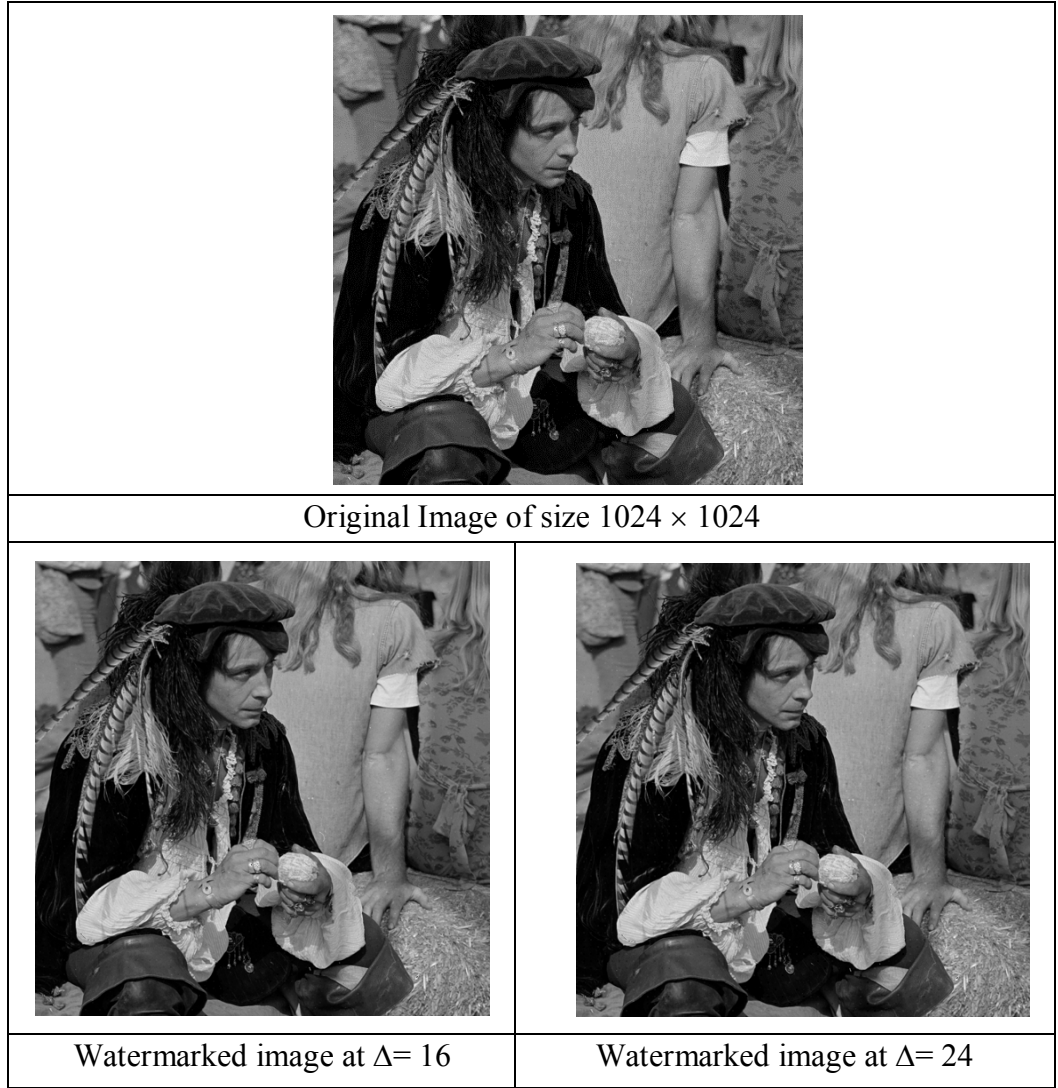


Figure 4.8: Original and watermarked images with high resolution.

4.4 DWT Embedding for Colour Images.

The proposed algorithm will be extended to colour images by using the DWT transform. The binary information watermark will be embedded in the LL sub band of the transformed host image. The watermark information is scrambled by a secret key before embedding into the host image. The watermark information is embedded many times. However, the shuffle process is applied on these copies before embedded in the host image.

4.4.1 Embedding and Extraction for Green Channel

The proposed algorithm uses a block based wavelet algorithm to embed the binary watermark into the colour host image. Colour images can be separated into three components R, G and B. In this algorithm the watermark information will be embedded in the green component. The green channel has been chosen for embedding process because it showed an excellent invisibility qualities and more robustness compared to the blue and red channel [5]. The green channel will be divided into blocks (8×8 block) in the spatial domain. The UAE mobile number with the international code (14 decimal digits) is used as the watermarking information. Binary coded decimal conversion is implemented to the 16 digits of the watermark information in order to convert the information into binary type. The scrambling with the secret key is applied on the binary watermarking information. The host image is transformed to the wavelet domain by using DWT transformation. The DWSC process is applied to choose one coefficient with the highest magnitude of the LL sub band in the transformed host image for embedding process. The watermark information size is small compared to the host image size. Therefore, many copies will be embedded in order to increase the robustness of the watermark. Alongside this the shuffle operation is used for every copy of the watermarking before the embedding to the host image. Finally the green channel is inversed to the spatial domain by using IDWT and combined it with the Red and Blue channels to get RGB watermarked colour image. The flow chart illustrating the embedding process is shown in figure 4.9.

On the other hand, the extraction process of the watermark information doesn't need the original host image because it is a blind type algorithm. The colour watermarked image at the decoder side is separated into RGB components. The G component is divided

into 8x8 blocks. Each block is converted into the DWT domain. The recovery process is the inverse of the embedding process as illustrated in figure 4.10. The secret key will be used in the reshuffle process to retrieve the watermark information. The formula which is used for the extraction the embedded bits is 4.5.

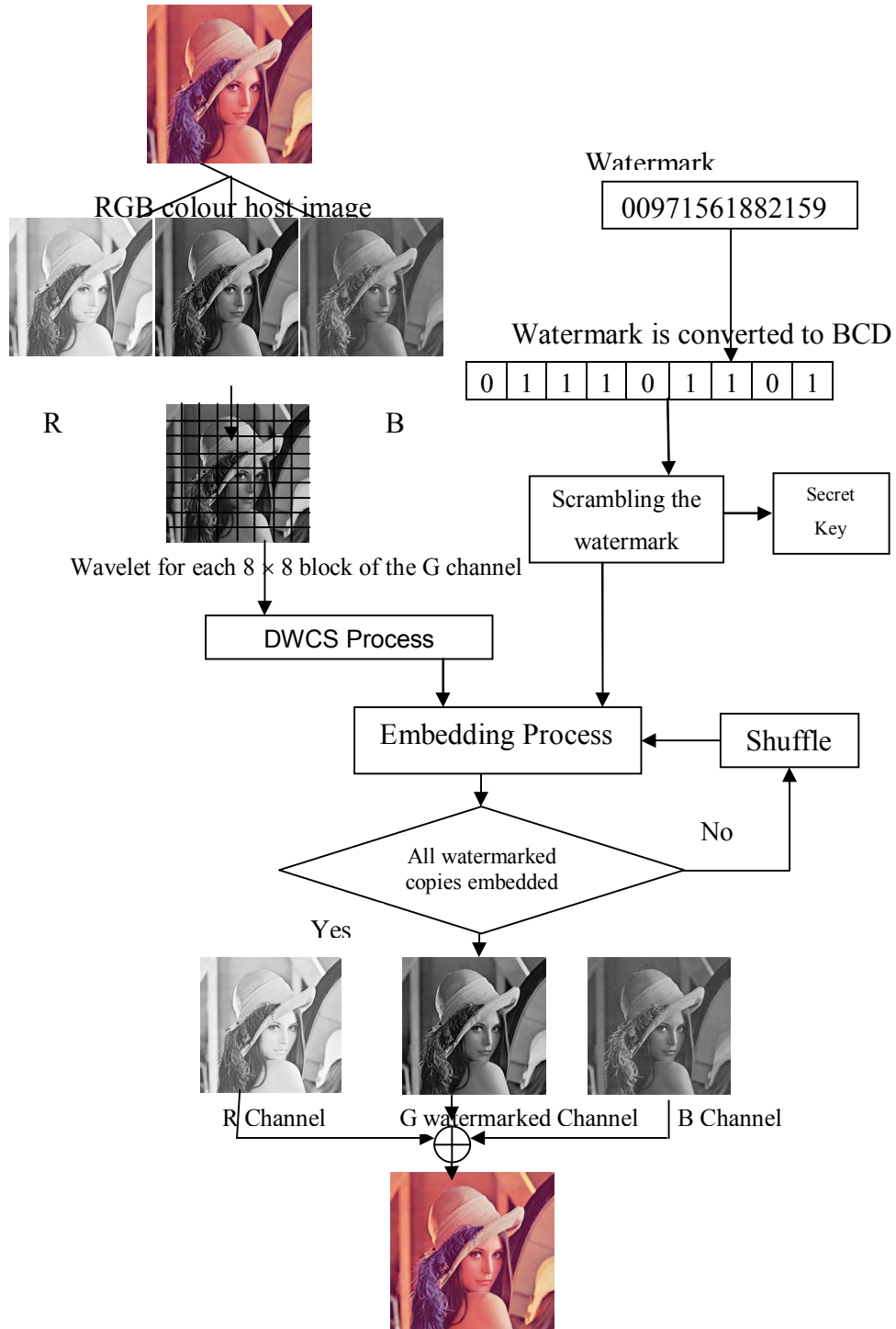


Figure 4.9: A flow chart of the embedding in the green channel

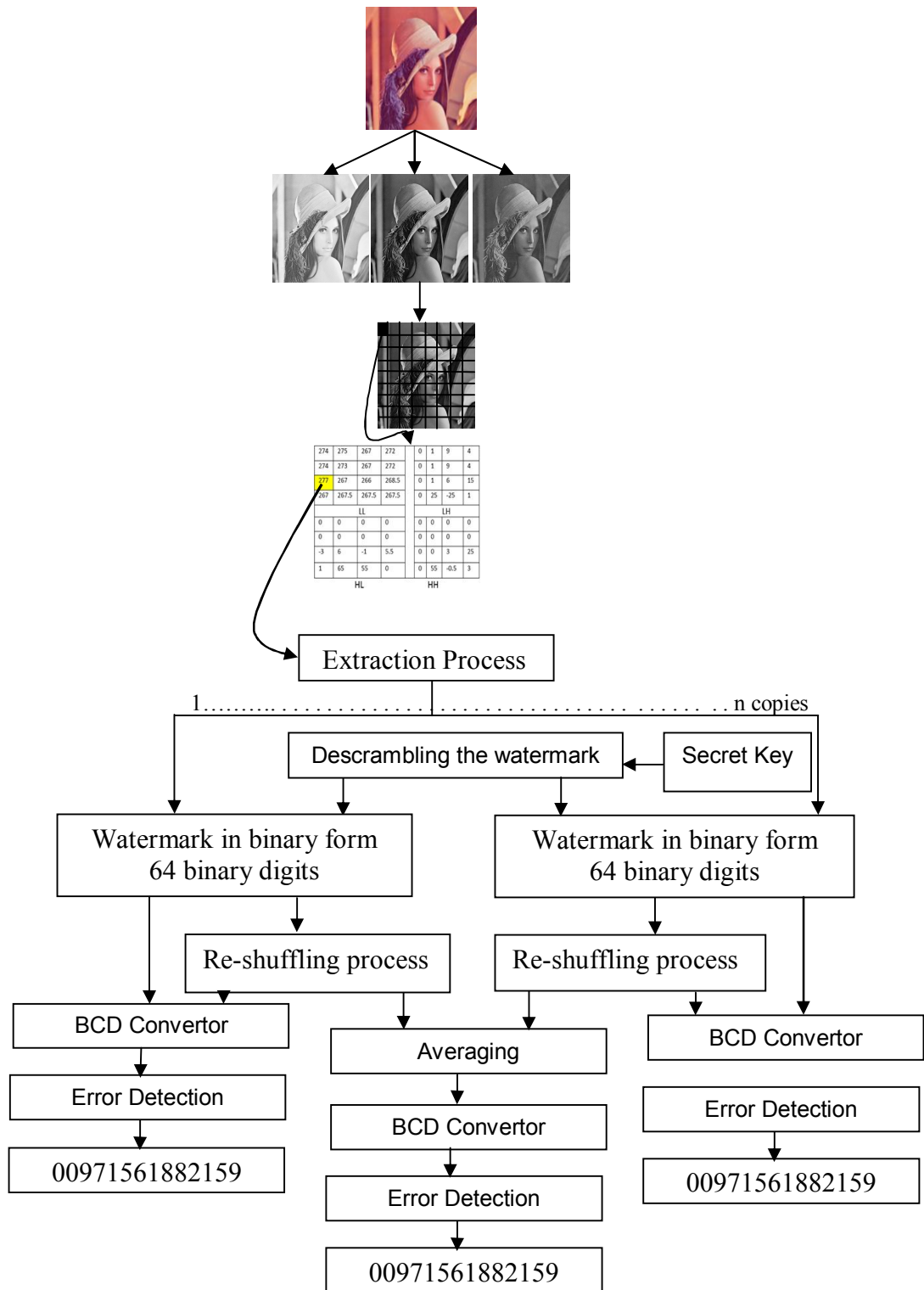


Figure 4.10: A flow chart of the extraction process.

4.4.2 Result of Green Channel Algorithm

Different colour images of size 512×512 with 24 bit/pixel have been used to test the proposed algorithm. There are two techniques used to assess the distortion caused to the image by watermarking process. PSNR between the original image and the watermarked image is the first technique used to evaluate the perceptual invisibility of the proposed algorithm at different embedding strength as shown in Table 4.4. The average PSNR values between the watermarked and original images using the phone number as the watermark information are shown in table 4.4. The PSNR is 57.5 dB for the original “Lena” and the watermarked image when the embedding strength is 8. However, it was reduced to 43.7 dB for embedding strength 40.

The distortion caused by the watermarking process can be evaluated also by using the second technique of assessment (SSIM). If the SSIM achieves a higher value (near 1), the similarity between the watermarked image and the original image is better. The SSIM at different embedding strength (Δ) is shown in Table 4.5. The perceptual quality at different strength has been examined by using the test images “Lena”, “Pepper” and “Baboon”. Even when the high value of the embedding strength is used ($\Delta = 40$), the distortion caused to the image is still imperceptible as illustrated in Table 4.5. The SSIM is very good and higher than 0.98.

To examine the robustness of the proposed algorithm, several common signal processing and geometric attacks are applied to the watermarked images. Moreover, for the same purpose the Stirmark software package is being used. The similarity between the original and extracted watermark can be measured by using the Normalized

Correlation Coefficient (NCC) as shown in Table 4.6. The watermark (mobile numbers) survived against many attacks such as: 3x3 and 5x5 low-pass , 3x3 wiener and median filtering filtering, cropping up to 80 % horizontally and 48 % vertically, salt and pepper noise, $d=0.02+$ median 3×3 , contrast enhancements intensity=0.3, 0.9 and rescale from 0.4 up to 2 factor. If the NCC value is less than one it indicates that the algorithm failed to restore the watermark.

In figure 4.11, the original colour Lena image and several watermarked images with different embedding strength are presented. It is clear that the distortion caused by the watermark is still imperceptible.

The proposed algorithm survived against different attacks. Figure 4.12 illustrates different kind of attacks on the watermarked image. Finally, high resolution images (large sizes images) have been used to evaluate the performance of the proposed algorithm as shown in Table 4.7

Table 4.4: PSNR with different colour images (green channel embedding)

Image	Lena	Pepper	Baboon
PSNR at $\Delta = 8$	57.541	57.346	57.532
PSNR at $\Delta = 12$	54.186	54.027	54.087
PSNR at $\Delta = 16$	51.554	51.540	51.474
PSNR at $\Delta = 20$	49.646	49.551	49.599
PSNR at $\Delta = 24$	48.075	48.036	48.023
PSNR at $\Delta = 30$	46.175	45.999	46.312
PSNR at $\Delta = 34$	44.959	45.057	45.101
PSNR at $\Delta = 40$	43.766	43.483	43.686

Table 4.5: SSIM with different colour images(green channel embedding)

Image	Lena	Pepper	Baboon
SSIM at $\Delta = 8$	0.999	0.999	1.000
SSIM at $\Delta = 12$	0.999	0.998	1.000
SSIM at $\Delta = 16$	0.997	0.997	0.999
SSIM at $\Delta = 20$	0.996	0.995	0.999
SSIM at $\Delta = 24$	0.994	0.993	0.998
SSIM at $\Delta = 30$	0.991	0.990	0.997
SSIM at $\Delta = 34$	0.989	0.988	0.996
SSIM at $\Delta = 40$	0.986	0.984	0.995

Table 4.6: The Normalized Correlation Coefficient (NCC) for Colour Lena image with different attacks (green channel), at $\Delta = 24$

Attacks	NCC	Attacks	NCC
Cropping 50% V	1	Low pass 3×3	1
Cropping 70% V	1	Low pass 5×5	1
Cropping 50% H	1	Wiener 3×3	1
Cropping 70% H	1	Wiener 5×5	1
Gaussian noise m=0, v=0.002	1	Median 3×3	1
Gaussian noise m=0, v=0.001	1	Median 5×5	0
S&P noise, d=0.02+ Median 3×3	1	JPEG 50	1
S&P noise, d=0.05+ Median 3×3	1	JPEG 25	1
Scale 2	1	Scale 0.4	1
Stirmark_AFFINE_3	1	Stirmark_CONV_1	0
Stirmark_AFFINE_8	0	Stirmark_RML_10	1
Stirmark_ROTSCALE_0.25	1	Stirmark_RML_50	1
Stirmark_ROT_-0.25	1	Stirmark_RML_100	1
Stirmark_ROTSCALE_-0.5	0	Stirmark_SS_1	1
Stirmark_ROT_0.25	1	Stirmark_SS_2	1
Stirmark_ROT_-0.5	0	Stirmark_SS_3	1
Stirmark_ROTSCROP_-0.5	0	Stirmark_ROTSCROP_0.25	1



Figure 4.11: Original Lena with different watermark strength (green channel).

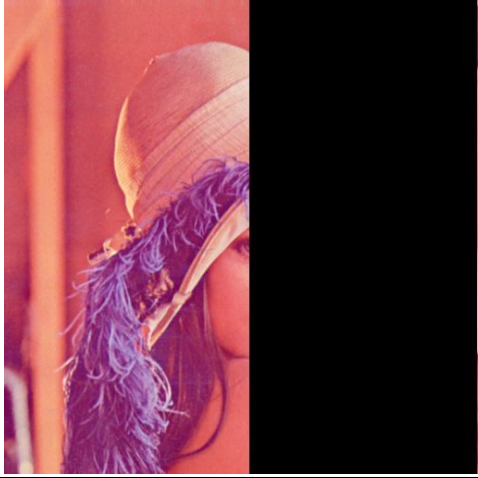
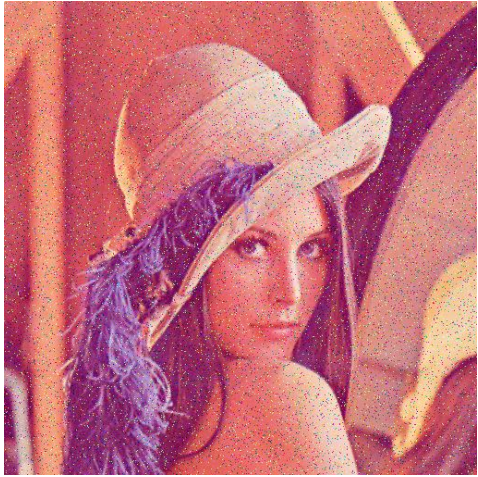
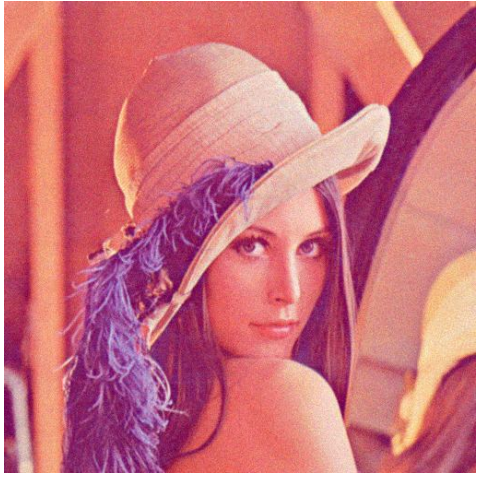





	
Cropping 48% V	Wiener filter 3×3
	
S&P noise attack, $d=0.05$ + Median 3×3	Gaussian noise $m=0$, $v=0.002$
	
15 % JPEG attack	Median filter attack 5× 5

Figure 4.12: Several attacks for colour watermarked image (green channel)

Table 4.7: High resolution colour images examined by the proposed algorithm for green channel

			
Original Image of size 1024×1024			
			
Watermarked image at $\Delta=24$		Watermarked image at $\Delta=16$	
PSNR	48.12	PSNR	51.657
SSIM	0.9937	SSIM	0.9971
Attacks	NCC	Attacks	NCC
Cropping 50 V	1	Cropping 50 % V	1
Low pass 3×3	1	Low pass 3×3	1
Median 3×3	1	Median 3×3	1
Wiener 3×3	1	Wiener 3×3	1
Gaussian noise $m=0$, $v=0.002$	1	Gaussian noise $m=0$, $v=0.002$	1
S&P noise, $d=0.02+$ Median 3×3	1	S&P noise, $d=0.02+$ Median 3×3	1

4.4.3 Y Channel Embedding and Extraction

There is another way to represent the colour with Y Cb Cr planes. Y component is the brightness (luma) while, the Cb and Cr represent the colour information. The Y-channel can be used as an image in grayscale [6]. Therefore, it has been chosen for the embedding process. The embedding process in the Y channel for the proposed algorithm starts by converting the RGB colour to the Y Cb Cr plane. Y Cb Cr Colour images can be separated into three components Y, Cb and Cr. The watermarking information will be embedded into the Y channel by using the equation 4.2 and 4.3. The watermarked Y channel will be added to Cb Cr in order to convert it to the RGB form. However, all the aforementioned watermarking are illustrated graphically in the diagram in Figure 4.13.

At the receiver side, the host image is not required for the extraction process, because the proposed algorithm is blind type. Basically the recovery process is the inverse of the embedding process as illustrated in figure 4.14. By using the same secret key and implementing the reshuffle process, the watermark can be recovered. The number of copies which are embedded several times into the host image depend on the size of the watermarking information and the size of the host image.

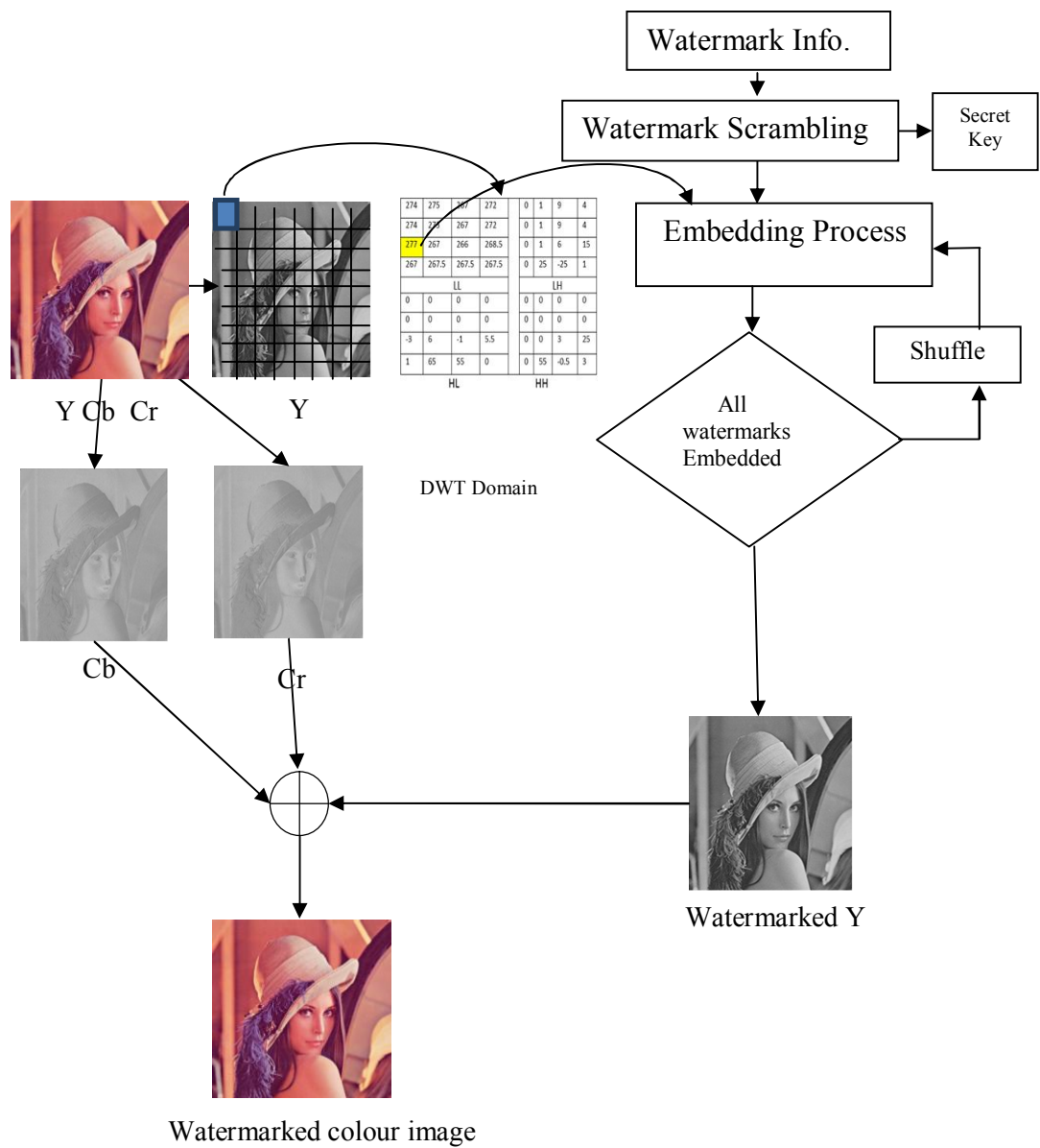


Figure 4.13: A flow chart of the embedding Y channel process

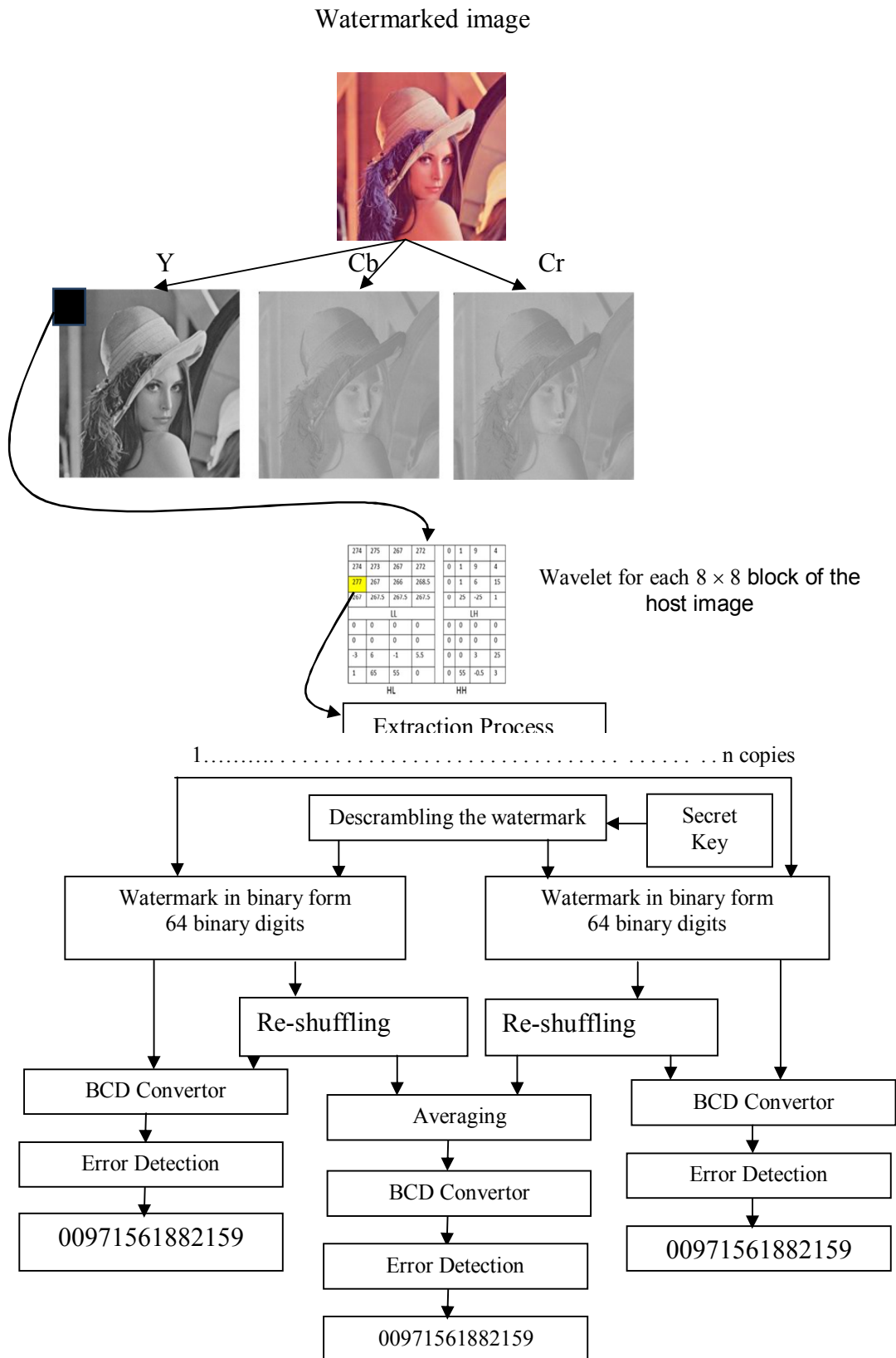


Figure 4.14: A flow chart of the extraction process.

4.4.4 Result of Y Channel Algorithm

The PSNR values were calculated with different embedding strengths. This is used to examine the perceptual invisibility of the proposed algorithm. The average values between the watermarked and host images (PSNR) by using the mobile phone number as watermarking information are as shown in Table 4.8. The PSNR varied from 57.5 dB to 44 dB with $\Delta=8$ and $\Delta=40$ respectively.

SSIM is another technique which is used to evaluate the similarity between the original image and the watermarked image. The proposed algorithm is assessed by using different colour images such as: “Lena”, “Pepper” and “Baboon”. In table 4.10, the SSIM measures the distortion caused by the watermarking process at different embedding strengths. It is clearly seen that in table 4.9, the SSIM is very good and higher than 0.98. Even though, high values of Δ are used but still the distortion caused by the watermarking to the images is imperceptible as shown in figure 4.15. Different watermarked images with different embedding strength and the host image are illustrated in figure 4.16.

The similarity between the original watermark and the extracted one can be measured by using the Normalized Correlation Coefficient (NCC). Various attacks were applied to the watermarked image to evaluate the robustness of the proposed algorithm. The StirMark software package was used for this purpose. Table 4.10. demonstrate the NCC when several attacks are applied on the watermarked image with different embedding strength. The algorithm showed robustness against several attacks such as cropping vertical and horizontal, low pass, wiener and median filtering, salt and pepper noise, Gaussian noise and high JPEG compression. Figure 4.15 shows several watermarked

images with different embedding strength and the host image as well. Moreover, figure 4.16 illustrates several watermarked image after been attacked by different types of attacks. Finally, the high resolution images were tested and the results are as shown in Table 4.11.

Table 4.8: PSNR with different colour images (Y channel embedding)

Image	Lena	Pepper	Baboon
PSNR at $\Delta = 8$	57.438	57.654	57.437
PSNR at $\Delta = 12$	54.156	54.120	54.232
PSNR at $\Delta = 14$	52.780	52.801	52.825
PSNR at $\Delta = 16$	51.813	51.543	51.512
PSNR at $\Delta = 20$	49.578	49.673	49.645
PSNR at $\Delta = 24$	48.144	48.194	48.082
PSNR at $\Delta = 30$	46.076	46.226	46.097
PSNR at $\Delta = 34$	45.129	44.964	44.953
PSNR at $\Delta = 40$	43.941	43.676	43.667

Table 4.9: SSIM with different colour images (Y channel embedding)

Image	Lena	Pepper	Baboon
SSIM at $\Delta = 8$	0.999	0.999	1.000
SSIM at $\Delta = 12$	0.998	0.998	0.999
SSIM at $\Delta = 14$	0.997	0.997	0.999
SSIM at $\Delta = 16$	0.997	0.997	0.999
SSIM at $\Delta = 20$	0.995	0.995	0.998
SSIM at $\Delta = 24$	0.993	0.993	0.997
SSIM at $\Delta = 30$	0.989	0.989	0.996
SSIM at $\Delta = 34$	0.987	0.986	0.995
SSIM at $\Delta = 40$	0.984	0.983	0.993

Table 4.10: The Normalized Correlation Coefficient (NCC) for Colour Lena image with different attacks (Y-channel), at $\Delta = 24$

Attacks	NCC	Attacks	NCC
Cropping 50% V	1	Low pass 3×3	1
Cropping 70% V	1	Low pass 5×5	1
Cropping 50% H	1	Wiener 3×3	1
Cropping 70% H	1	Wiener 5×5	1
Gaussian noise m=0, v=0.002	1	Median 3×3	1
Gaussian noise m=0, v=0.001	1	Median 5×5	0
S&P noise, d=0.02+ Median 3×3	1	JPEG 50	1
S&P noise, d=0.05+ Median 3×3	1	JPEG 25	1
Scale 2	1	Scale 0.4	1
Stirmark_AFFINE_3	1	Stirmark_CONV_1	0
Stirmark_AFFINE_8	0	Stirmark_RML_10	1
Stirmark_ROTSCALE_0.25	1	Stirmark_RML_50	1
Stirmark_ROT_-0.25	1	Stirmark_RML_100	1
Stirmark_ROTSCALE_-0.5	0	Stirmark_SS_1	1
Stirmark_ROT_0.25	1	Stirmark_SS_2	1
Stirmark_ROT_-0.5	0	Stirmark_SS_3	1
Stirmark_ROTROP_-0.5	0	Stirmark_ROTROP_0.25	1

	
Original image	
	
Watermarked image at $\Delta= 12$	Watermarked image at $\Delta= 16$
	
Watermarked image at $\Delta= 24$	Watermarked image at $\Delta= 34$

Figure 4.15: Original Lena with different watermark strength (Y- channel)





	
Cropping 48% V	Wiener filter 3×3
	
S&P noise attack, $d=0.05$ + Median 3×3	Gaussian noise $m=0$, $v=0.002$
	
AFFINE_8 Stirmark	CONV_1 Stirmark

Figure 4.16: Several attacks for colour watermarked image (Y- channel)

Table 4.11: High resolution colour images examined by the proposed algorithm for Y-channel

			
Original Image of size 1024×1024			
			
Watermarked image at $\Delta=24$		Watermarked image at $\Delta=16$	
PSNR	47.8013	PSNR	52.0059
SSIM	0.9914	SSIM	0.9969
Attacks	NCC	Attacks	NCC
Cropping 50 V	1	Cropping 50 % V	1
Low pass 3×3	1	Low pass 3×3	1
Median 3×3	1	Median 3×3	1
Wiener 3×3	1	Wiener 3×3	1
Gaussian noise $m=0$, $v=0.002$	1	Gaussian noise $m=0$, $v=0.002$	1
S&P noise, $d=0.02+$ Median 3×3	1	S&P noise, $d=0.02+$ Median 3×3	1

4.5 Comparison with previous work

The proposed algorithm has been compared with other watermarking method reported in [7], [8], [9], [10] and [11]. The first comparison is the Normalised Correlation Coefficient between the previous method and the proposed in table 4.12. It is clearly shown that the extracted watermarking information after different types of attacks is exactly the same as the watermarking information at the transmitter side while the extracted watermarking information in [7], [8], [9], [10] and [11] could not survive against some attacks.

The PSNR is considered as a robustness factor in the second comparison. Table 4.13 shows the PSNR for the proposed algorithm and other methods algorithms. The proposed algorithm recorded higher PSNR compared to other methods algorithm under the sane conditions.

Finally, Table 4.14 explains the comparison between the proposed algorithm and other method based on SSIM. The proposed algorithm achieved almost the same SSIM of the other method.

Table 4.12: The Normalized Correlation Coefficient for Lena colour image at $\Delta = 24$

Attacks	Proposed Method	[8]	[10]	[11]
Cropping 50% V	1	0.739	0.97	0.999
Cropping 50% H	1	1	0.98	0.999
Cropping 75% H	1	1	1	1
Gaussian noise $m=0$, $v=0.002$	1	0.8	0.85	0.7801
S&P noise, $d=0.02$ + Median 3×3	1	1	0.99	0.9925
Scale 2	1	1	1	1
Low pass 3×3	1	1	0.99	0.981
Wiener 3×3	1	1	0.99	0.9931
Median 3×3	1	1	0.99	0.992
JPEG 50	1	1	0.99	1
JPEG 25	1	1	0.98	0.963
Scale 0.4	1	1	0.88	0.88

Table 4.13: The PSNR for Lena colour image with different Δ

	Proposed method	[7]	[8]	[9]
PSNR at $\Delta = 16$	51.813	44.2	51.440	38.5
PSNR at $\Delta = 24$	48.144	41.1	47.876	37.4
PSNR at $\Delta = 34$	45.129	38.2	44.798	35.2
PSNR at $\Delta = 40$	43.941	36.1	43.222	34.4

Table 4.14: The SSIM for Lena colour image with different Δ

	Proposed method	[7]	[9]
SSIM at $\Delta = 16$	0.997	0.998	0.997
SSIM at $\Delta = 24$	0.994	0.995	0.985
SSIM at $\Delta = 34$	0.989	0.990	0.975
SSIM at $\Delta = 40$	0.986	0.987	0.971

4.6 Final Remarks

In this chapter, robust algorithms for grey and colour images have been developed. The proposed algorithms have used DWT block based transformation. The developed algorithms showed resistivity against several attacks such as: cropping small degrees of rotation, additive noise, JPEG compression, scaling, filtering attacks and Stirmark attacks. The mobile number including the international code has been used as watermarking information rather than the traditional watermarking information. The embedding process has been taking place in the LL sub-band of the transformed host image. Only one bit in the LL sub-band has been used for embedding the watermark information. The developed algorithms are blind. The shuffle process has been applied to increase the robustness against cropping attacks. The PSNR for the proposed algorithms recorded high values. Two-level of DWT will be used in the next chapter

4.7 References

- [1] P. Devi and et al, "Reversible Image Authentication with Tamper Localization Based on Integer Wavelet Transform", *(IJCSIS) International Journal of Computer Science and Information Security*, vol. 6, No. 2, pp. 67–74, 2009.
- [2] "Kodak Images", in <http://r0k.us/graphics/kodak/>.
- [3] P. J. Fleet, *Discrete Wavelet Transformation*, New Jersey, A JOHN WILEY & SONS, INCC., 2007.
- [4] M. Kutter, F. Petitcolas, "A Fair Benchmark for Image Watermarking Systems", *Electronic Imaging '99. Security and Watermarking of Multimedia Contents*, Vol. 3657, pp. 1-14 , January, 1999.
- [5] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji and A. Tawfik, "A Novel Blind Watermarking Technique for Colour RGB Images in the DCT Domain Using

Green Channel ”, *Communications, Computers and Applications, MIC-CCA 2008. Mosharaka International Conference on*, pp. 26 - 31, August, 2009.

- [6] Q. Liu, “An Adaptive Blind Watermarking Algorithm for ColorImage”, *Telkominka*, Vol.11, No.1, pp. 302-309, January 2013.
- [7] I. Kong and C. Pun, “*Digital Image Watermarking with Blind detection for Copyright Verification* ”, IEEE computer society, 2008 Congress on Image and Signal Processing, Vol. 1, pp. 504-508, May 2008.
- [8] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji and A. Tawfik, “A New Watermarking Scheme For Colour Images Captured By Mobile Phone Cameras”, *IJCSNS International Journal of Computer Science and Network Security*, VOL.9 No.7, pp. 248 - 254, July 2009.
- [9] V. Sreejith, K. Sritith and R. Roy, “Robust Blind Digital Watermarking in Contourlet Domain”, *International Journal of Computer Application*, Vol. 58, No. 12, pp. 13 – 19, November, 2012.
- [10] A. Al Gindy, “A Frequency Domain adaptive Watermarking Algorithm for still Colour Images ”, *International Conference on Advances in Computational Tools for Engineering Application*, pp. 186- 191, September,2009.
- [11] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji and A. Tawfik, “Watermarking of Colour Images in the DCT Domain Using Y Channel”, *IEEE/ ACS International Conference on Computer Systems and Applications*, Morocco, pp. 1025 – 1028, 2009.

CHAPTER 5

Two-level DWT Robust Watermarking

5.1 Introduction

This chapter deals with a powerful robust watermarking algorithm by using two-level wavelet based algorithm. The aim of the algorithm is to design a unique technique that will verify the copyright of still colour images. The proposed algorithm uses a mobile phone number as a watermarking information with the international code. This algorithm is carried out using coefficients of the second level Low Low sub-bands of DWT. The offered algorithm embeds the watermark information in the Green channel of the RGB of the still colour image. The chapter covers grey images and colour images. The chapter also includes a comparison between the two-level DWT and the one-level algorithms.

5.2 Two-level DWT Watermarking Scheme for Grey Images

The proposed algorithm is blind and does not require the original host image in the receiver side during the watermarking information extraction. The embedding process will take place in the second level LL (Low Low) sub-bands coefficients of the DWT domain. The embedding coefficients are chosen to offer robustness against some image

processing on the watermarked image for example the JPEG compression attack is targeting the high frequency's coefficients [1]. In addition to that, any manipulation in the LL sub-bands will lead to severe image degradation and this will be obvious before the watermark is destroyed. The watermarking information is scrambled by using a secret key in order to make it a difficult task for attackers even though if they succeeded to extract the watermarking information from the watermarked image. The size of the digital watermarking information is small if it is compared to the size of the host image, which will offer the opportunity to embed the watermarking information more than once and this multi embedding process will increase the robustness of the algorithm. The shuffle process is applied to each copy of the digital watermarking information which will minimize the spatial correlation between the watermark and the host image [2].

5.2.1 Proposed 2-levels DWT Robust Grey Image Watermark Algorithm

The proposed algorithm is based on the two-level wavelet block based watermarking scheme to embed the digital watermarking information into the grey host image. The host image is divided into 16×16 block before the DWT first level is applied on each block. Therefore, each block in the spatial domain will be divided into four parts in the DWT domain; LL1 (low low frequencies), LH1 (low high frequency), HL1 (high low frequencies) and HH1 (high high frequencies) and each part has 8×8 pixels. The second level of the DWT is applied to only the LL1 (8×8) parts in the first level. Each LL1 will be divided into four sub-parts; LL2 (low low frequencies), LH2 (low high frequency), HL2 (high low frequencies) and HH2 (high high frequencies) and each part has 4×4 pixels. The embedding process will use only one coefficient in the LL2.

5.2.2 The Embedding Process

The embedding process is illustrated in figure 5.1 which can be explained as follows:

1. The DWT first level is applied on the host image after dividing it into blocks (16×16) in the spatial domain. Each block is converted to four parts in the DWT domain; LL1 (8×8) pixels, LH1 (8×8) pixels, HL1 (8×8) pixels and HH1 (8×8) pixels.
2. The second level of DWT is applied only to the LL1 from each block which will lead to 4 sub blocks (4×4) coefficients. These sub blocks are LL2, LH2, HL2 and HH2.
3. The mobile number with its international code is used as the watermarking information. The sum of the mobile number digits (2 digits) will be added at the end of the mobile number. The watermark with the the sum will become 16 decimal digits.
4. Each decimal digit in the watermarking information is converted to 4 bits using the BCD conversion. The result will be 64 bits.
5. The watermarking information is scrambled before embedded to host image. The scrambling process increases the security of the watermarking process.
6. Only one coefficient will be used to embed one digit from the watermark per each LL2 part. The Discrete Wavelet Coefficient Selection (DWCS) process is used to choose the right coefficient for embedding. Only 64 blocks (16×16) of the host image are needed to complete the embedding of all the digits of the watermark.
7. The digital watermarking information has small size compared to the size of the host image. Therefore, the embedding process will be repeated several times in order to increase the robustness of the algorithm.

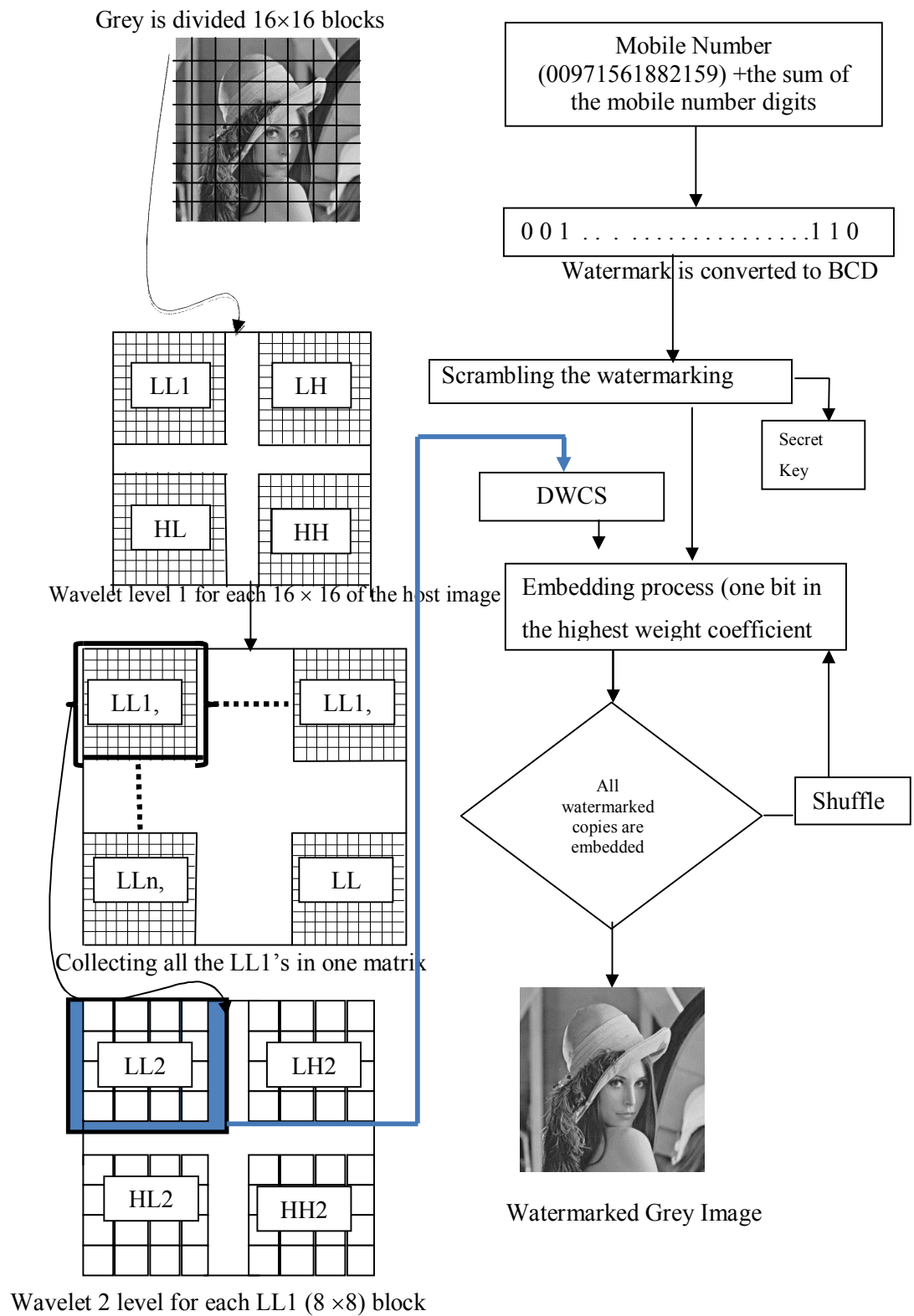


Figure 5.1: Embedding process.

8. The shuffling process is implemented to avoid the auto correlation between the watermarking information and the host image.
9. After all copies have been embedded into the host image, the IDWT level1 of the (8×8) is applied.
10. The output blocks of IDWT level1 will be the LL1 of the (16×16) block.
11. The same process is repeated to reconstruct the watermarked image.

5.2.3 The Extraction Process

At the decoder side, the watermarked image is divided into blocks of 16×16 pixels, then the DWT level 1 is applied on each block. Later, the DWT level 2 is applied to each LL1 from the first level. The recovery process is the inverse of the embedding process.

From each block, there is one coefficient which carries one bit only of the embedded watermark. This bit will be extracted by using the aforementioned method. The recovered watermark is created from the extracted bits. However, the reshuffling process is required to recover the watermark in the right order. Moreover, the recovered watermark is still scrambled. Therefore, the same secret key which was initially used at the transmitter side will be used to descramble the watermarks. The proposed algorithm does not require the original image to recover the watermark. The check sum will be used to ignore the wrong extracted watermarks. The summing of the correct watermarks based on the check sum parameter is divided onto the number of the correct watermarks number in order to find the average correct watermark. The extraction process is shown in Figure 5.2.

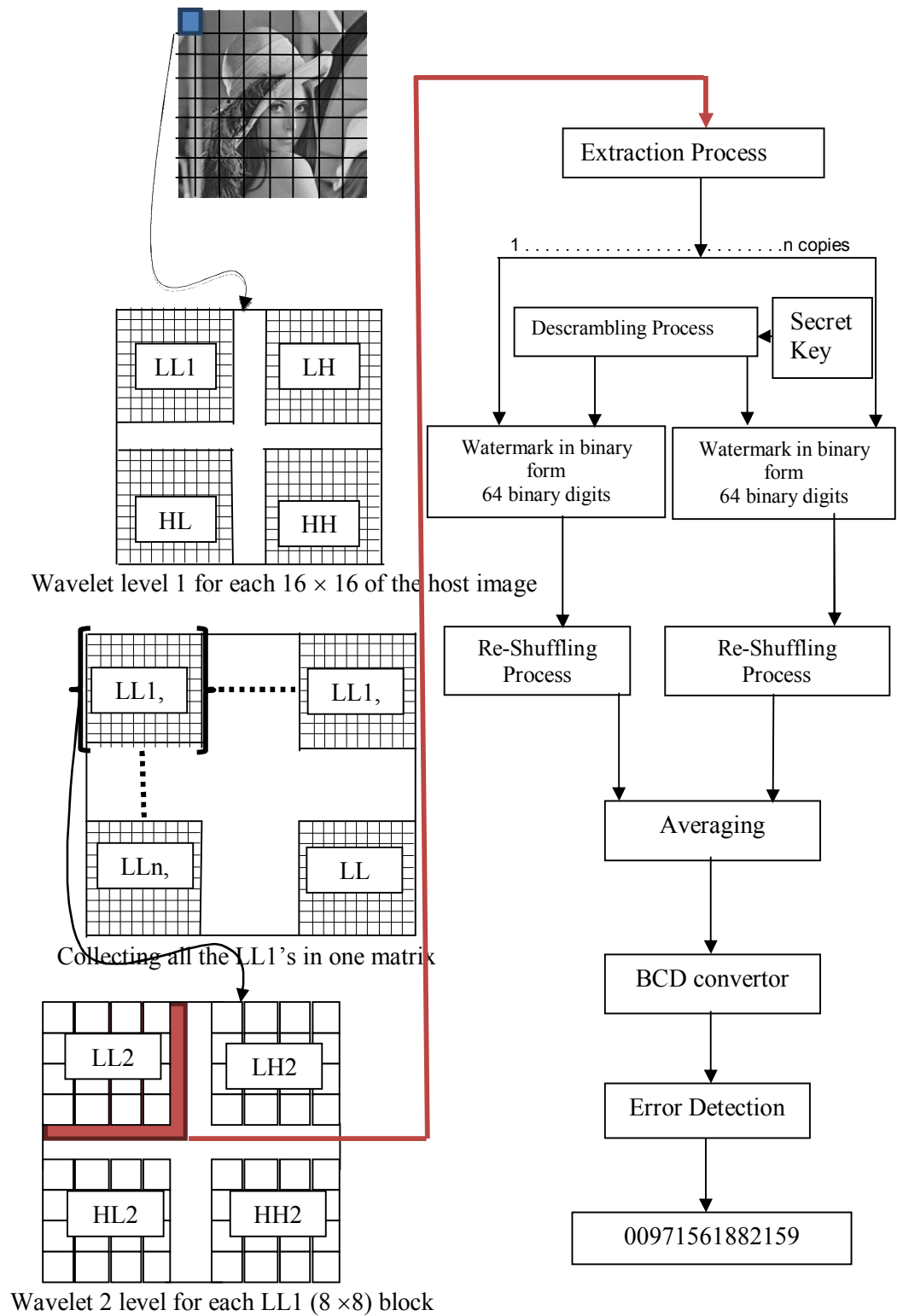


Figure 5.2: The extraction process.

5.2.4 Results

The proposed algorithm is examined using several grey images of size 512×512 with 8 bits per pixel and different watermarking information (different mobile numbers). The grey image which are used for testing are: “Lena”, “Pepper” and “Baboon”. The mobile numbers which are used as watermarking information are: UK mobile number, Iraq mobile number and UAE mobile number with the international code. PSNR and SSIM techniques have been used to evaluate the perceptual invisibility of the watermark in the watermarked image [3]. Several attacks have been used on the watermarked images to test the robustness of the algorithm by using the Stirmark software package.

The perceptual invisibility of the host image and the watermarked image with different embedding strength are shown in Table 5.1. The PSNR values show that the distortion caused to the image is invisible. For instant, the PSNR is 58.2 dB for watermarking strength $\Delta=8$ and even though the watermarking strength was increased to 40 the PSNR value is still high 44.8 dB.

The distortion caused to the image by the watermarking process is evaluated using the SSIM technique. The SSIM between the host image and the watermarked image is recorded for different values for the watermarking strength Δ in table 5.2. The SSIM is high even for the high watermarking strength Δ . The SSIM is varied from 0.999 to 0.995 for the watermarking strength $\Delta =8$ to the watermarking strength $\Delta = 40$ respectively.

The Stirmark software package offers several attacks which are applied to the watermarked image in order to evaluate the robustness of the proposed algorithm. The

Normalized Correlation Coefficient (NCC) factor is used to measure the similarity between the original and extracted watermark as shown in table 5.3.

The algorithm is robust against several attacks such as: low-pass filter (3×3 and 5×5), wiener filter (3×3), median filter, 80 % vertically cropping and 75% horizontal attacks, JPEG compression attack up to 35, scale 0.4 and 2 attack, Gaussian noise attack and salt and pepper noise attack.

Table 5.1: PSNR with different grey images

Image	Lena	Pepper	Baboon
PSNR at $\Delta = 8$	58.224	58.461	58.380
PSNR at $\Delta = 14$	54.000	53.997	54.048
PSNR at $\Delta = 16$	52.869	52.961	52.926
PSNR at $\Delta = 20$	50.974	50.865	50.979
PSNR at $\Delta = 24$	49.094	49.523	49.218
PSNR at $\Delta = 30$	47.424	47.371	47.448
PSNR at $\Delta = 34$	46.450	46.385	46.384
PSNR at $\Delta = 40$	44.815	45.134	44.913

Table 5.2: SSIM with different grey images

Image	Lena	Pepper	Baboon
SSIM at $\Delta = 8$	0.999	1.000	1.000
SSIM at $\Delta = 14$	0.999	0.999	0.999
SSIM at $\Delta = 16$	0.998	0.998	0.999
SSIM at $\Delta = 20$	0.997	0.997	0.999
SSIM at $\Delta = 24$	0.996	0.996	0.998
SSIM at $\Delta = 30$	0.994	0.994	0.997
SSIM at $\Delta = 34$	0.993	0.992	0.997
SSIM at $\Delta = 40$	0.989	0.990	0.995



Figure 5.3: Original Lena and watermarked Lena images with different strengths.

Table 5.3: The Normalized Correlation Coefficient (NCC) for Lena image with different attacks, at $\Delta = 16$

Attacks	NCC	Attacks	NCC
Cropping 50% V	1	Low pass 3×3	1
Cropping 80% V	1	Low pass 5×5	1
Cropping 50% H	1	Wiener 3×3	1
Cropping 75% H	1	Wiener 5×5	1
Gaussian noise m=0, v=0.002	1	Median 3×3	1
Gaussian noise m=0, v=0.003	1	Median 5×5	0
S&P noise, d=0.02+ Median 3×3	1	JPEG 50	1
S&P noise, d=0.05+ Median 3×3	1	JPEG 35	1
Scale 2	1	Scale 0.4	1
Stirmark_AFFINE_3	1	Stirmark_CONV_1	0
Stirmark_AFFINE_8	0	Stirmark_RML_10	1
Stirmark_ROTSCALE_0.25	1	Stirmark_RML_50	1
Stirmark_ROT_-0.25	1	Stirmark_RML_100	1
Stirmark_ROTSCALE_-0.5	0	Stirmark_SS_1	1
Stirmark_ROT_0.25	1	Stirmark_SS_2	1
Stirmark_ROT_-0.5	0	Stirmark_SS_3	1

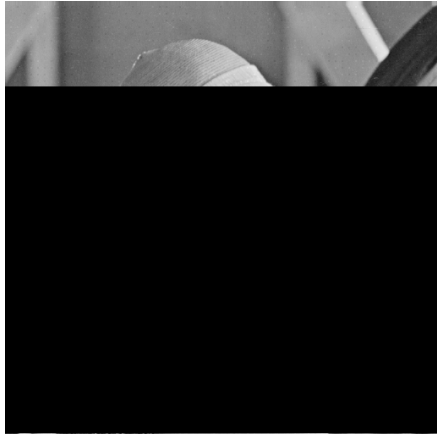




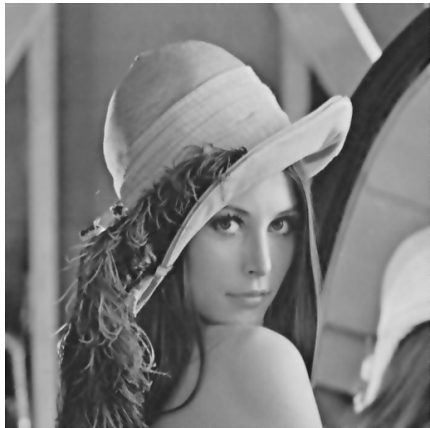
	
Cropping attack 80 % H	Gaussian noise $m=0$, $v=0.003$
	
S&P noise attack, $d=0.02$ + Median 3×3	Contrast enhancements attack intensity=0.3, 0.9
	
JPEG 20 attack	Wiener filter attack 5×5

Figure 5.4: Several attacks for watermarked image.

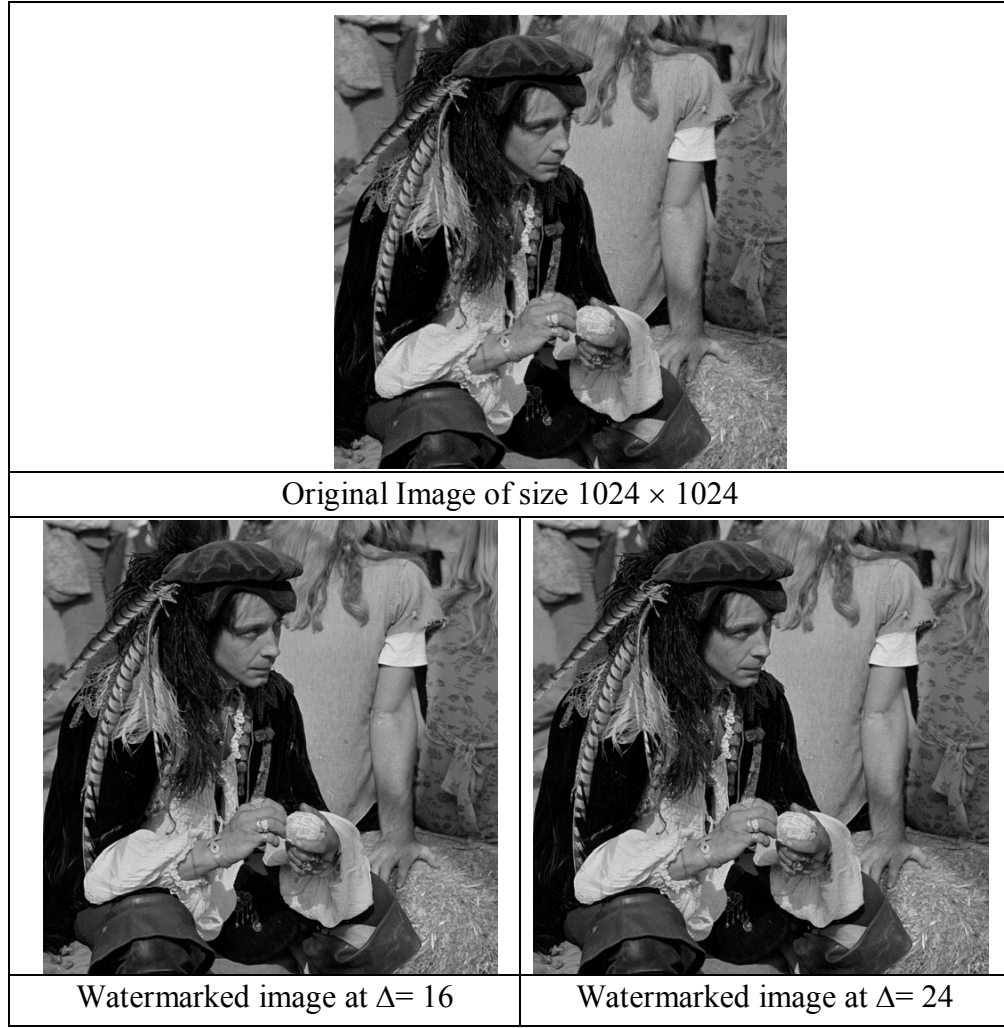


Figure 5.5: Original and watermarked images with high resolution.

5.3 Two-level DWT Watermarking Scheme for Colour Images

The proposed algorithm is designed for the colour still image by using two-level DWT transform. The new algorithm will embed the watermark in the green channel.

5.3.1 The Embedding Process

The still colour image can be divided into three components Red (R), Green (G) and Blue (B). The proposed algorithm uses the two-level wavelet block based algorithm. The Green component is divided into blocks of 16×16 pixels in the spatial domain. The DWT is applied for each block of the host image. The second DWT is applied to the LL1 from the first level transformation. The digital watermarking information is mobile number with the international code plus the check sum digits (16 digits) and it is

embedded in one components of the second level DWT. Each binary digit will be embedded in one coefficient per one LL2 sub-bands. The DWSC process is applied to choose the highest magnitude coefficient which will be used for embedding. The embedding process is illustrated in figure 5.6.

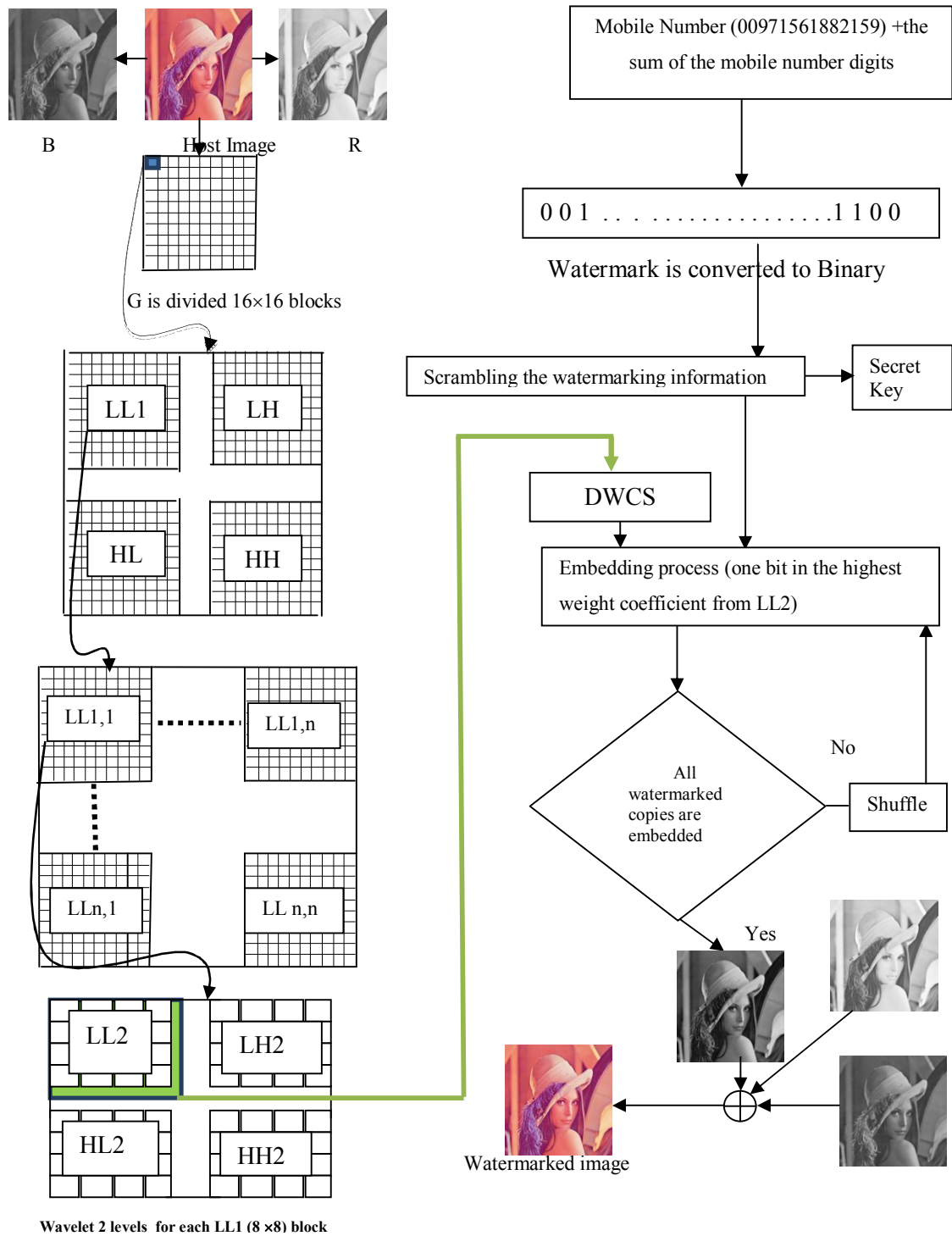


Figure 5.6: The Embedding process.

5.3.2 The Extraction Process.

At the receiver side, the watermarked colour image (RGB) is divided into the three components R, G and B. The Green component is divided into 16×16 blocks. The DWT first level is applied on each block of 8×8 sub-bands (LL1, LH1, HL1 and HH1). The second level of DWT is applied on each LL1 sub-bands only to achieve 4×4 sub-band (LL2, LH2, HL2 and HH2). However, the recovery process is the inverse of the embedding process.

The embedding coefficient is in the LL2 sub-bands only. The extraction of each bit from the LL2 will be by using the same process of embedding but in reverse direction. All bits are accumulated in one vector per each watermark copy. The reshuffling operation is applied to get the watermarks copies in the right order. The check parameter is used to ignore the wrong copies. However, the descramble process is applied of the correct watermark to get the correct watermark in the right order. The extraction process is shown in figure 5.7.

5.3.3 Results

The proposed algorithm has been tested by using different colour images of size 512×512 with 24 bits per pixel. The mobile number with the international code has been used as a digital information watermarking. Table 5.4 shows the PSNR values for different embedding strength. The PSNR is measured between the original image and the watermarked image. The proposed algorithm has achieved higher than 63 dB for Lena image at embedding strength (Δ) = 8. However, the PSNR is still high even for high values of embedding strength. For example, PSNR is 49.7 dB at $\Delta=40$.

The similarity between the original image and the watermarked image is an important parameter which is a measure of the distortion caused by the watermarking process on the host image. The SSIM technique is used to measure the similarity between the original image and the watermarked one. Table 5.5 shows the SSIM for different images of different embedding strength. It is clear that the proposed algorithm has achieved 0.9998 to 0.996 for Δ 8 to 40 respectively. Lena, Pepper and Baboon images are used in the aforementioned tables.

Furthermore, several attacks are applied to the watermarked image by using the Stirmark software package. The similarity between the watermark at the decoder side and the extracted watermark at the receiver side can be measured by using the Normalized Correlation Coefficient factor (NCC). Table 5.6 show the NCC values for the proposed algorithm at different embedding strength. The watermarking information which is used in the proposed algorithm is a mobile number. The proposed algorithm showed high resistivity against several attacks as shown in table 5.7. For example; low-pass, vainer and Gaussian filter attacks, scale attacks (0.4 and 2), cropping attacks (up to 80% vertical and 75% horizontal), salt and pepper attack, median attack. The NCC for the proposed algorithm should be 1 otherwise the extracted watermark will be different values of the original watermark because the mobile number has been used as watermarking information.

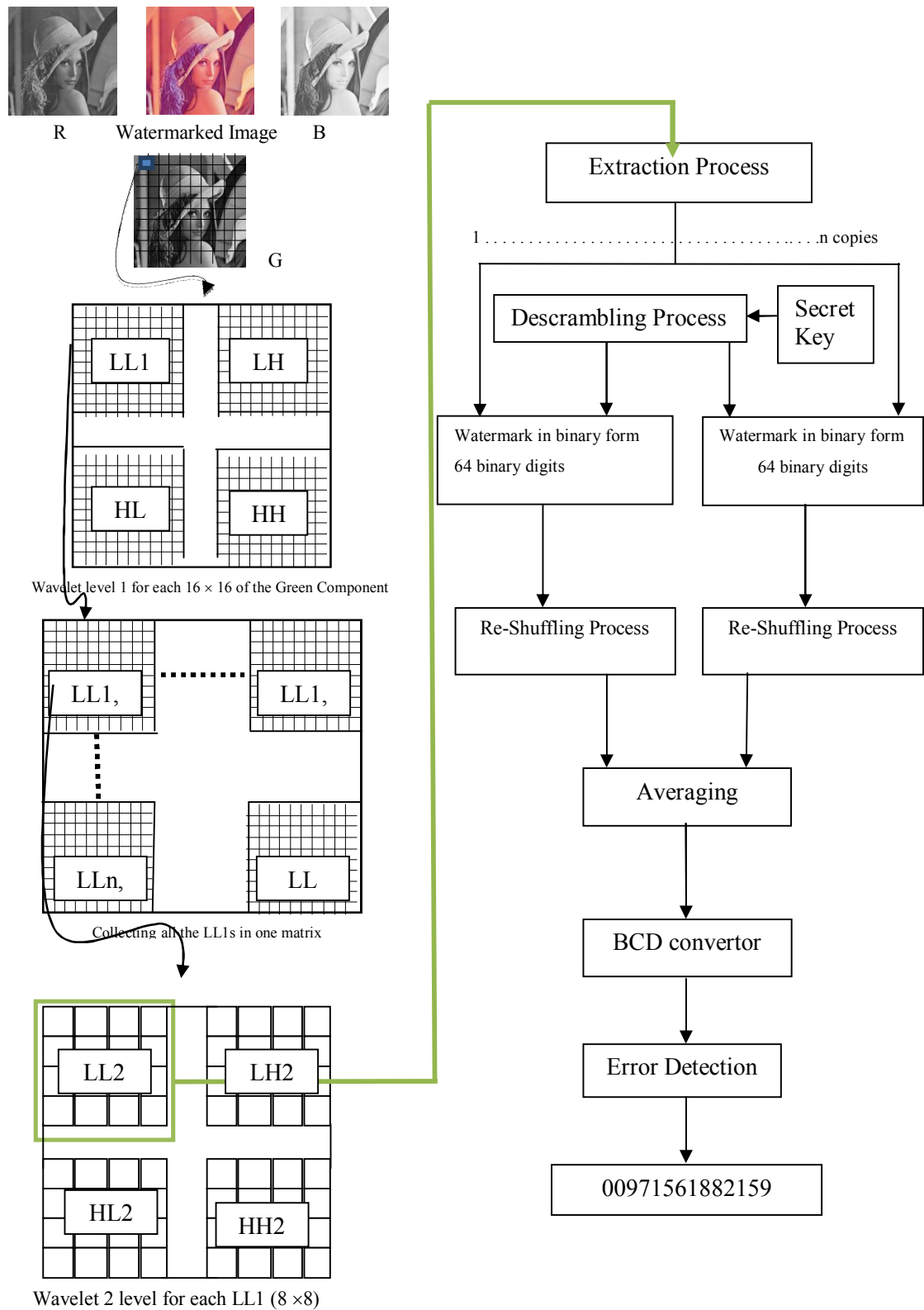


Figure 5.7: The extraction process.

Figure 5.8 shows the watermarked images with different embedding strength. The proposed algorithm showed that the watermarking information is invisible even with high values of the embedding strength.

The proposed algorithm showed that the distortion caused by the watermark is still invisible. Figure 5.9 shows the Lena colour image before any attack and after several attacks.

Finally, figure 5.10 illustrates the proposed algorithm can be implemented with high resolution images (large size). The evaluation of the proposed algorithm performance is examined and it is shown in table 5.8 .

Table 5.4: PSNR with different colour images (green channel embedding)

Image	Lena	Pepper	Baboon
PSNR at $\Delta = 8$	63.050	63.061	63.257
PSNR at $\Delta = 12$	58.886	59.066	58.864
PSNR at $\Delta = 16$	57.712	57.587	57.445
PSNR at $\Delta = 20$	55.738	55.646	55.698
PSNR at $\Delta = 24$	54.007	54.058	53.789
PSNR at $\Delta = 30$	52.109	52.267	52.306
PSNR at $\Delta = 34$	51.114	50.954	51.109
PSNR at $\Delta = 40$	49.738	49.731	49.760

Table 5.5: SSIM with different colour images (green channel embedding)

Image	Lena	Pepper	Baboon
SSIM at $\Delta = 8$	0.9998	0.9998	1.0000
SSIM at $\Delta = 12$	0.9996	0.9995	0.9999
SSIM at $\Delta = 16$	0.9995	0.9993	0.9998
SSIM at $\Delta = 20$	0.9991	0.9989	0.9998
SSIM at $\Delta = 24$	0.9987	0.9984	0.9996
SSIM at $\Delta = 30$	0.9981	0.9979	0.9994
SSIM at $\Delta = 34$	0.9976	0.9973	0.9993
SSIM at $\Delta = 40$	0.9966	0.9964	0.9991

Table 5.6: The Normalized Correlation Coefficient (NCC) for Lena image with different attacks, at $\Delta=16$

Attacks	NCC	Attacks	NCC
Cropping 50% V	1	Low pass 3×3	1
Cropping 80% V	1	Low pass 5×5	1
Cropping 50% H	1	Wiener 3×3	1
Cropping 75% H	1	Wiener 5×5	1
Gaussian noise m=0, v=0.002	1	Median 3×3	1
Gaussian noise m=0, v=0.003	1	Median 5×5	0
S&P noise, d=0.02+ Median 3×3	1	JPEG 50	1
S&P noise, d=0.05+ Median 3×3	1	JPEG 35	1
Scale 2	1	Scale 0.4	1
Stirmark_AFFINE_3	1	Stirmark_CONV_1	0
Stirmark_AFFINE_8	0	Stirmark_RML_10	1
Stirmark_ROTSCALE_0.25	1	Stirmark_RML_50	1
Stirmark_ROT_-0.25	1	Stirmark_RML_100	1
Stirmark_ROTSCALE_-0.5	0	Stirmark_SS_1	1
Stirmark_ROT_0.25	1	Stirmark_SS_2	1
Stirmark_ROT_-0.5	0	Stirmark_SS_3	1

	
Original Image	
	
Watermarked image at $\Delta=12$	Watermarked image at $\Delta=16$
	
Watermarked image at $\Delta=24$	Watermarked image at $\Delta=34$

Figure 5.8: Original Lena with different watermark strength (green channel).








	
Cropping 48% V	Wiener filter 3×3
	
S&P noise attack, $d=0.05$ + Median 3×3	Gaussian noise $m=0$, $v=0.002$

Figure 5.9: several attacks for colour watermarked image (green channel).

Table 5.7: High resolution colour images examined by the proposed algorithm for green channel

			
Original Image of size 1024×1024			
			
Watermarked image at $\Delta = 24$		Watermarked image at $\Delta = 16$	
PSNR		PSNR	
SSIM		SSIM	
Attacks	NCC	Attacks	NCC
Cropping 50 V	1	Cropping 50 % V	1
Low pass 3×3	1	Low pass 3×3	1
Median 3×3	1	Median 3×3	1
Wiener 3×3	1	Wiener 3×3	1
Gaussian noise $m=0$, $v=0.002$	1	Gaussian noise $m=0$, $v=0.002$	1
S&P noise, $d=0.02+$ Median 3×3	1	S&P noise, $d=0.02+$ Median 3×3	1

5.4 Comparison with previous work

The proposed algorithm of two-level DWT has been compared with one-level DWT algorithm in chapter four and the watermark algorithm method stated in [4], [5] and [6]. Table 5.11 shows the PSNR for the proposed algorithm and other algorithms. It is clear that the proposed algorithm has achieved the highest PSNR with different embedding strength.

Table 5.12 deals with the SSIM comparison between the proposed algorithm and other algorithms. The proposed algorithm gives a higher SSIM for different embedding strengths than the others.

Table 5.8: The PSNR for Lena colour image with different Δ

Attacks	Two-level DWT	One-level DWT	[4]	[5]	[6]
PSNR at $\Delta = 16$	57.712	51.813	44.2	51.440	38.5
PSNR at $\Delta = 24$	54.007	48.144	41.1	47.876	37.4
PSNR at $\Delta = 34$	51.114	45.129	38.2	44.798	35.2
PSNR at $\Delta = 40$	49.738	43.941	36.1	43.222	34

Table 5.9: The SSIM for Lena colour image with different Δ

Attacks	Two-level DWT	One-level DWT	[5]	[6]
SSIM at $\Delta = 16$	0.9995	0.997	0.998	0.997
SSIM at $\Delta = 24$	0.9987	0.994	0.995	0.985
SSIM at $\Delta = 34$	0.9976	0.989	0.990	0.975
SSIM at $\Delta = 40$	0.9966	0.986	0.987	0.971

5.5 Final Remarks

In this chapter, the novel robust watermarking algorithms for grey and colour images are proposed. The information watermarking is a mobile number with international code. 2DWT two-level are applied on block based of the host image. Several attacks applied to the proposed algorithm in order to test the robustness of the algorithm for example: cropping up to 80%, JPEG compression, small degrees of rotation up to 0.25%, scaling down to 80%, additive noise, filtering operations and Stirmark attacks. It was proved that the watermark information in the proposed algorithm survived against these attacks. The proposed algorithm achieved high values of PSNR. The proposed algorithm recorded high values of SSIM. The aim of the scheme is to protect the copyright ownership of the image. The robust algorithms will be further developed in the next chapter to include methods for authentication of images.

5.6 References

- [1] P. Singh, R S Chadha, “A Survey of Digital Watermarking Techniques, Applications and Attacks”, *International Journal of Engineering and Innovative Technology (IJEIT)*, Volume 2, Issue 9, March 2013.
- [2] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji & A. Tawfik, “A novel blind image watermarking technique for colour RGB images in the DCT domain using green channel, ” *Communications, Computers and Applications*, 2008. MIC-CCA 2008. Mosharaka International Conference on, Aug. 2008, pp26-31.
- [3] Z. Wang, A. C. Bovik, “Image Quality Assessment: From Error Visibility to Structural Similarity”, *IEEE transactions on image processing*, Vol. 13, No. 4, pp. 600-612, April 2004.
- [4] I. Kong and C. Pun, “Digital Image Watermarking with Blind detection for Copyright Verification ”, *IEEE computer society, 2008 Congress on Image and Signal Processing*, Vol. 1, pp. 504-508, May 2008.
- [5] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji and A. Tawfik, “A New Watermarking Scheme For Colour Images Captured By Mobile Phone Cameras”, *IJCSNS International Journal of Computer Science and Network Security*, VOL.9 No.7, pp. 248 - 254, July 2009.
- [6] V. Sreejith, K. Sritith and R. Roy, “Robust Blind Digital Watermarking in Contourlet Domain”, *International Journal of Computer Applicationa*, Vol. 58, No. 12, pp. 13 – 19, November, 2012.

CHAPTER 6

Fragile and Robust Watermarking

6.1 Introduction

This chapter presents a fragile watermarking algorithm for still images in the spatial domain. The hash code is used as watermarking information which is embedded to the host image. The proposed algorithm is used to detect any occurrence of tampering in the host image. Then combined algorithms of the robust algorithm and the fragile one are introduced. The combined algorithm does not need the original image in order to extract the watermark. The fragile watermark is very sensitive to any kind of attacks or image manipulations. On the other hand, the robust watermark causes minimal distortion to the host images.

6.2 Fragile Watermarking Scheme for Grey Level images

The proposed fragile watermarking scheme uses the spatial domain to embed the hash function code as binary watermark information. The hash code function is calculated for the host image. It is a very sensitive code [1], therefore any tampering with the host

image either in the spatial domain or in the frequency domain will be detected. The hash function which is used in the proposed algorithm is MD5 [2].

6.2.1 The Embedding and Extraction Process for Grey Images

The embedding process is as illustrated in figure 6.1 and can be described as follows for an image which is 512×512 .

1. Extract the first row of pixels from the host image in the spatial domain. This will be one dimensional vector (1×512) pixels.
2. The hash function code (MD5) is calculated for the remaining image (511×512) pixels. The code is 32 digits in hexadecimal form.
3. The hash code is converted from the hexadecimal form to the binary form (128 bits). The 128 binary bits is representing the watermarking information.
4. The watermarking information is embedded into the one dimensional vector of the host image.
5. The watermarked vector is added to the 511×512 of the host image to get the watermarked image

It should be noted that any row or vector can be used for this purpose.

At the decoder side, the extraction process is as shown in figure 6.2 and can be explained as follows:

1. The first row from the watermarked image is extracted.
2. The extraction process of the binary watermarking information is applied on the one dimensional vector (first row in this example).
3. The hash code function is calculated for the image after excluding the first row
4. The calculated hash code is converted from the hexadecimal form to the binary form.

5. The comparison is taken place between the extracted watermark and the original watermark. If the result is zero, the image is authentic. Otherwise the watermarked image has been tampered with.

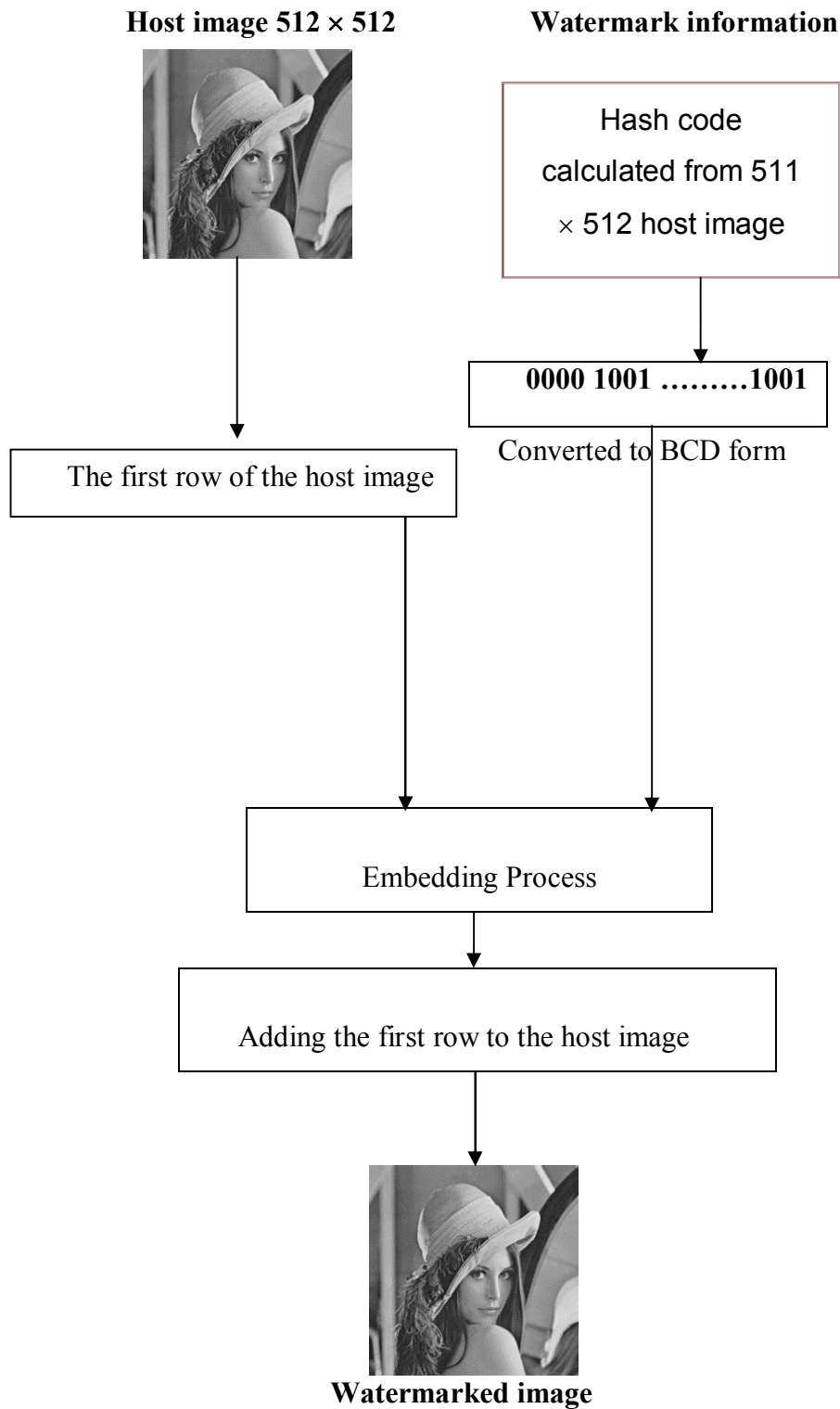


Figure 6.1: The embedding process.

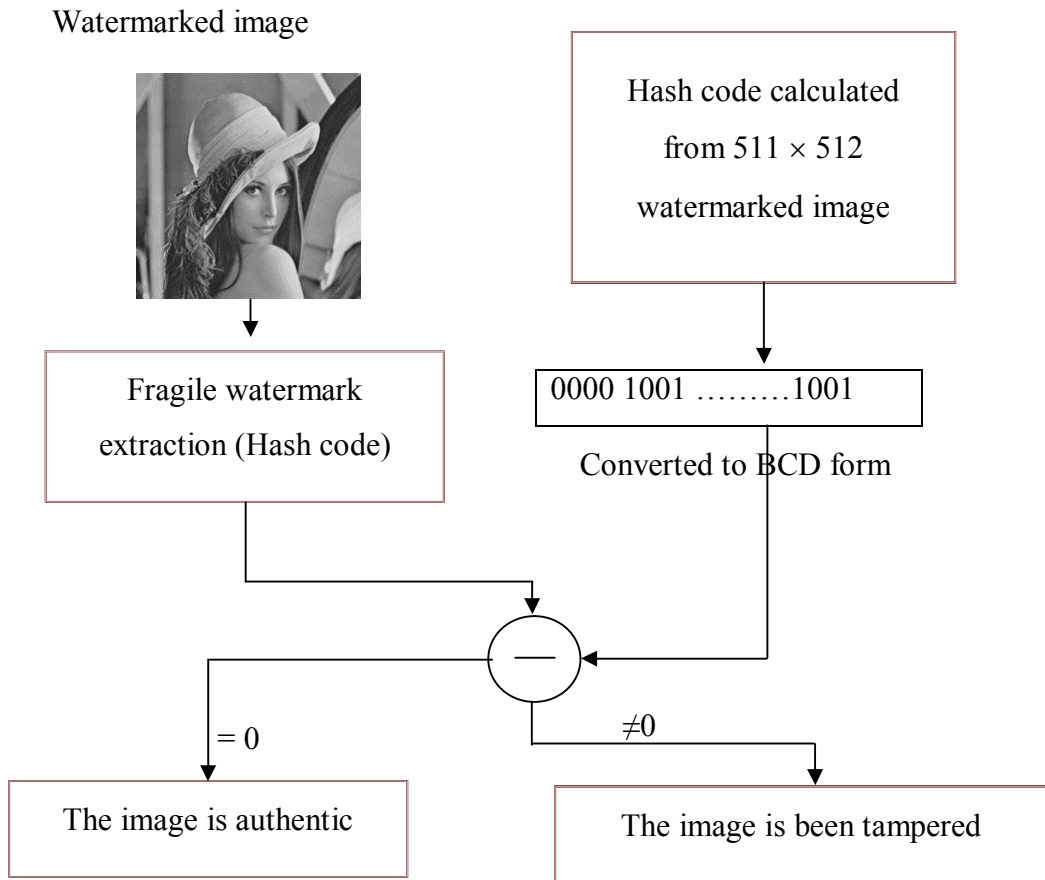
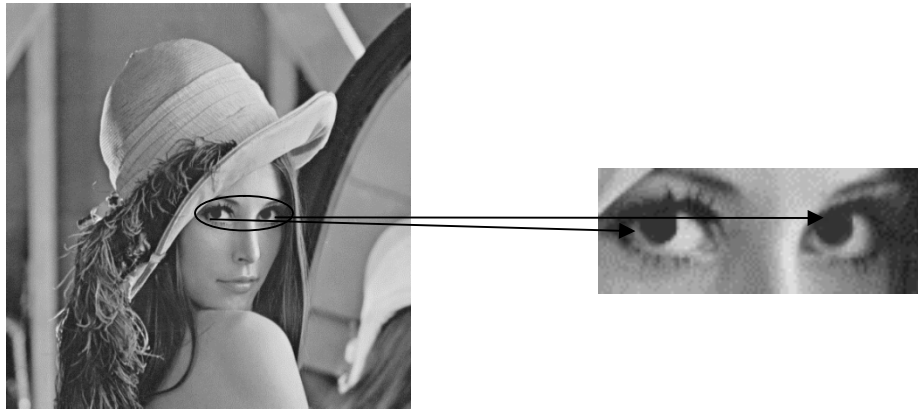


Figure 6.2: The extraction process.

6.2.2 Results

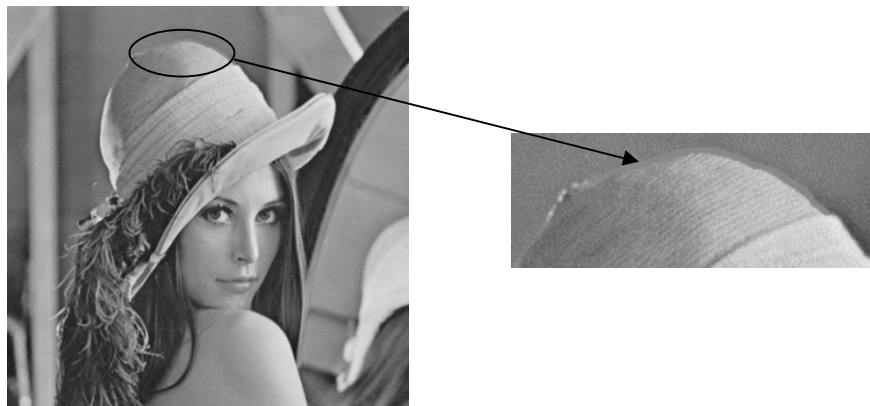
This algorithm is examined using different grey images of size 512×512 with 8 bits per pixel. Test grey images are “Lena”, “Pepper” and “Baboon”. The watermarking information is the hash code function of the host image in the special domain. In order to evaluate the proposed algorithm, the hash code of the watermarked image has been tested by editing the watermarked image in different areas as shown in figure 6.3. The difference between the hash code for the host image and the edited ones are illustrated in table 6.1. It shows the hash code cannot be recovered for any kind of image editing, including a single change in one pixel.



a. Editing Eyes



b. Editing Hair



c. Editing Hat

Figure 6.3: Different examples of image editing.

Table 6.1: MD5 Hash code Calculation

Hash for Original Image	Hash for Modified Image	Editing type
'7f36f4419577494fd88333a3e90eda05'	'fb498c0b28a08758e714e315d0183ca1'	Eye editing
'7f36f4419577494fd88333a3e90eda05'	'23e925a041bd25497fd68b3780a6abbe'	Hat editing
'7f36f4419577494fd88333a3e90eda05'	'f3a53fc927d25f50622ee24390c2aa06'	Hair editing

6.3 Fragile Watermarking Scheme for RGB Images

The previous algorithm was used with colour images. The hash code functions for the green, red and blue channels are used as watermarking information. The embedding process used the frame of the aforementioned channels to embed the watermarking in the spatial domain.

6.3.1 Embedding and Extraction Process for RGB Images

At the encoder site, the embedding process of the proposed algorithm for the RGB colour images is as illustrated in figure 6.4 and can be explained as follows:

1. The host RGB colour image is separated into the R, G and B channels.
2. The hash code function (MD5 type) has been calculated for the pixels of R, G and B images separately excluding the frame (first row, last row, first column and last column).
3. The resultant hexadecimal hash code is converted to the binary code.
4. The extracted rows and columns from each channel are converted to one dimensional vector. These vectors will be used for embedding the fragile watermark information in each channel.

5. The embedding process will take place into R, G and B channels separately.
6. The watermarked RGB is reconstructed from the watermarked channels.

At the decoder side, the extraction process for the fragile watermarks information is shown in figure 6.5 and can be explained as follows:

1. The watermarked RGB colour image is divided into R, G and B watermarked channels.
2. The watermarking information is extracted separately from the frame of each channel.
3. The hash code function for each channel after excluding the frame is calculated.
4. The calculated hash codes are converted from the hexadecimal form to the binary one.
5. The comparison between the extracted watermarks and the original watermarks are applied for each channel individually. If the result is zero in all channels, the image is authentic. Otherwise the watermarked image has been tampered with.

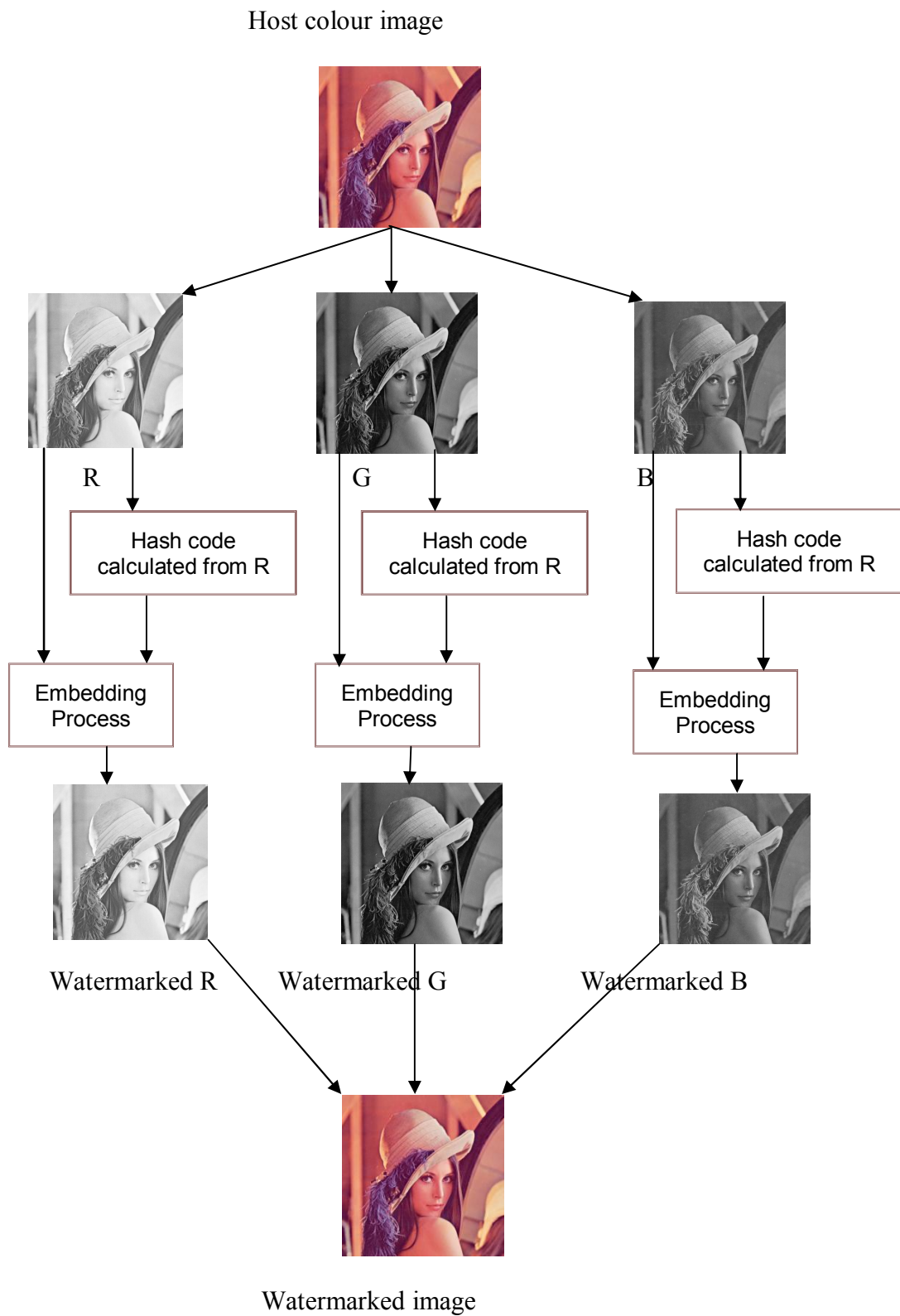


Figure 6.4: The embedding process

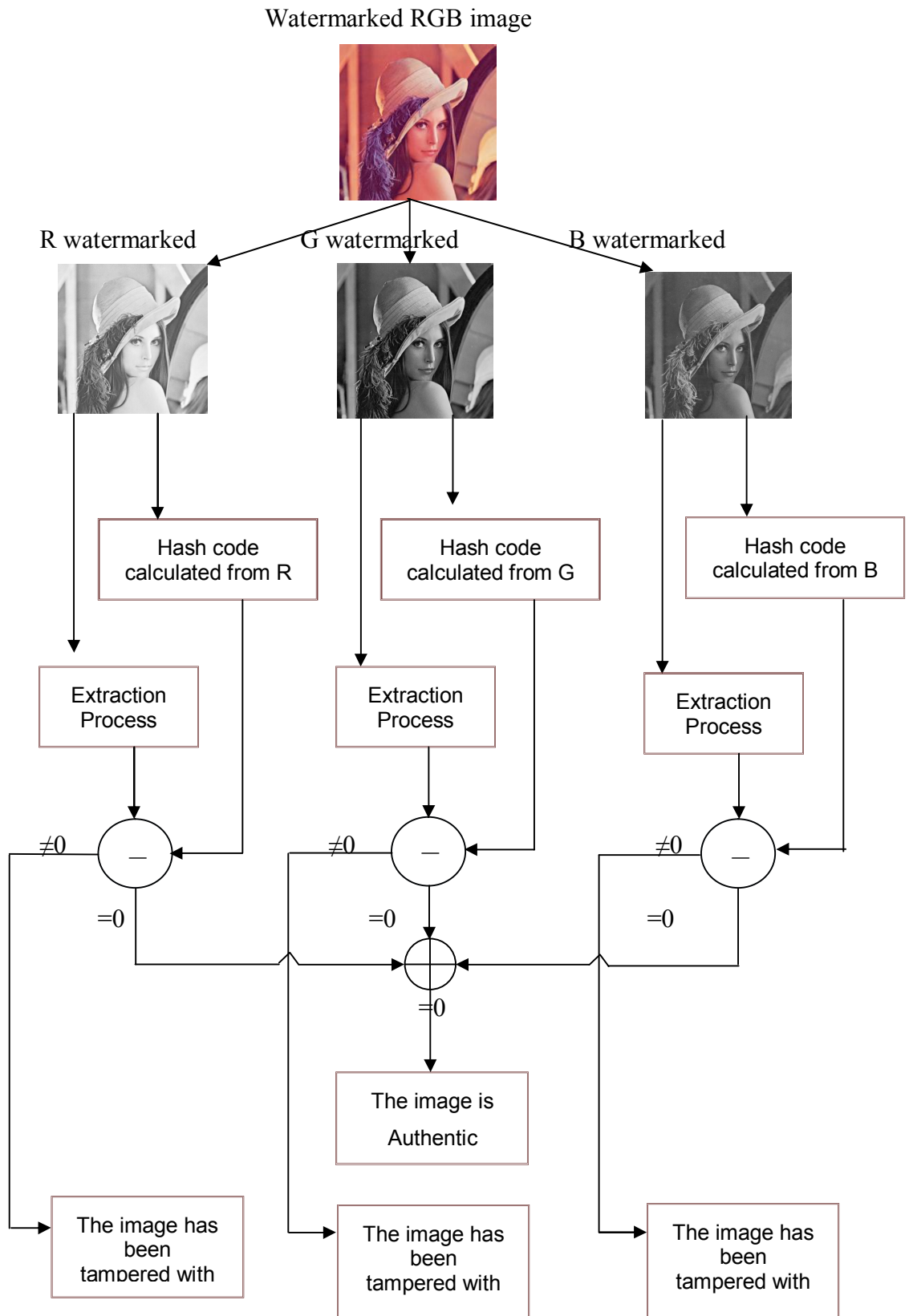
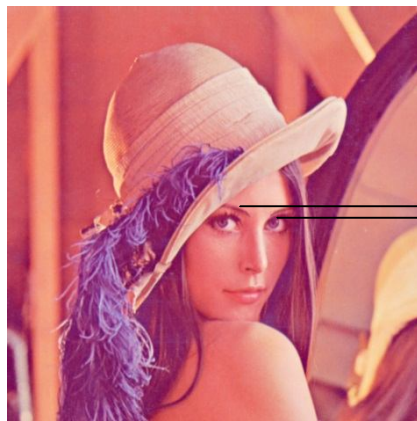


Figure 6.5: The extraction process.

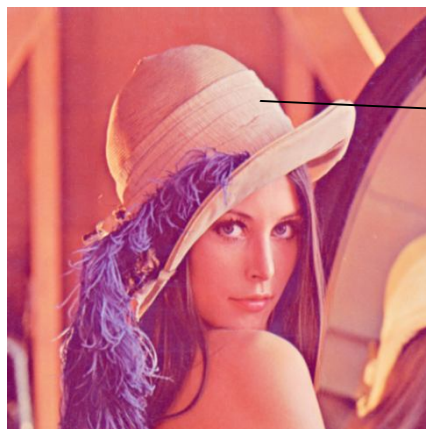
6.3.2 Results

The algorithm is tested using different colour image of size 512×512 with 24 bits per pixel. Test colour images are “Lena”, “Pepper” and “Baboon”.

The fragile watermark information is not recovered if the watermarked image has been tampered with [3]. To evaluate the proposed algorithm, the fragile watermark has been examined by editing the watermarked image in different areas. The editing process might take place at different areas in the colour host image directly as shown in figure 6.6 or the editing process might happens on the R, G and B channels as illustrated in figure 6.7. The differences between the hash code (fragile watermark) for the host image and the edited ones are explained in Table 6.2 and Table 6.3 respectively.



a. Editing eyebrow



b. Editing hat

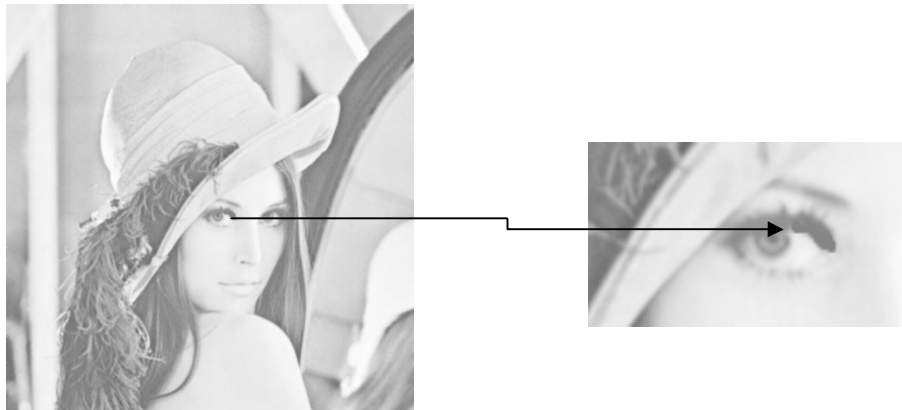


c. Editing lips

Figure 6.6: Different examples of colour image editing.

Table 6.2: MD5 Hash code Calculation for Editing Colour Images

Hash Code	Hash for Original Image	Hash for Modified Image	Editing type
R	'41411a93896f03c683afc433770442d6'	'e61af8c9302e9aa43fbd0734689abdbc'	Eyebrow editing
G	'f6d3857b6ae8885369754cf55a92a16f'	'0bc55902e20d1de56e70562fbfdbdd8d'	Eyebrow editing
B	'13fe4d29a0f703da5a556980d38763a4'	'0d0c8a9bde039e0449d524699a425954'	Eyebrow editing
R	'41411a93896f03c683afc433770442d6'	'136ce6661902eab1c63178e9fc5c8be7'	Hat editing
G	'f6d3857b6ae8885369754cf55a92a16f'	'9338c68129c8b07f7576620524f2c6bd'	Hat Editing
B	'13fe4d29a0f703da5a556980d38763a4'	'e85a509c0d1294aff89a412a11055cde'	Hat Editing
R	'41411a93896f03c683afc433770442d6'	'bb583c256a5681107a3d17cf22ccc471'	Lips Editing
G	'db7567d2fe717dff688a3769cda65b65'	'd5a7b7296580111fdb2fd2fcfc1820a'	Lips Editing
B	'13fe4d29a0f703da5a556980d38763a4'	'31b7a3b2a571e7635d8698df8fe8517e'	Lips Editing



a. Editing eye in the red channel



b. Editing nose in the green channel



c. Editing shoulder in the blue channel

Figure 6.7: Different examples of image editing in different channels

Table 6.3: MD5 Hash code calculations for editing different channels

Hash Code	Hash for Original Image	Hash for Modified Image	Editing type
R	'41411a93896f03c683afc433770442d6'	'fcc0cb5182af0332f51f7780320c7739'	Eye editing in R channel
G	'db7567d2fe717dff688a3769cda65b65'	'db7567d2fe717dff688a3769cda65b65'	Eye editing in R channel
B	'13fe4d29a0f703da5a556980d38763a4'	'13fe4d29a0f703da5a556980d38763a4'	Eye editing in R channel
R	'41411a93896f03c683afc433770442d6'	'41411a93896f03c683afc433770442d6'	Nose editing in G channel
G	'db7567d2fe717dff688a3769cda65b65'	'8c0c08794eeb5227e3985e83bbcccb9b'	Nose editing in G channel
B	'13fe4d29a0f703da5a556980d38763a4'	'13fe4d29a0f703da5a556980d38763a4'	Nose editing in G channel
R	'41411a93896f03c683afc433770442d6'	'41411a93896f03c683afc433770442d6'	Shoulder editing in B channel
G	'db7567d2fe717dff688a3769cda65b65'	'db7567d2fe717dff688a3769cda65b65'	Shoulder editing in B channel
B	'13fe4d29a0f703da5a556980d38763a4'	'43acc4a2f45c0d0e00bdf48ab1f6af0'	Shoulder editing in B channel

6.4 Combined Watermarking

6.4.1 Combined the one-level DWT robust algorithm with the fragile algorithm.

This algorithm combines the DWT robust algorithm (explained in chapter four and chapter five) with the fragile algorithm. The new proposed algorithm is used for authentication checking and copyright protection.

6.4.2 The embedding process and the extraction process

The embedding process for the combined algorithm starts with embedding the robust watermark first, then the fragile watermark. Conversely, the extraction process starts with the extraction of the fragile watermarking information before the robust watermarking information extraction takes place.

The first stage of the embedding process is embedding the robust watermarking in the host image. The robust watermarking information used is a mobile phone number including its international code. The second step in the embedding process is embedding the fragile watermarking information in the watermarked image. The fragile watermark information used a hash code function of the image. The RGB watermarked image is transferred to the R, G and B channels separately. The hash code has been calculated (Hexadecimal form) for the pixels of R, G and B images individually excluding the frame (first row, last row, first column and last column). The calculated hash code function for each channel is converted into binary code and embedded into selective pixels of the frame vector. The two steps of the embedding process for the combined algorithm are shown in figure 6.8.

The extraction process starts with the detection of the fragile watermarking first then the robust one. At the decoder side, the R, G and B are found from the colour watermarked image. The fragile watermarking information (hash codes) is extracted from the frame of the R, G and B images individually. Then the hash codes of the pixels of each image without the frame are calculated. The comparison process between the calculated hash code and the extracted one per each image is applied. If there is any difference between

the two codes it means the watermarked image has been tampered with. If not then it means that the watermarked image is authentic.

The second step of the extraction process is the detection of the robust watermarking (phone number). The watermarked image after fragile extraction is divided into 8x8 blocks. The DWT transformation function is applied on each block in order to convert it to the wavelet domain. The recovery process is the inverse of the the embedding process. The extracted bits will create the embedded watermark information. Then it will be converted to the decimal form to obtain the phone number. The reshuffling process is implemented to extract all the copies of the watermark information. The scrambled watermarks are descrambled to get the original watermarks. The check sum will be used to discard the wrongly extracted phone numbers. Figure 6.9 illustrates the extraction process.

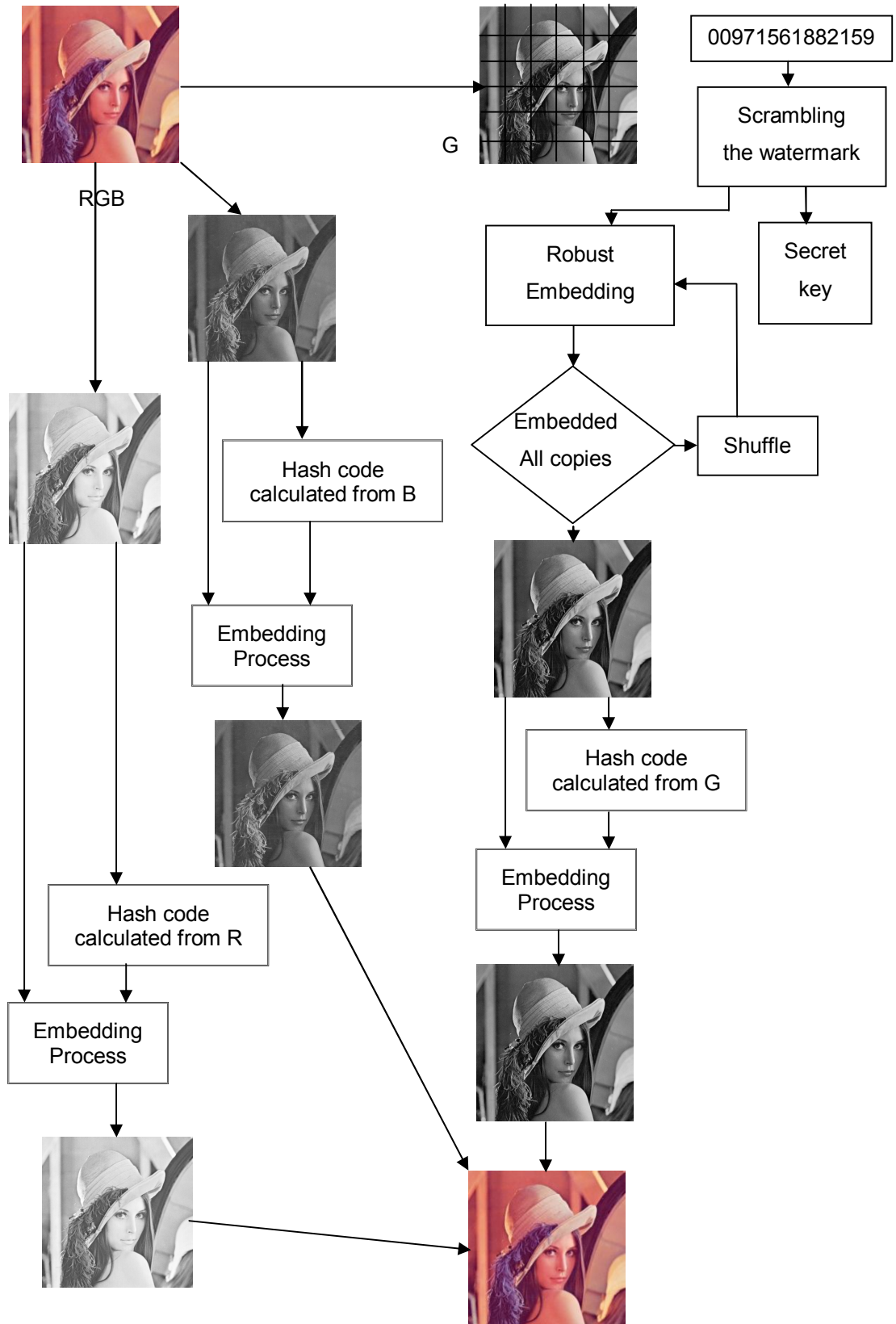


Figure 6.8: The embedding process combined algorithm of one-level DWT robust and fragile algorithms.

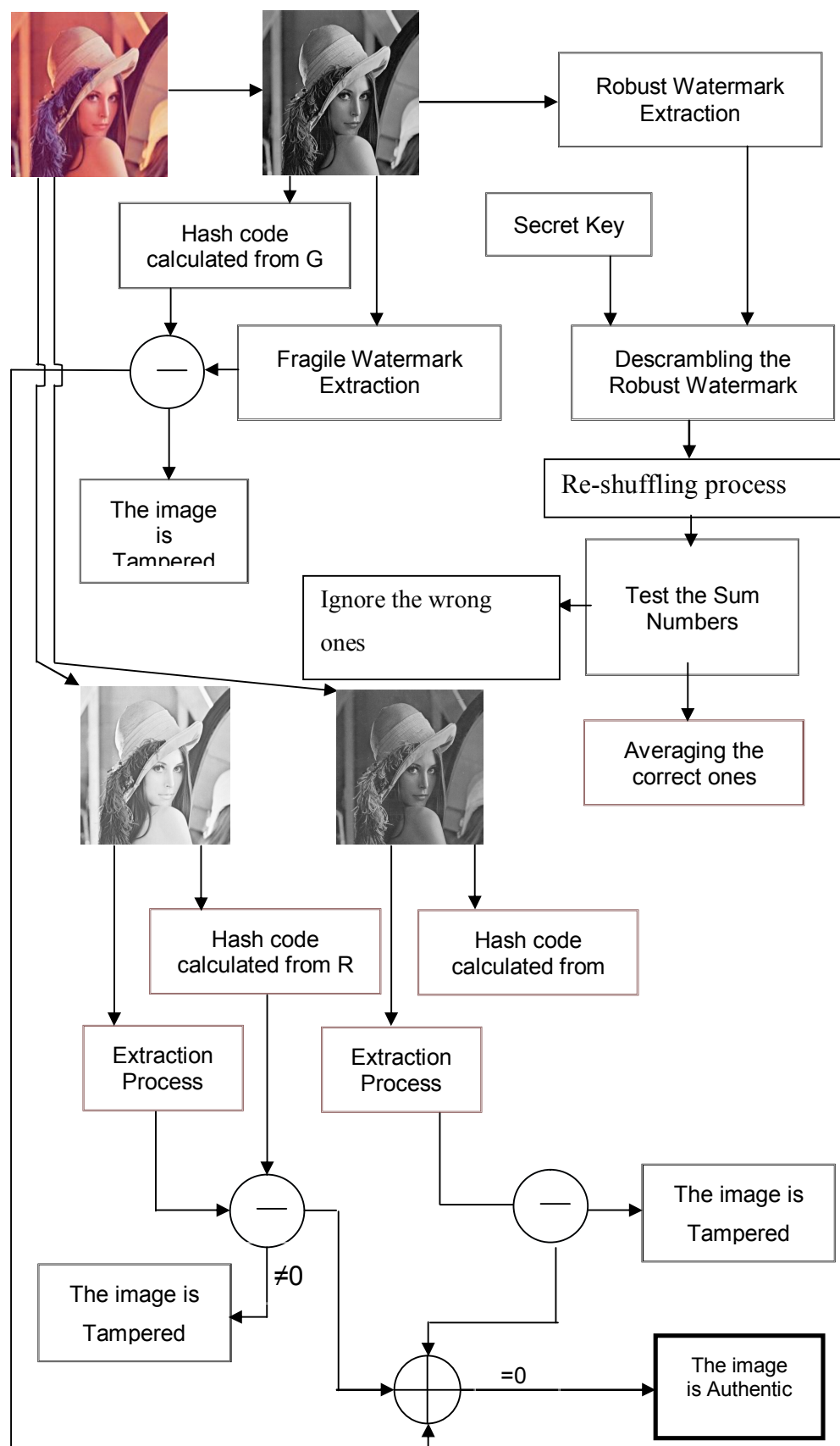


Figure 6.9: The extraction process combined algorithm of one-level DWT robust and fragile algorithms.

6.4.3 Results

The proposed algorithm contains two different types of watermarking information (Robust and Fragile). Several colour images of 512×512 with 24 bit/pixel have been used to test the robust and fragile parts of the proposed algorithm. There are two techniques that will be used to evaluate the distortion caused to the image by the watermarking. These two techniques are PSNR and SSIM.

Table 6.4 shows the PSNR between the host image and the watermarked image with different embedding strengths in order to assess the perceptual invisibility of the proposed algorithm. The average PSNR values between the watermarked and original images using the phone number as a robust watermarking information and hash function code as a fragile information watermark is tabulated in Table 6.4. The PSNR is 57dB for “Lena” with embedding strength Δ of 8. However, it is 43 dB for embedding strength Δ equals 40.

Table 5.5 shows SSIM at different embedding strengths (Δ). The test images “Lena”, “Pepper” and “Baboon” have been used to examine the perceptual quality at different embedding strength in Table 5.5. It showed that even though for the high value of the embedding strength ($\Delta = 40$), the SSIM is as high as 0.984 value. The distortion caused to the image is still imperceptible.

To assess the robustness of the combined proposed algorithm, a number of common signal processing and geometric attacks are applied to the watermarked images. In addition to that, Stirmark software has been used for the same reason. The Normalized Correlation Coefficient (NCC) is used to measure the similarity between the original and extracted robust watermark as shown in Table 6.6. The robust watermark survived against many attacks for example:

3x3 and 5x5 low-pass , 3x3 wiener and median filtering, cropping up to 80 % horizontally and 48 % vertically, salt and pepper noise, $d=0.02+$ median 3x3, contrast enhancements intensity=0.3, 0.9 and rescale from 0.4 up to 2 factor.

The fragile watermark in the combined proposed algorithm is destroyed if the watermarked image has been edited. To assess the fragile part in the combined proposed algorithm, the watermarked image is edited in different area. For example, the editing process may happen at different places in the colour image itself as shown in figure 6.10. The calculated hash code (fragile watermark) for the host image and the extracted fragile watermarked for the editing process are listed in Table 6.7.

Table 6.4: PSNR with different colour images for the combined algorithm

Image	Lena	Pepper	Baboon
PSNR at $\Delta = 8$	57.033	56.864	57.132
PSNR at $\Delta = 12$	53.684	53.492	53.695
PSNR at $\Delta = 16$	51.100	50.901	51.179
PSNR at $\Delta = 20$	49.225	49.105	49.229
PSNR at $\Delta = 24$	47.721	47.554	47.595
PSNR at $\Delta = 30$	45.662	45.524	45.687
PSNR at $\Delta = 34$	44.634	44.534	44.769
PSNR at $\Delta = 40$	43.206	43.132	43.229

Table 6.5: SSIM with different colour images for the combined algorithm

Image	Lena	Pepper	Baboon
SSIM at $\Delta = 8$	0.999	0.999	1.000
SSIM at $\Delta = 12$	0.998	0.998	0.999
SSIM at $\Delta = 16$	0.997	0.997	0.999
SSIM at $\Delta = 20$	0.995	0.995	0.999
SSIM at $\Delta = 24$	0.993	0.993	0.998
SSIM at $\Delta = 30$	0.990	0.990	0.997
SSIM at $\Delta = 34$	0.987	0.988	0.996
SSIM at $\Delta = 40$	0.984	0.984	0.995

Table 6.6: The Normalized Correlation Coefficient (NCC) for Colour Lena image with different attacks at $\Delta = 24$

Attacks	NCC	Attacks	NCC
Cropping 50% V	1	Low pass 3×3	1
Cropping 70% V	1	Low pass 5×5	1
Cropping 50% H	1	Wiener 3×3	1
Cropping 70% H	1	Wiener 5×5	1
Gaussian noise m=0, v=0.002	1	Median 3×3	1
Gaussian noise m=0, v=0.001	1	Median 5×5	0
S&P noise, d=0.02+ Median 3×3	1	JPEG 50	1
S&P noise, d=0.05+ Median 3×3	1	JPEG 25	0
Scale 2	1	Scale 0.4	1
Stirmark_AFFINE_3	1	Stirmark_CONV_1	0
Stirmark_AFFINE_8	0	Stirmark_RML_10	1
Stirmark_ROTSCALE_0.25	1	Stirmark_RML_50	1
Stirmark_ROT_-0.25	1	Stirmark_RML_100	1
Stirmark_ROTSCALE_-0.5	0	Stirmark_SS_1	1
Stirmark_ROT_0.25	1	Stirmark_SS_2	1
Stirmark_ROT_-0.5	0	Stirmark_SS_3	1



a. Edited hair



b. Edited background



c. Edited mirror

Figure 6.10: Different examples of colour image editing.

Table 6.7: MD5 Hash code Calculation for Editing Colour Images.

Hash Code	Hash for Original Image	Hash for Modified Image	Editing type
R	'41411a93896f03c683afc433 770442d6'	'8aea6bc8dd54fd609212 74fd15e51620'	Edited hair
G	'bd1fb94a2b42ea2d5190371 3c3724754'	'e3911e7b68583f8b0bca c861fb6d6b30'	Edited hair
B	'13fe4d29a0f703da5a556980 d38763a4'	'2650a911ccaa2bffb22 8b4c8c6936d7'	Edited hair
R	'41411a93896f03c683afc433 770442d6'	'6eff381c4d5dc8ed5bf3a 5ab24dbfe03'	Edited background
G	'b99c4875ab51fe45deed308c 0053813a'	'a3e92d7210e9523f80ea 81411079d2c6'	Edited background
B	'13fe4d29a0f703da5a556980 d38763a4'	'68848d5c1f2655147c0c 18734de81b62'	Edited background
R	'41411a93896f03c683afc433 770442d6'	'c3edbebc3aed02c5d03b b855237da9a7'	Edited mirror
G	'2f5e4c8e79226e69246e34ef fe91ea30'	'858e9efdef529125075a 07c9770f7f81'	Edited mirror
B	'13fe4d29a0f703da5a556980 d38763a4'	'096ad0bfda8690f49454 891328b9d5c9'	Edited mirror

6.4.4 Combined the two-level DWT robust algorithm with the fragile algorithm.

The two-level DWT robust algorithm is combined with the fragile algorithm. The block based wavelet two-level is used to embed the watermarking information into the host image. The first level of the DWT transformation is applied on 16×16 blocks of the host image. All the coefficients of the 8×8 low-low (LL1) first level sub-band are grouped into one matrix. The second level of the DWT is then applied to the grouped matrix

from the first level transformation. The area of embedding is the LL2. Only one coefficient will be used in each 4×4 block (LL2) for embedding. This coefficient has been selected by using DWCS process. On the other hand, the special domain is used in the fragile algorithm for embedding the watermarking information. The hash code is used as fragile information.

6.4.5 The embedding process and the extraction process

The embedding process for the combined algorithm is as follows:

1. The first embedding process is the robust watermarking part.
2. The robust watermarking information is a mobile phone number including its international code.
3. The sum of the decimal digital of the mobile number is added to the end of the mobile number and used as a checking parameter at the receiver side.
4. The watermark information is converted to the binary form by using BCD operation.
5. The secret key is used to scramble the watermarking information in order to increase the security of the robust algorithm part.
6. The host colour image is divided into R, G and B components.
7. The green image is divided into 16×16 blocks in the spatial domain before conversion to the DWT domain.
8. The first level of DWT is then applied to convert each block to DWT domain.
9. The second level of DWT is applied on each LL1 (8×8) blocks [5].
10. The LL2 sub block is used for the embedding process

11. The highest weight coefficient (by using DWCS process) from each block of the LL2 is used to embed one bit for the watermarking information.
12. The embedding process will be repeated several times because the size of the host image is much bigger than the 64 bits watermark.
13. A shuffling process will be used to increase the robustness of the algorithm against the vertical cropping attack.
14. The second part of the combine algorithm is the fragile watermarking part.
15. The hash code is calculated per R, G and B separately. The calculation for the pixels of R,G and B image individually excluding the frame of the image (first row, last row, first column and last column).
16. The hash code is converted to the binary form and embedded to selective pixels of the frame vector.

The embedding process for both part (robust and fragile) are shown in figure 6. 11.

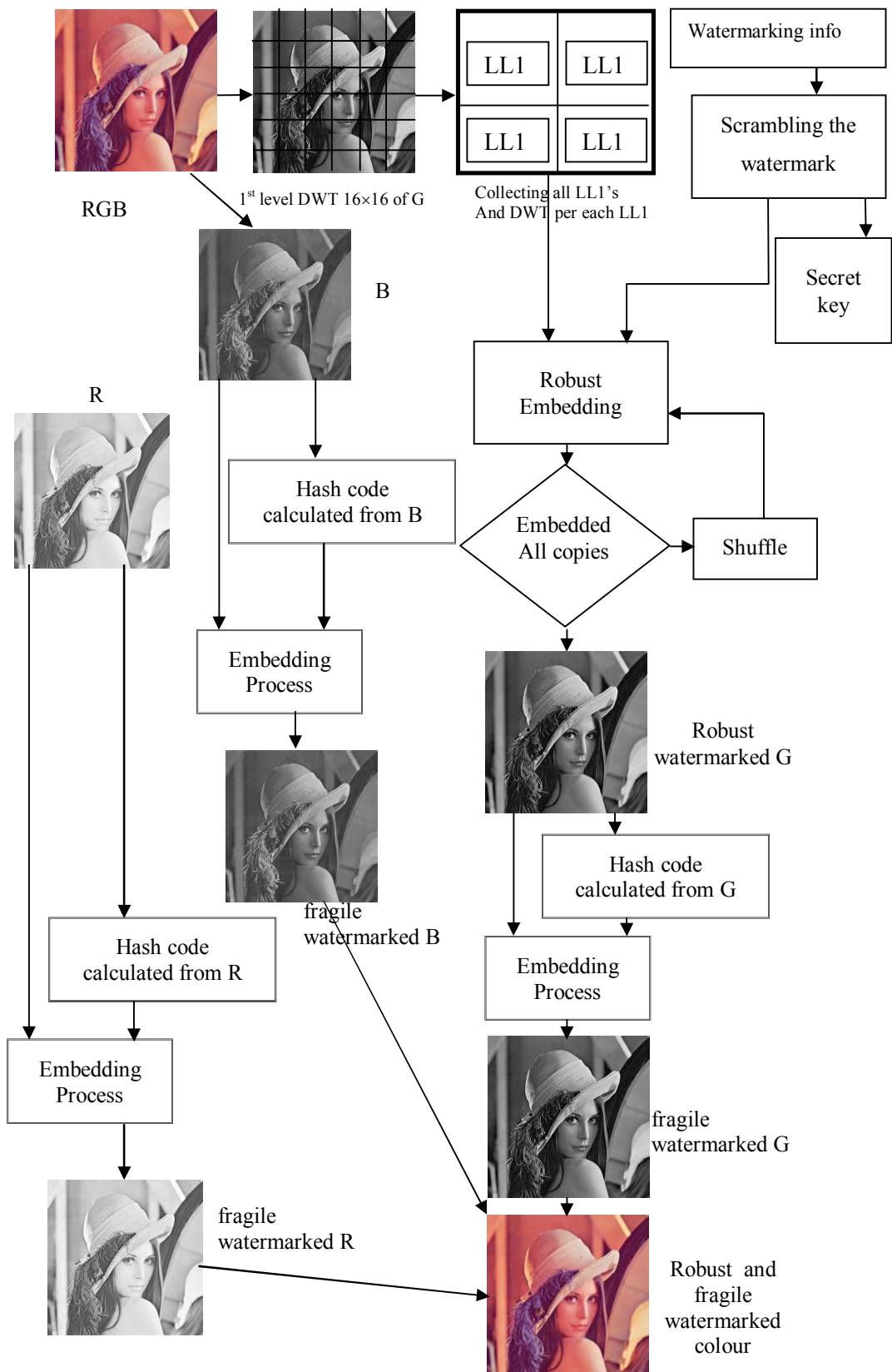


Figure 6.11: Embedding Process Combined Algorithm of two-level DWT robust and fragile algorithms.

At the decoder side, the extraction process as follows:

1. The first step is extraction the fragile watermarking.
2. The watermarked colour image is divided to R, G and B components.
3. The fragile watermarking information (Hash codes) is extracted from the frame of the R,G and B separately.
4. The hash codes are calculated like the encoder side.
5. If there is any difference between the extracted code and the calculated code for any component it means that the watermarked image has been manipulated. Otherwise it means the watermarked image is authentic.
6. The robust watermark extraction process is started after the fragile process finished.
7. The G component is divided into 16×16 blocks.
8. The DWT transformation is applied in each block to get the first level of the DWT.
9. Then the DWT level two is applied on each LL1 (8×8) block.
10. The watermarking information recovery is the inverse of the embedding process.
11. To achieve the original watermarking bits order. The watermarking bits order is achieved by applying the reverse shuffling process.
12. The secret key is used to descramble the obtained watermark to get the correct one.
13. Checksum error detection process is used at the extraction process to discover the wrong extracted watermarks and discard them before applying the averaging process.
14. The averaging process is important to enhance the quality of the extracted watermarks.

The extraction process is illustrated in figure 6.12.

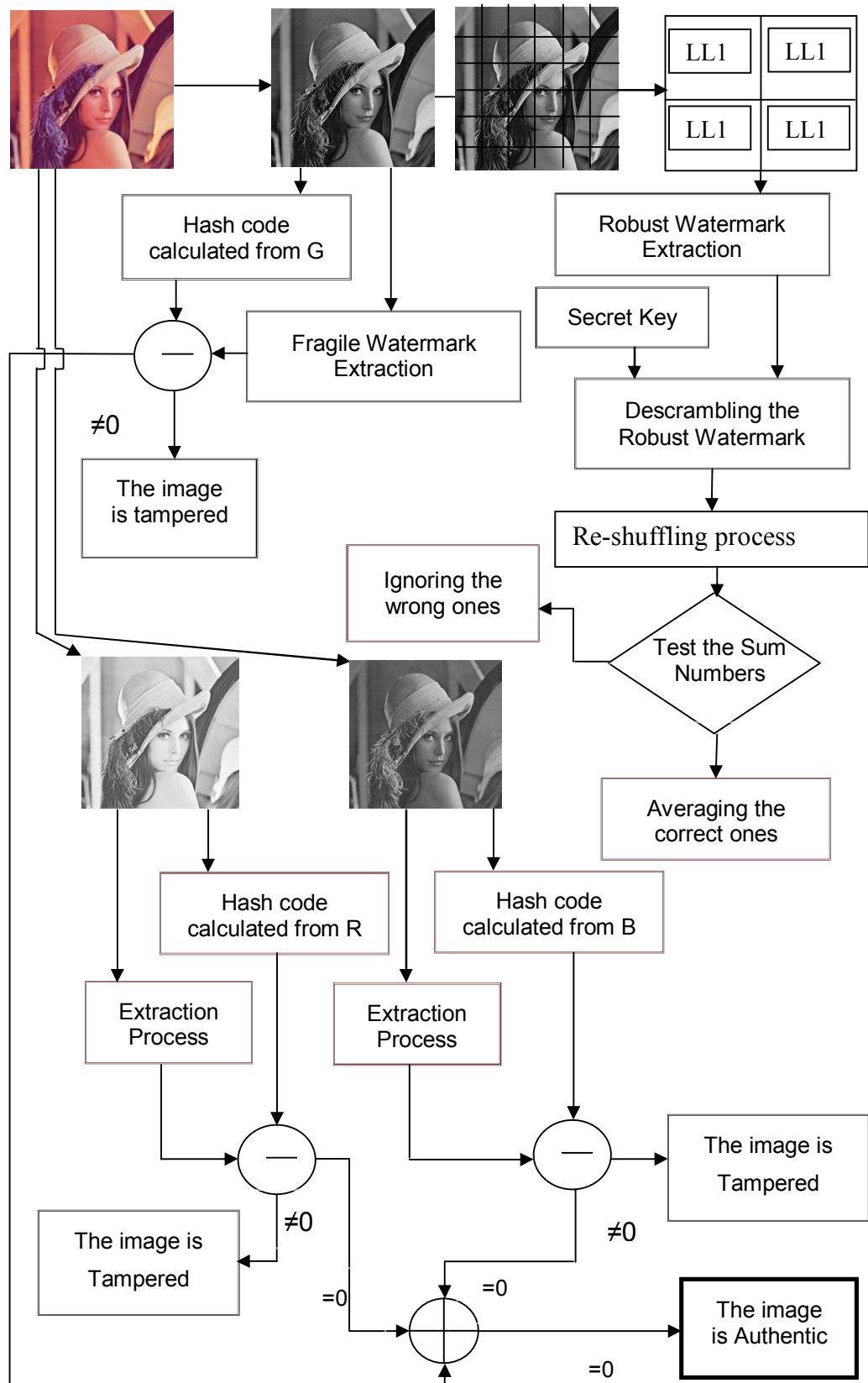


Figure 6.12: Embedding Process Combined Algorithm of two-level DWT robust and fragile algorithms.

6.4.6 Results

There are two different kinds of watermarking information (Robust and fragile) among the proposed algorithm. The proposed combined algorithm is tested by using several colour images of 512×512 with 24 bit/pixel. PSNR and SSIM techniques are used to evaluate the distortion caused to the image by the watermarking process.

The PSNR values between the watermarked and host colour image is explained in table 6.7. The PSNR recorded 61.7 dB and 48.3 dB for the original “Lena” and the watermarked image when the embedding strength (Δ) is 8 and 40 respectively.

The perceptual quality has been tested at different embedding strength on different test images (Lena, Pepper and Baboon) is shown table 6.8. The SSIM are still high values even for the high values of the embedding strength. The SSIM is achieved 0.999 value at the embedding strength ($\Delta = 40$) which means the distortion caused to the image is still unnoticeable.

The Normalized Correlation Coefficient (NCC) is used to measure the similarity between the original and the extracted robust watermark as shown in table 6.9. There are different geometric attacks and some of common signal processing is applied to the watermarked images. Moreover, Stirmark software is been used for the same reason. The robust watermark in the combined algorithm shows persist against many attacks for example: low pass, vainer and median filters, cropping up to 80 % vertically and up to 70 % horizontally, slat and pepper noise, rescale from 0.4 up to 2 factor and contrast enhancement intensity=0.3,0.9.

The fragile watermark among the combined algorithm is damaged if the watermarked is been tampered. Figure 6.13 shows examples of the edited watermarked images at different places. Table 6.10 illustrates the calculated hash code for the host images and the extracted one from the edited watermarked images.

Table 6.8: PSNR with different colour images for the combined algorithm

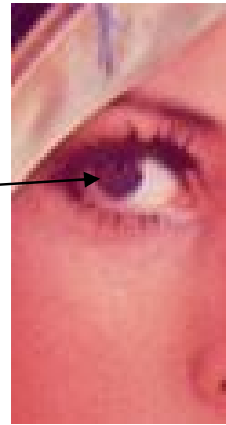
Image	Lena	Pepper	Baboon
PSNR at $\Delta = 8$	61.790	61.528	61.686
PSNR at $\Delta = 12$	58.301	58.028	58.365
PSNR at $\Delta = 16$	56.028	55.774	55.869
PSNR at $\Delta = 20$	54.179	54.241	54.119
PSNR at $\Delta = 24$	52.344	52.445	52.584
PSNR at $\Delta = 30$	50.599	50.557	50.548
PSNR at $\Delta = 34$	49.558	49.459	49.520
PSNR at $\Delta = 40$	48.286	48.229	48.313

Table 6.9: SSIM with different colour images for the combined algorithm

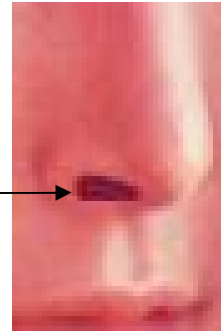
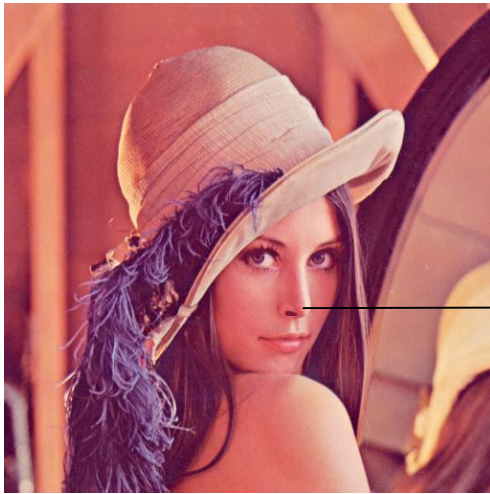
Image	Lena	Pepper	Baboon
SSIM at $\Delta = 8$	0.9999	0.9998	0.9999
SSIM at $\Delta = 12$	0.9997	0.9995	0.9999
SSIM at $\Delta = 16$	0.9995	0.9991	0.9998
SSIM at $\Delta = 20$	0.9992	0.9989	0.9997
SSIM at $\Delta = 24$	0.9988	0.9983	0.9996
SSIM at $\Delta = 30$	0.9982	0.9978	0.9995
SSIM at $\Delta = 34$	0.9977	0.9971	0.9993
SSIM at $\Delta = 40$	0.9969	0.9963	0.9990

Table 6.10: The Normalized Correlation Coefficient (NCC) for Colour Lena image with different attacks at $\Delta = 24$

Attacks	NCC	Attacks	NCC
Cropping 50% V	1	Low pass 3×3	1
Cropping 80% V	1	Low pass 5×5	1
Cropping 50% H	1	Wiener 3×3	1
Cropping 75% H	1	Wiener 5×5	1
Gaussian noise m=0, v=0.002	1	Median 3×3	1
Gaussian noise m=0, v=0.001	1	Median 5×5	0
S&P noise, d=0.02+ Median 3×3	1	JPEG 50	1
S&P noise, d=0.05+ Median 3×3	1	JPEG 25	0
Scale 2	1	Scale 0.4	1
Stirmark_AFFINE_3	1	Stirmark_CONV_1	0
Stirmark_AFFINE_8	0	Stirmark_RML_10	1
Stirmark_ROTSCALE_0.25	1	Stirmark_RML_50	1
Stirmark_ROT_-0.25	1	Stirmark_RML_100	1
Stirmark_ROTSCALE_-0.5	0	Stirmark_SS_1	1
Stirmark_ROT_0.25	1	Stirmark_SS_2	1
Stirmark_ROT_-0.5	0	Stirmark_SS_3	1



Edited eye



Edited nose



Edited eyebrow

Figure 6.13: Different examples of colour image editing

Table 6.11:MD5 Hash code Calculation for Editing Colour Images.

Hash Code	Hash for Original Image	Hash for Modified Image	Editing type
R	'25d0836df47ee3faeba0e1221d7692ec'	'3fd8996617f3cd58ee864bd5580029e1'	Edited eye
G	'7b9083044f1036175895faec0dcf57d6'	'5cfab2cdcc34acae40e552d10ab29ebb'	Edited eye
B	'f6d3857b6ae8885369754cf55a92a16f'	'64f93030bf787057c966702803142766'	Edited eye
R	'25d0836df47ee3faeba0e1221d7692ec'	'ee2db95f1903c33a5789f94f0a928b2f'	Edited nose
G	'7b9083044f1036175895faec0dcf57d6'	'0a7290cb9b6e79d06d0c43214b4b5370'	Edited nose
B	'f6d3857b6ae8885369754cf55a92a16f'	'e29458dad839a9fc48873f53b374f602'	Edited nose
R	'25d0836df47ee3faeba0e1221d7692ec'	'47d34736a4c04425caf218a56e2901fc'	Edited eyebrow
G	'7b9083044f1036175895faec0dcf57d6'	'819fb5fb0bdab111e0688d85e1149576'	Edited eyebrow
B	'f6d3857b6ae8885369754cf55a92a16f'	'2e156adc1e03fe2a9de81acaded9634c'	Edited eyebrow

6.5 Comparison with Previous Work

The comparisons between the proposed combined algorithms for the robust and fragile watermarking, the proposed algorithm for the robust watermark (chapter four) and the watermark algorithm method stated in [6], [7], [8], [9] and [10].

Table 6.8 shows the comparison between algorithms in PSNR for different embedding strengths. It should be noted that the PSNR for the combined algorithm which contain two-level DWT robust and fragile watermarks (fragile and robust) and the two-level robust algorithm are better than one-level DWT robust and the DCT algorithm [6], [7] and [8].

The similarity between the watermarked image and the host image is another important factor which must be considered for the watermarking algorithms. Table 6.9 lists the comparison between SSIM for different embedding algorithms. Even though the combined algorithm contains two watermarks, the SSIM values are still acceptable and higher than in [7] and [8].

The similarity between the original watermark and the extracted one can be measured by the Normalized Correlation Coefficient (NCC). For the algorithm which used the mobile number as a watermark information, NCC should be 1 otherwise the watermark information cannot be recovered correctly. Table 6.10 shows the comparison between algorithms in NCC for different types of attacks. It can be noticed that extracted watermark is identical with the original watermark with many attacks and the proposed algorithm is more robust to attacks.

Table 6.12: The PSNR for Lena colour image with different Δ

	(2 levels robust +fragile)	(1level robust +fragile)	2 levels DWT	One-level DWT	[6]	[7]	[8]
$\Delta= 16$	56.028	51.099	57.712	51.813	44.2	51.440	38.5
$\Delta= 24$	52.344	47.720	54.007	48.144	41.1	47.876	37.4
$\Delta= 34$	49.558	44.634	51.114	45.129	38.2	44.798	35.2
$\Delta= 40$	48.286	43.207	49.738	43.941	36.1	43.222	34

Table 6.13: The SSIM for Lena colour image with different Δ

	(2 levels robust +fragile)	(1level robust +fragile)	2 levels DWT	One- level DWT	[7]	[8]
$\Delta=16$	0.999	0.997	0.999	0.997	0.998	0.997
$\Delta=24$	0.999	0.993	0.999	0.994	0.995	0.985
$\Delta=34$	0.998	0.987	0.998	0.989	0.990	0.975
$\Delta=40$	0.997	0.984	0.997	0.986	0.987	0.971

Table 6.14: The NCC for Lena colour image with different types of attacks

Attacks	(2 levels robust +fragile)	(1level robust +fragile)	2 levels DWT	One-level DWT	[7]	[9]	[10]
Cropping 50% V	1	1	1	1	0.793	0.97	0.999
Cropping 50% H	1	1	1	1	1	0.98	0.999
Cropping 75% H	1	1	1	1	1	1	1
Gaussian noise $m=0$, $v=0.002$	1	1	1	1	1	0.85	0.7801
S&P noise, $d=0.02+$ Median 3×3	1	1	1	1	1	0.99	0.9925
Scale 2	1	1	1	1	1	1	1
Low pass 3×3	1	1	1	1	1	0.99	0.981
Wiener 3×3	1	1	1	1	1	0.99	0.9931
Median 3×3	1	1	1	1	1	0.99	0.992
JPEG 50	1	1	1	1	1	0.99	1
JPEG 25	1	1	1	1	1	0.98	0.963
Scale 0.4	1	1	1	1	1	0.88	0.88

6.6 Final Remarks

In this chapter, the aims of this scheme discussed are copyright protection and the authentication. The proposed algorithms used two different types of watermarking information, the mobile number as a robust watermarking and the hash function for the host image as fragile watermarking information. Even though the scheme is combined two algorithms, it is still blind and the PSNR is still very high. Moreover, the SSIM values are high which means the difference between the watermarked image and the host image is not noticeable.

The robust part of the scheme has survived several attacks such as 70 % cropping (horizontal and vertical), scaling up to 80%, additive noise, filtering and StirMark attacks. The fragile watermark is destroyed if the watermarked image is edited.

6.7 References

- [1] V. Kitanovski, D. Taskovski, and S. Bogdanova “Combined Hashing/Watermarking Method for Image Authentication”, *International Journal of Information and Communication Engineering* , pp 223-229, 2007.
- [2] A. G. Konheim, “*Hashing in Computer Science: Fifty Years of Slicing and Dicing*”, John Wiley & Sons, INCC, 2010.
- [3] S. Radharani, and M.L. Valarmathi, “A Study on Watermarking Schemes for Image Authentication”, *International Journal of Computer Applications*, Vol. 2 No.4, pp 24-32 June 2010.
- [4] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji & A. Tawfik, “A new watermarking scheme for colour images captured by mobile phone cameras,” *International Journal of Computer Science and Network Security*, vol. 9 No. 7, July 2009, pp248-254.

- [5] N. Kashyap, and G. Sinha, “Image Watermarking Using 2-Level DWT”, *Advances in Computational Research*, ISSN: 0975 - 3273 & E- ISSN: 0975-9085, Vol. 4, Issue 1, pp.-42-45, 2012.

- [6] I. Kong and C. Pun, “Digital Image Watermarking with Blind detection for Copyright Verification ”, *IEEE computer society, 2008 Congress on Image and Signal Processing*, Vol. 1, pp. 504-508, May 2008.

- [7] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji and A. Tawfik, “A New Watermarking Scheme For Colour Images Captured By Mobile Phone Cameras”, *IJCSNS International Journal of Computer Science and Network Security*, VOL.9 No.7, pp. 248 - 254, July 2009.

- [8] V. Sreejith, K. Sritith and R. Roy, “Robust Blind Digital Watermarking in Contourlet Domain”, *International Journal of Computer Applicationa*, Vol. 58, No. 12, pp. 13 – 19, November, 2012.

- [9] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji and A. Tawfik, “A Frequency Domain Adaptive Watermarking Algorithm for Still Colour Images,” *International Conference on Advances in Computational Tools for Engineering Application, ACTEA '09*, Lebanon, pp. 186 – 191, 2009.

- [10] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji and A. Tawfik, “Watermarking of Colour Images in the DCT Domain Using Y Channel”, *IEEE/ ACS International Conference on Computer Systems and Applications*, Morocco, pp. 1025 – 1028, 2009.

CHAPTER 7

Conclusion and Recommendation for Future Works

7.1 Introduction

Digital image watermarking for still images is a hot topic of research. Many researches are working to overcome some problems related to watermarking. However, many drawbacks and challenges are still waiting to be studied. There are a lot of steps that are required to be achieved before using the watermarking technology in court in copyright cases. This chapter presents a summary of the work, emphasizing the main conclusions and submitting some recommendations for further work.

7.2 Work Summary

The presented research in this thesis can be categorized as follows:

- The robust watermarking algorithms for copyright protection based on block based Discrete Wavelet Transform.
- The fragile watermarking algorithm for authentication based on hash function.
- The combined fragile and robust algorithms for copyright protection and authentication.

The first category is the development and assessment of a blind Discrete Wavelet Transform block based images algorithms for copyright protection suitable for grey and colour still images using mobile number as a watermarking digital information. The Low Low sub-bands have been chosen for embedding the watermarking information because the other sub-bands like High High sub-bands may be discarded in some image processing like JPEG compression process. The digital information watermarking has been scrambled by using a secret key in order to increase the security of the algorithm. The spatial autocorrelation between the watermark and the image problem have been solved by implementing a shuffle scheme. The shuffling process is improved the robustness against the vertical cropping attack. The watermarking information is embedded several times in the host image which increased the robustness against different attacks. The distortion caused due to the embedding of the watermarking into the host image is light and it is not noticeable. The recovered watermarking is digital numbers and evaluated by using Normalized Correlation Coefficient (NCC). The robust algorithms showed robustness against low-pass filter attack, wiener filter attack, median filter attack, scale attack, JPEG attack, salt and pepper noise attack, Gaussian noise attack and Stirmark attack. More than 25 colour images were used to examine the algorithms. The sizes of the images are 512×512 and high resolution images 1024×1024 were also used. The PSNR and SSIM techniques were used to evaluate the algorithms.

The second category is the fragile algorithm based on using the hash function. The algorithm operates in the spatial domain. The algorithm has used the hash function as a fragile watermark. The fragile algorithm showed high sensitivity to any kind of attacks or image manipulation. MD5 hash code has been used in the algorithm. The hash code

is calculated for the host image a part from the first row, last row, first column and last column were excluded. The hash code is embedded on the frame of the host image. The distortion caused by embedding the hash function is very little and does not affect the host image. The hash function for the colour image is embedded in all image RGB components. Therefore, any tampering in any component or on the colour image will result in the destructions the fragile watermark.

The third category is combining the fragile algorithm with the robust algorithm. This combination works as a multitasking system. The combined algorithm is used for authentication checking and copyright protection. The multi-task combined algorithm has shown high resistivity against several attacks by the robust attack. On the other hand the fragile part is very sensitive against any attack or image tampering.

7.3 Conclusions

The following remarks can be concluded:

The robust algorithms can be used with different format files, different sizes and types of images. They use block base Discrete Wavelet Transform in one-level and two-levels; with the watermarking information being a digital mobile number with an international code. The Low Low sub-bands have also been used for embedding, with the embedding coefficient chosen based on the DWCS process.

Scrambling of the watermarking information is applied by using a secret key to increase the security of the algorithm. The embedding process is repeated several times, because the size of the watermarking information is small, compared with the size of the host image. The shuffle process is used for repeating the watermark, so to avoid auto

correction between the watermark and the host image. The robust algorithms are completely blind and there is no need for the original image to be used in the receiver side during the extracting watermarking process. The PSNR values are higher than 63 dB for the two-level DWT transform algorithm with the SSIM recorded as 0.9998, for the two-level DWT transform algorithm.

The robust algorithm can survive against JPEG of up to a compression factor of 25. The scale factor attack from 0.4 up to 2 does not affect the robust algorithm. The new algorithms are robust against low-pass, median and Wiener filter attacks and noise attacks, such as Gaussian and salt and pepper, have no effect on the robust algorithm. The fragile algorithm showed sensitivity against any attack or image tampering. For the colour host images, embedding takes place in all the image components (R, G and B). Any tampering, in one of the watermarked components or the colour host image itself, will destroy the fragile watermark. However even though the combined algorithm contained two different watermarking embedding, the PSNR recorded above 57 dB and the SSIM was 0.999, which means the distortion caused by both watermarking methods is still low and not noticeable. The combined algorithms can be used for more than one purpose. They can be used for copyright ownership and the authentication of the media content.

7.4 Recommendations for Future Work

There are different directions for further work of research that may improve the performance and achieve greater benefits. Suggestions and recommendations for the future include the focus on high resolution images, as new digital camera devices and mobile phones have high resolution images; including the real time implementation of the run algorithms is an interesting area to investigate, in order to utilise the algorithms in mobile devices. Also other types of watermarking information may be used; such as handwritten signatures, images, logos and text. Semi fragile watermarks may be added to the combined algorithm in order to get one system which has combined robust, fragile and semi fragile watermarks. Also the combined algorithm can be oriented towards medical image applications with the developed combined algorithm being tested for medical images in the future. Finally audio and video applications are not covered within the scope of the thesis, therefore future work may try to implement the development algorithms in audio and video applications.

Appendix A

LIST OF PUBLICATIONS

1. **T Jassim**, RA Abd-Alhameed, H Al-Ahmad, A Al-Gindy, “A Block Based Wavelet Algorithm for Watermarking Still Colour Images Captured by Mobile Phone Cameras”, *Information Science and Digital Content Technology (ICIDT)*, 2012 8th International Conference on, Jeju Island, Korea (South), 2012, Vol. 2, pp. 287- 292.
2. **T Jassim**, RA Abd-Alhameed, H Al-Ahmad, “ A New Robust and Fragile Watermarking Scheme for Images Captured by Mobile Phone Cameras”, *Communications, Signal Processing, and their Applications (ICCSPA)*, 2013 1st International Conference on, Sharjah, UAE, 2013, pp. 1-5.
3. **T Jassim**, RA Abd-Alhameed, H Al-Ahmad, “ New Robust and Fragile Watermarking Scheme for Colour Images Captured by Mobile Phone Cameras”, *Computer Modelling and Simulation (UKSim)*, 2013 UKSim 15th International Conference on , Cambridge, UK, 2013, pp. 465 - 469.
4. **T Jassim**, RA Abd-Alhameed, H Al-Ahmad, A Al-Gindy, “Two-level Block Based Wavelet Watermarking Algorithm For Still Colour Images”, *BCS International IT Conference 2014*, Abu-Dhabi, UAE, 2014.

A Block Based Wavelet Algorithm For Watermarking Still Colour Images Captured By Mobile Phone Cameras

T. Jassim
School of Engineering
University Of Bradford
Bradford
UK
taha.jassim@adveti.ac.ae

H. Al-Ahmad
ECE Department
Khalifa University of Science, Technology and Research
Sharjah
UAE
alahmad@kustar.ac.ae

R A Abd-Alhameed
School of Engineering
University Of Bradford
Bradford
UK
r.a.a.abd@bradford.ac.uk

A. Al-Gindy
Engineering College
Ajman University for Science and Technology
Ajman
UAE
agindy@hotmail.com

Abstract—This paper deals with a block based wavelet algorithm for digital watermarking of still colour images captured by mobile phone cameras. The algorithm use mobile phone numbers including the international code as the watermarking information. The host image is divided into 8×8 blocks and the watermark is embedded into one block of the LL sub-band coefficients of the green channel of the RGB colour image. The embedding is done into one of the higher weight coefficients of the LL sub-band. The algorithm is blind and does not require the original image for extracting the watermark. The watermarking caused minimal distortion to the host images and the PSNR is > 50dB. The robustness of the proposed algorithm is tested against several attacks and it survived cropping, scaling, filtering, additive noise and JPEG compression.

Keywords: *Wavelet transform; watermarking; image processing.*

I. INTRODUCTION

Digital data can be copied and transferred easily from one place to another. This leads to unauthorized replication problem which caused many copyright disputes regarding the ownership of the digital contents. Watermarking of digital data by using hidden information is one of the solutions to this problem. There are different watermarking techniques for digital images and they can be classified into spatial and transformed domains. Usually transformed domain techniques are more robust compared to spatial domain ones. Different transformations are used in watermarking such as the discrete cosine transform, Fourier transform and wavelet transform.

There are a lot of wavelet based watermarking algorithms for gray level images. On the other hand algorithms for colour images are not as common as those for gray level images. Colour images are more common in real life and

have a large amount of information compared to gray images. This information can be utilised for embedding more watermarking information [1]. A watermarking algorithm for colour images by using the wavelet transform was discussed in [2]. To ensure the invisibility of the watermark, the algorithm was carried out in the YCbCr colour space. However, the PSNR for this algorithm is low (between 31dB to 34 dB). Another algorithm is proposed for colour images, providing robustness against a set of attacks in [3]. The authors have used a wavelet transform algorithm then the discrete Hadamard transform (DHT) is applied. These cascaded algorithms gave them the opportunity to select the most appropriate coefficients, which are close to the low and middle frequencies. These frequencies are uncorrelated in nature. However, this technique is not blind and the original image is required to extract the watermark. An image authentication and recovery algorithm which operates in the wavelet domain is proposed in [4]. Another algorithm that applies a casting operation of a binary message onto the wavelet coefficients of coloured images decomposed at multi-level resolution is proposed in [5]. In the extraction process, the original “unwatermarked” image is used to estimate the embedded bit-stream. A reversible image authentication technique with tamper localization based on watermarking in integer wavelet transform is proposed in [6]. If the image authenticity is verified, then the distortion due to embedding the watermark can be completely removed from the watermarked image. If the image is tampered with then the tampering positions can also be localized. A robust watermarking algorithm using the wavelet transform and edge detection is presented in [7]. The efficiency of this algorithm depends on the preservation of visually significant information. This is attained by embedding the watermark transparently with the maximum possible

strength. The watermark information is embedded in the sub-band coefficients that lie on edges, where distortions are less noticeable.

The watermarking information used in the previous techniques were signatures, logos or pseudo random numbers. In this paper the watermarking information is the mobile number including the international code. For images captured by a mobile phone camera the best watermark information is the mobile phone number including the international code. The reason for this is each individual has a unique number all over the world [8]. The distortion caused to the original image by the watermarking process can be assessed by using the peak to signal to noise ratio (PSNR) and the structured similarity index (SSIM) [9].

In this paper, a new robust wavelet watermarking technique is presented. The algorithm is blind and does not require the original image for extracting the watermark. There are four sections in this paper. Sections II deals with the watermarking embedding and extraction algorithms. The experimental results are given in Section III, followed by the conclusions in Section IV.

II. THE PROPOSED WATERMARKING ALGORITHM

The new algorithm uses a block based wavelet algorithm to embed the binary watermark into the colour host image. The wavelet transformation is applied and divided the components into four parts LL (low low frequencies), LH (low high frequency), HL (high low frequencies) and HH (high high frequencies). The embedding is done in the LL. Since small high frequency components may be discarded in some image processing operation such as JPEG compression, the very low frequency components of the colour host image will be utilized during the watermark embedding. Only 8 coefficients will be used in each 8×8 block for embedding.

A. The Embedding Algorithm

Colour images can be separated into three components R, G and B. In this algorithm the watermark information will be embedded in the green component. The watermarking information used is the mobile number including the international code. The UAE number contains 14 decimal digits. We added the sum of these 14 digits (2 digits) at the end of the mobile number. The 2 decimal digits will be used as a checking parameter for the correct number after extracting it at the receiver side. The watermark plus the sum will be 16 decimal digits. Each decimal number is converted into 4 bit using BCD code. Therefore the watermarking information will be 64 bits. A secret key has been used to scramble the binary watermark digits randomly. The scramble process is important to reduce the correlation between the host image and the embedded watermark. The host image will be divided into 8×8 blocks in the spatial domain then each block will be converted using the wavelet transformation. This will result in 4 sub blocks each block is 4×4 coefficients. These sub blocks are: Low Low frequency coefficients (LL),

Low High coefficients (LH), High Low coefficients (HL) and High High coefficients (HH). In this algorithm, one binary digit will be embedded in one of the higher coefficients of LL sub block. The watermarking information will be repeated several times because the size of the image is much bigger than the 64bit watermark. The shuffling process will be used [8] to improve the robustness against vertical cropping.

Assume that $f(i,j)$ represents the pixel of the G component of the RGB representation of the colour host image, $w(i,j)$ represents the binary pixel of the watermark and

$$F_k(u,v) = DWT\{f_k(i,j)\},$$

If $w(i,j)=1$ then

$$F(x,y) = \left(\frac{\Delta Q_e \left(\frac{F_k(x,y)}{\Delta} \right)}{F_k(x,y)} \right) \quad \begin{matrix} x_{LL} \neq H_k \\ x_{LH} \neq H_k \end{matrix} \quad \begin{matrix} 1 \text{ if } x_{LL} \neq H_k \\ 1 \text{ if } x_{LH} \neq H_k \end{matrix} \quad \dots \quad (1)$$

If $w(i,j)=0$ then

$$F(x,y) = \left(\frac{\Delta Q_o \left(\frac{F_k(x,y)}{\Delta} \right)}{F_k(x,y)} \right) \quad \begin{matrix} x_{LL} \neq H_k \\ x_{LH} \neq H_k \end{matrix} \quad \begin{matrix} 1 \text{ if } x_{LL} \neq H_k \\ 1 \text{ if } x_{LH} \neq H_k \end{matrix} \quad \dots \quad (2)$$

Where $1 \leq x, y \leq 8$, and Q_e is the quantization to the nearest even number and Q_o is the quantization to the nearest odd number, Δ is a scaling quantity and it is also the quantization step used to quantize either to the even or odd number. The 8×8 block is converted back to the spatial domain and the process is repeated with the other blocks. The watermarked G component is added to the R and B components to produce the watermarked colour image. Figure 1 illustrates the embedding process.

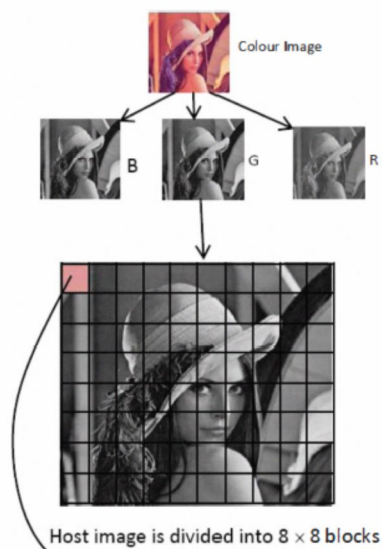
B. The Extraction Algorithm

In order to extract the watermarking information, the watermarked colour image is separated into RGB components. The G component is divided into 8×8 blocks. Each block is converted into the DWT domain. The recovery process is the inverse of the embedding process. Each predefined frequency coefficient is quantized by Δ and rounded to the nearest integer. The formula used for extracting is defined as follows:

$$\text{If } Q \left(\frac{F_k(x,y)}{\Delta} \right) \text{ is odd then } w(i,j) = 0$$

$$\text{If } Q \left(\frac{F_k(x,y)}{\Delta} \right) \text{ is even then } w(i,j) = 1 \quad \dots \quad (3)$$

Where: Q is rounded to the nearest integer.



274	275	267	272	0	1	9	4
274	273	267	272	0	1	9	4
277	267	266	268.5	0	1	6	15
267	267.5	267.5	267.5	0	25	-25	1
LL				LH			
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
-3	6	-1	5.5	0	0	3	25
1	65	55	0	0	55	-0.5	3
HL				HH			

Wavelet for each 8×8 blocks of the host

Figure I –A Embedding Process

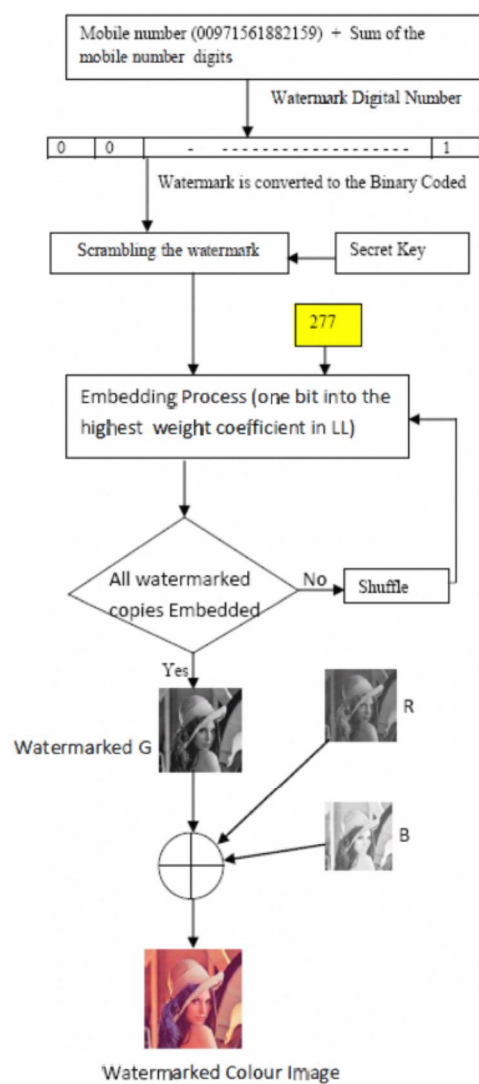


Figure I –B Embedding Process

Δ is the same parameter which has been used in the embedding process. An extraction process is as shown in Figure II.

Each coefficient of the image that carries one bit of the embedded watermarks can be extracted by using the above method. These extracted bits will create the embedded watermarks information $w(i,j)$. The watermarking can be obtained by implementing the reverse shuffling process. The same secret key I used in the initial scrambling operation will be used. The scrambled watermarks are descrambled to obtain the original watermarks. In the extraction process there is no need for the original image. The check sum will be used to discard the wrong extracted numbers.

III. RESULTS

The proposed algorithm is examined using different colour images of size 512×512 with 24 bits per pixel. The mobile number has been used as the watermarking information because it is unique and is more intuitive for representing one's identity. Two techniques have been used to assess the distortion caused to the image by the watermarking process. The first one is the PSNR between the host original image and the watermarked image. Table I illustrate the perceptual invisibility of the proposed algorithm at different embedding strengths. The average PSNR values between the watermarked and original images using the phone number as the watermark information are shown in table I. The second one is the SSIM between the host image and the watermarked image. The higher the SSIM percentage is, the larger the similarity between the compared images. In table I, the distortion caused by the watermarking process is assessed using SSIM at different embedding strengths. Test colour images "Lena", "Pepper" and "Baboon" have been used to examine the perceptual quality at different embedding strengths as shown in table I. The PSNR achieved with different images are higher than 40 dB. The SSIM is very good and higher than 0.98. Figure III shows the images using different strengths. It is clear that the distortion caused to the images is imperceptible even with high values of Δ .

Several attacks were applied to the watermarked images to assess the robustness of the proposed algorithm. Stirmark software package was used for this purpose. The normalized correlation (NC) is used to measure the similarity between the original and the extracted watermark as shown in table II. The algorithm survived 3×3 and 5×5 low-pass filtering, cropping up to 75% horizontally and vertically, high JPEG compression and Gaussian and salt and pepper noise.

The new algorithm managed to achieve very high PSNR and SSIM values and survived many attacks compared the DCT algorithm used in [8].

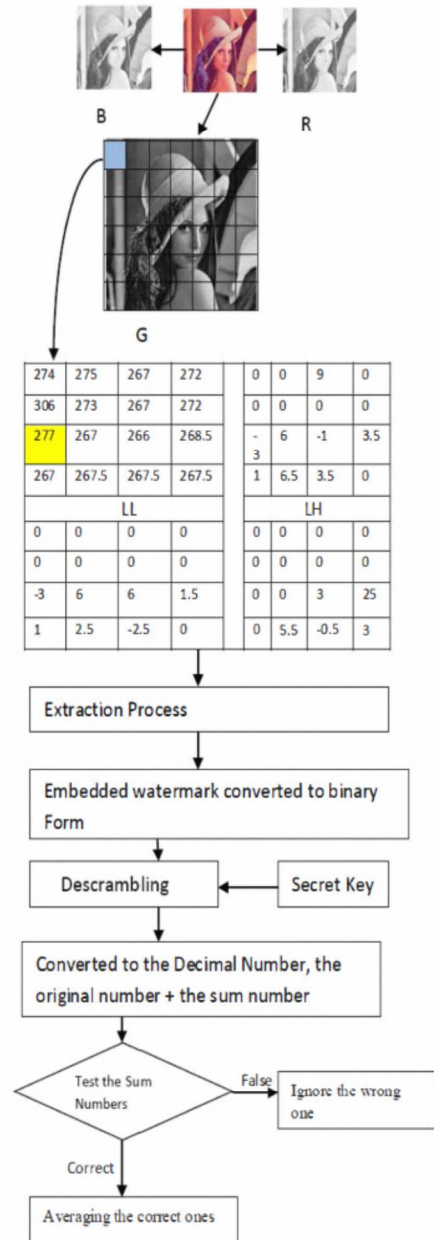


Figure II Extraction Process

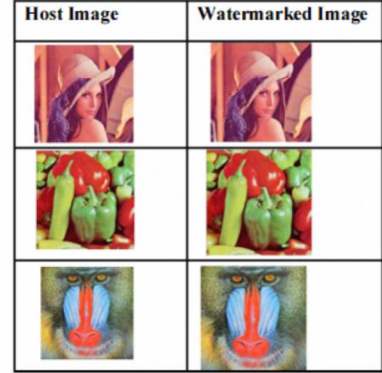
Table I PSNR and SSIM at Different Embedding Strengths

Image	Lena	Pepper	Baboon
PSNR at $\Delta = 8$	57.53 dB	57.4368 dB	57.49 dB
PSNR at $\Delta = 12$	54.05 dB	54.0909 dB	54.148 dB
PSNR at $\Delta = 24$	48.11 dB	47.9852 dB	48.08 dB
PSNR at $\Delta = 30$	46.12 dB	46.0101 dB	46.22 dB
PSNR at $\Delta = 34$	45.097 dB	45.0135 dB	45.11 dB
PSNR at $\Delta = 40$	43.875 dB	43.5268 dB	43.61 dB
SSIM at $\Delta = 8$	0.9993	0.9991	0.9998
SSIM at $\Delta = 12$	0.9985	0.9982	0.9995
SSIM at $\Delta = 24$	0.9943	0.9931	0.9981
SSIM at $\Delta = 30$	0.9914	0.9897	0.9972
SSIM at $\Delta = 34$	0.989	0.9874	0.9963
SSIM at $\Delta = 40$	0.9861	0.9839	0.9948

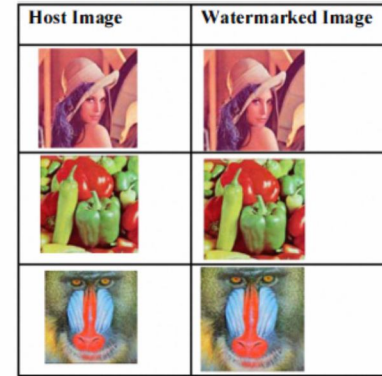
Table II The normalized correlation (NC) for Lena image with different attacks, Watermark size 96×64 , at $\Delta = 34$.

Attacks	NC	Attacks	NC
Cropping 75% V	1	Low pass 3×3	1
Cropping 50% V	1	Low pass 5×5	1
Cropping 75% H	1	Wiener 3×3	1
Cropping 75% V+H	1	Wiener 5×5	1
Scale 2	1	Median 3×3	1
Scale 0.75	1	Median 5×5	1
Gaussian noise $m=0, v=0.002$	1	JPEG 75	1
Gaussian noise $m=0, v=0.001$	1	JPEG 50	1
S&P noise, $d=0.02$ Median 3×3	1	JPEG 25	1
S&P noise, $d=0.05$ Median 3×3	1	JPEG 20	1
S&P noise, $d=0.02$	1	Scale 0.4	1

Figure III Watermarked images with different strengths $\Delta = 24$



$\Delta = 24$



$\Delta = 40$

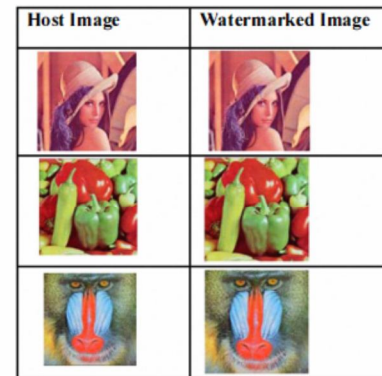


Table III Comparison of PSNR at Different Embedding Strengths for Our Proposed Algorithm and the DCT Algorithm [8]

Image	DCT Lena	Wavelet Lena	DCT Pepper	Wavelet Pepper
PSNR at $\Delta = 16$	51.4395	51.573	50.6715	51.3598
PSNR at $\Delta = 24$	47.8758	48.11	46.5765	47.9716
PSNR at $\Delta = 34$	44.7981	45.0981	43.1761	45.0135
PSNR at $\Delta = 40$	43.2219	43.875	42.0291	43.5268

Table IV Comparison of Structural Similarity Index Measurements SSIM at Different Embedding Strengths for Our Proposed Algorithm and the DCT Algorithm [8]

Image	DCT Lena	Wavelet Lena	DCT Pepper	Wavelet Pepper
SSIM at $\Delta = 16$	0.9979	0.9973	0.9963	0.9966
SSIM at $\Delta = 24$	0.995	0.9943	0.9918	0.9931
SSIM at $\Delta = 34$	0.9902	0.989	0.9829	0.9878
SSIM at $\Delta = 40$	0.9865	0.9863	0.9778	0.9834

IV. CONCLUSIONS

A new watermarking algorithm for colour images using the green channel has been presented. The algorithm used the mobile phone number as the watermarking information. To increase the invisibility qualities a suitable DWT coefficient selection process has been applied with high magnitudes. Several watermarking strengths have been examined and the best watermarking strength is found to be $\Delta=34$. The algorithm achieved PSNR > 40 dB and SSIM > 0.98. The proposed algorithm is blind and robust against attacks. The proposed algorithm has shown to be resistant to JPEG compression, additive noise, cropping, scaling and low-pass filters attacks. The new wavelet algorithm achieved better results compared to the DCT algorithms.

REFERENCES

- [1] S. Batmavady, K. Manivannan, "Wavelet based Watermarking of fused image for Telemedicine Applications", Int. J. on Recent Trends in Engineering & Technology, vol. 05, no. 01, pp 70-73 March 2011
- [2] F. LIANG, L. WANG, "An Improved Wavelet-Based Color Image Watermark Algorithm", Journal of Computational Information Systems, pp 2013-2020, 2011.
- [3] G.S.El-Taweel, Onsi, M.Samy, M.G. Darwish, "Secure and Non-Blind Watermarking Scheme for Color Images Based on DWT",

ICGST International Journal on Graphics, Vision and Image Processing GVIP, vol. 05, Issue 4, pp 1-5, April 2005.

- [4] S. Lee, et.al, "Reversible Image Watermarking Based on Integer-to-Integer Wavelet Transform", IEEE Transaction on Information Forensics and Security, vol. 2, No. 3, pp. 321-330, September 2007.
- [5] A. Khalifa and S. Hamad, "A Robust Non-blind Algorithm for Watermarking Color Images using Multi-resolution Wavelet Decomposition", International Journal of Computer Applications, vol. 37, No.8, pp. 33 - 39, January 2012.
- [6] P. Devi and et al, "Reversible Image Authentication with Tamper Localization Based on Integer Wavelet Transform", (IJCSIS) International Journal of Computer Science and Information Security, vol. 6, No. 2, pp. 67-74, 2009.
- [7] J. Ellinas, "A Robust Wavelet-Based Watermarking Algorithm Using Edge Detection", World Academy of Science, Engineering and Technology, vol. 34, pp. 291-296, 2007.
- [8] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji & A. Tawfik, "A new watermarking scheme for colour images captured by mobile phone cameras," International Journal of Computer Science and Network Security, vol. 9 No. 7, July 2009, pp248-254.
- [9] Z. Wang, A. Bovik, H. Sheikh, and E. Simoncelli, "Image quality assessment: From Error visibility to structural Similarity", IEEE Transactions on Image Processing, vol. 13, Issue 4, pp. 600-612, 2004.

A New Robust and Fragile Watermarking Scheme for Images Captured by Mobile Phone Cameras

Taha Jassim and Raed Abd-Alhameed
School of Engineering
University Of Bradford
UK

taha.jassim@sts.adveti.ac.ae r.a.a.abd@bradford.ac.uk

Hussain Al-Ahmad
ECE Department
Khalifa University of Science, Technology and Research
UAE

alahmad@kustar.ac.ae

Abstract—This paper deals with a watermarking scheme for images captured by mobile phone cameras. The new scheme embeds two watermarks in the images for authentication checking and copyright protection. The mobile phone number including the international code is used as the first robust watermark. The number is embedded using the discrete wavelet transform. Hash code of the image is used as a fragile watermark and inserted in the spatial domain. The scheme is blind and does not require the original image in order to extract the watermarks. The fragile watermark is very sensitive to any kind of attacks or image manipulations. On the other hand, the robust watermark causes minimal distortion to the host images. The robustness of the proposed algorithm has been tested against several attacks and it survived cropping, scaling, filtering, additive noise and JPEG compression.

Keywords—component; Watermarking, Robust, Fragile, Authentication, Digital Images

I. INTRODUCTION

Nowadays, digital information content such as: audio, image and video can be easily copied, manipulated and distributed. This leads to unauthorized replication problems which causes many copyright disputes regarding the ownership of the digital contents. Watermarking of digital data by using hidden information is one of the solutions to this problem [1]. Digital watermarking techniques are classified according to different criteria such as robustness, perceptibility, embedding and retrieval methods. Robustness is a vital measure which means the ability of the watermark to resist common image processing operations. Watermarking techniques based on robustness can be further divided into two categories; robust and fragile watermarking [2]. While the robust watermarking schemes are used for proving ownership claims, the fragile watermarking schemes are deployed to authenticate multimedia content. The robust watermarking will survive against a multiplicity of attacks such as: cropping, scaling, filtering, additive noise and JPEG compression. The aim of using the fragile watermarks is to identify and report every possible tampering in the watermarked digital media [3].

There are different watermarking techniques for digital images and they can be classified into spatial and transformed domains [4]. Usually transformed domain techniques are more robust compared to spatial domain ones. Different transformations are used in watermarking such as the discrete cosine transform, Fourier transform and discrete wavelet transform (DWT). DWT has been given special attention in digital image watermarking due to its excellent spatial localization and multi-resolution characteristics that are similar to the theoretical models of the human visual system [5]. The transformed domain has been applied for copyright protection and image authentication [6].

Images captured by mobile phone cameras require both robust and fragile watermarking which is the subject of this paper. A new robust wavelet watermarking and fragile hash code watermarking techniques will be presented. The new scheme is blind and does not require the original image for extracting the robust watermark. On the other hand, the fragile watermark is used to detect any occurrence of tampering in the host image. There are four sections in this paper. Section II deals with the watermarking scheme. The experimental results are given in Section III, followed by the conclusions in Section IV.

II. THE PROPOSED WATERMARKING ALGORITHM

The proposed algorithm is divided into two parts: robust watermarking and fragile watermarking. In the first part the robust algorithm uses a block based wavelet algorithm to embed the binary watermark into the gray host image. The wavelet transformation is applied and the components are divided into four parts LL (low low frequencies), LH (low high frequency), HL (high low frequencies) and HH (high high frequencies). The embedding is done in the LL. Since small high frequency components may be discarded in some image processing operation such as JPEG compression, the very low frequency components of the host image will be utilized during the watermark embedding. Only one coefficient will be used in each 8×8 block for embedding. The second algorithm

calculates the hash code of the watermarked image and embeds this fragile watermark in the first row of the watermarked image in the spatial domain [7].

2.1 The Embedding Algorithm

The robust watermarking information used is a mobile phone number including its international code. The UAE number contains 14 decimal digits. We added the sum of these 14 digits (2 digits) to the end of the mobile number. The 2 decimal digits are used as a checking parameter for the correct number after extracting it by the receiver. The watermark plus the sum will be 16 decimal digits. Each decimal number is converted into 4 bits using the binary coded decimal (BCD) code. Therefore the watermarking information will be 64 bits. A secret key has been used to scramble the binary watermark digits randomly.

The host image will be divided into 8×8 blocks in the spatial domain then each block will be converted into the DWT domain. This will result in 4 sub blocks each block being 4×4 coefficients. These sub blocks are: Low Low frequency coefficients (LL), Low High coefficients (LH), High Low coefficients (HL) and High High coefficients (HH). In this algorithm, one binary digit will be embedded in one of the higher coefficients of LL sub block. The watermarking information will be repeated several times because the size of the image is much bigger than the 64bit watermark. A shuffling process will be used [8] to improve the robustness against vertical cropping.

Assuming that $f(i,j)$ represents the pixel of the host image, $w(i,j)$ represents the binary pixel of the watermark and

$$F_k(u,v) = DWT\{f_k(i,j)\},$$

If $w(i,j)=1$ then

$$F(x,y) = \begin{cases} \Delta Q_e\left(\frac{F_k(x,y)}{\Delta}\right) & x,y \in H_k \\ F_k(x,y) & x,y \notin H_k \end{cases} \quad 1 \leq k \leq N_{HB} \quad (1)$$

If $w(i,j)=0$ then

$$F(x,y) = \begin{cases} \Delta Q_o\left(\frac{F_k(x,y)}{\Delta}\right) & x,y \in H_k \\ F_k(x,y) & x,y \notin H_k \end{cases} \quad 1 \leq k \leq N_{HB} \quad (2)$$

Where $1 \leq x, y \leq 8$, and Q_e is the quantization to the nearest even number and Q_o is the quantization to the nearest odd number, Δ is a scaling quantity and it is also the quantization step used to quantize either -even or odd numbers. The 8×8 block is converted back to the spatial domain and the process is repeated with the other blocks.

The second part of the embedding algorithm uses hash code as a watermark signal. The hash code has been calculated for the pixels of the image excluding the first row. For example if we want to watermark 512×512 image then the hash code of the 511×512 will be calculated and inserted in the first row of the

image. The resultant hexadecimal hash code is converted into binary code and embedded in the least significant bits of the first row of the image. Fig. 1 illustrates the embedding process.

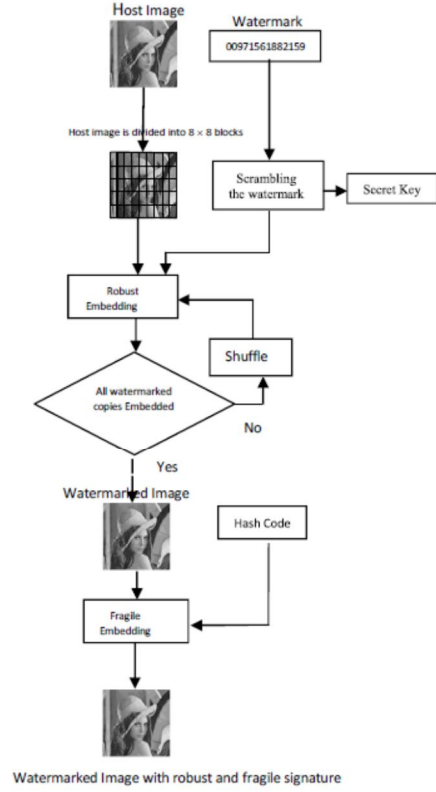


Figure 1 The embedding process

2.2 The Extraction Algorithm

First of all, the hash code is extracted from the first row of the watermarked image. Then the hash code of the pixels of the image excluding the first row is calculated. If there is any difference between the two codes it means that the watermarked image has been edited and manipulated. If not then it means that the image is authentic.

The next step is to extract the robust watermark (phone number). The watermarked image is divided into 8×8 blocks. Each block is converted into the DWT domain. The recovery process is the inverse of the embedding process. Each predefined frequency coefficient is quantized by Δ and rounded

to the nearest integer. The formula which is used for extracting the embedded bits is defined as follows:

$$\begin{aligned} \text{If } Q\left(\frac{F_k(x,y)}{\Delta}\right) \text{ is odd then } w(i,j) &= 0 \\ \text{If } Q\left(\frac{F_k(x,y)}{\Delta}\right) \text{ is even then } w(i,j) &= 1 \end{aligned} \quad (3)$$

Where: Q is rounded to the nearest integer.

Each coefficient of the image that carries one bit of the embedded watermarks can be extracted by using the above method. These extracted bits will create the embedded watermark information $w(i,j)$. The phone numbers can be obtained by implementing a reverse shuffling process. The scrambled watermarks are descrambled to obtain the original watermarks. In the extraction process there is no need for the original image. The checked sum will be used to discard the wrongly extracted phone numbers. Fig.2 illustrates the extraction process.

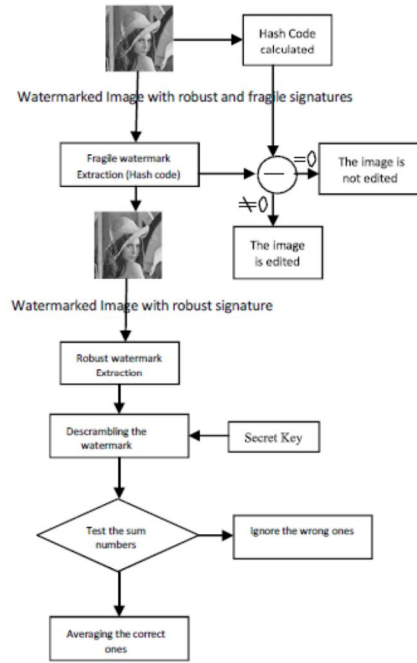


Figure 2 The extraction process

III. RESULTS

The proposed algorithm was examined using different gray level images of size 512×512 . Two techniques have been used to assess the distortion caused to the image by the watermarking process. The first one is the PSNR between the host original image and the watermarked image. Table I illustrates the perceptual invisibility of the proposed algorithm at different embedding strengths. The average PSNR values between the watermarked and original images using the phone number as the watermark information are shown in table I. The PSNR achieved with different images is higher than 40 dB. The second one is the structural similarity index measure (SSIM) [9] between the host image and the watermarked image. The higher the SSIM percentage is the larger the similarity between the compared images. In Table II, the distortion caused by the watermarking process is assessed using SSIM at different embedding strengths. Test images "Lena", "Pirate", "Baboon" and "Cameraman" have been used to examine the perceptual quality at different embedding strengths as shown in Table II. The SSIM is very good and higher than 0.98. It is clear that the distortion caused to the images is imperceptible even with high values of Δ shown in figure 3 different watermarked images with $\Delta = 32$.

TABLE I PSNR AT DIFFERENT EMBEDDING STRENGTHS

Image	Lena	Pirate	Baboon	cameraman
PSNR at $\Delta = 16$	46.56347	46.59480863	46.62452449	46.63492512
PSNR at $\Delta = 20$	44.72933	44.45094582	44.69542947	44.7021045
PSNR at $\Delta = 24$	43.04471	43.12502426	43.17094665	43.24089615
PSNR at $\Delta = 28$	41.73988	41.93567896	41.77353576	41.86942965
PSNR at $\Delta = 32$	40.61793	40.63452918	40.68261194	40.78512446
PSNR at $\Delta = 36$	39.66947	39.50208721	39.52702595	39.77573008
PSNR at $\Delta = 40$	38.66067	38.38821713	38.73529651	38.73743346

TABLE II SSIM AT DIFFERENT EMBEDDING STRENGTHS

Image	Lena	Pirate	Baboon	cameraman
SSIM at $\Delta = 16$	0.990494	0.993053064	0.996051612	0.988202485
SSIM at $\Delta = 20$	0.986201	0.988497607	0.993849363	0.982071193
SSIM at $\Delta = 24$	0.980119	0.985495771	0.991514897	0.9764793
SSIM at $\Delta = 28$	0.973953	0.981251131	0.98871849	0.968890462
SSIM at $\Delta = 32$	0.966734	0.974668969	0.986008835	0.960992969
SSIM at $\Delta = 36$	0.960891	0.967382497	0.982056289	0.952044316
SSIM at $\Delta = 40$	0.951134	0.958914896	0.977993121	0.941664147



Figure 3 Different watermarked images with $\Delta = 32$.

Fig. 4 illustrates some examples of editing of the original image in different areas. Table III shows the difference between the hash code for the original image and the edited ones. The hash code of the watermarked image (fragile watermarking information) has been examined. It shows the hash code cannot be recovered for any kind of image editing.

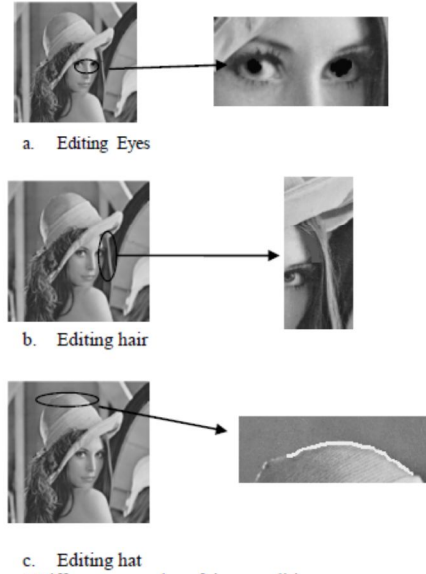


Figure 4 Different examples of image editing.

TABLE III MD5 HASH CODE CALCULATION

Hash for Original Image	Hash for Modified Image	Editing type
'3b0388a18bbef8bf5006cbf206531d74'	'7bf3ba7088382b392c37273f129786f3'	Eye editing
'3b0388a18bbef8bf5006cbf206531d74'	'34927f969f31fbc4bde eac25016580a5'	Hat editing
'3b0388a18bbef8bf5006cbf206531d74'	'ddc302e5cb00eb7c8755d3073861a657'	Hair editing

On the other hand, the mobile number has been used as the robust watermarking information because it is unique and is more intuitive for representing one's identity. In Table IV, several attacks were applied to the watermarked image "Lena" to assess the robustness of the proposed algorithm. The Stirmark software package was used for this purpose. The normalized correlation (NC) is used to measure the similarity between the original and the extracted watermark as shown in Table IV. The algorithm survived 3x3 low-pass filtering, cropping up to 75% horizontally and vertically, high JPEG compression and Gaussian and salt and pepper noise. Meanwhile, the fragile watermark was destroyed by every attack.

TABLE IV THE NORMALIZED CORRELATION (NC) FOR LENA IMAGE WITH DIFFERENT ATTACKS, WATERMARK SIZE 96×64, AT $\Delta = 34$.

Attacks	NC	Hash Code	Watermark
Cropping 50% V	1	not recovered	recovered
Cropping 75% V	1	not recovered	recovered
Cropping 50% H	1	not recovered	recovered
Cropping 70% H	1	not recovered	recovered
Gaussian noise m=0, v=0.002	1	not recovered	recovered
Gaussian noise m=0, v=0.001	1	not recovered	recovered
S&P noise, d=0.02+ Median 3×3	1	not recovered	recovered
S&P noise, d=0.05+ Median 3×3	1	not recovered	recovered
Scale 2	1	not recovered	recovered
Scale 0.4	1	not recovered	recovered
Low pass 3×3	1	not recovered	recovered
Wiener 3×3	1	not recovered	recovered
Median 3×3	1	not recovered	recovered
JPEG 50	1	not recovered	recovered
JPEG 75	1	not recovered	recovered

IV. CONCLUSION

A new robust wavelet and fragile hash code watermarking scheme has been presented. The algorithm is blind and does not require the original image for extracting the watermark. On the other hand, the fragile watermark is used to detect any occurrence of tampering in the host image. The robust algorithm uses a mobile phone number as the basis of the watermarking information. To increase the quality of invisibility a suitable DWT coefficient selection process has been applied with high magnitudes. Several watermarking strengths have been examined and the best watermarking strength has been found to be $\Delta=32$. The algorithm achieved PSNR > 40 dB and SSIM > 0.98. The proposed algorithm has been shown to be resistant to JPEG compression, additive noise, cropping, scaling and low-pass filters attacks.

References

- [1] I. R. Farah, I. B. Ismail, and M. B. Ahmed, "A Watermarking System Using the Wavelet Technique for Satellite Images", *International Journal of Engineering and Applied Sciences*, 2007, pp. 197-201.
- [2] S. P. Mohanty, N. Ranganathan, and R. K. Namballa, "VLSI Implementation of Invisible Digital Watermarking Algorithms Towards the Development of a Secure JPEG Encoder," *IEEE Workshop on Signal Processing Systems (SIPS)*, 2003 pp. 183-188.
- [3] S. Radharani, and M.L. Valarmathi, "A Study on Watermarking Schemes for Image Authentication", *International Journal of Computer Applications* Vol. 2 No.4, June 2010, pp 24-32.
- [4] N. Kashyap, and G. Sinha, "Image Watermarking Using 2-Level DWT", *Advances in Computational Research*, ISSN: 0975 - 3273 & E-ISSN: 0975-9085, Vol. 4, Issue 1, 2012, pp. -42-45
- [5] H. Abdallah, M. Hadhoud, A. Shaalan and F. Abd El-samie " Blind Wavelet-Based Image Watermarking", *International Journal of Signal Processing, Image Processing and Pattern Recognition*, Vol. 4, No. 1, March 2011, pp. 15-28
- [6] D. Bhattachatya, J. Dutta, P. Das, and T. Kim, 'Discrete Cosine Transformation Based Image Authentication and Secret Message Transmission Scheme', *Computational Intelligence, Communication Systems and Networks*, 2009. CICSYN '09. First International Conference, July 2009, pp. 374 – 379.
- [7] A. G. Konheim, "Hashing in Computer Science: Fifty Years of Slicing and Dicing", John Wiley & Sons, Inc, 2010.
- [8] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji & A. Tawfik, "A new watermarking scheme for colour images captured by mobile phone cameras," *International Journal of Computer Science and Network Security*, vol. 9 No. 7, July 2009, pp248-254.
- [9] Z. Wang, A. Bovik, H. Sheikh, and E. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity", *IEEE Transaction On Image Processing*, Vol. 13, NO. 4, Apr. 2004, pp. 1-1

New Robust and Fragile Watermarking Scheme for Colour Images Captured by Mobile Phone Cameras

Taha. Jassim and Raed Abd-Alhameed

School of Engineering
University Of Bradford
UK

taha.jassim@sts.adveti.ac.ae
r.a.abd@bradford.ac.uk

Hussain Al-Ahmad

ECE Department
Khalifa University of Science, Technology and
Research
UAE

alahmad@kustar.ac.ae

Abstract— This paper examines and evaluates a new robust and fragile watermarking scheme for colour images captured by mobile phone cameras. The authentication has been checked by using the fragile watermarking, while the copyright protection has been examined by using the robust one. The mobile phone number, including the international code, is a unique number across the whole world and it is used as a robust watermark. The number is embedded in the frequency domain using the discrete wavelet transform. On the other hand, hash codes are used as fragile watermarks and inserted in the spatial domain of the RGB image. The scheme is blind and the extraction process of the watermarks (Robust and Fragile) does not require the original image. The fragile watermark can detect any tampering in the image while the robust watermark is strong enough to survive against several attacks. The watermarking algorithm causes minimal distortion to the images. The proposed algorithm has been successfully tested, evaluated and compared with other algorithms.

Keywords—component; Watermarking, Robust, Fragile, Authentication, Digital Colour Images.

I. INTRODUCTION

Digital image processing offers many features such as easy editing and easy duplication. Digital watermarking has been used to authenticate images and overcome the problems associated with the protection of copyright [1,2]. There are two types of watermarking systems; robust and fragile. Robust watermarks are considered to curb illegal copying and are intended for the copyright protection. The robust watermarking schemes are used for verifying ownership claims while the fragile watermarking schemes are set up to authenticate multimedia content. The robust watermarking will persist against a diversity of attacks such as compression, filtering, scaling cropping, and collusion attacks among many other digital signal processing operations. However, fragile watermarks are being destroyed whenever the image is modified and indicate the existence of tampering. The goal of using the fragile watermarks is to detect and report every probable tampering in the watermarked digital media [3].

The watermarking techniques for digital images can be broadly classified into spatial and transformed domains [4]. Commonly transformed domain techniques are stronger (more robust) compared to spatial domain ones. Different transformations are used in watermarking such as the fast Fourier transform (FFT), discrete Fourier transform (DFT), discrete cosine transform (DCT), and discrete Wavelet Transform (DWT) [5, 6]. The DWT has many features such as special localization, frequency spread and multi-resolution characteristics which are approximating to the theoretical models of the human visual system (HVS). The transformed domain can be used for copyright protection and image authentication. The robust watermark can be inserted in either the green or the Y channel of the color image [7,8].

Nowadays, there are many mobile phones, especially the smart phones, which are equipped with high resolution digital cameras. The captured images can be shared or sent as e-mail attachments, MMS messages or via Bluetooth. These captured images require both robust and fragile watermarking which is the subject of this paper

A new watermarking technique is presented in this paper with fragile hash code watermarking and robust wavelet watermarking. The fragile watermarks are used to spot any incident of tampering in the RGB host images. On the other hand the new scheme is blind and does not require the original image for extracting the robust watermark. There are four sections in this paper. Section II deals with the watermarking scheme. The experimental results are given in Section III, followed by the conclusions in Section IV.

II. THE PROPOSED WATERMARKING ALGORITHM

The proposed algorithm is divided into two parts: robust watermarking and fragile watermarking. In the first part the host colour image is separated into RGB components. The embedding of the robust watermark is done in the green channel. The green channel is divided into 8×8 blocks. The wavelet transformation is applied into each block. Each block is converted to four blocks in the frequency domain. The blocks are LL (low low frequencies), LH (low high frequency), HL (high low frequencies) and HH (high high frequencies) respectively. Because some image processing

operation, such as JPEG compression, targets some high frequency components the LL has been chosen for the embedding process. Only one coefficient will be used in each LL block. The fragile algorithm calculates the hash code for the RGB components separately and embeds the data in each component in the spatial domain.

A. The Embedding Algorithm

The mobile phone number including its international code has been used as robust watermarking information [5]. The UAE number comprises 14 decimal digits. We have added the sum of these 14 digits (2 digits) to the end of the mobile number. The reason behind adding the sum is to use it as a checking parameter for the correct number after extracting it by the receiver. The total digits will 16 decimal digits. Each decimal number is converted into 4 bits using the binary coded decimal (BCD) code. Hence the watermarking information will be 64 bits. To scramble the binary watermark digits randomly we have added a secret key.

The embedding process will be repeated several times. In order to improve the robustness against vertical cropping, a shuffling process will be used [5].

Assuming that $f(i,j)$ represents the pixel of the host image, $w(i,j)$ represents the binary pixel of the watermark and

$$F_k(u,v) = DWT\{f_k(i,j)\},$$

$$\text{If } w(i,j) = 1 \text{ then}$$

$$F(x,y) = \left(\begin{array}{ccc} \Delta Q_e \left(\frac{F_k(x,y)}{\Delta} \right) & xy \in H_k & 1 \Delta \Delta N_{H_k} \\ F_k(x,y) & xy \in H_k & 1 \Delta \Delta N_{H_k} \end{array} \right) \dots \dots (1)$$

If $w(i,j) = 0$ then

$$F(x,y) = \left(\begin{array}{ccc} \Delta Q_o \left(\frac{F_k(x,y)}{\Delta} \right) & xy \in H_k & 1 \Delta \Delta N_{H_k} \\ F_k(x,y) & xy \in H_k & 1 \Delta \Delta N_{H_k} \end{array} \right) \dots \dots (2)$$

where $1 \leq x, y \leq 8$, and Q_e is the quantization to the nearest even number and Q_o is the quantization to the nearest odd number, Δ is a scaling quantity and it is also the quantization step used to quantize either even or odd numbers. The 8x8 block is converted back to the spatial domain and the process is repeated with the other blocks.

The second part of the embedding algorithm uses hash code as the watermarking data. The hash code has been calculated for the pixels of R, G and B images separately excluding the first row. For example if we want to watermark 512x512 image then the hash code of the 511x512 will be calculated and inserted in the first row of the image. The resultant hexadecimal hash code is converted into binary code and embedded in the least significant bits of the first row of the image. Fig. 1 illustrates the embedding process.

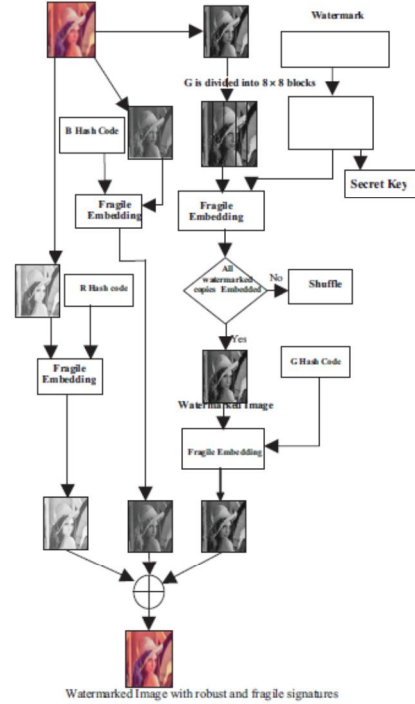


Figure 1. The embedding process.

B. The Extraction Algorithm

First of all, the R, G and B are separated from the color watermarked image. The hash codes are extracted from the selected row of the R, G and B images separately. Then the hash codes of the pixels of each image excluding that row are calculated. If there is any difference between the two codes it means that the watermarked image has been edited and manipulated. If not then it means that the image is authentic.

The next step is to extract the robust watermark (phone number). The watermarked image is divided into 8x8 blocks. Each block is converted into the DWT domain. The recovery process is the inverse of the embedding process. Each predefined frequency coefficient is quantized by Δ and rounded to the nearest integer. The formula which is used for extracting the embedded bits is defined as follows:

$$\text{If } Q\left(\frac{F_k(x,y)}{\Delta}\right) \text{ is odd then } w(i,j) = 0$$

If $Q\left(\frac{B_{ij} - w_{ij}}{2}\right)$ is even then $w_{ij} = 1, \dots, (3)$

where: Q is rounded to the nearest integer.

Each coefficient of the image that carries one bit of the embedded watermarks can be extracted by using the above method. These extracted bits will create the embedded watermark information $w(i,j)$. The phone numbers can be obtained by implementing a reverse shuffling process. The scrambled watermarks are descrambled to obtain the original watermarks. In the extraction process there is no need for the original image. The checked sum will be used to discard the wrongly extracted phone numbers. Fig.2 illustrates the extraction process.

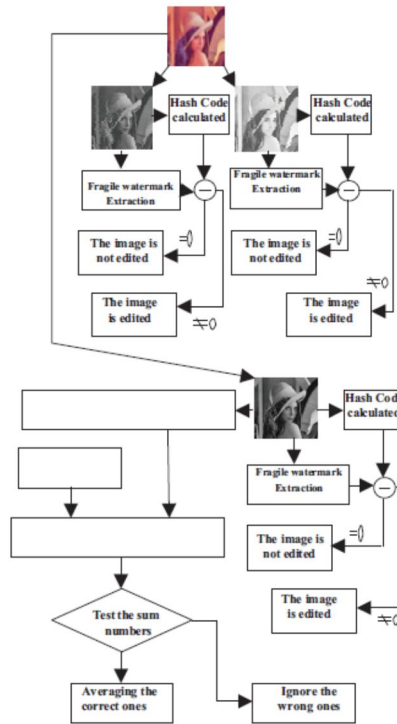


Figure 2. The extraction process.

III. RESULTS

Different colour images of size 512×512 were used to evaluate and test the proposed algorithm. To assess the

distortion to the image by the watermarking process we have used two techniques. The first one is to calculate the peak signal to noise ratio (PSNR) between the host original image and the watermarked image. The other one is using the structural similarity index measurement (SSIM) between the host image and the watermarked image [9]. Table I shows the PSNR for different images with different embedding strength (Δ). It is clear that the PSNR is more than 45 dB for different values of Δ with different images. Moreover, it illustrates the perceptual invisibility of the proposed algorithm at different embedding strengths. The second technique is calculating the SSIM. It is a measuring tool to evaluate the distortion affected by the watermarking process. Table II illustrates the distortion of the watermarked image due to the embedding process. Test images 'Lena', 'Pepper' and 'Baboon' have been used to assess the perceptual quality at different strengths (Δ). It shows that SSIM is very good and higher than 0.985. As shown in Fig. 3, even though with high values of Δ , the distortion caused to the images is still invisible.

TABLE I. PSNR AT DIFFERENT EMBEDDING STRENGTHS

Image	Lena	pepper	Baboon
PSNR at $\Delta = 24$	47.57609	47.64660774	47.59496971
PSNR at $\Delta = 28$	46.37793	46.13540792	46.24337939
PSNR at $\Delta = 32$	45.07759	45.20131091	45.05428463
PSNR at $\Delta = 36$	44.27578	44.09631016	44.14011288
PSNR at $\Delta = 40$	43.50154	43.11854666	43.3124933

TABLE II. SSIM AT DIFFERENT EMBEDDING STRENGTHS

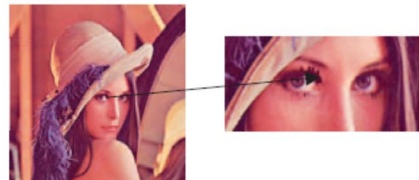
Image	Lena	Pepper	Baboon
SSIM at $\Delta = 24$	0.994119	0.993331784	0.998054064
SSIM at $\Delta = 28$	0.992594	0.990941407	0.997267633
SSIM at $\Delta = 32$	0.990116	0.98907989	0.996531748
SSIM at $\Delta = 36$	0.988336	0.986824313	0.996074774
SSIM at $\Delta = 40$	0.986584	0.983910615	0.994905285



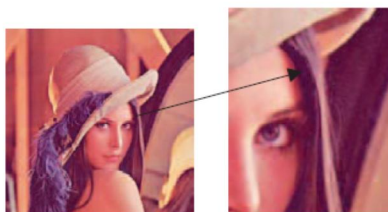
Figure 3 Different watermarked images with $\Delta = 32$.

We have made some editing of the original image (Lena) in different areas. Figure 4 shows the editing examples with the original image. Table III illustrates the difference between the original image and the edited ones and also the difference between the hash code for the original image and the edited ones.

We have made some editing of the original image (Lena) in different areas. Figure 4 shows the editing examples with the original image. Table III illustrates the difference between the original image and the edited ones and also the difference between the hash code for the original image and the edited ones.



a. Editing Eyes



b. Editing hair



c. Editing hat

Figure 4. Different examples of image editing

TABLE III MD5 HASH CODE CALCULATION

Hash Code	Hash for Original Image	Hash for Modified Image	Editing type
<i>R</i>	'25d0836df47ee3fae3ba0e1221d7692ec'	'fb353d7b5506c5d57372d6b5cc27c711'	Eye editing
<i>B</i>	'f6d3857b6ae8885369754cf5a92a16f'	'16e5596f5873005f6c8223dea62cbf9'	Hat Editing
<i>G</i>	'4feb43fc26d9fa23a08d15c989fe20b'	'943699a4b01bbab4d45d4155d955305a4'	Hair Editing

Figure 5 shows another type of editing. The RGB watermarked image has been separated to the R, G and B channels. The editing is in the eyebrow of the Green channel. Table IV illustrates the difference between the hash code for the original image and the edited one. It is clear that the effected hash code is for the Green channel only and there are no changes in the R and B channels. It is clear that the slightest editing will change the hash code of the image.



Figure 5 Editing Eyebrow in the Green Channel

TABLE IV. MD5 HASH CODE FOR RGB CALCULATION

Hash Code	Hash for Original Image	Hash for Modified Image
<i>R</i>	'25d0836df47ee3fae3ba0e1221d7692ec'	'25d0836df47ee3fae3ba0e1221d7692ec'
<i>B</i>	'f6d3857b6ae8885369754cf5a92a16f'	'f6d3857b6ae8885369754cf5a92a16f'
<i>G</i>	'4feb43fc26d9fa23a08d15c989fe20b'	'f00a3c31c1035aab9a41f09430e3e4b0'

IV. CONCLUSION

A new robust wavelet and fragile hash code watermarking scheme for the colour images has been presented. There is no need for the original image to extract the watermark because it is a blind algorithm. On the other hand, the fragile watermark has the ability to highlight any occurrence of tampering in the host image. The watermarking information of the robust algorithm is a mobile phone number. The quality of the invisibility has been increased by choosing a suitable DWT coefficient which has high magnitude. Several watermarking strengths have been tested and the best watermarking strength has been found to be $\Delta=32$. The algorithm achieved PSNR > 45 dB and SSIM > 0.985. The robust watermark has survived the following attacks: JPEG compression, additive noise, cropping, scaling and low-pass filters attacks.

REFERENCES

- [1] S. Katzenbeisser, and F. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, London, 2000.
- [2] I. Cox, M. Miller, and J. Bloom, Digital Watermarking, Morgan Kaufmann Publishers, San Francisco, 2001.

- [3] R. Al Omari, A. Al-Jaber "A Fragile Watermarking Algorithm for Content Authentication", International Journal of Computing and Information Sciences, Vol. 2, No. 1, April 2004, pp. 27-37.
- [4] S. Radharani, and M.L. Valarmathi, "A Study on Watermarking Schemes for Image Authentication", International Journal of Computer Applications Vol. 2 No.4, June 2010, pp 24-32.
- [5] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji & A. Tawfik, "A new watermarking scheme for colour images captured by mobile phone cameras," International Journal of Computer Science and Network Security, vol. 9 No. 7, July 2009, pp248-254.
- [6] T. Jassim, H. Al-Ahmad, R.A. Abd-Alhameed and A. Al-Gindy, "A block based wavelet algorithm for watermarking still images captured by mobile phone cameras", Proceedings of the 8th International Conference on Information Science and Digital Content Technology, Korea, July 2012, pp 287-292.
- [7] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji, and A. Tawfik, "A novel blind Image watermarking technique for colour RGB images in the DCT domain using green channel " in Moshanka International Conference on Communications, Computers and Applications (MIC-CCA 2008), Amman, Jordan, 2008, pp. 26-31
- [8] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji & A. Tawfik, "Watermarking of colour images in the DCT domain using Y channel", Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications, Morocco, 2009, pp 1025-1028.
- [9] Z. Wang, A. Bovik, H. Sheikh, and E. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," IEEE Transactions on Image Processing, 2004, pp. 600-612.

Two Levels Block Based Wavelet Watermarking Algorithm For Still Colour Images

Taha Jassim¹, Hussain Al-Ahmad², Raed A. Abd-Alhameed¹ and Ahmed Al-Gindy³

¹School of Engineering, University of Bradford, UK

²Electrical and Computer Engineering Department, Khalifa University, UAE

³School of Engineering and Information Technology, Computer College, UAE

Abstract—A robust watermarking technique is implemented for copyright protection. The proposed method is based on 2-level discrete wavelet transform (DWT). The embedded watermarking information is a mobile phone number including the international code. The first level of the DWT transformation is applied on 16×16 blocks of the host image. All the coefficients of the 8×8 low-low (LL1) first level sub-band are grouped into one matrix. The second level of the DWT is then applied to the grouped matrix from the first level transformation. The highest coefficient from the LL2 sub-band (4×4) is used for embedding the watermark information. The extracting process is blind since it does not require the original image at the receiver side. The distortion in the host image due to the watermarking process is minimal and the PSNR is greater than 60 dB. The proposed algorithm showed robustness against several attacks such as scaling, filtering, cropping, additive noise and JPEG compression.

Keywords; Image processing; DWT; Watermarking;

I. INTRODUCTION

Digital media can be copied easily and therefore there is a need for protecting the copyright. One of the most important methods which deal with the protection of copyrights for the digital images is the use of the digital watermarking. Digital watermarking embeds secret information such as; logos, images, text, ...etc into the digital media by certain algorithms. The spatial domain or the frequency domain can be used for the embedding process and each one has their own pros and cons and is used in different scenarios [1]. In general, the frequency domain techniques are more robust than spatial domain ones [2]. The common transforms in frequency domain are: Wavelet Transform (DWT), Discrete Fourier Transform (DFT) and Discrete Cosine Transform (DCT). DWT has been used in watermarking due to the excellent spatial localization and multiresolution characteristics of the DWT [3].

Many researchers have used the DWT. For example the author in [4] has used the DWT in his proposed watermarking scheme. The middle and high frequency bands of the host image have been used for embedding the watermark information. The watermarking information was modelled as Gaussian noise. The drawback of this algorithm is the need for the original image during the extraction process. Another algorithm used 1-level DWT for a robust image watermarking technique [5]. Alpha blending technique has been used as an embedding technique. However, the embedding and the

extraction process are relying on the value of alpha [6]. The authors in [7] proposed a semi-blind watermarking scheme by using the DWT. A grey scale logo image is used as the watermarking information. The host image is transformed into the wavelet domain and the directive contrast with wavelet coefficients have been used for embedding the watermark information. The singular values of the watermark information are embedded by modifying the singular values of the host image. The author in [8] used pixel wise masking for watermarking in a wavelet-based algorithm. The adaptive watermark information is added to the largest detail bands. The product of data extracted from the HVS model is represented by the watermarking weighing function. The extraction process of the watermarking information at the receiver side can be found by correlation. The proposed method showed robustness against several attacks. However, this method is more complex than other transform techniques [8]. The authors in [9] applied a wavelet-based transform and discrete Hadamard transform (DHT) respectively. The proposed cascaded algorithms allowed them to choose the suitable coefficients that are close to the middle and low frequencies. However, the host image is required to recover the watermarking information at the receiver side.

In the previous techniques, the watermarking information used digital signature, images, logos and pseudo random numbers. However, the watermarking information that is used in our algorithm is the mobile number with the international code. It is a unique number all over the world [9]. Peak signal to noise ratio (PSNR) and the structured similarity index (SSIM) will be used to evaluate the distortion caused to the host image by the watermarking process [10].

In this paper, a robust two level wavelet watermarking technique is presented. The proposed method uses different block-based dimensions before embedding the watermark information. This paper is divided into 4 sections. Section II deals with the watermark embedding and extraction algorithms. The experimental results are given in section III, followed by the conclusions in section IV.

II. THE PROPOSED WATERMARKING ALGORITHM

The proposed algorithm uses two level DWT block based process to embed the watermarking information. The first level wavelet transformation is applied on the (16×16) blocks of the

original image. Each block is divided into four groups of coefficients; LL1 (low-low frequencies), LH1 (low-high frequency), HL1 (high-low frequencies) and HH1 (high-high frequencies). The second level of DWT is applied on the LL1 part of each block. Accordingly, the LL2 are selected to embed the watermark information. The highest coefficient in the LL2 is used to embed one bit from the watermarking information. The watermark is embedded multiple times using a shuffling process applied to the host image [11].

A. The Embedding Algorithm

The colour image is separated into three components R, G and B. In this algorithm, the green component (G) has been chosen for the embedding process [12]. The mobile phone number with the international code (14 decimal digits) is used as watermarking information. The sum of the 14 digits (2 extra decimal digits) is added to make it 16 decimal digits. These two digits will be used as checksum error detection at the receiver side. In order to embed the watermarking information, the 16 decimal numbers are converted to 64 BCD bits. The watermarking information is scrambled by using a secret key. The scramble process is important to reduce the correlation between the host image and the embedded watermark.

The host image is divided into 16×16 blocks in the spatial domain. The first level of DWT is then applied to convert each block to DWT domain. Following this, the second level of DWT is applied on each LL1 (8×8) blocks. The LL2 sub block is used for embedding process. The highest weight coefficient from each block of the LL2 is used to embed one bit for the watermarking information. The embedding process will be repeated several times because the size of the host image is much bigger than the 64 bits watermark. A shuffling process will be used to increase the robustness of the algorithm against the vertical cropping attack [12].

Assume that $f(i,j)$ represents the pixel of the Green component of the RGB representation of the colour host image, $w(i,j)$ represents the binary pixel of the watermark.

$$F_k(u,v) = DWT\{f_k(i,j)\},$$

$$\text{If } w(i,j)=1 \text{ then}$$

$$F_k(x,y) = \begin{cases} \Delta Q_e(\frac{F_k(x,y)}{\Delta}) & x,y \in H_k \quad 1 \leq k \leq N_{HB} \\ F_k(x,y) & x,y \notin H_k \quad 1 \leq k \leq N_{HB} \end{cases}$$

$$\text{If } w(i,j)=0 \text{ then} \quad (1)$$

$$F_k(x,y) = \begin{cases} \Delta Q_o(\frac{F_k(x,y)}{\Delta}) & x,y \in H_k \quad 1 \leq k \leq N_{HB} \\ F_k(x,y) & x,y \notin H_k \quad 1 \leq k \leq N_{HB} \end{cases}$$

Where Q_e is the quantization to the nearest even number and Q_o is the quantization to the nearest odd number. Δ is a scaling quantity (watermarking strength) and it is also the quantization step used to quantize to either even or odd number. The 4×4 LL2 block is converted back to the first level

by using the inverse DWT. The result from the first inverse is the LL1 (8×8) block from the 16×16 original block. Then 16×16 original block is converted to the spatial domain by using inverse DWT again and the process is repeated with the other blocks. The watermarked G component is added to the R and B components, to produce the watermarked colour image. Figure 1 illustrates the embedding process.

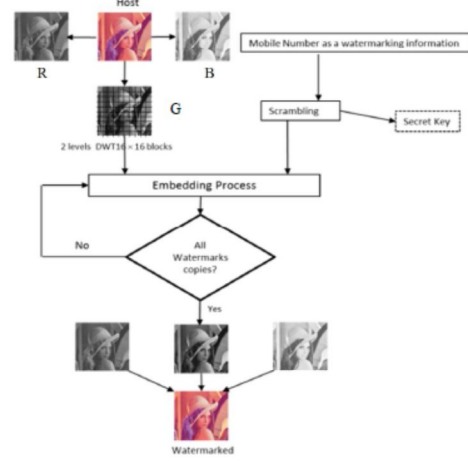


Figure 1. Graphical representation for Embedding Process

B. The Extraction Algorithm

At the receiver side, the watermarked colour image is separated into RGB components. The G component is divided into 16×16 blocks. The DWT transformation is applied in each block to get the first level of the DWT. Then the DWT level two is applied on each LL1 (8×8) block. The watermarking information recovery is the inverse of the embedding process. Each predefined frequency coefficient is quantized by Δ and rounded to the nearest integer. The formula which is used for extracting the embedded bits is defined as follows:

$$\text{If } Q(\frac{F_k(x,y)}{\Delta}) \text{ is odd then } w(i,j)=0$$

$$\text{If } Q(\frac{F_k(x,y)}{\Delta}) \text{ is even then } w(i,j)=1 \quad (2)$$

Where, Q is rounded to the nearest integer. Δ is the same as that used in the embedding process. The watermark can be retrieved by using the same secret key. The extraction process is shown in Figure 2.

The above method is used to extract one bit of the embedded watermarking from each coefficient of the watermarked image. The embedded watermarks information $w(i,j)$ are created from

the extracted bits. The reverse shuffling process is applied to achieve the original watermarking bits order. The obtained watermark is descrambled to get the correct one by using the same secret key K . Checksum error detection process is used at the extraction process to discover the wrong extracted watermarks and discard them before applying the averaging process. The averaging process is important to enhance the quality of the extracted watermarks.

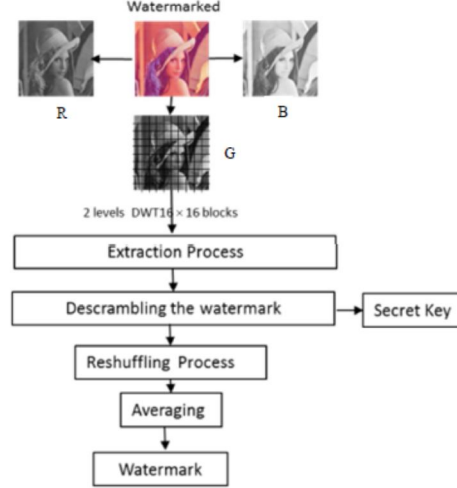


Figure 2. Graphical representation for Extraction Process

III. SIMULATION AND RESULTS

Different colour images of size 512×512 with 24 bits per pixel have been used to examine the proposed algorithm. The watermarking information in the proposed algorithm is the mobile number with the international code. In order to evaluate the distortion caused to the host image by the watermarking process, two well known techniques are being used. The first one is the PSNR between the host image and the watermarked image. The perceptual invisibility of the proposed algorithm at different embedding strengths is shown in Table I. The second technique is the SSIM between the host image and the watermarked image. When the highest value of the SSIM is equal to one, it means that the watermarked image becomes the same as the host image. Table I illustrates the similarity difference between the host image and the watermarked image which is assessed by SSIM at different embedding strength.

Colour images such as "Lena", "Pepper" and "Baboon" have been used to test the perceptual quality at different embedding strengths as shown in Table I. The PSNR achieved for different images are higher than 49 dB. The SSIM is also higher than 0.99. Figure 3 shows the images using different

strengths. It is clear that the distortion caused to the images is invisible even with high values of Δ .

The robustness of the proposed algorithm has been examined by applying several attacks. Stirmark software package was used for this purpose. The normalized correlation (NC) is used to measure the similarity between the original and the extracted watermark as shown in Table II. The algorithm survived 3×3 and 5×5 low-pass filtering, cropping up to 75% horizontally and vertically, high JPEG compression, Gaussian, salt and pepper noise. Figure 4, shows some attacks on watermarked image.

TABLE I. PSNR AND SSIM AT DIFFERENT EMBEDDING STRENGTH

Image	Lena	Pepper	Baboon
PSNR at $\Delta = 8$	63.05020629	63.0611911	63.25698538
PSNR at $\Delta = 14$	58.88645215	59.0664543	58.86390361
PSNR at $\Delta = 16$	57.71243706	57.58727376	57.44486623
PSNR at $\Delta = 20$	55.73828475	55.64622098	55.6975083
PSNR at $\Delta = 24$	54.00715257	54.05791866	53.78892308
PSNR at $\Delta = 30$	52.10894478	52.26684452	52.30582113
PSNR at $\Delta = 34$	51.1137	50.95428376	51.10934502
PSNR at $\Delta = 40$	49.73766586	49.73135453	49.7601575
SSIM at $\Delta = 8$	0.9998316	0.999777	0.999955878
SSIM at $\Delta = 14$	0.9995802	0.99945	0.999876271
SSIM at $\Delta = 16$	0.9994517	0.999277	0.999821182
SSIM at $\Delta = 20$	0.9991439	0.998893	0.999763544
SSIM at $\Delta = 24$	0.998661	0.998432	0.999606253
SSIM at $\Delta = 30$	0.9980988	0.997868	0.9994492
SSIM at $\Delta = 34$	0.9975622	0.997298	0.999316282
SSIM at $\Delta = 40$	0.9966325	0.996425	0.999058593

TABLE II. RELATION (NC) FOR LENA IMAGE WITH DIFFERENT ATTACKS AT $\Delta = 20$.

Attacks	NC	Attacks	NC
Cropping 80% V	1	Low pass 3×3	1
Cropping 50% V	1	Low pass 5×5	1
Cropping 75% H	1	Wiener 3×3	1
Cropping 50% H	1	Wiener 5×5	1
Scale 2	1	Median 3×3	1
Scale 0.4	1	Median 5×5	1
Gaussian noise $m=0$, $v=0.002$	1	JPEG 75	1
Gaussian noise $m=0$, $v=0.001$	1	JPEG 50	1
S&P noise, $d=0.02+$ Median 3×3	1	JPEG 35	1
S&P noise, $d=0.05+$ Median 3×3	1	JPEG 30	1
JPEG 28	1	JPEG 25	0



Figure 3. Original Lena with different watermark strength (green channel).

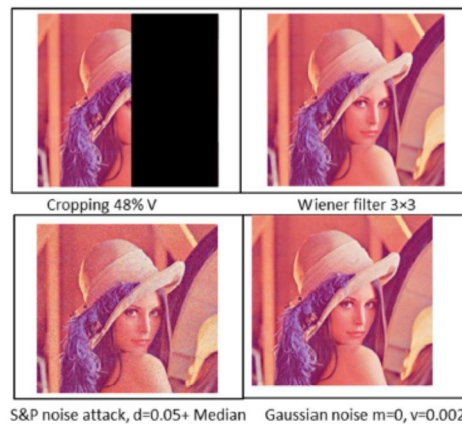


Figure 4. Several attacks for colour watermarked image

IV. CONCLUSIONS

A block based blind watermark algorithm for colour image has been presented. Two levels of DWT have been applied on the colour host images. The highest magnitude coefficient from the LL2 has been used for the embedding process to increase the robustness of the algorithm. The proposed algorithm has been tested on different colour images and the best value of the embedding strength is $\Delta = 20$. PSNR and SSIM have been used to evaluate the distortion caused to the original image due to the watermarking data. PSNR larger than 55 dB and SSIM larger than 0.99 have been achieved. The proposed algorithm showed resistance against several attacks such as: vertical cropping, horizontal cropping, scaling, JPEG compression, additive noise, low-pass filter, and Gaussian filter.

REFERENCES

- [1] P. Singh, R. S. Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", *International Journal of Engineering and Innovative Technology (JEIT)* Volume 2, Issue 9, March 2013.
- [2] J. Manoharan, et al., "Performance Analysis of Spatial and Frequency Domain Multiple Data Embedding Techniques towards Geometric Attacks", *International Journal of Security (IJS)*, Volume (4), Issue (3), July, 2010.
- [3] N. Kashyap, G. SINHA, "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)", *IJ. Modern Education and Computer Science*, pp. 50-56, March 2012.
- [4] X. Xia, C. Boncelet, and G. Arce, "A Multiresolution Watermark for Digital Images", *Proc. IEEE Int. Conf. on Image Processing*, Oct. 1997.
- [5] H. Danyali, M. Makhloghi, and F. Tab, "Robust Blind DWT Based Digital Image Watermarking Using Singular Value Decomposition", *International Journal of Innovative Computing, Information and Control*, Vol. 8, No. 7(A), July, pp. 4691-4703.
- [6] A. Shing, A. Mishra, "Wavelet Based Watermarking on Digital Image", *Indian Journal of computer Science and Engineering*, 2011.
- [7] G. Bhatnagar and B. Raman, "A new robust reference watermarking scheme based on DWTSVD", Elsevier B.V. All rights reserved, 2008.
- [8] M. Barni, P. Bartolini, "An Improved Wavelet Based Watermarking Through Pixelwise Masking", *IEEE transactions on image processing*, Vol. 10, No. 5, May, 2001, pp. 783-791.
- [9] S. Lee, et al., "Reversible Image Watermarking Based on Integer to Integer Wavelet Transform", *IEEE Transaction on Information Forensics and Security*, vol. 2, No. 3, September 2007, pp. 321-330.
- [10] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji & A. Tawfik, "A new watermarking scheme for colour images captured by mobile phone cameras", *International Journal of Computer Science and Network Security*, vol. 9 No. 7, July 2009, pp. 248-254.
- [11] P. Khatkale, K. Jadhav & M. Khasne, "Digital Watermarking Technique for Authentication of Color Image", *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, Issue 7, July 2012, pp. 454-460.
- [12] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji & A. Tawfik, "A novel blind image watermarking technique for colour RGB images in the DCT domain using green channel", *Communications, Computers and Applications*, 2008. MIC-CCA 2008. Mosharaka International Conference on, Aug. 2008, pp. 26-31.

Appendix B

LIST OF PROGRAMMES

1. A Discrete Wavelet Coefficient Selection (DWCS) algorithm.
2. DWT robust watermarking algorithm for grey level images.
3. DWT robust watermarking algorithm for colour images (green channel).
4. DWT robust watermarking algorithm for colour images (Y channel).
5. Two-level DWT watermarking algorithm for grey level images.
6. Two-level DWT watermarking algorithm for colour images
7. Fragile watermarking algorithm for grey level images.
8. Fragile watermarking algorithm for colour images.
9. Combined one-level DWT robust algorithm and the fragile algorithm.
10. Combined two-level DWT robust algorithm and the fragile algorithm.