ÇANKAYA UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
COMPUTER ENGINEERING

MASTER THESIS

EFFICIENCY OF DISCRETE WAVELET TRANSFORM IN DIGITAL WATERMARKING

AHMED MOHAMMED

FEBRUARY 2014

Title of the Thesis: **Efficiency of Discrete Wavelet Transform in Digital Watermarking**

Submitted by **Ahmed MOHAMMED**

Approval of Graduate School of Natural and Applied Science, Çankaya University

Prof. Dr. Taner ALTUNOK

Director

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

Assist. Prof. Dr. Murat SARAN

Acting Head of Department

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

Assoc. Prof. Dr. H.Hakan MARAŞ

Supervisor

Examination Date: 21.02.2014

Examining Committee Members

Assoc.Prof.Dr.Hadi Hakan MARAŞ (Çankaya Univ.)

Assist.Prof.Dr.Reza ZARE HASSANPOUR (Çankaya Univ.)

Assoc.Prof.Dr.Ersin ELBAŞI (TÜBITAK)

STATE OF NON-PLAGIARISM

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

Name, Last Name: Ahmed MOHAMMED

Signature:

Date: 21/02/2014

ABSTRACT

EFFICIENCY OF DISCRETE WAVELET TRASNFORM IN DIGITAL WATERMARKING

MOHAMMED, Ahmed
M.Sc., Department of Computer Engineering
Supervisor: Assoc. Prof. Dr. H. Hakan MARAŞ

February 2014, 158 Pages

Digital watermarks have recently emerged as a possible solution for protecting the copyright of digital materials. The work presented in this thesis is concerned with the Discrete Wavelet Transform DWT based digital watermarking, and how the DWT is an efficient transform in the field of digital watermarking. Four efficiency test algorithms were proposed in this work, each uses a different level of DWT decomposition as an embedding domain for the binary pattern watermarks used, the four efficiency test algorithms were applied on both gray scale and colored images with RGB (green and blue channels were used only) and Ycbcr (Y luminance was used only) color spaces.

Fifteen important watermark attacks were applied on the four algorithms. Results were studied and examined carefully, and that led to obtain an optimum algorithm which is based on multi-level embedding criteria. The optimum algorithm was tested against even harder attacks which were the dual attacks (more than one attacks at a time) and a Hard

crop attack that removes almost 90% of the watermarked image data, then the performance of the optimum algorithm has been compared with some selected literature algorithms in the field.

Keywords: Discrete Wavelet Transform, Digital Watermarking, Watermark Attacks, PSNR, Correlation Coefficient.

ÖZ

SAYISAL DAMGALAMADA AYRIK DALGACIK DÖNÜŞÜMÜNÜN ETKİNLİĞİ

MOHAMMED, Ahmed
Yüksek Lisans, Bilgisayar Mühendisliği Anabilim Dalı
Tez Yöneticisi : Doç. Dr. H.Hakan MARAŞ

Şubat 2014, 158 sayfa

Sayısal damgalar, günümüzde telif haklarının korunmasında olası çözüm olarak ortaya çıkmaktadır. Bu tezde sunulan çalışmada, sayısal damgalamaya dayalı Ayrık Dalgacık Dönüşümü (ADD) ve ADD'nün sayısal damgalamada ne kadar etkin bir dönüşüm olduğu araştırılmıştır. Bu çalışmada, her biri değişik seviyede, kullanılan ikili şablon damgaları için bir gömülü alan olarak ADD ayrışımı yapan dört etkinlik testi algoritması önerilmiştir. Dört adet etkinlik testi algoritması hem gri-tonlu görüntülere hem renkli hem de YCbCr (sadece Y aydınlanma değeri kullanılmıştır) renk uzaylarına uygulanmıştır.

On beş önemli damgalama atağı dört algoritmaya da uygulanmıştır. Çok seviyeli damga gömme kıstaslarına dayalı bir şekilde en uygun algoritmanın belirlenmesine yönelik olarak, sonuçlar dikkatlice incelenmiş ve üzerinde çalışılmıştır. En uygun algoritma, çifte saldırı (bir anda biden fazla saldırı) gibi daha güçlü saldırılara ve damgalanmış görüntünün yaklaşık %90'ını yok eden aşırı kırpma saldırılarına karşı da test edilmiş, sonrasında en

uygun algoritmanın performansı literatürden seçilen bu konudaki diğer algoritmalar ile test edilmiştir.

Anahtar Kelimeler: Ayrık Dalgacık Dönüşümü, Sayısal Damgalama, Damgalama Saldırıları, Doruk Sinyal Gürültü Oranı (DSGO), Korelasyon Katsayısı.

ACKNOWLEDGEMENTS

I would like to express my special appreciation and thanks to my supervisor Assoc. Prof. Dr. Hadi Hakan MARAŞ, you have been a tremendous mentor for me. I would like to thank you for encouraging my research and for allowing me to grow as a research scientist. I would also like to thank my committee members, Assist. Prof. Dr. Reza ZARE HASSANPOUR, Assoc. Prof. Dr. Ersin ELBAŞI for serving as my committee members even at hardship. I also want to thank you for letting my defense be an enjoyable moment, and for your brilliant comments and suggestions, thanks to you.

A special thanks to my family. Words cannot express how grateful I am to my mother, and father.

At the end I would to like express appreciation to my beloved wife who spent sleepless nights with me and was always my support in the moments when there was no one to answer my queries.

TABLE OF CONTENTS

STATE OF NON-PLAGIARISM ..... **III**

ABSTRACT ..... **IV**

ÖZ ..... **VI**

ACKNOWLEDGEMENTS ..... **VIII**

TABLE OF CONTENTS ..... **IX**

LIST OF TABLES ..... **XIII**

LIST OF FIGURES ..... **XIV**

LIST OF ABBREVIATIONS ..... **XXII**

1. INTRODUCTION **1**

1.1 LITERATURE REVIEW 2

1.2 AIM OF WORK 4

1.3 THESIS OVERVIEW 5

2. WATERMARKING PRINCIPLES **6**

2.1 INFORMATION HIDING 6

2.2 WATERMARKING VS. STEGANOGRAPHY 7

2.3 TERMINOLOGY 8

2.4 MULTIMEDIA 8

2.5 BASIC WATERMARKING SCHEMES AND EVALUATIONS 9

2.5.1 Peak signal to noise ratio (PSNR) 10

2.5.2 The mean square error (MSE) 10

2.5.3 Correlation coefficients 11

2.6 DESIGN REQUIREMENTS 11

2.6.1 Robustness 11

2.6.2 Imperceptibility 12

2.6.3 Security 12

2.7 WATERMARKING APPLICATIONS 13

2.7.1 Watermarking for copyright protection 13

2.7.2 Watermarking for copy protection 14

2.7.3 Fingerprinting for pirate tracing 14

2.7.4 Watermarking for authentication 14

2.7.5 Watermark recovery 14

2.7.6 Low cost embedding and recovery 15

3. DIGITAL WATERMARKING TECHNIQUES AND ATTACKS 16

3.1 CLASSIFICATION OF WATERMARKING ALGORITHMS 16

3.1.1 Embedding and extraction domain 16

3.1.1.1 Discrete Fourier transform (DFT) 17
3.1.1.2 Discrete cosine transform (DCT) 17
3.1.1.3 The wavelet transform 18
3.1.1.4 Choosing a transform 22
3.1.2 Availability of reference data 23
3.1.3 Embedded data locations 23
3.1.4 Host data modified method 24
3.1.4.1 Additive algorithms 24
3.1.4.2 Quantization algorithms 24
3.1.5 Encoding the payload 25
3.1.5.1 Arnold cat's map (Arnold's transform) 25
3.2 ATTACKS ON WATERMARKS 27
3.2.1 Simple attacks 28
3.2.2 Geometric attacks 28
3.2.3 Collusion attacks 28
4. THE WAVELET-BASED ALGORITHMS 29
4.1 THE WAVELET-BASED ALGORITHMS 30
4.1.1 Watermark scrambling 32
4.1.2 Watermark embedding process 33
4.1.3 Attacks used in this work 37

4.1.4 Watermark extraction process 38

5. SIMULATION RESULTS 39

5.1 GRAY SCALE IMAGES EFFICIENCY TEST ALGORITHMS RESULTS 39

5.2 COLORED IMAGES EFFICIENCY TEST ALGORITHMS RESULTS 61

5.2.1 RGB - green channel efficiency test algorithms results 61

5.2.2 RGB - blue channel efficiency test algorithms results 83

5.2.3 Ycbcr luminance channel (Y) efficiency test algorithms results 96

5.3 OPTIMUM ALGORITHM RESULTS 110

5.3.1 Optimum algorithm vs. dual attacks 121

6. CONCLUSIONS AND FUTURE WORK 127

6.1 CONCLUSIONS 127

6.2 FUTURE WORK 129

REFERENCES 130

CURRICULUM VITAE 136

LIST OF TABLES

Table 5.1: PSNR in dB of all Efficiency Test Algorithms with Attacks 52

Table 5.2: Extracted Watermarks Correlations of all Efficiency Test Algorithms.....54

Table 5.3: PSNR in dB of all Efficiency Test Algorithms with Attacks 75

Table 5.4: Extracted Watermarks Correlations of all Efficiency Test Algorithms.....77

Table 5.5: PSNR in dB of all the Efficiency Test Algorithms with Attacks 88

Table 5.6: Extracted Watermarks Correlations of all the Efficiency Test Algorithms....90

Table 5.7: PSNR in dB of all Efficiency Test Algorithms with Attacks 101

Table 5.8: Extracted Watermarks Correlations of all Efficiency Test Algorithms.....103

Table 5.9: PSNR in dB of the Optimum Algorithm with Attacks 111

Table 5.10: Optimum Algorithm Extracted Watermarks Correlations with Attacks.....113

Table 5.11: Optimum Algorithm PSNR in dB for Different Images.....116

Table 6.1: Optimum Algorithm PSNR in dB of Lena Image vs. Some Other Publications 129

LIST OF FIGURES

Figure 2.1: Information Hiding 6

Figure 2.2: A Generic Scheme of Watermarking Embedding Module 9

Figure 2.3: A Generic Scheme of Watermarking Recovery Module 9

Figure 2.4: Design Requirements 13

Figure 3.1: DWT for Two Dimensional Images 21

Figure 3.2: The Pyramidal Two-Level Decomposition of an Image. 21

Figure 3.3: Energy Distribution in the Transform Domain 22

Figure 3.4: Arnold's Transform Steps 26

Figure 3.5: Arnold Scrambling With Different Number of Iterations 26

Figure 4.1: Daubechies Wavelets Family 30

Figure 4.2: Levels of DWT Decomposition Used 32

Figure 4.3: (a) Original Watermark, (b) Scrambled Watermark 33

Figure 4.4: Gray Scale Image Watermarking System 34

Figure 4.5: RGB Image Watermarking System 35

Figure 4.6: Ycbcr Watermarking System 36

Figure 5.1: (a) Original Watermark, (b) Scrambled Watermark 39

Figure 5.2: Cover Image 40

Figure 5.3: First Level Decomposition 40

Figure 5.4: Gray Scale First Algorithm Watermarked Image, PSNR=43.3780 dB.....41

Figure 5.5: JPEG, Q=100%, PSNR=43.1404 dB.....42

Figure 5.6: JPEG, Q=75%, PSNR=42.0614 dB.....42

Figure 5.7: JPEG, Q=50%, PSNR=40.6153 dB.....43

Figure 5.8: JPEG, Q=25%, PSNR=38.4487 dB.....43

Figure 5.9: JPEG 2000, PSNR= 36.8535 dB 44

Figure 5.10: Gaussian Noise, Mean=0, Variance=0.001, PSNR= 29.8000 dB 44

Figure 5.11: Salt & Pepper Noise, Density=0.01, PSNR=25.5313 dB.....45

Figure 5.12: Mean Filter, Window (3X3), PSNR= 37.5261 dB 45

Figure 5.13: Resizing 50%, PSNR=39.2585 dB.....46

Figure 5.14: Rotation -20^0, PSNR=11.6438 dB.....46

Figure 5.15: Histogram Equalization, PSNR=17.1786 dB 47

Figure 5.16: Intensity Adjustment, PSNR=17.1035 dB.....47

Figure 5.17: Gamma Correction, PSNR=17.7670 dB 48

Figure 5.18: Cropping, PSNR=14.4924 dB 48

Figure 5.19: Motion Blurred, PSNR=34.1108 dB 49

Figure 5.20: Gray Scale Image second Level Decomposition.....49

Figure 5.21: Gray Scale Second Algorithm Watermarked Image, PSNR= 44.1927 dB .50

Figure 5.22: Gray Scale Image Third Level Decomposition 50

Figure 5.23: Gray Scale Third Algorithm Watermarked Image, PSNR= 47.5072 dB 51

Figure 5.24: Gray Scale Image fourth Level Decomposition 51

Figure 5.25: Gray Scale fourth Algorithm Watermarked Image, PSNR= 48.7859 dB ... 52

Figure 5.26: PSNR in dB of all Efficiency Test Algorithms with Attacks 53

Figure 5.27: First Efficiency Test Algorithm Extractions 56

Figure 5.28: Second Efficiency Test Algorithm Extractions 57

Figure 5.29: Third Efficiency Test Algorithm Extractions 58

Figure 5.30: Fourth Efficiency Test Algorithm Extractions 59

Figure 5.31: Extracted Watermarks Correlations of all Efficiency Test Algorithms with Attacks 60

Figure 5.32: (a) Original Watermark, (b) Scrambled Watermark 61

Figure 5.33: Cover Image 62

Figure 5.34: Green Channel 62

Figure 5.35: First Level Decomposition of Green Channel 63

Figure 5.36: Watermarked Green Channel, PSNR= 40.4899 dB 63

Figure 5.37: Green Channel First Algorithm Watermarked Image, PSNR=45.2611 dB 64

Figure 5.38: JPEG, Q=100%, PSNR=42.2276 dB 65

Figure 5.39: JPEG, Q=75%, PSNR=36.7660 dB 65

Figure 5.40: JPEG, Q=50%, PSNR=35.4178 dB 66

Figure 5.41: JPEG, Q=25 %, PSNR= 33.5714 dB 66

Figure 5.42: JPEG 2000, PSNR=35.5017 dB 67

Figure 5.43: Gaussian Noise, Mean=0, Variance=0.001, PSNR=29.8844 dB 67

Figure 5.44: Salt & Pepper Noise, Density=0.01, PSNR= 25.0817 dB 68

Figure 5.45: Mean Filter, Window size 3X3, PSNR=36.9799 dB 68

Figure 5.46: Resizing 50%, PSNR= 37.7731 dB 69

Figure 5.47: Rotation -20^0, PSNR=11.1773 dB 69

Figure 5.48: Histogram Equalization, PSNR=14.2044 dB 70

Figure 5.49: Intensity Adjustment, PSNR=18.2211 dB 70

Figure 5.50: Gamma Correction, PSNR=18.2868 dB 71

Figure 5.51: Cropping, PSNR=14.4645 dB 71

Figure 5.52: Motion Blur, PSNR=32.6677 dB 72

Figure 5.53: Second level Decomposition of Green Channel 72

Figure 5.54: Green Channel Second Algorithm Watermarked Image, PSNR=46.4652 dB 73

Figure 5.55: Third Level Decomposition of Green Channel 73

Figure 5.56: Green Channel Third Algorithm Watermarked Image, PSNR=48.7566 dB 74

Figure 5.57: Fourth Level Decomposition of Green Channel 74

Figure 5.58: Green Channel Fourth Algorithm Watermarked Image, PSNR=52.3074 dB 75

Figure 5.59: PSNR in dB of all Efficiency Test Algorithms with Attacks 76

Figure 5.60: Green Channel First Efficiency Test Algorithm Extractions 79

Figure 5.61: Green Channel Second Efficiency Test Algorithm Extractions 80

Figure 5.62: Green Channel Third Efficiency Test Algorithm Extractions 81

Figure 5.63: Green Channel Fourth Efficiency Test Algorithm Extractions 82

Figure 5.64: Extracted Watermarks Correlations of all Efficiency Test Algorithms with Attacks 83

Figure 5.65: First level decomposition of Blue Channel 84

Figure 5.66: Blue Channel First Algorithm Watermarked Image, PSNR=45.2616 dB .. 84

Figure 5.67: Second level Decomposition of Blue Channel 85

Figure 5.68: Blue channel Second Algorithm Watermarked Image, PSNR=46.4652 dB 85

Figure 5.69: 3rd level decomposition of Blue Channel 86

Figure 5.70: Blue Channel Third Algorithm Watermarked Image, PSNR=48.7566 dB . 86

Figure 5.71: Fourth level Decomposition of Blue Channel 87

Figure 5.72: Blue Channel Fourth Algorithm Watermarked Image, PSNR=52.3074 dB 87

Figure 5.73: PSNR in dB of all Efficiency Test Algorithms with Attacks 89

Figure 5.74: Blue channel First Efficiency Test Algorithm Extractions 92

Figure 5.75: Blue Channel Second Efficiency Test Algorithm Extractions 93

Figure 5.76: Blue Channel Third Efficiency Test Algorithm Extractions 94

Figure 5.77: Blue Channel Fourth Efficiency Test Algorithm Extractions 95

Figure 5.78: Extracted Watermarks Correlations of All the Efficiency Test Algorithms with Attacks.....96

Figure 5.79: First level Decomposition of Y Luminance Channel 97

Figure 5.80: Y Channel First Algorithm Watermarked Image, PSNR=43.4232 dB 97

Figure 5.81: Second level Decomposition of Y Luminance Channel.....98

Figure 5.82: Y Channel Second Algorithm Watermarked Image, PSNR=44.3791 dB..98

Figure 5.83: Third level Decomposition of Y Luminance Channel.....99

Figure 5.84: Y Channel Third Algorithm Watermarked Image, PSNR= 45.1978 dB.....99

Figure 5.85: Fourth level Decomposition of Y Luminance Channel.....100

Figure 5.86: Y Channel Fourth Algorithm Watermarked Image, PSNR= 46.1773 dB.100

Figure 5.87: PSNR in dB of all Efficiency Test Algorithms with Attacks.....102

Figure 5.88: Y Channel First Efficiency Test Algorithm extractions.....105

Figure 5.89: Y Channel Second Efficiency Test Algorithm Extractions.....106

Figure 5.90: Y Channel Third Efficiency Test Algorithm Extractions.....107

Figure 5.91: Y Channel Fourth Efficiency Test Algorithm Extractions.....108

Figure 5.92: Extracted Watermarks Correlations of all Efficiency Test Algorithms with Attacks.....109

Figure 5.93: First level Decomposition of Blue Channel 110

Figure 5.94: Fourth level Decomposition of Blue Channel 110

Figure 5.95: Optimum Algorithm Watermarked Image, PSNR= 46.7582 dB 111

Figure 5.96: Optimum Algorithm PSNR in dB with Attacks 112

Figure 5.97: Optimum Watermarks Extractions 114

Figure 5.98: Optimum Watermarks Correlations with Attacks 115

Figure 5.99: Crop Attack at Different Rations 117

Figure 5.100: Correlation vs. Cropping Ratio 117

Figure 5.101: Hard Crop 1, PSNR= 5.6567 dB 118

Figure 5.102: Extracted Watermarks, Correlation of Selected Watermark= 0.6096 118

Figure 5.103: Hard Crop 2, PSNR= 5.3887 dB 119

Figure 5.104: Extracted Watermarks, Correlation of Selected Watermark= 0.4230 119

Figure 5.105: Gaussian Nosie Attack with Different Variances 120

Figure 5.106: Correlation vs. Gaussian Nosie variance 120

Figure 5.107: Optimum Algorithm Noisy Watermarked Image, Mean=0, Variance=0.01, PSNR= 20.1961 dB 121

Figure 5.108: JPEG, Q=25%, PSNR= 26.3874 dB 122

Figure 5.109: JPEG 2000, PSNR= 18.4732 dB 122

Figure 5.110: Salt & Pepper, PSNR= 19.0360 dB 123

Figure 5.111: Resizing at 50%, PSNR= 31.4692 dB 123

Figure 5.112: Mean Filter, PSNR=28.8921 dB 124

Figure 5.113: Rotation -20 Degrees, PSNR=10.9991 dB 124

Figure 5.114: Cropping at 75%, PNSR= 6.5377 dB 125

Figure 5.115: Motion Blurred, PSNR=29.1967 dB 125

Figure 5.116: Optimum Algorithm Multiple Dual Attacks Extractions with Correlations Values In Blue Color 126

LIST OF ABBREVIATIONS

DWT	Discrete Wavelet Transform
2D	Two-Dimensional
LSB	Least Significant Bit
SVD	Singular Value Decomposition
DRM	Digital Rights Management
IHW	Information Hiding Workshop
PSNR	Peak Signal to Noise Ratio
MSE	Mean Square Error
DFT	Discrete Fourier Transform
DCT	Discrete Cosine Transform
IDFT	Inverse Discrete Fourier Transform
IDCT	Inverse Discrete Cosine Transform
HVS	Human Visual System
JPEG	Joint Photographic Expert Group
JPEG 2000	Joint Photographic Expert Group in 2000

CHAPTER ONE

INTRODUCTION

The development of the image processing techniques and the fast growth in communication via the internet led to the ease of both exchange and access to data and information [1]. Besides the existence of the electronic spyware, the information security, content ownership and protection of copyrighted multimedia content has become the focus of attention especially in sectors of government, Military and other fields [2].

As well known, the internet is an open environment, there is a need to provide new efficient ways to protect the data information from copying or illegal manipulation, among these methods the encryption techniques, which are considered one of the traditional methods of information security.

Encryption techniques meant to provide protection of confidential data by converting it to some sort of a rubbish form [1], and that must be done before exchanging information between the two communication parties. But the encrypted data are unclear and raises doubts and attracts the attention of hackers and those who are interested in knowing what information it holds, making them trying to break and destroy the code. Meanwhile, the information hiding techniques development provided a solution to protect this data by adopting techniques that are based on the exchange of confidential data in a way through which the secret connection cannot be detected [3].

Digital watermarking is used for the purpose of rapid and non-expensive deployment of digital multimedia in addition to the secret data exchange via the Internet. Its technologies subsequently adopted for the purpose of achieving the reliability of the data by protecting copyrights and ownership, which increased the need for it with the rapid development in communication [4]. In recent times the field of researches is not only limited to the development of Digital Watermarking techniques, but also to achieve a good integration

with other scientific fields where the digital image processing algorithms are adopted to develop the Digital Watermarking techniques and improve their requirements [5, 6].

1.1 Literature Review

The name Watermark was derived from the German word (Wassermarke), its first appearance was in Fabriano – Italy, in 1282 during the making of a special mark seal on paper. Also in 1887 William Gongreve invented a technique for adding a colored material to the center of the paper during the manufacturing process. Where in 1979 the watermarking pattern was developed by szepansk making it more robust against manipulation attempts.

After that the watermark draws more attention until 1996 when the watermark gained its first worldwide acceptance and considered one of the main subjects in Information Hiding Workshop (IHW). Later on the Watermarking Techniques were adopted as an efficient way to prove the Ownership and protect the information. Some of the earliest publications concerning Digital watermarking of (still images) include Tanaka et al. [7], and Tirkel et al. [8]. Next in this section a short review of important Discrete Wavelet Transform (DWT) Based Digital Watermarking Algorithms are given.

In 1998, Deepa Kundur and Dimitrios Hatzinakos [9] worked on the non-blind digital watermarking based on the multi-resolution property of wavelets, and compared their results with other domains watermarking methods. Also in 2000, Patrick Loo and Nick Kingsbury [10] presented a blind digital watermarking system in the complex wavelet domain.

Where in 2002, YiweiWang et al. [11] discussed the practical requirements of digital watermarking system in the DWT domain besides the invisibility and robustness of the digital watermarking system, S.A.M.Gilani et al. [12] in 2002 offered a color image blind watermarking system in the wavelet domain with an alternative color space to RGB due to its high correlation property, they used color spaces with linear relationship with RGB but low correlated component.

In 2003, Zhuan Qing Huang and Zhuhan Jiang [13] proposed a digital watermarking system for the purpose of image ownership verification using a private key pattern and wavelet filters. Peining Taoa and Ahmet M. Eskicioglu [14] in 2004 worked on the non-blind watermarking system and embedded four binary watermarks in the four bands given by the DWT first level decomposition, and their second algorithm was to embed four binary watermarks in the second level decomposition. Again in the same year P. Kumhom et al. [15] implemented a non-blind watermarking system that concentrate on the selection of the high frequency range which contains large amount of information.

In the year of 2005, Nagaraj Dharwadkar and B.B.Amberker [16] presented a new secure digital watermarking system in the wavelet domain that uses visual cryptography scheme which has an adaptive order dithering technique, then embedding one share into the high textured sub-band of the color image's luminance channel. Jila Ayubi et al. [17] In 2011 came with a watermarking system based on chaotic maps and DWT. While in 2012 Amal Khalifa and Safwat Hamad [18] introduced a novel algorithm that applies casting operation of the binary message onto the DWT coefficients of the colored images with multi-level decomposition.

In the same year Kiran Kumar et al. [19] used Haar wavelet scheme for perfectly reconstructed filter banks and then hide the data in the Least Significant Bits (LSB) of details coefficient. Again in this year, Timmy Gupta [20] studied the type of watermarks and their characteristics and embedded these type in DWT domain. Also in 2012, Parthiban V and Ganesan R [6] improved the robustness of his system through combination of DWT and Singular Value Decomposition (SVD) method.

In 2013, Nasseer M. Basheer and Shaymaa S. Abdulsalam [21] proposed a genetic algorithm that embeds the Watermark components in the approximation band of the DWT fourth level of decomposition, by quantizing the coefficients of the DWT 4^{th} level decomposition (LL) band of the cover image in order to improve the watermark the Genetic Algorithm is used for optimizing the quantization step size parameter, and the strength of factors robustness.

1.2 Aim of Work

Presented in this research a study aims to test the efficiency of the DWT in1 digital watermarking through the integration of DWT based digital watermarking techniques and the digital image processing techniques. Also another aim of this work is to find an optimum and secure algorithm that embeds the watermarks in the most suitable frequency bands in order to resist the most important and harmful attacks on watermarks. The motivation behind this work is to keep the Peak Signal to Noise Ratio (PSNR) value between the original un-watermarked cover image and the watermarked image above 45 dB with an efficient ability to extract the embedded watermarks with minimum loss of details and keep the correlation coefficient value between original and extracted watermark around the value of 0.9 (correlation coefficient value varies from 0 to 1 and the closer the correlation to 1 the more the similarity between the compared objects, and a correlation of 1 means that the two objects are identical).

The main property of this work is to take the watermarking algorithms to a higher robustness test level by attacking the optimum algorithm with the new attacks used in this work which are the dual attacks (more than one attack at the same time) and the hard cropping attack (cropping more that 90% of the image).

The efficiency test algorithms are four main algorithms, the first algorithm embeds the watermarks in the four frequency sub-bands given by the DWT first level decomposition, the second algorithm uses the DWT second level decomposition for embedding the watermarks, the third algorithm uses the third level decomposition, and the fourth uses the fourth level decomposition. And all of the algorithms follow the same procedures where the DWT of two-dimensional (2D) images was adopted to transform the images into their frequency domain into which the watermarks will be embedded. Six gray scale and six colored images in both RGB (for both Blue and Green channels) and Ycbcr color spaces were used in this work which means that the total number of efficiency test algorithms is sixteen algorithm as following:

- The four efficiency test algorithms were applied on six gray scale images.

- The four efficiency test algorithms were applied on six colored images using the Green channel of the RGB color space.
- The four efficiency test algorithms were applied on six colored images using the Blue channel of the RGB color space.
- The four efficiency test algorithms were applied on six colored images using the Y channel of the Ycbcr color space.

Four watermarks will be embedded in each algorithm in the four bands given by the DWT (Approximation, Horizontal detail, Vertical detail and Diagonal detail), the watermarks were scrambled by Arnold's cat map before embedding to increase the system's security and robustness, embedding, attacking (with fifteen important attacks) and extraction of the embedded watermarks is done. An optimum algorithm that keeps the Cover image un-distorted with an efficient capability to extract the embedded watermarks at the highest accuracy possible is determined and implemented depending on the results obtained from the efficiency test algorithms. This work is implemented using MATLAB Version 7.12.0 (R2011a).

1.3 Thesis Overview

This thesis consists of six chapters where a brief description of watermarking and its motivations is provided in chapter one, an adequate background is given in Chapter 2 covering all about watermarking history, terminology, basic schemes, applications and evaluations. Chapter 3 surveys current watermarking techniques and attacks on watermarking systems. In particular, watermarking techniques are classified in the light of the domain they operate in, how the watermark is encoded, how the embedding locations are chosen, how the watermark is combined with the cover signal and how the watermark is extracted. Attacks on watermarks are classified into three categories, simple attacks, geometric attacks, and collusion attacks.

Chapter 4 described the algorithms used in this work, whereas chapter 5 presents the simulation results. Conclusion and future work are presented in chapter 6.

CHAPTER TWO

WATERMARKING PRINCIPLES

2.1 Information Hiding

One of the image processing techniques to hide the transmission of confidential data and remove doubt in the existence of hidden information, concealment techniques have been used for thousands of years as a means to achieve the secret connection. And one of the most famous information hiding techniques is Steganography and Watermark. There are some challenges facing information hiding that can be mentioned as follows:

- Embedding the secret information without distorting the Cover image, and make it undetectable.
- Protecting the embedded information from deliberate attacks and Smart attempts to manipulate or remove those data.
- Embedding of data directly into the digital content and not in the header to prove no change happens under different file formats, the Figure (2.1) illustrates the classification of information hiding.

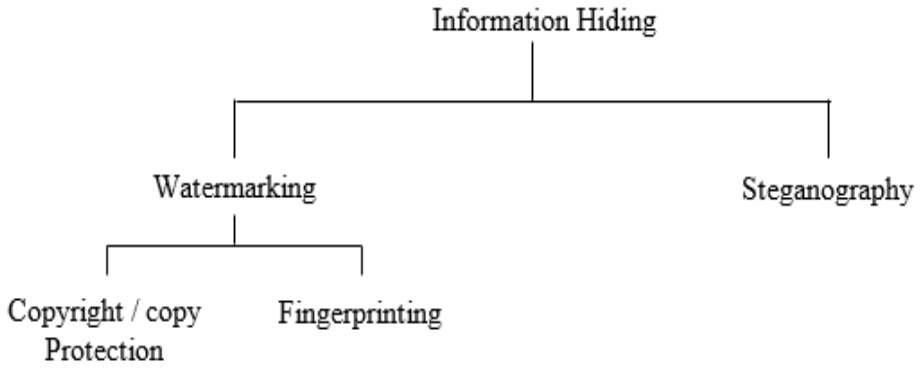


Figure 2.1: Information Hiding

2.2 Watermarking vs. Steganography

Digital watermark represents a code that is added or embedded in an ordinary host data which will be called the host or cover data, the embedded information has to be robust enough facing any intended removal by attackers. Unlike cryptography, where the presence of information is known but not the meaning of it, in digital watermarking the aim is hiding the entire existence of the information.

The relationship between watermarking and steganography is that, both describe techniques that are used to transfer information using a hidden manner. They are both related to a wider subject called information hiding. However, the underlying philosophy of the two is different. Steganography is a point-to-point communication between two parties. In this way, steganography is usually not very robust against multiple kinds of modification that may occur in the data, or sometimes has limited robustness and tends to secure the information against some technical modifications that could possibly occur during the transmission and storage.

Moreover, watermarking is usually a point-to-multipoint communication and any hidden message must be robust against attempts aiming to extract it or remove it. Thus, watermarking is important whenever the cover data can be available to those who know the presence of hidden information and probably have the interest to extract or remove it. The most popular application of watermarking is copyright protection, i.e., embedding copyright statements that prove the ownership of original data. Clearly, the copyright information should resist any modifications or manipulations that may attempt to remove it. Fingerprinting used to distinguish distributed data sets, is another application of digital watermarks and has its own special requirements [22, 23, 24].

Digital watermarking is considered an important field of information security, and the perfect way to define and prove the reliability, copyright and ownership. Lately digital watermarking started drawing a great attention and used in different systems of Digital Rights Management (DRM).

2.3 Terminology

For classifying watermarking techniques, there are several names that have been used. In this section these names are summarized.

Cover or host data is the digital part of data into which the information to be hidden, where the payload represents the hidden data or information. The watermarks can be visible or invisible, the visible watermarks are those who are added to the cover data as visual patterns (e.g. logos), and the invisible watermarks which are used by the majority of watermarking systems and it should cause no alteration or degradation to the cover data. The Non-blind watermarking scheme is the system that requires the original un-watermarking cover data to extract the hidden information, sometimes it's also called non-oblivious watermarking scheme. Unlike blind watermarking scheme which is the system that doesn't require the original un-watermarked cover data in order to extract the hidden information. Finally the watermarking system that requires a secret or a public key to extract the hidden information is called a semi-blind watermarking scheme. The fragile watermarks have limited robustness, and they are usually used for the reason of detecting any modifications that could occur in the cover data [25].

2.4 Multimedia

The term multimedia points to the diverse classes of media which are employed to represent information. It can be classified as:

- Continuous Media, e.g. Videos and Audios.
- Discrete Media, e.g. Images and Text Files.

In this thesis only still images were used (Gray scale and Colored images in Both RGB and Ycbcr spaces).

2.5 Basic Watermarking Schemes and Evaluations

All watermarking schemes consist of two stages, namely the embedding stage and the recovery stage (also called extraction stage), which are shown in Figures (2.2) and (2.3) respectively.

The embedding function takes the cover data, the payload and a (public/secret) key (Optional) to produce the watermarked data. The goal of using the key is to increase watermarks robustness against attacks. Supposedly, the watermark can't be read or removed without knowing this key [25].

The recovery stage takes the watermarked data which may be modified, the key and/or original un-watermarked data depending on the watermarking technique used. This part returns either the extracted payload (decoded watermark) or a dependable measurement of how likely a specific watermark is present (detected watermark).

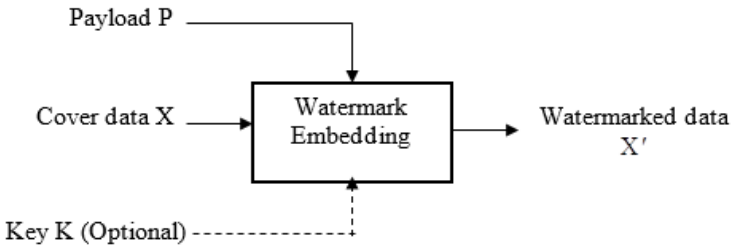


Figure 2.2: A Generic Scheme of Watermarking Embedding Module

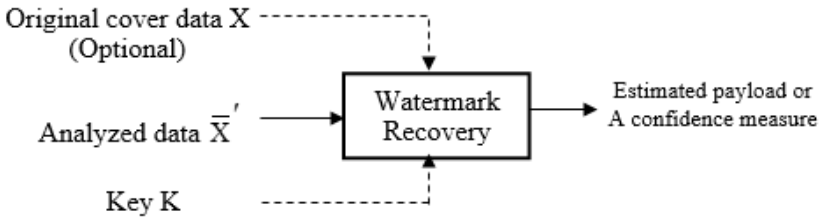


Figure 2.3: A Generic Scheme of Watermarking Recovery Module

The evaluations used in this work are as follows:

2.5.1 Peak signal to noise ratio (PSNR)

In watermarking, the PSNR is the most measurement of quality of an image reconstruction used. It is a ratio between the magnitudes of background noise and the maximum signal (watermarked image) value. It easier definition by the Mean squared error (MSE). The PSNR calculated in this work is between the un-watermarked cover image and the watermarked image to determine the quality of reconstruction. The PSNR is defined as follows:

$$PSNR = 10log_{10}\left(\frac{MAX^2}{MSE}\right) \tag{2.1}$$

Where:

MAX^2: The maximum value of the cover image to the power of 2.

MSE: The Mean square error, between the un-watermarked cover image and the watermarked image.

2.5.2 The mean square error (MSE)

MSE is an old, proven measure of control and quality the MSE is defined as follows:

$$MSE = \frac{\sum_{x,y}[f(x,y) - f'(x,y)]}{M \times N} \tag{2.2}$$

Where:

$f(x,y)$: Is the un-watermarked Cover image or the original Watermark image

$f'(x,y)$: Is the Watermarked Image or the Extracted watermark image

M, N: Original Image dimensions.

2.5.3 Correlation coefficients

Used for the purpose of similarity measure, and its value varies from (0-1) the closer the value to 1 the higher the similarity between the two matrices and vice versa. It's been used in this thesis to measure the similarity between extracted watermarks and original ones, it's defined as follows:

$$CC = \frac{\sum_m \sum_n \left(A_{m,n} - \overline{A}\right)\left(B_{m,n} - \overline{B}\right)}{\sqrt{\left(\sum_m \sum_n \left(A_{m,n} - \overline{A}\right)^2\right)\left(\sum_m \sum_n \left(B_{m,n} - \overline{B}\right)^2\right)}} \quad (2.3)$$

Where:

$A_{m,n}$: Un-watermarked cover image or original watermark image

$B_{m,n}$: Watermarked or Extracted watermark image

$\overline{A}$: Mean of the un-watermarked cover image or original watermark image

$\overline{B}$: Mean of the watermarked or extracted watermarked image

m, n: Original Image dimensions

2.6 Design Requirements

An effective watermarking system should have several features whose importance vary depending on the application area. These features are described in the following sections.

2.6.1 Robustness

Ideally, a robust watermarking scheme should resist any form of malicious distortion which does not render the image useless. Some attacks will be more important than others depending on a particular application and the media used (e.g. image, audio or video) [26]. It is probably more efficient to employ a method working in transform domain rather than

to use a method working in spatial domain [25]. Various types of attacks will be discussed in more details in the next chapter.

2.6.2 Imperceptibility

To preserve the quality of a watermarked document, the watermark should not be distorting the original document noticeably, which means that the original and watermarked documents have to be perceptually identical [27]. Without consideration to the application or the purpose of the watermarking a data, the embedded information has to be minimally perceptible by the human visual or auditory systems [28].

Imperceptibility and robustness are the most important requirements for an effective watermarking system. Unfortunately, these requirements are conflicted and all watermarking algorithms design involves determining a tradeoff between these two conflicting requirements. The higher is the embedding strength of the watermark, the more robust it is but will also be more visible. Using a good perceptual model will allow us to maximize the energy of watermark while keeping its visibility to minimum [29, 30].

2.6.3 Security

Unauthorized parties should be unable to read or alter the watermark. Security should be assured for most watermarking applications such as copyright protection. Sometimes, a secret key might be used with the embedding and extracting processes. It's not possible for a user to find out whether a piece of data is watermarked until he/she has this (private) key. In other words, a secret key based watermarking systems have a major disadvantage, and the main reason for that is that they do not allow a public recovery of the watermark. In order to overcome this problem, public key watermarking algorithms have been proposed. A public and a private key algorithms are used. For example, an image could be watermarked using a private key, and still a public key can be used to verify the mark [25]. Some public key based watermarking algorithms are presented in [25, 31]. Figure (2.4) illustrates the three important issues.

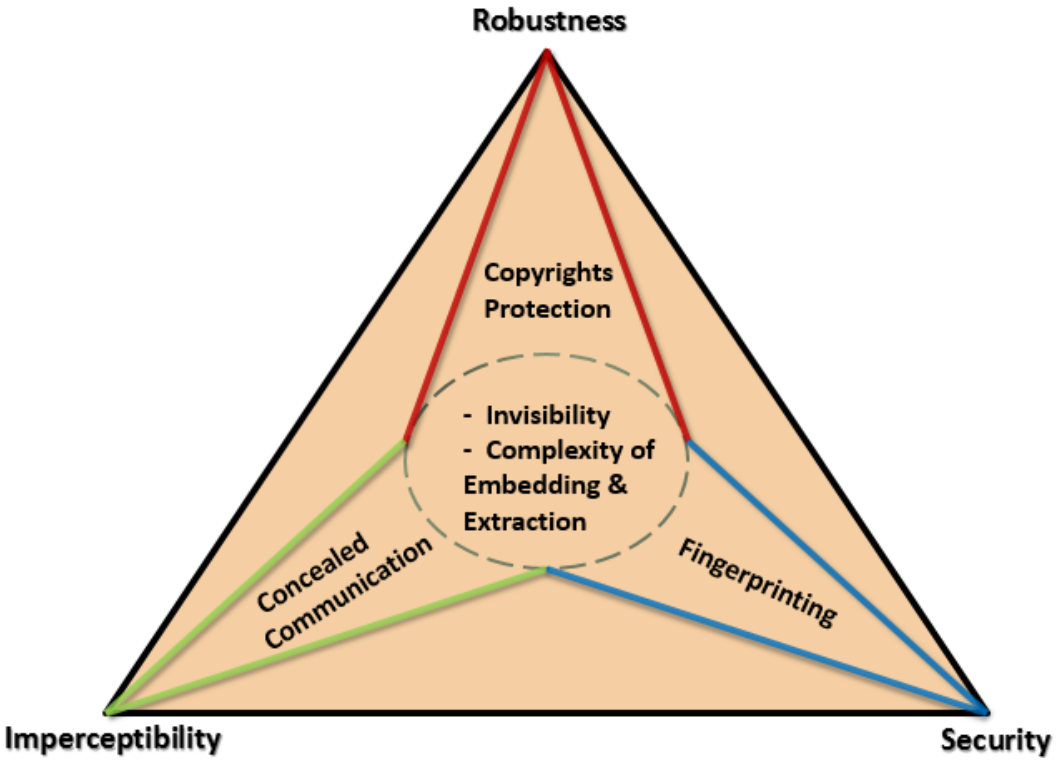


Figure 2.4: Design Requirements

2.7 Watermarking Applications

Different watermarking applications have different requirements. In the following sections, some of these applications are presented.

2.7.1 Watermarking for copyright protection

The image owner can embed a robust, impreceptable and quickly extractable watermark to identify any unauthorized versions or copies and at the same time prevent others from claiming the copyright of the image. Therefore, such application demands a high level of robustness. Note that a watermark for copyright protection does not prevent people from copying the digital data. They rather simply exist as means for owners to assure their ownership over the digital data [4].

2.7.2 Watermarking for copy protection

Copy protection means disallowing the unauthorized copying of digital data. In open systems like the Internet, it is very difficult to achieve copy protection but, it is possible to enforce copy protection in a controlled system like the DVD player. For example, the watermark that exists on a DVD tells the compliant DVD player whether a user is allowed to copy the video or not [24].

2.7.3 Fingerprinting for pirate tracing

The copy holder (image seller) might want to figure out which customer has leaked the un-authorized version or copy. Hence fingerprinting is important in identifying both the seller and the buyer of the un-authorized copy. For this aim more requirements should be considered, for example the insertion of multiple watermarks and a large number of watermarks generation should be possible [25].

2.7.4 Watermarking for authentication

The objective of authentication applications is to detect modifications of the data (e.g. [32, 33]. Fragile watermarks are used to authenticate digital data. If the image, for example, is modified by a malicious party, then watermark will probably be destroyed. Hence, if the watermark still can be retrieved by a recipient, then the image is considered authentic. Otherwise, it is not and has to be discarded.

For data authentication purpose, the embedded watermark has to be invisible to a human observer. Moreover, it's preferred to make it harder to insert additional watermarks without causing some degradation to the watermarked image (e.g. [34]). However, a fragile watermark will have some robustness rather than like a checksum, which fails even if only 1 bit of the data has been changed.

2.7.5 Watermark recovery

In some applications like the video watermarking, it may be unpractical to use the un-watermarked (original) data in the recovery process due to the large amount of data that

would have to be processed (e.g. Blind Watermarking). However in many other applications, the original data are used to recover or verify the watermark (e.g. Non-Blind Watermarking).

2.7.6 Low cost embedding and recovery

One of the most important features of the watermarking algorithm is that, it should have low complexity and perform simple operations [27, 35]. The speed of watermarking embedding and recovery processes is important for some applications like video applications because of the large amount of data to be processed.

CHAPTER THREE

DIGITAL WATERMARKING TECHNIQUES AND ATTACKS

Recently, plentiful digital watermarking algorithms were developed for the purpose of helping and protecting the copyright of digital data and to verify the multimedia data integrity, in this chapter different image watermarking techniques are classified according to the most significant criteria, also a classification of attacks on watermarking systems is explained in this chapter.

3.1 Classification of Watermarking Algorithms

Watermarking algorithms can be distinguished according to

- Embedding /extraction domain.
- Availability of reference data (e.g. the original host image) for the watermark extraction process.
- Locations where the watermark to be embedded.
- Host data modified method.
- Encoding of the payload.

Each of the above features will be discussed in details in the following sections.

3.1.1 Embedding and extraction domain

An algorithm may modify the pixels of an image in the spatial domain directly in order to embed the watermark. Some published papers in this domain are [36, 37, 38, 39, 40], Another alternative is to transform the image into some other domain (for example, Discrete Fourier Transform DFT [41], Discrete Cosine Transform DCT [42], or Discrete Wavelet Transform DWT [20], then embed the watermark and use the inverse transform of the result to obtain the watermarked image.

3.1.1.1 Discrete Fourier transform (DFT)

DFT is useful in watermarking because it is helpful in selecting appropriate parts of the image for the purpose of embedding to have high invisibility and robustness. Given a two-dimensional signal f(x,y). Then the Two dimensional DFT is defined as in equation (3.1) [43]:

$$f(u,v) = \frac{1}{MN}\sum_{x-0}^{M-1}\sum_{y-0}^{N-1} f(x,y)\, e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)} \tag{3.1}$$

For u= 0,1,2…,M-1, v= 0,1,2,..,N-1.

Where *M*, *N* represent the dimensions of the image

The inverse of two dimensional DFT (IDFT) is given by the equation (3.2) [43]:

$$f(x,y) = \frac{1}{MN}\sum_{u-0}^{M-1}\sum_{v-0}^{N-1} f(u,v)\, e^{j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)} \tag{3.2}$$

3.1.1.2 Discrete cosine transform (DCT)

DCT is the domain used for JPEG and MPEG. Thus, it has been commonly used for watermarking purposes because watermarks which are embedded in the DCT domain are usually more robust against both JPEG and MPEG compression.

The two dimensional DCT forward transform given by equation (3.3) [44]:

$$f(u,v) =$$

$$\frac{2C(u)C(v)}{\sqrt{MN}}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} p(i,j)\cos\left(\frac{(2i+1)u\pi}{2M}\right)\cos\left(\frac{(2j+1)v\pi}{2N}\right) \tag{3.3}$$

$p(i,j)$: Pixel level at the location(i,j).

$f(u,v)$: DCT coefficients at the frequency indices(u,v).

M, *N*: represent the dimensions of the image

And the Inverse of the two dimensional DCT transform is given by equation (3.4) [44]:

$$p(i,j) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1}\frac{2C(u)C(v)}{\sqrt{MN}}F(u,v)\cos(\frac{(2i+1)u\pi}{2M})\cos(\frac{(2j+1)v\pi}{2N}) \quad (3.4)$$

Several authors used the DCT in their watermarking process [48, 49, 50, 51, 52, 53], some add the coefficients of the DCT of the image to the coefficients of the watermark [45, 46] or select some of the coefficients of the DCT of the image for embedding [47].

3.1.1.3 The wavelet transform

The wavelet transform is one of the famous types of transformation that are used extensively in digital image processing in many applications such as finger print verification and compression, also the wavelet transform is widely used in digital signal processing [54, 55].

The basis of the DWT first appeared in 1976 when Croiser, Esteban, and Galand came up with a technique that decomposes discrete time signals. Crochiere. Flanagan and Weber also made a similar technique regarding the speech signals coding. Then they named their system or scheme as sub-band coding. Later in 1983 Burt called it the pyramidal coding which is also known as the multi-resolution analysis [56]. The DWT basic idea for a one dimensional signal is as follows. A signal is to be split into two parts, and those are usually high frequencies and low frequencies. From an image point of view the edge components of the image are mostly limited in the image high frequency parts. While the low frequency parts are split again into two parts of high frequency and low frequency. Then this process is continued until the signal is fully decomposed. For watermarking and compression application no more than five decomposition steps (five levels of DWT

decompositions) are decomposed. Moreover, from the coefficients of DWT, the reconstruction of the original image is possible. The process of reconstruction is referred to as the inverse DWT (IDWT). Mathematically, the DWT and IDWT are stated in equation (3.5) and (3.6). Let:

$$H(\omega) = \sum_{k} h_k \,.\, e^{-jk\omega} \tag{3.5}$$

And

$$G(\omega) = \sum_{k} g_k \,.\, e^{-jk\omega} \tag{3.6}$$

$H(\omega)\ and\ G(\omega)$ be a low-pass and a high-pass filters respectively, which will satisfy the certain conditions for the stated reconstruction later. F(n)is a discrete signal and it can be decomposed repeatedly as in equations (3.7) and (3.8) [57].

$$f_{j-1}^{low}(k) = \sum_{n} h_{n-2k} f_j(n) \tag{3.7}$$

And

$$f_{j-1}^{high}(k) = \sum_{n} g_{n-2k} f_j(n) \tag{3.8}$$

For $j = J+1, J, ..., J_0$ where $f_{J+1}(k) = F(f), k \in Z.J+1$ is the index of highest resolution level and J_0 is the low resolution level index. The coefficients $f_{J_0}^{low}(k), f_{J_0}^{high}(k), f_{J_{0+1}}^{high}(k), ..., f_{J}^{high}(k)$ are the signal F(n) DWT, where $f_{J_0}^{low}(k)$ is the part that represents the lowest resolution of F(n) (the approximation) and $f_j^{high}(k)$ represents the details of F(n) at various bands of frequencies. Moreover, the F(n) signal can be

reconstructed from the DWT coefficients of this signal recursively as in equation (3.9) [57].

$$f_j^{low}(n) = \sum_k h'_{n-2k} . f_{j-1}^{low}(k) + \sum_k g'_{n-2k} . f_{j-1}^{high}(k) \tag{3.9}$$

To satisfy the above relationship of IDWT and DWT, the following condition of orthogonality on the filters $G(w)$ and $H(w)$ is required:

$$|H(\omega)|^2 + |G(\omega)|^2 = 1 \tag{3.10}$$

An case of such $G(w)$ and $H(w)$ is given by the equations (3.11) and (3.12) [57]:

$$H(\omega) = \frac{1}{2} + \frac{1}{2} e^{-jw} \tag{3.11}$$

And

$$G(\omega) = \frac{1}{2} - \frac{1}{2} e^{-jw} \tag{3.12}$$

Which is well known as the Haar wavelet. There more filters which are commonly used in the field of image processing are like the Daubechies orthogonal family (D-4, D-6, D-8, D-10, D-12) also the bi-orthogonal ones (B-5/3, B-7/9). The DWT and IDWT for a two dimensional image F(m,n) can be defined by the same way through the implementing one dimensional DWT and IDWT for m and n separately and as shown in figure (3.1) resulting in the image pyramidal representation which is shown in figure (3.2).

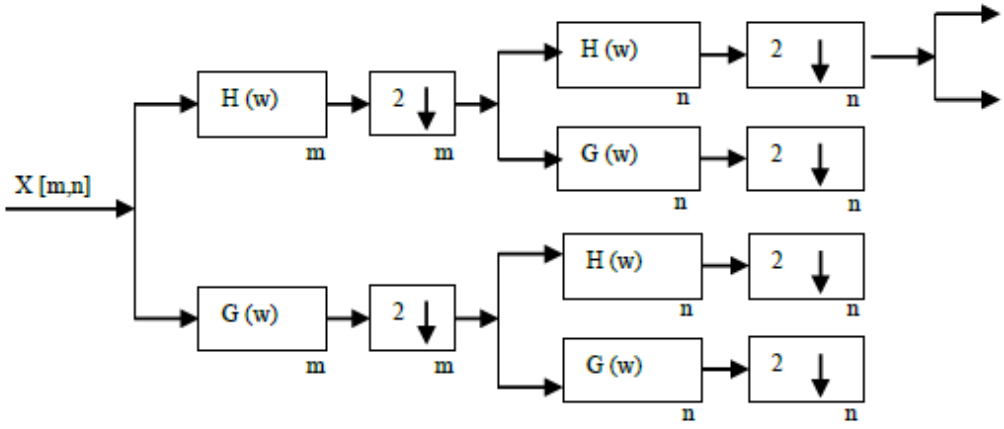
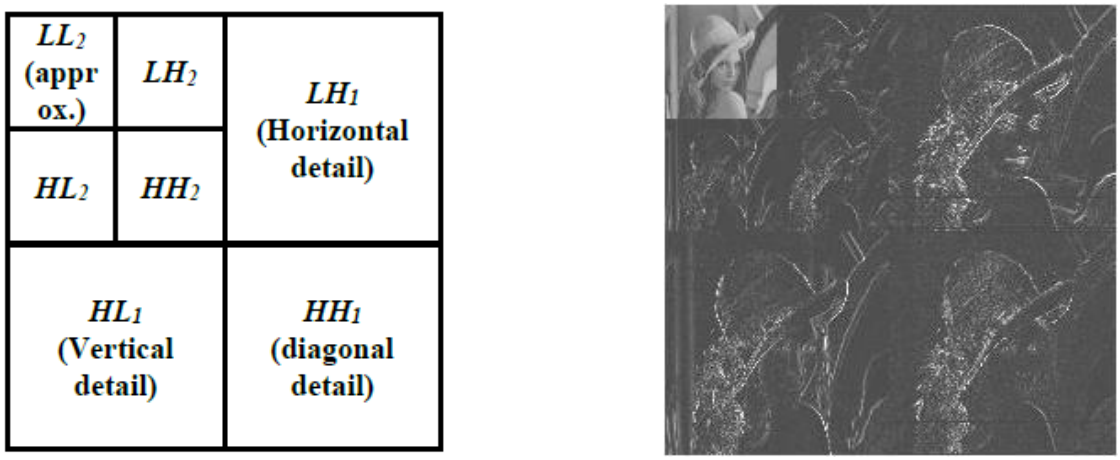


Figure 3.1: DWT for Two Dimensional Images



(a) Decomposition Structure (b) Decomposed Image

Figure 3.2: The Pyramidal Two-Level Decomposition of an Image.

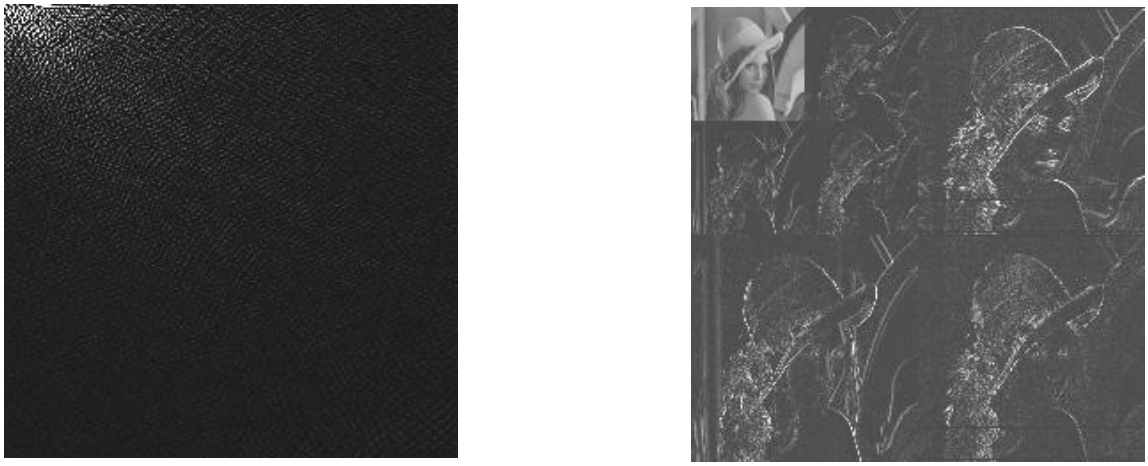
The wavelet transform has many advantages over the DCT and those are:

- In the DCT domain, the energy is concentrated in the low frequency regions around the upper-left corner. The multi-resolution DWT representation contains the low frequency component of the image signal in the approximation sub-band, also

located in the upper-left corner, while the high frequency components are represented in the detailed sub-bands at several resolutions (see figure 3.3). Most energy of the detailed sub-bands is situated in edge areas and textured regions.

- The DWT is a multi-resolution of an image, a sequential decoding can be processed from lower to higher resolution.

- The DWT is a better human visual system (HVS) than DCT. Where the artifacts that are introduced by DWT at high compression ratio are less disturbing than the artifacts showing by the DCT at the same bit rate, i.e. (JPEG block-shaped artifacts) and the reason for that is the DCT image coding is based on independent (8X8) blocks processing.



(a) DCT (b) DWT

Figure 3.3: Energy Distribution in the Transform Domain.

3.1.1.4 Choosing a transform

Applications and attacks on watermarks sometimes affect the choosing of a certain transform. Generally, watermarking in spatial domain is fast and hence it is suitable for real time applications like video watermarking applications. Watermarking in frequency

domain needs more time for processing but it is resilient to some attacks. The magnitude of DFT coefficients is less affected by spatial shifts than the value of the pixels. Hence, watermarking embedding in DFT for example makes the watermark more robust against translation than watermark embedded in spatial domain. Again, watermarking schemes based on DCT are more robust against JPEG compression. The most important advantage of watermarking in frequency domain is that it offers the ability to process the image components in different frequency bands independently.

3.1.2 Availability of reference data

The watermarking system which allows extracting the embedded data without using a reference data (e.g. un-watermarked cover image), is called blind or oblivious watermarking scheme. Else, it is called non blind or non-oblivious.

Sometimes, there are also detection or extraction methods that use some of the data or features originated from the original un-watermarked cover image or by the use of a public secret key. These watermarking schemes are called semi-blind or semi-oblivious.

3.1.3 Embedded data locations

An important requirement for any watermarking scheme is to produce invisible and robust watermarks. The Human eyes are less sensitive to noise occurring in regions with textures than in smooth regions of an image, others argue to embed watermarks in the most perceptually significant part of an image, because an attacker cannot remove watermark from these areas easily without distorting the image significantly [47]. Embedding a watermark in the mid frequency of DCT coefficients was also proposed, because these locations tend to survive JPEG compression [49]. In wavelet domain, authors have proposed various techniques that select significant wavelet coefficients for watermarking.

Some authors use a key, (usually a random number seed), to select the marked coefficients in addition to choosing locations based on their visual significance. W Bender et al. Selects n pairs of pixels using a key [28]. The luminance of half of the selected pixels is incremented by 1 while the second half is decremented by 1. In the decoding process, the

same key is used to select the same pairs of pixels and compare the difference between the mean of the two halves. The algorithm, however cannot extract the payload, instead it allows to verify the existence of the mark.

3.1.4 Host data modified method

The host data, image in our work, can be modified either by using linear addition of the watermark or by non-linear quantization strategy. Additive watermark embedding techniques are known by the cover image linear modification of the. The quantization embedding schemes perform non-linear modifications.

3.1.4.1 Additive algorithms

In additive algorithms, sometimes called multiplicative algorithms, the watermark is a sequence of numbers or bits with length of N to be embedded in a properly chosen locations in the cover image coefficients, f. The most widely used formula is (3.13):

$$f'(m,n) = f(m,n)(1 + \alpha w(i,j)) \tag{3.13}$$

Where α is the weighting factor, where f' is the coefficients of the modified data that carry the information of the watermark, w is the embedded watermark. Another encoding as in the equation (3.14) [47]:

$$f'(m,n) = f(m,n) + \alpha w(i,j) \tag{3.14}$$

Then the watermark w can be extracted as the equation (3.15) shows:

$$w(i,j) = \frac{f'(m,n) - f(m,n)}{\alpha} \tag{3.15}$$

3.1.4.2 Quantization algorithms

Quantization is the process of mapping a large set of values to a smaller set. Hence, this process is very important for many lossy compression schemes. There are two types of

quantization, namely scalar and vector quantization. In the former, the quantizer takes and outputs scalar values, while in the latter, the quantizer operates on vectors [58].

The quantizer is consisting from two stages; the encoder and the decoder. The encoder which is responsible for dividing the range of source values into a number of intervals. A code word is representing each interval. The encoder represents all the source values that are falling into a particular interval by the code word assigned to that interval. The decoder generates a reconstruction value for every code word generated by the encoder.

Some publications on quantization based watermarking techniques [49]. This algorithm embeds a binary watermark into a pseudo randomly selected DCT coefficients blocks and within each block, two coefficients from the mid frequency range are again selected pseudo randomly. D. Kundur and D. Hatzinakos Propose a technique to embed a binary sequence value in pseudo randomly selected locations in the detailed sub-bands [9]. N. Abdulaziz and K. Pang Propose also a technique that codes the data to be embedded by vector quantization and the indices obtained in the process are to be embedded in the DWT coefficients of the cover image [59].

3.1.5 Encoding the payload

The watermark can either be embedded directly into the cover data or it may be passed through some processes before the embedding.

3.1.5.1 Arnold cat's map (Arnold's transform)

That is based on the stretching and folding of the trajectories in the phase space, this simple system's phase space can be illustrated by a square and the stretch and fold process is more obvious if a cat picture is placed within this square. Then one can see the system's time evolution via observing how the cat image is getting stretched, cut up and put back into the square.

Typically observed, any two points that are firstly pretty close to each other, quickly become away and separated from each other after many repeated iterations of the map. Arnold's transform is invertible because the matrix has determinant of 1 and therefore its

inverse has integer entries" [60]. The Figures (3.4) and (3.5) below show this transform's steps.

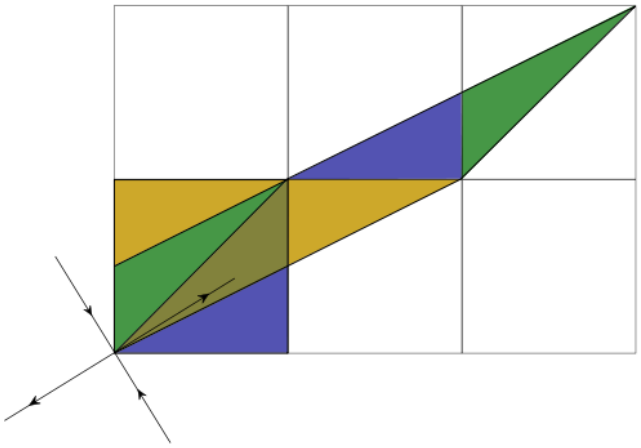


Figure 3.4: Arnold's Transform Steps

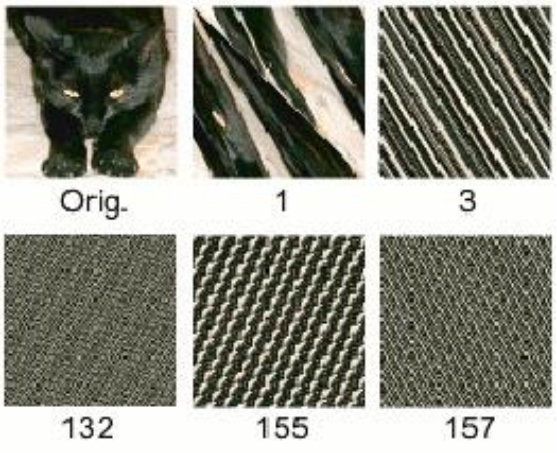


Figure 3.5: Arnold Scrambling With Different Number of Iterations

This transform was used to scramble the watermarks to give a secondary security to the system. Because even if the attacker was able to extract the watermark from the watermarked image, the attacker still needs to know the scrambling algorithm to be able to read or understand the watermark. After scrambling the image with this transform the

spatial relationship between the watermark image pixels has been destroyed and they're completely and evenly distributed inside the image space, which improves the robustness of the system. The use of this scrambling transform in this work was to increase both security and robustness of the system [61].

Arnold transform can be defined as in equation (3.16):

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod\ N \tag{3.16}$$

Where:

(x, y): The coordinates of the pixels.

(x', y'): are the coordinates of the pixels after iterative scrambling computation.

N : is the square image dimensions.

3.2 Attacks on Watermarks

Attacks on watermarks can be of different types depending on the cause of an attack that is applied on a watermarked image and such purposes are [25, 62]:

- Malicious attacks or sometimes called hostile, those are attempting to remove, alter or weaken the watermark.
- Coincidental attacks, those may occur due to common image processing and they are not aimed to tamper the watermark.
- The attack is considered successful if the watermark becomes undetectable any more but the image is still intelligibly used for any purpose.

The following sections introduce three classes of attacks, namely simple attacks, geometric attacks, and collusion attacks.

3.2.1 Simple attacks

The aim of such attacks is to add distortion to the watermarked image in order to leave the watermark undetectable or unreadable. These attacks are [63]:

- Lossy image compression.
- Addition of Gaussian noise or any other noise.
- Low pass, high pass, median, and mean filtering.
- Rescaling or resampling.

3.2.2 Geometric attacks

Geometric attacks alter the geometry of the image when the image is subjected to translation, scaling, and/or cropping. Jitter attack is a special geometric attack that prevents watermark locations from being found (e.g., by removal and insertion of pixel rows or columns). In fact, jittering is generally not very efficient in images because the resulting artifacts become visible. It is rather more efficient in audio watermarking because audio samples are much less significant with respect to the entire piece of audio compared to a line with respect to an image.

3.2.3 Collusion attacks

It is another important class of attacks, which aims to reduce the power of the watermark by averaging many different watermarked copies of the same image.

CHAPTER FOUR

THE WAVELET-BASED ALGORITHMS

In this chapter, four non-blind wavelet-based watermarking efficiency test algorithms are proposed. Each algorithm uses different level decomposition of DWT where the First algorithm uses a first level decomposition of DWT, the Second algorithm uses the second level decomposition and so on (up to four levels). Except for the fifth algorithm which uses more than one level of decomposition as an embedding domain. The purpose behind using different levels of DWT decomposition in each algorithm starting for the first level decomposition and up to the fourth level is to study and examine how different attacks affect different frequency bands at different levels of DWT decomposition.

For the purpose of testing and examining the efficiency and capacity of this transform, four binary visual watermarks are embedded in all four sub-bands (Approximation, Horizontal detail, Vertical detail and Diagonal) given by the DWT at each level of decomposition. This procedure gave the algorithms extraction alternatives in different frequency ranges. Main reason for this is that, some attacks destroy watermarks embedded in high frequencies, others hit the ones in middle frequencies, etc.

The embedding, attacking (by 15 different attacks) and extraction is done over the whole four Efficiency Test Algorithms to compare the results and choose the best frequency sub-bands to embed the watermarks. Finally a fifth optimum algorithm is determined after both examining of the four previous algorithms results. Having full visualization on the frequency sub-bands selection and their robustness against different types of attacks where some frequency bands at a certain level of decomposition are more robust than others under certain attacks. The algorithm has high invisibility and robustness as the experimental results demonstrate in the next chapter.

The Wavelet family used is Daubechies, specifically db4. The Figure (4.1) below shows Daubechies wavelets family.

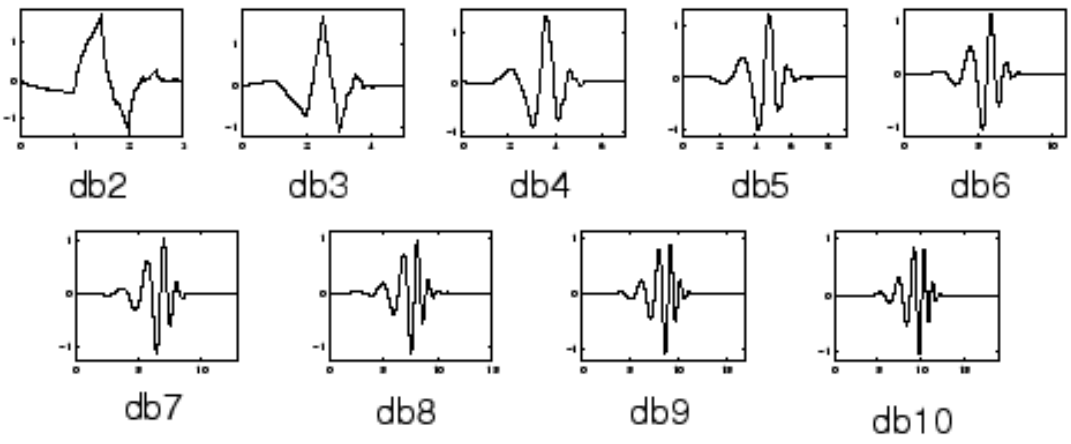


Figure 4.1: Daubechies Wavelets Family

4.1 The Wavelet-Based Algorithms

The efficiency test algorithms are implemented by using the characteristics of an image and the HVS for robustness and imperceptibility issues. The binary visual watermarks are scrambled by Arnold's Transform before embedding them in the wavelet decomposition frequency sub-bands. The watermarks are embedded into the four sub-bands by modifying their coefficients, by using different strength factors depending on the level of DWT decomposition and the frequency sub-band. Five main algorithms were implemented in this work where each of them uses a cover image with the size of (1024X1024), and they are as follows:

- First Efficiency Test Algorithm: Embeds four Binary pattern watermarks with the size of (512X512) each scrambled by Arnold's transform with 6 iterations in the four frequency sub-bands (LL1, HL1, LH1, HH1) given by first level decomposition of the DWT of the cover image whose size is (1024X1024).

- Second Efficiency Test Algorithm: Embeds four Binary pattern watermarks with the size of (256X256) each scrambled by Arnold's transform with 6 iterations in the

four frequency sub-bands (LL2, HL2, LH2, HH2) given by the second level decomposition of DWT of the cover image whose size is (1024X1024).

- Third Efficiency Test Algorithm: Embeds four Binary pattern watermarks with the size of (128X128) each scrambled by Arnold's transform with 5 iterations in the four frequency sub-bands (LL3, HL3, LH3, HH3) given by the third level decomposition of DWT of the cover image whose size is (1024X1024).

- Fourth Efficiency Test Algorithm: Embeds four Binary pattern watermarks with the size of (64X64) each scrambled by Arnold's transform with 4 iterations in the four frequency sub-bands (LL4, HL4, LH4, HH4) given by the fourth level decomposition of DWT of the cover image whose size is (1024X1024).

- Fifth (Optimum) Algorithm: The first 3 binary pattern watermarks with the size of (64X64) were scrambled by Arnold's transform with 4 iterations and embedded in the three sub-bands (HL1, LH1, HH1) given by the first level decomposition of DWT of the cover image whose size is (1024X1024), on the other hand a fourth binary watermark with the size (64X64) again was scrambled by Arnold's transform with 4 iterations and embedded in the approximation sub-band (LL4) given by the fourth level decomposition of DWT of the same cover image. See Figure (4.2)

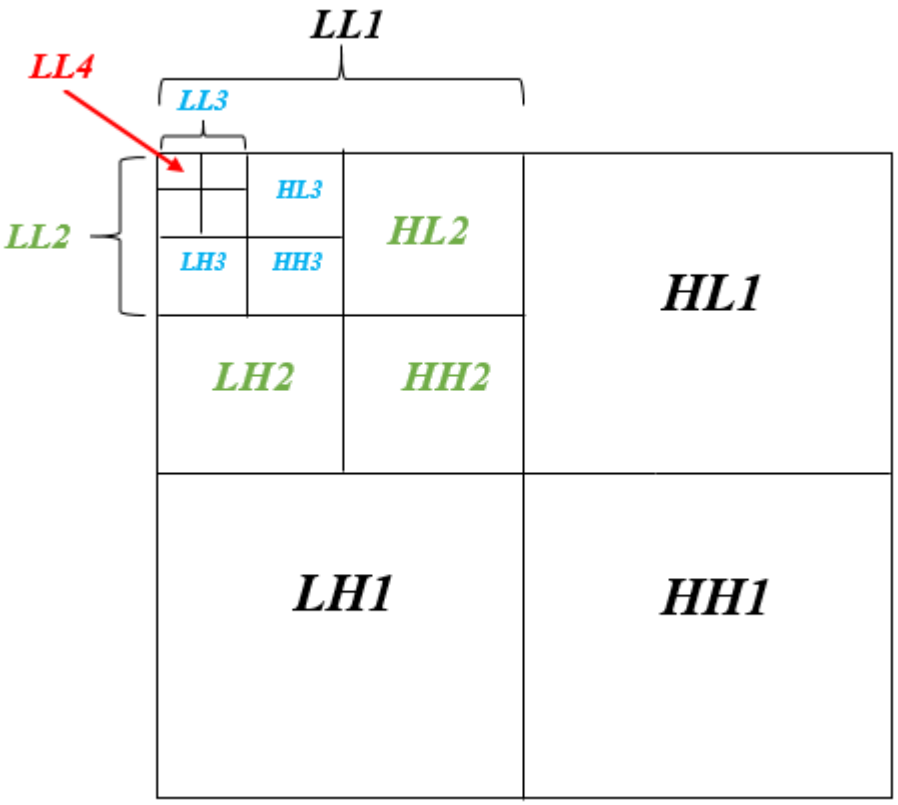
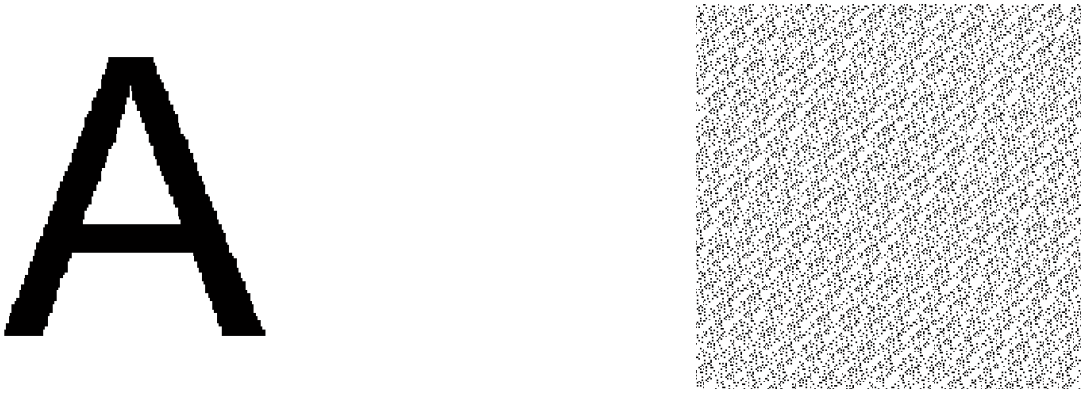


Figure 4.2: Levels of DWT Decomposition Used

All the above algorithms are applied on Gray scale images and colored images (RGB and Ycbcr spaces), in the RGB space both Blue and Green channels were used, on the other hand only the Y (luminance) channel is used from the Ycbcr space. Except for the fifth algorithm which is applied using the RGB blue channel only due to its low sensitivity to human perception [64].

4.1.1 Watermark scrambling

The binary pattern watermark is scrambled by Arnold's Cat map to increase the system's security and robustness, different number of iterations are used depending on the size of the watermark as mentioned in the above section. This new representation of the watermark increased the system security because if the attacker extracted the watermark he still needs to know the algorithm by which the watermark is scrambled. Figure (4.3) shows the both original and the scrambled watermark used in this work.



(a) (b)

Figure 4.3: (a) Original Watermark, (b) Scrambled Watermark

4.1.2 Watermark embedding process

The following embedding procedures are used with all the Algorithms with respect to the Level of Decomposition:

1. Getting the DWT (first, second, third or fourth) level decomposition of the cover image I (selected channel (Blue, Green or Y luminance in case of colored images).

2. Adding the four watermarks to the four sub-bands at a certain level by modifying their coefficients and the embedding equation can be defined as follows:

$$f'(i,j) = f(i,j) + w(i,j) * \alpha \quad (5.1)$$

3. Apply the inverse of DWT transform to get the Watermarked image I'

The figure (4.4) shows the embedding scheme used in this work for the Gray Scale images.

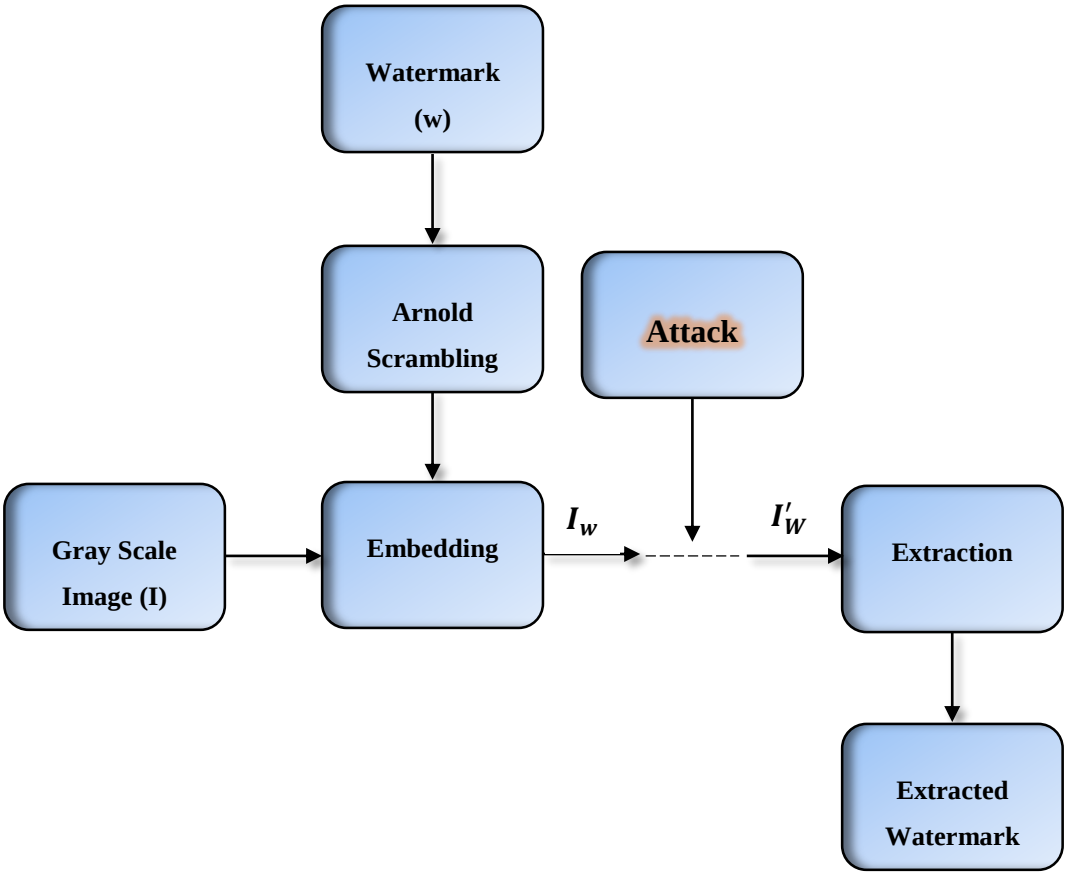


Figure 4.4: Gray Scale Image Watermarking System

The figure (4.5) shows the embedding scheme used in this work for the colored RGB images.

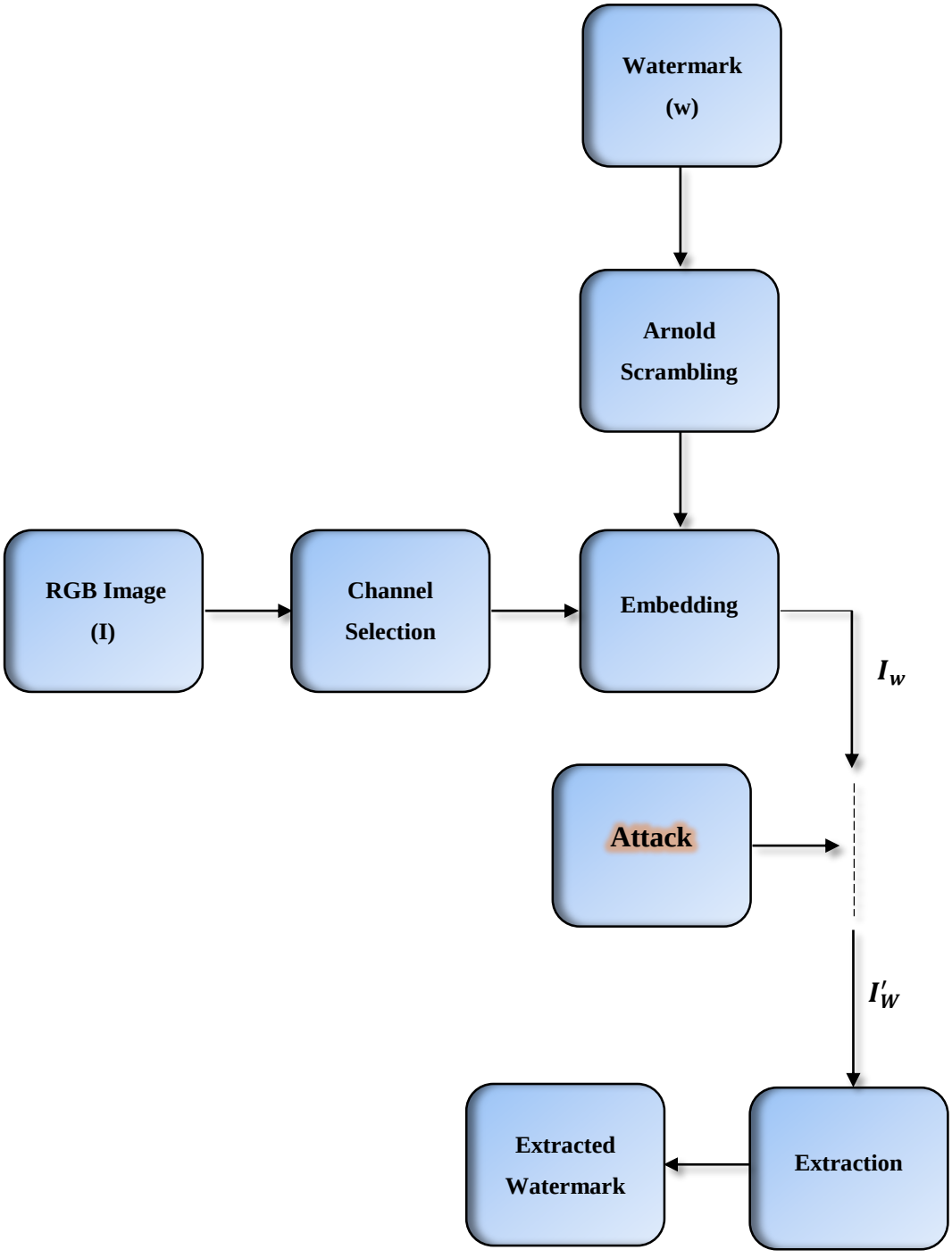


Figure 4.5: RGB Image Watermarking System

The figure (4.6) shows the embedding scheme used in this work for the colored Ycbcr images

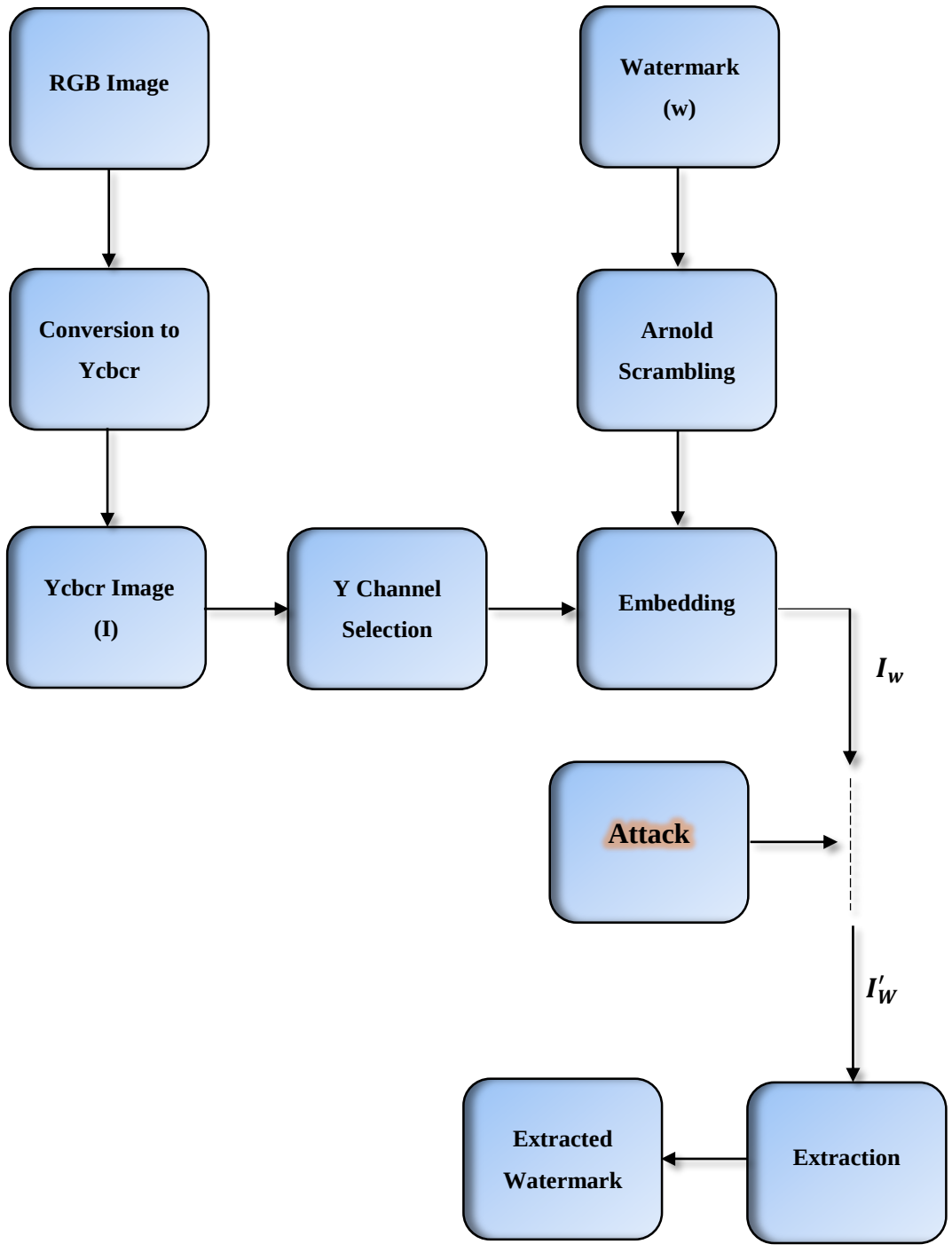


Figure 4.6: Ycbcr Watermarking System

4.1.3 Attacks used in this work

In this work fifteen attacks were used to test the efficiency of the algorithms implemented, the attacks are as follows:

1. JPEG compression attack with quality factor = 100%.
2. JPEG compression attack with quality factor = 75%.
3. JPEG compression attack with quality factor = 50%.
4. JPEG compression attack with quality factor = 25%.
5. Gaussian Noise attack with mean=0, and Variance=0.001.
6. Mean Filter with Window size (3X3).
7. Resizing at 50%.
8. Rotation with -20.
9. Histogram Equalization.
10. Gamma Correction.
11. Intensity Adjustment.
12. Cropping attack.
13. Salt & Pepper Nosie with Density=0.01.
14. JPEG 2000, with compression ratio up to 150:1
15. Motion Blur attack.

4.1.4 Watermark extraction process

The following extracting procedures are used with all the algorithms with respect to the level of decomposition:

1. Getting the DWT (first, second, third or fourth) level decomposition of the watermarked image I' (selected channel (Blue, Green or Y luminance in case of colored images) which could possibly be attacked.

2. Extract the watermark from all sub-bands LL, LH, HL, and HH as in equation (5.2):

$$w'(i,j) = (f'(i,j) - f(i,j))/\alpha \tag{5.2}$$

3. The extraction threshold determination was based on [14] and as in equation (5.3):

$$w'(i,j) > 0.5 \; then \; w'(i,j) = 1 \; else \; w'(i,j) = 0 \tag{5.3}$$

CHAPTER FIVE

SIMULATION RESULTS

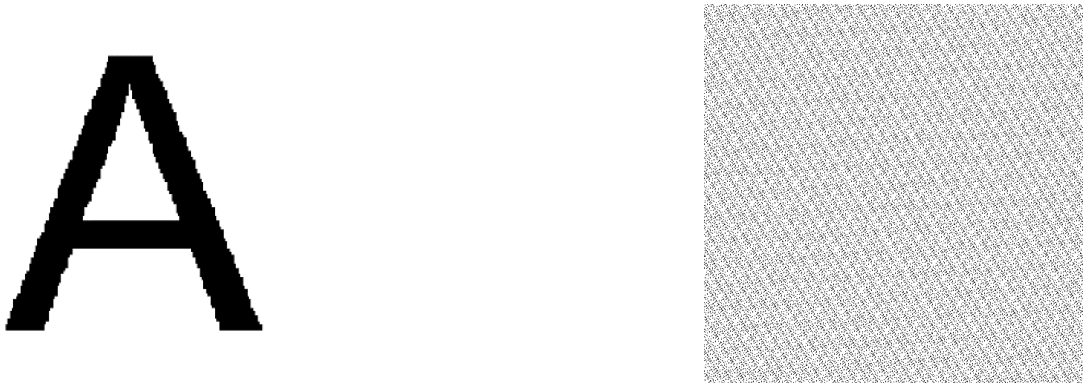
Several gray scale and colored images with the size of (1024X1024) were used as cover images in this work. Lena image is chosen as the standard cover image to demonstrate the results through this chapter. Binary visual watermarks with the size of (512X512), (256X256), (128X128) and (64X64) are used in the 1st, 2nd, 3rd and 4th efficiency test algorithms respectively as mentioned in the previous chapter. The Optimum algorithm uses a (64X64) size of watermark.

5.1 Gray Scale Images Efficiency Test Algorithms Results

In this section, gray scale images results for all four efficiency test algorithms are presented.

- First Efficiency Test Algorithm Embedding Results:

The Figure (5.1) shows of both the original and scrambled watermarks.



(a) (b)

Figure 5.1: (a) Original Watermark, (b) Scrambled Watermark

The Figures (5.2), (5.3) and (5.4) show the original cover (un-watermarked), the used level of DWT decomposition (1st level) and the watermarked image respectively.

Figure 5.2: Cover Image

Figure 5.3: First Level Decomposition

Figure 5.4: Gray Scale First Algorithm Watermarked Image, PSNR=43.3780 dB

- **Attacks Results:**

The fifteen attacks mentioned in the previous chapter (section 4.1.3) are applied on each one of the four gray scale images Efficiency Test algorithms, they will be presented only once for gray scale images in this chapter, and that is for the first Efficiency Test algorithm for gray images. Because they are causing the same perceptual effect and artifacts in all of the four algorithms, next the Figures (5.5), (5.6), (5.7), (5.8), (5.9), (5.10), (5.11), (5.12), (5.13), (5.14), (5.15), (5.16), (5.17), (5.18), (5.19) show the attacks JPEG,Q=100%, JPEG,Q=75%, JPEG,Q=50%, JPEG,Q=25%, JPEG 2k, Gaussian Noise, Salt & Pepper Noise, Mean Filter, Resizing, Rotation, Histogram Equalization, Intensity adjustment, Gamma Correction, Cropping and Motion Blur respectively.

Figure 5.5: JPEG, Q=100%, PSNR=43.1404 dB

Figure 5.6: JPEG, Q=75%, PSNR=42.0614 dB

Figure 5.7: JPEG, Q=50%, PSNR=40.6153 dB

Figure 5.8: JPEG, Q=25%, PSNR=38.4487 dB

Figure 5.9: JPEG 2000, PSNR= 36.8535 dB

Figure 5.10: Gaussian Noise, Mean=0, Variance=0.001, PSNR= 29.8000 dB

Figure 5.11: Salt & Pepper Noise, Density=0.01, PSNR=25.5313 dB

Figure 5.12: Mean Filter, Window (3X3), PSNR= 37.5261 dB

Figure 5.13: Resizing 50%, PSNR=39.2585 dB

Figure 5.14: Rotation -20^0, PSNR=11.6438 dB

Figure 5.15: Histogram Equalization, PSNR=17.1786 dB

Figure 5.16: Intensity Adjustment, PSNR=17.1035 dB

Figure 5.17: Gamma Correction, PSNR=17.7670 dB

Figure 5.18: Cropping, PSNR=14.4924 dB

Figure 5.19: Motion Blurred, PSNR=34.1108 dB

- Second Efficiency Test Algorithm Embedding Results:

The next Figures (5.20) and (5.21) show the level of DWT decomposition used (2^{nd} Level) and the Watermarked image.

Figure 5.20: Gray Scale Image second Level Decomposition

Figure 5.21: Gray Scale Second Algorithm Watermarked Image, PSNR= 44.1927 dB

- Third Efficiency Test Algorithm Embedding Results:

The next Figures (5.22) and (5.23) show the level of DWT decomposition used (3rd Level) and the Watermarked image.

Figure 5.22: Gray Scale Image Third Level Decomposition

Figure 5.23: Gray Scale Third Algorithm Watermarked Image, PSNR= 47.5072 dB

- Fourth Efficiency Test Algorithm Embedding Results:

The next Figures (5.24) and (5.25) show the level of DWT decomposition used (4^{th} Level) and the Watermarked image.

Figure 5.24: Gray Scale Image fourth Level Decomposition

Figure 5.25: Gray Scale fourth Algorithm Watermarked Image, PSNR= 48.7859 dB

Below the Table (5.1) shows the PSNR values for all efficiency test algorithms.

Table 5.1: PSNR in dB of all Efficiency Test Algorithms with Attacks

No.	Case	1st Alg.	2nd Alg.	3rd Alg.	4th Alg.
1	No Attack	43.3780	44.1927	47.5072	48.7859
2	JPEG, Q=100	43.1404	44.0052	47.1973	48.3832
3	JPEG, Q=75	42.0614	41.8389	43.1144	43.5377
4	JPEG, Q=50	40.6153	40.2374	41.0156	41.2530
5	JPEG, Q=25	38.4487	38.0646	38.4172	38.5228
6	Gaussian Noise	29.8000	29.8389	29.9104	29.9371
7	Mean Filter	37.5261	37.3549	37.5428	37.5821
8	Resizing 50%	39.2585	39.0630	39.3150	39.3864
9	Rotation 20^0	11.6438	11.6434	11.6439	11.6447
10	Histogram Equalization	17.1786	17.1918	17.2168	17.2209
11	Intensity Adjustment	17.1035	17.1162	17.1700	17.1839
12	Gamma Correction	17.7670	17.7581	17.7139	17.7027
13	Cropping	14.4924	14.4932	14.4954	14.4959
14	Salt & Pepper Noise,	25.5313	25.4786	25.5872	25.5809
15	Motion Blur	34.1108	34.0884	34.1209	34.1202
16	JPEG 2000	36.8535	36.7896	36.8641	36.8665

The Figure (5.26) next, presents how the PSNR value varies through the fourth efficiency test algorithms with both cases without and with attacks.

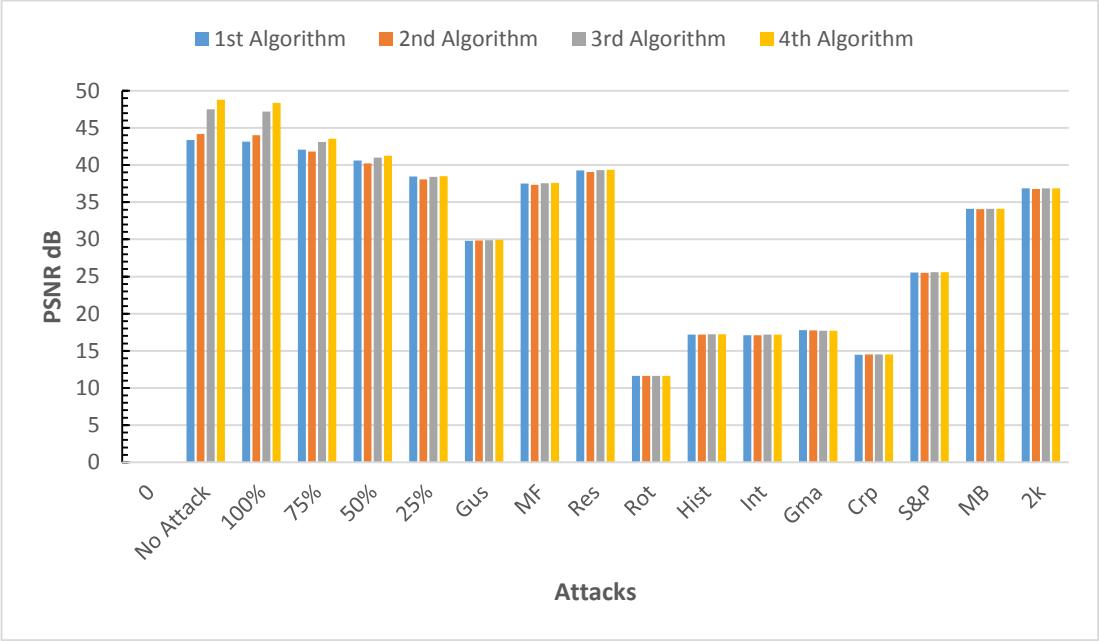


Figure 5.26: PSNR in dB of all Efficiency Test Algorithms with Attacks

The results in the Figure (5.26) above indicate that in the case of no attack, the PSNR value increase with the deeper level of DWT decomposition used with respect to the scaling factor, i.e. the PSNR at the first efficiency test algorithm which uses the 1st level of decomposition is (43.3780 dB), while the fourth test algorithm gave a higher PSNR value of (48.7859 dB). The rest of PSNR values at different attack cases vary just a little through different efficiency test algorithms.

Next the Table (5.2) presents the correlation coefficients values of watermarks extractions in all efficiency test algorithms with both cases without and with attacks.

Table 5.2: Extracted Watermarks Correlations of all Efficiency Test Algorithms

No.	Case	LL	HL	LH	HH	Level
1	No Attack	1	1	1	1	***1st***
		1	1	1	1	***2nd***
		1	1	1	1	***3rd***
		1	1	1	1	***4th***
2	JPEG, Q=100%	1	0.9885	0.9836	0.9851	***1st***
		1	0.9999	1	0.9999	***2nd***
		1	1	1	1	***3rd***
		1	1	1	1	***4th***
3	JPEG, Q=75%	0.7300	0.0627	0.0480	0.0092	***1st***
		0.9997	0.3090	0.2933	0.1698	***2nd***
		1	0.5705	0.5548	0.4823	***3rd***
		1	0.5075	0.5216	0.5481	***4th***
4	JPEG, Q=50%	0.3552	0.0282	0.0251	0.0027	***1st***
		0.9000	0.1271	0.1399	0.0452	***2nd***
		1	0.2508	0.2833	0.2062	***3rd***
		1	0.2305	0.2737	0.2353	***4th***
5	JPEG, Q=25%	0.1146	0.0047	0.0075	0.0019	***1st***
		0.4590	0.0427	0.0463	0.0156	***2nd***
		0.5061	0.0940	0.1254	0.0533	***3rd***
		0.8406	0.1287	0.1391	0.1352	***4th***
6	Gaussian Noise	0.2883	0.0703	0.0693	0.0736	***1st***
		0.5387	0.1013	0.1047	0.1105	***2nd***
		0.6824	0.1489	0.1643	0.1401	***3rd***
		0.9183	0.1569	0.1411	0.1324	***4th***
7	Mean Filter	0.4196	2.2364e-004	0.0245-	4.6842e-004	***1st***
		0.8557	0.2021	0.1716	0.1132	***2nd***
		0.9392	0.5319	0.4586	0.3967	***3rd***
		0.9731	0.5612	0.4730	0.4379	***4th***
8	Crop	0.9236	0.8771	0.8457	0.9221	***1st***
		0.9218	0.8274	0.8094	0.8502	***2nd***
		0.9199	0.8179	0.7915	0.8303	***3rd***
		0.9148	0.8003	0.7768	0.8142	***4th***
9	Histogram Equalization	0.0458	0.4861	0.4436	0.5956	***1st***
		0.0472	0.3523	0.2975	0.4127	***2nd***

Table 5.2 continued.

		0.0371	0.2998	0.2360	0.3414	***3rd***
		0.0202	0.1752	0.1163	0.2118	***4th***
10	Resizing 50%	0.2705	0.0087	0.0038	0.0017-	***1st***
		0.6777	0.1203	0.1019	0.0667	***2nd***
		0.8254	0.3410	0.2864	0.2222	***3rd***
		0.9481	0.4045	0.3489	0.3205	***4th***
11	Rotation -20^0	0.8080	0.3596	0.3688	0.2740	***1st***
		0.8956	0.4869	0.4230	0.3883	***2nd***
		0.9091	0.6548	0.6017	0.6082	***3rd***
		0.9065	0.6182	0.5786	0.5648	***4th***
12	Gamma Correction	NaN	0.8879	0.8181	0.9888	***1st***
		NaN	0.7247	0.6211	0.8480	***2nd***
		NaN	0.5810	0.4599	0.6952	***3rd***
		NaN	0.3748	0.2458	0.4662	***4th***
13	Intensity Adjustment	NaN	0.7906	0.7039	0.9519	***1st***
		NaN	0.6022	0.5001	0.7418	***2nd***
		NaN	0.4769	0.3686	0.5880	***3rd***
		NaN	0.2986	0.1963	0.3908	***4th***
14	JPEG 2000	0.0315	0.0084	0.0113	0.0080	***1st***
		0.1076	0.0318	0.0341	0.0157	***2nd***
		0.3030	0.0075	0.0109	0.0017-	***3rd***
		0.4854	0.1296	0.0970	0.0569	***4th***
15	Motion Blur	0.0785	0.0393	0.0414	0.0557-	***1st***
		0.1896	0.0560	0.0469	0.1096-	***2nd***
		0.5790	0.1022	0.0792	0.0483-	***3rd***
		0.7670	0.2071	0.1370	0.0819	***4th***
16	Salt & Pepper	0.9291	0.9310	0.9293	0.9300	***1st***
		0.7617	0.7663	0.7653	0.7689	***2nd***
		0.5051	0.4410	0.4377	0.4318	***3rd***
		0.7074	0.1001	0.1266	0.1519	***4th***

The above table can be used for objective assessment purposes. Next the Figures (5.27), (5.28), (5.29) and (5.30) show the watermarks extracted images in all efficiency test algorithms with both cases without and with attacks. For all the extraction results below, the chosen extracted watermark with highest correlation value is referred to by a surrounding red squared frame for identification purpose only.

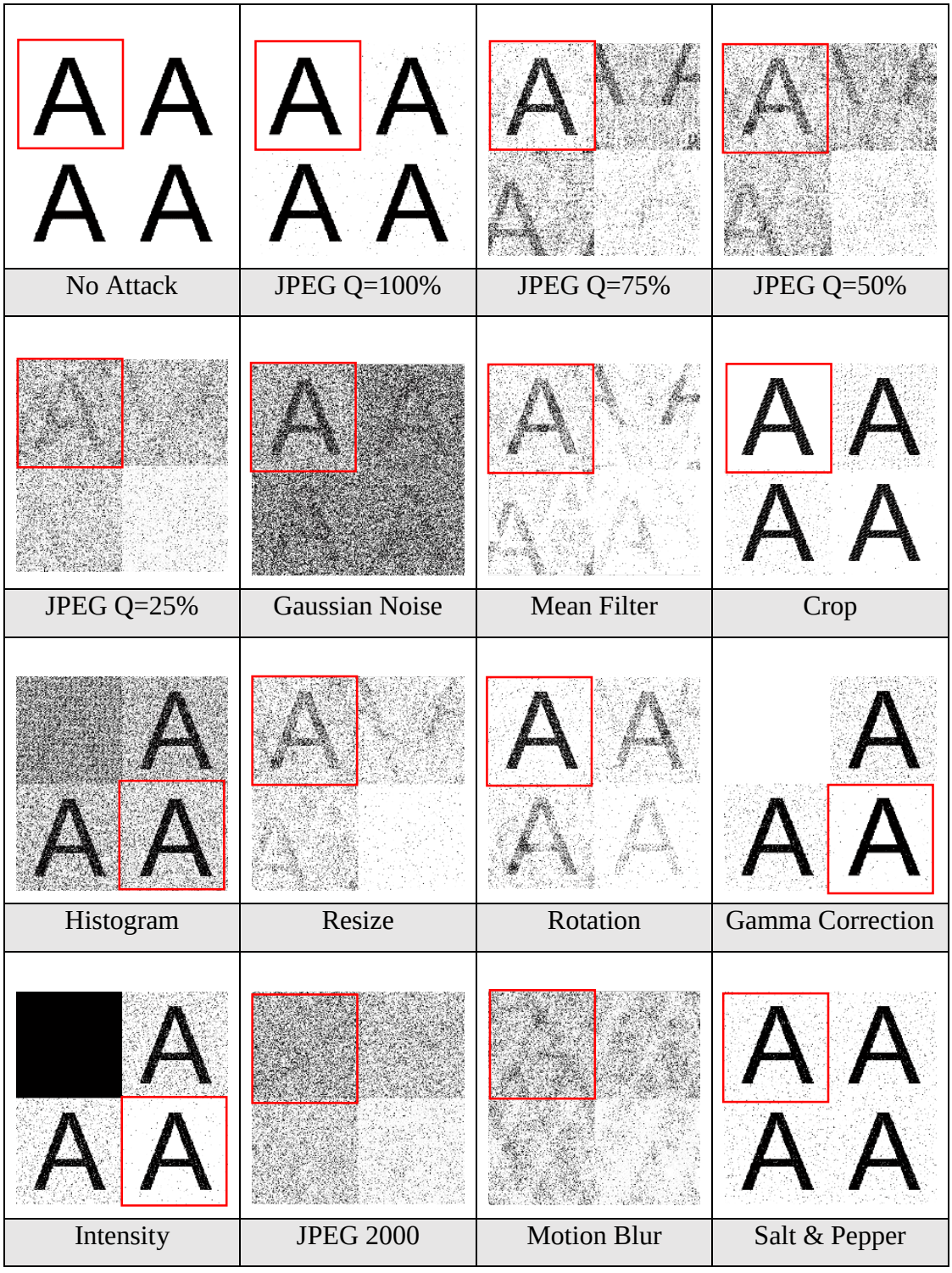


Figure 5.27: First Efficiency Test Algorithm Extractions

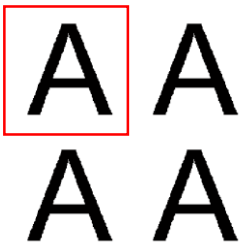
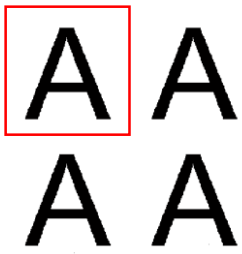
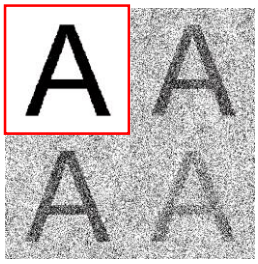
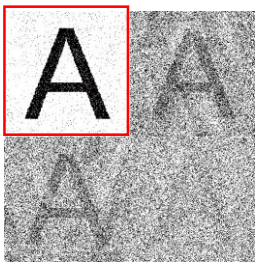
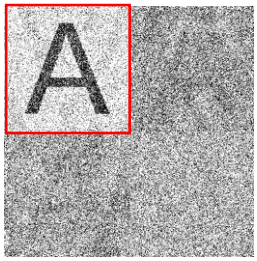
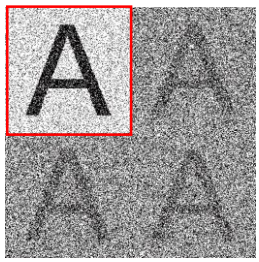
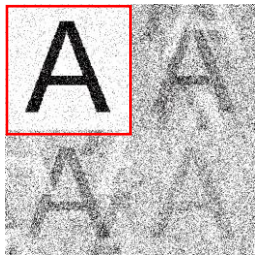
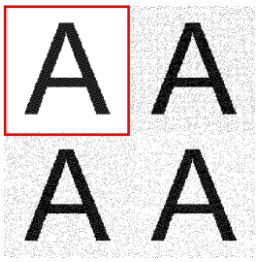
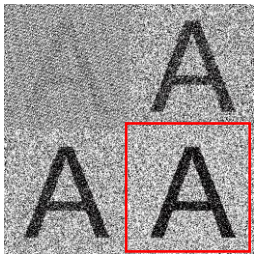
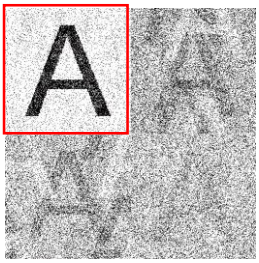
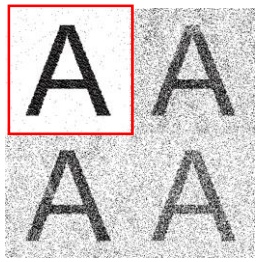
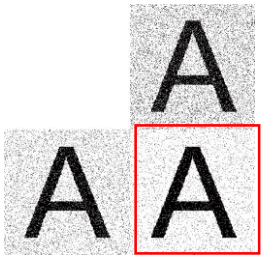
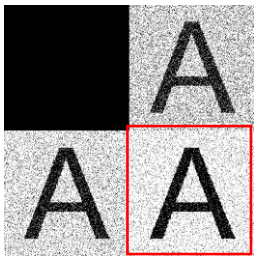
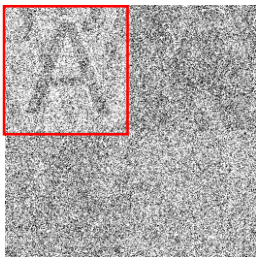
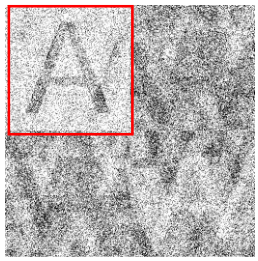
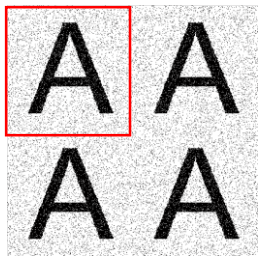
			
No Attack	JPEG Q=100%	JPEG Q=75%	JPEG Q=50%
			
JPEG Q=25%	Gaussian Noise	Mean Filter	Crop
			
Histogram	Resize	Rotation	Gamma Correction
			
Intensity	JPEG 2000	Motion Blur	Salt & Pepper

Figure 5.28: Second Efficiency Test Algorithm Extractions

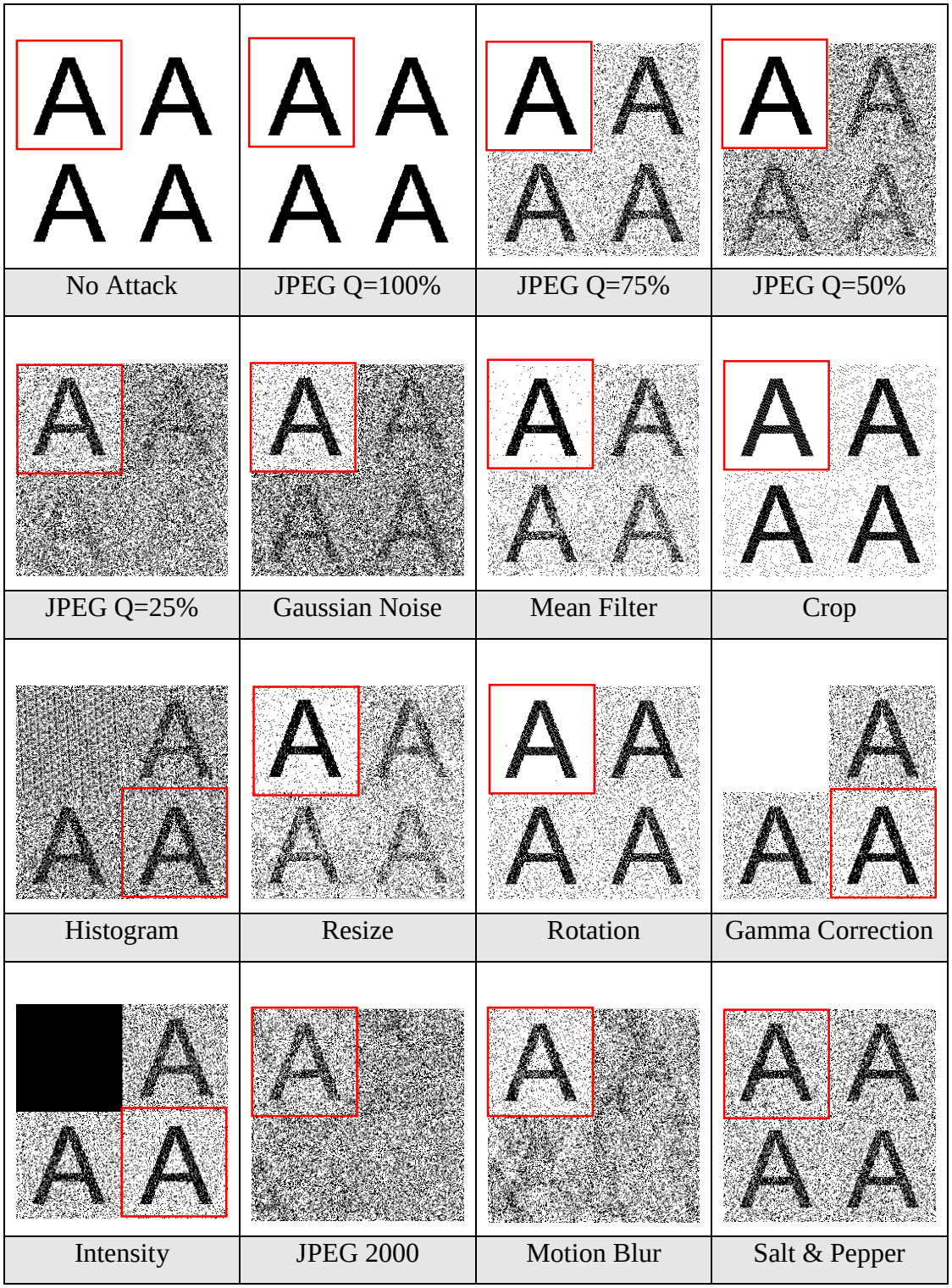


Figure 5.29: Third Efficiency Test Algorithm Extractions

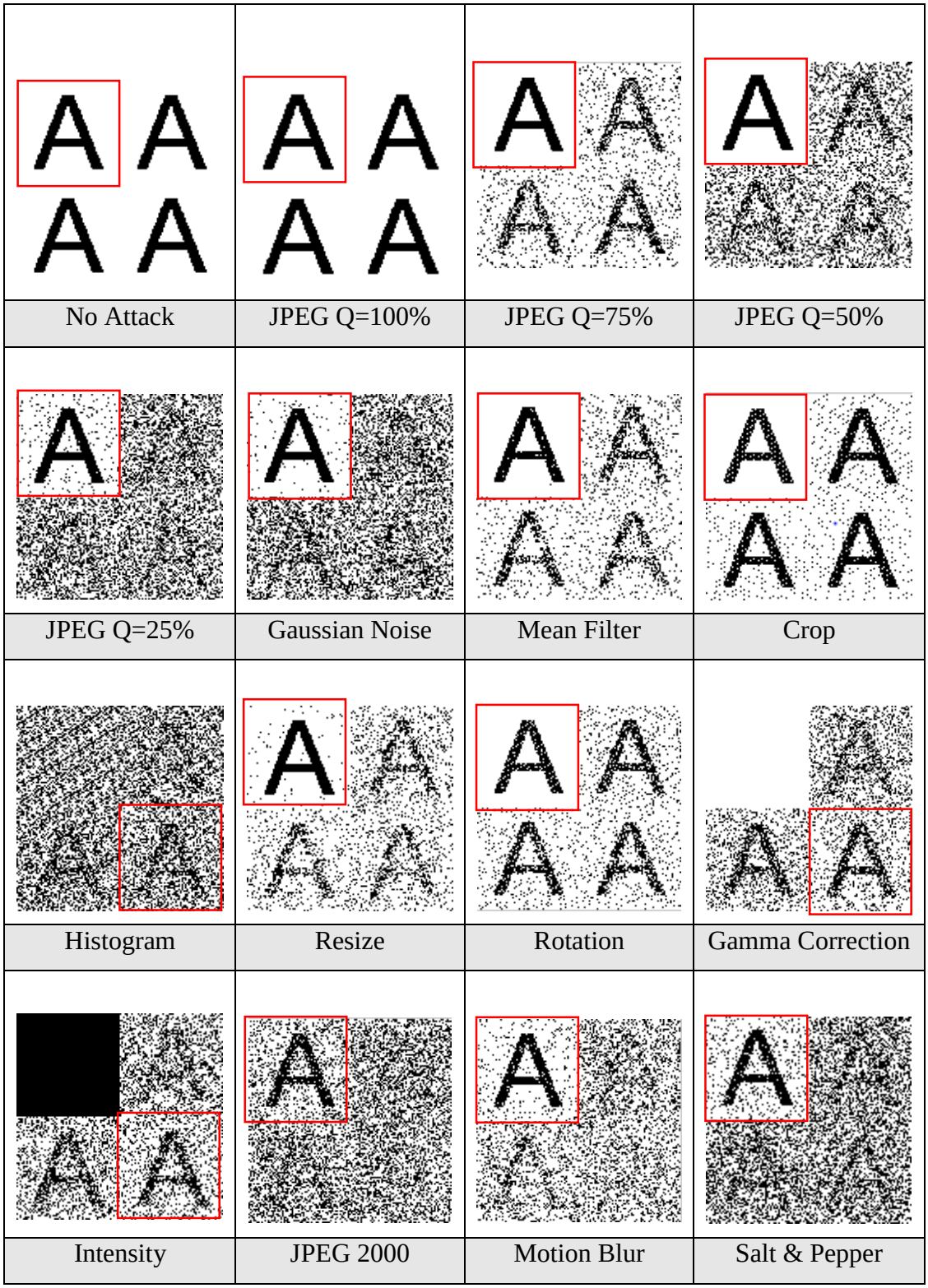


Figure 5.30: Fourth Efficiency Test Algorithm Extractions

The above figures can be used for subjective assessment purposes.

Below the Figure (5.31) presents how the correlation coefficient value varies through the fourth efficiency test algorithms with both cases without and with attacks.

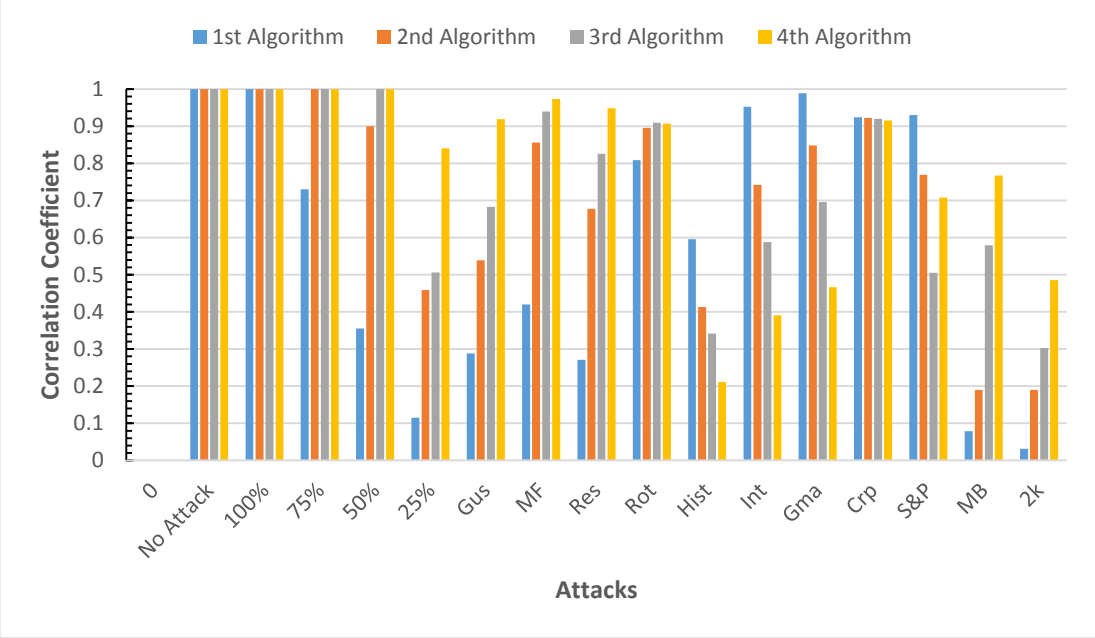


Figure 5.31: Extracted Watermarks Correlations of all Efficiency Test Algorithms with Attacks

The figure above shows that some attacks destroy the high frequency components of the image and others destroy mid or low frequency components. In case of high frequency components loss, then the watermarks extracted from the lowest frequency components hold the highest correlation coefficient value, while in the other case i.e. loss of low frequency components, then the watermarks extracted from the highest frequency components hold the highest correlation value. And that means that the watermarks must be embedded in the highest and lowest frequencies given by the DWT.

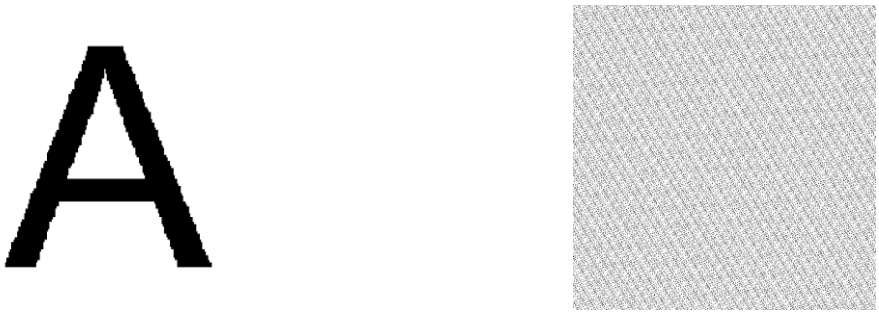
5.2 Colored Images Efficiency Test Algorithms Results

In this section, RGB (Green & blue channels) and Ycbcr color spaces results are presented.

5.2.1 RGB - green channel efficiency test algorithms results

- First Efficiency Test Algorithm Embedding Results:

The Figure (5.32) shows both of the original and scrambled watermarks.



(a) (b)

Figure 5.32: (a) Original Watermark, (b) Scrambled Watermark

The Figures (5.33), (5.34), (5.35), (5.36) and (5.37) show the original cover (un-watermarked), the used green channel, the used level of DWT decomposition (1st level), watermarked green channel and the watermarked image respectively.

Figure 5.33: Cover Image

Figure 5.34: Green Channel

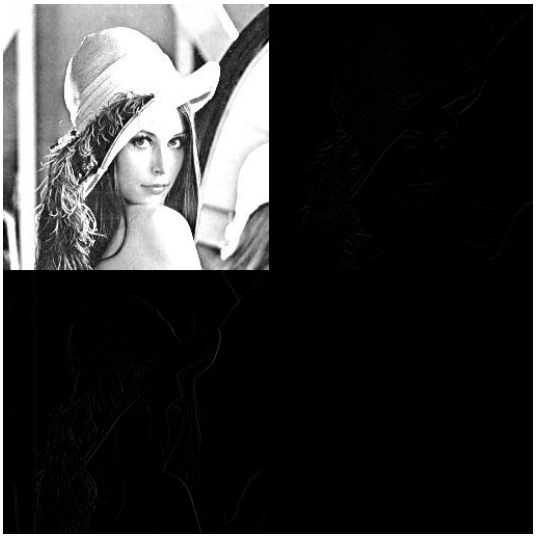


Figure 5.35: First Level Decomposition of Green Channel

Figure 5.36: Watermarked Green Channel, PSNR= 40.4899 dB

Figure 5.37: Green Channel First Algorithm Watermarked Image, PSNR=45.2611 dB

- Attacks Results:

The fifteen attacks mentioned in the previous chapter (section 4.1.3) are applied on each one of the four colored images Efficiency Test algorithms with both spaces (RGB, Ycbcr), they will be presented only once for colored images in this chapter, and that is for the first Efficiency Test algorithm for green channel of RGB space. Because they are causing the same perceptual effect and artifacts in all of the four algorithms, next the Figures (5.38), (5.39), (5.40), (5.41), (5.42), (5.43), (5.44), (5.45), (5.46), (5.47), (5.48), (5.49), (5.50), (5.51), (5.52) show the attacks JPEG,Q=100%, JPEG,Q=75%, JPEG,Q=50%, JPEG,Q=25%, JPEG 2k, Gaussian Noise, Salt & Pepper Noise, Mean Filter, Resizing, Rotation, Histogram Equalization, Intensity adjustment, Gamma Correction, Cropping and Motion Blur respectively.

Figure 5.38: JPEG, Q=100%, PSNR=42.2276 dB

Figure 5.39: JPEG, Q=75%, PSNR=36.7660 dB

Figure 5.40: JPEG, Q=50%, PSNR=35.4178 dB

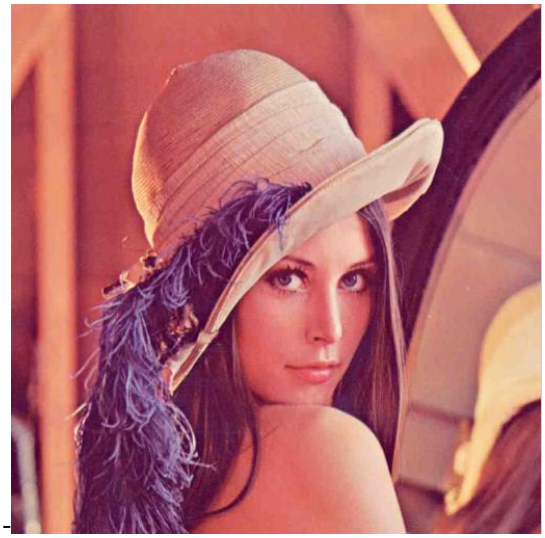


Figure 5.41: JPEG, Q=25 %, PSNR= 33.5714 dB

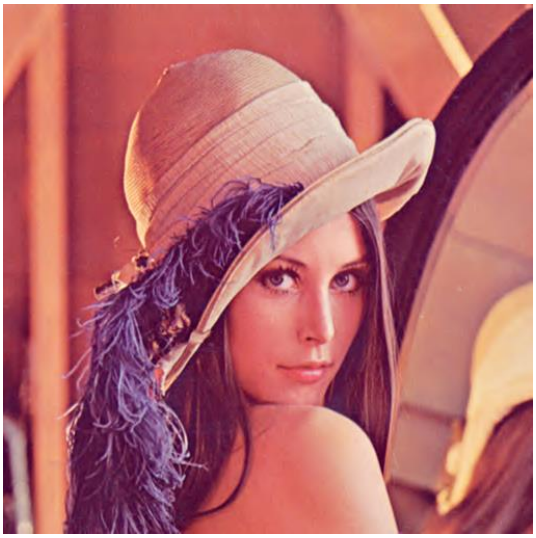


Figure 5.42: JPEG 2000, PSNR=35.5017 dB

Figure 5.43: Gaussian Noise, Mean=0, Variance=0.001, PSNR=29.8844 dB

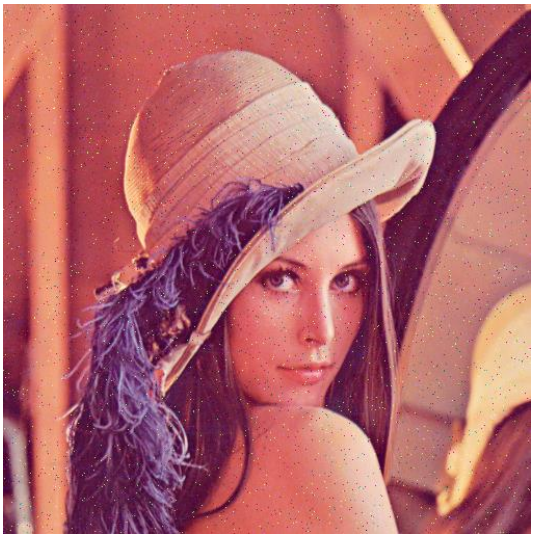


Figure 5.44: Salt & Pepper Noise, Density=0.01, PSNR= 25.0817 dB

Figure 5.45: Mean Filter, Window size 3X3, PSNR=36.9799 dB

Figure 5.46: Resizing 50%, PSNR= 37.7731 dB

Figure 5.47: Rotation -20^0, PSNR=11.1773 dB

Figure 5.48: Histogram Equalization, PSNR=14.2044 dB

Figure 5.49: Intensity Adjustment, PSNR=18.2211 dB

Figure 5.50: Gamma Correction, PSNR=18.2868 dB

Figure 5.51: Cropping, PSNR=14.4645 dB

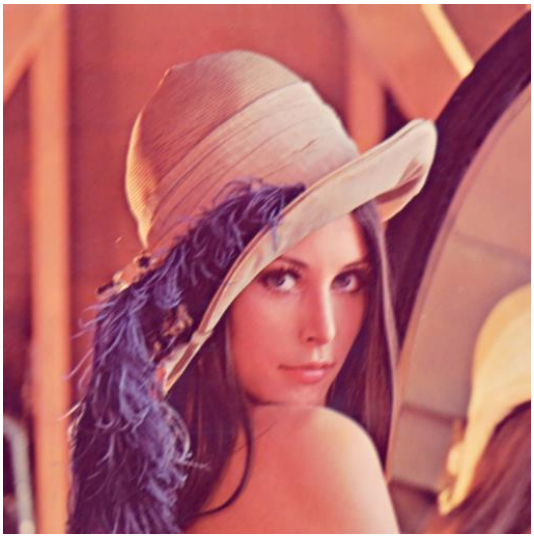


Figure 5.52: Motion Blur, PSNR=32.6677 dB

- Second Efficiency Test Algorithm Embedding Results:

The next Figures (5.53) and (5.54) show the level of DWT decomposition used (2^{nd} Level) and the Watermarked image.

Figure 5.53: Second level Decomposition of Green Channel

Figure 5.54: Green Channel Second Algorithm Watermarked Image, PSNR=46.4652 dB

- Third Efficiency Test Algorithm Embedding Results:

The next Figures (5.55) and (5.56) show the level of DWT decomposition used (3rd Level) and the Watermarked image.

Figure 5.55: Third Level Decomposition of Green Channel

Figure 5.56: Green Channel Third Algorithm Watermarked Image, PSNR=48.7566 dB

- Fourth Efficiency Test Algorithm Embedding Results:

The next Figures (5.57) and (5.58) show the level of DWT decomposition used (4^{th} Level) and the Watermarked image.

Figure 5.57: Fourth Level Decomposition of Green Channel

Figure 5.58: Green Channel Fourth Algorithm Watermarked Image, PSNR=52.3074 dB

Below the Table (5.3) shows the PSNR values for all efficiency test algorithms.

Table 5.3: PSNR in dB of all Efficiency Test Algorithms with Attacks

No.	Case	1st Alg.	2nd Alg.	3rd Alg.	4th Alg.
1	No Attack	45.2611	46.4652	48.7566	52.3074
2	Green Channel	40.4899	41.6940	43.9853	47.5362
3	JPEG, Q=100	42.2276	42.7754	43.5080	44.2553
4	JPEG, Q=75	36.7660	36.7423	36.8995	37.0552
5	JPEG, Q=50	35.4178	35.3669	35.4652	35.5866
6	JPEG, Q=25	33.5714	33.5060	33.5494	33.6135
7	Gaussian Noise	29.8844	29.9160	29.9534	29.9831
8	Mean Filter	36.9799	36.9024	36.9590	37.0674
9	Resizing 50%	37.7731	37.6996	37.7410	37.8763
10	Rotation 20^0	11.1773	11.1771	11.1773	11.1779
11	Histogram Equalization	14.2044	14.2049	14.2085	14.2099
12	Intensity Adjustment	18.2211	18.2303	18.2481	18.2696
13	Gamma Correction	18.2868	18.2819	18.2698	18.2531
14	Cropping	14.4645	14.4653	14.4663	14.4671
15	Salt & Pepper Noise,	25.0817	25.1552	18.1908	18.2106
16	Motion Blur	32.6677	32.6612	32.6624	32.6881
17	JPEG 2000	35.5017	35.4645	35.4607	35.5282

The Figure (5.59) next, presents how the PSNR value varies through the fourth efficiency test algorithms with both cases without and with attacks.

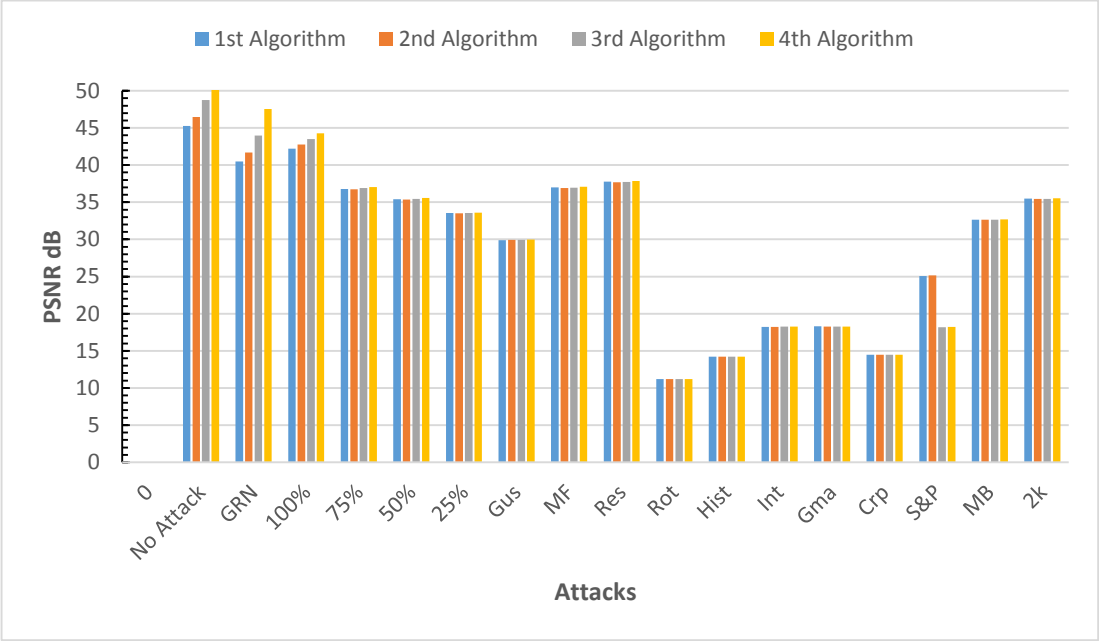


Figure 5.59: PSNR in dB of all Efficiency Test Algorithms with Attacks

The results in the Figure (5.59) above indicate that in the case of no attack, the PSNR value increase with the deeper level of DWT decomposition used with respect to the scaling factor, i.e. the PSNR at the first efficiency test algorithm which uses the 1st level of decomposition is (45.2611dB), while the fourth test algorithm gave a higher PSNR value of (52.3074 dB). The rest of PSNR values at different attack cases vary just a little through different efficiency test algorithms.

Next the Table (5.4) presents the correlation coefficients values of watermarks extractions in all efficiency test algorithms with both cases without and with attacks.

Table 5.4: Extracted Watermarks Correlations of all Efficiency Test Algorithms

No.	Case	LL	HL	LH	HH	Level
1	No Attack	1	1	1	1	***1st***
		1	1	1	1	***2nd***
		1	1	1	1	***3rd***
		1	1	1	1	***4th***
2	JPEG, Q=100%	0.9827	0.7033	0.7207	0.8035	***1st***
		0.9999	0.7356	0.6551	0.7535	***2nd***
		1	0.8788	0.8487	0.9022	***3rd***
		1	0.9465	0.9281	0.9550	***4th***
3	JPEG, Q=75%	0.3819	0.0470	0.0390	0.0033	***1st***
		0.7916	0.1572	0.1433	0.0848	***2nd***
		0.9907	0.2938	0.2725	0.2316	***3rd***
		1	0.4265	0.4244	0.3933	***4th***
4	JPEG, Q=50%	0.2043	0.0177	0.0182	9.3322e-004	***1st***
		0.5394	0.0765	0.0829	0.0228	***2nd***
		0.8090	0.1953	0.1595	0.1294	***3rd***
		0.9457	0.2252	0.2474	0.2058	***4th***
5	JPEG, Q=25%	0.0794	0.0046	0.0106	6.8475e-005	***1st***
		0.2860	0.0296	0.0340	0.0019	***2nd***
		0.4367	0.0902	0.0964	0.0409	***3rd***
		0.6017	0.1612	0.1269	0.1276	***4th***
6	Gaussian Noise	0.3854	0.1053	0.1051	0.1077	***1st***
		0.6766	0.1455	0.1386	0.1432	***2nd***
		0.8870	0.2067	0.2105	0.2052	***3rd***
		0.9756	0.2739	0.2859	0.2863	***4th***
7	Mean Filter	0.4280	0.0026	0.0274-	2.0456e-004	***1st***
		0.8560	0.1785	0.1605	0.0898	***2nd***
		0.9584	0.5357	0.4753	0.4048	***3rd***
		0.9785	0.7171	0.6295	0.6549	***4th***
8	Crop	0.9236	0.8733	0.8469	0.9237	***1st***
		0.9218	0.8225	0.8089	0.8399	***2nd***
		0.9199	0.8151	0.7867	0.8250	***3rd***
		0.9148	0.7956	0.7710	0.8117	***4th***

Table 5.4 continued.

9	Histogram Equalization	0.1278	0.5608	0.5071	0.6660	***1st***
		0.1246	0.3540	0.3013	0.4463	***2nd***
		0.0962	0.3144	0.2483	0.3632	***3rd***
		0.0566	0.2204	0.1599	0.2865	***4th***
10	Resizing 50%	0.2589	0.0085	0.0029	0.0011	***1st***
		0.6707	0.1115	0.0938	0.0497	***2nd***
		0.8369	0.3220	0.2853	0.2117	***3rd***
		0.9249	0.5583	0.4798	0.4738	***4th***
11	Rotation -20^0	0.7999	0.3543	0.3784	0.2978	***1st***
		0.8976	0.4257	0.3845	0.3321	***2nd***
		0.9135	0.6620	0.6075	0.6107	***3rd***
		0.9093	0.6994	0.6495	0.6721	***4th***
12	Gamma Correction	NaN	0.8002	0.7380	0.9428	***1st***
		NaN	0.5753	0.5189	0.6804	***2nd***
		NaN	0.4904	0.4104	0.5711	***3rd***
		NaN	0.3575	0.2578	0.4423	***4th***
13	Intensity Adjustment	0.0262	0.8382	0.7631	0.9678	***1st***
		0.0198	0.5761	0.4911	0.7337	***2nd***
		0.0060	0.4768	0.3838	0.5793	***3rd***
		NaN	0.3364	0.2492	0.4412	***4th***
14	JPEG 2000	0.0574	0.0200	0.0225	0.0148	***1st***
		0.1799	0.0568	0.0518	0.0204	***2nd***
		0.5350	0.0327	0.0389	0.0127	***3rd***
		0.6569	0.1590	0.1391	0.1135	***4th***
15	Motion Blur	0.0729	0.0427	0.0442	0.0464-	***1st***
		0.2017	0.0465	0.0417	0.1019-	***2nd***
		0.6003	0.1131	0.0916	0.0388-	***3rd***
		0.7657	0.2869	0.2076	0.1592	***4th***
16	Salt & Pepper	0.9294	0.9300	0.9300	0.9301	***1st***
		0.7740	0.7679	0.7646	0.7662	***2nd***
		0.2415	0.1014	0.1084	0.1075	***3rd***
		0.2007	0.0661	0.0780	0.0915	***4th***

The above table can be used for objective assessment purposes. Next the Figures (5.60), (5.61), (5.62) and (5.63) show the watermarks extracted images in all efficiency test algorithms with both cases without and with attacks.

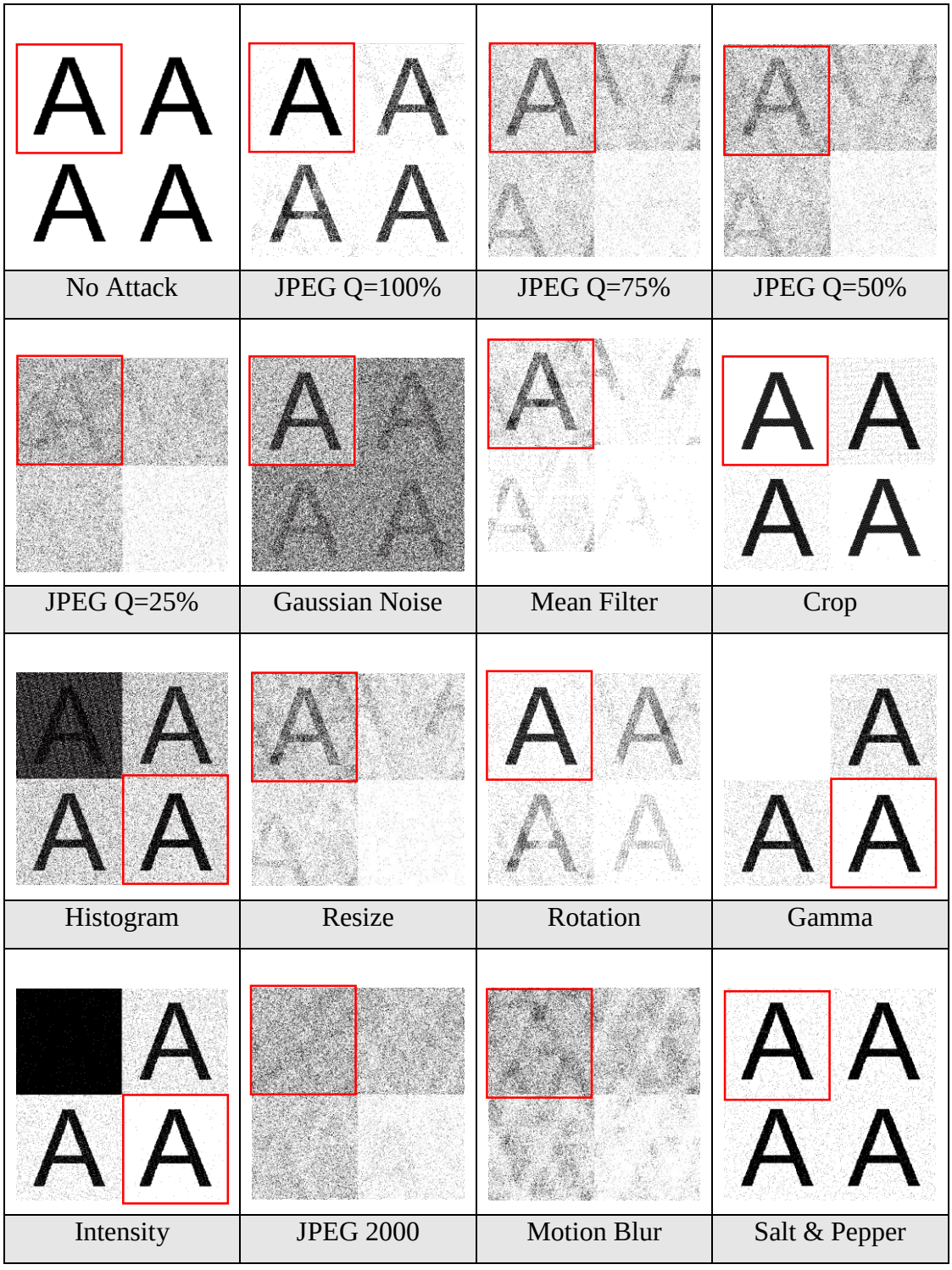


Figure 5.60: Green Channel First Efficiency Test Algorithm Extractions

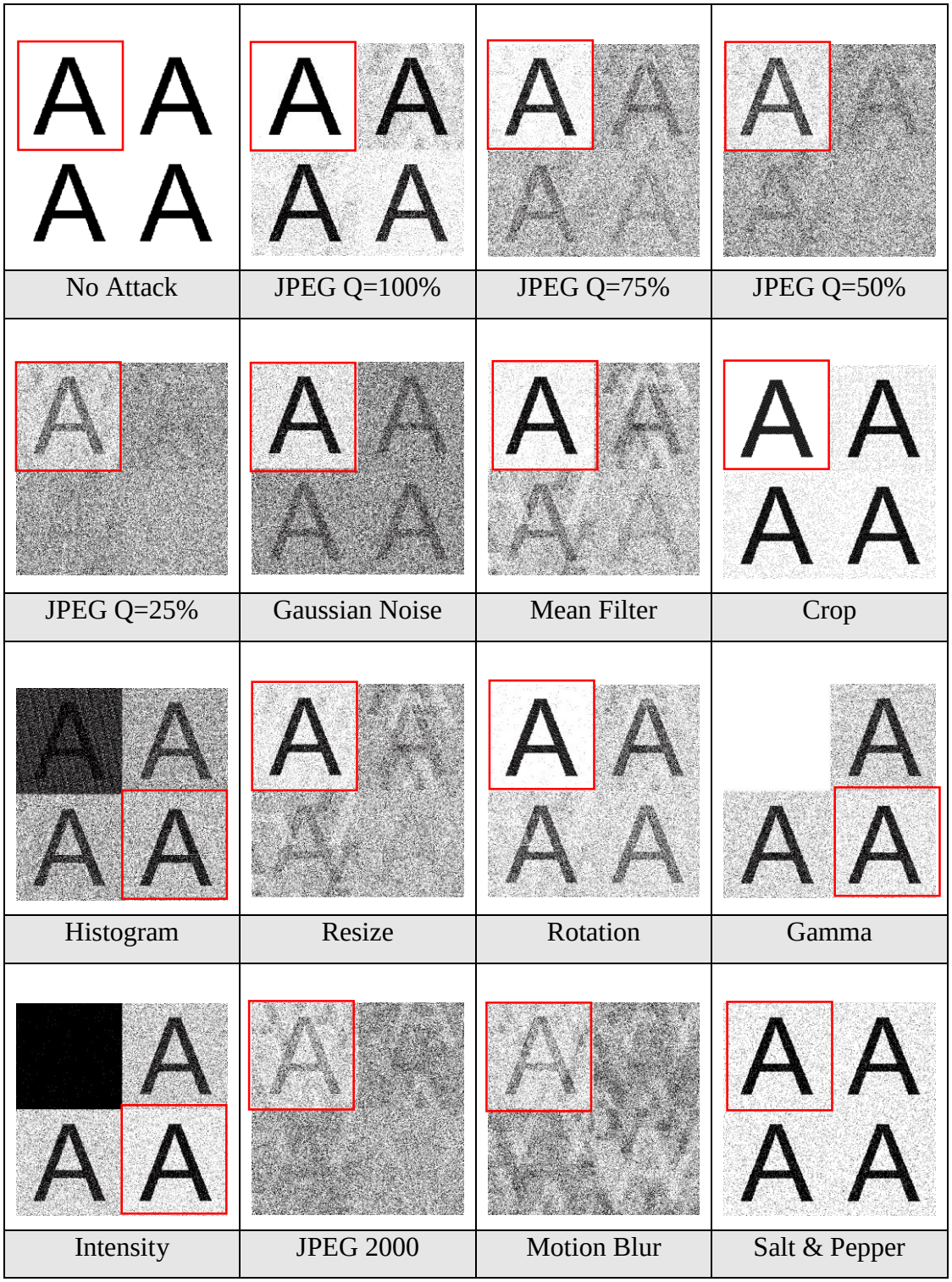


Figure 5.61: Green Channel Second Efficiency Test Algorithm Extractions

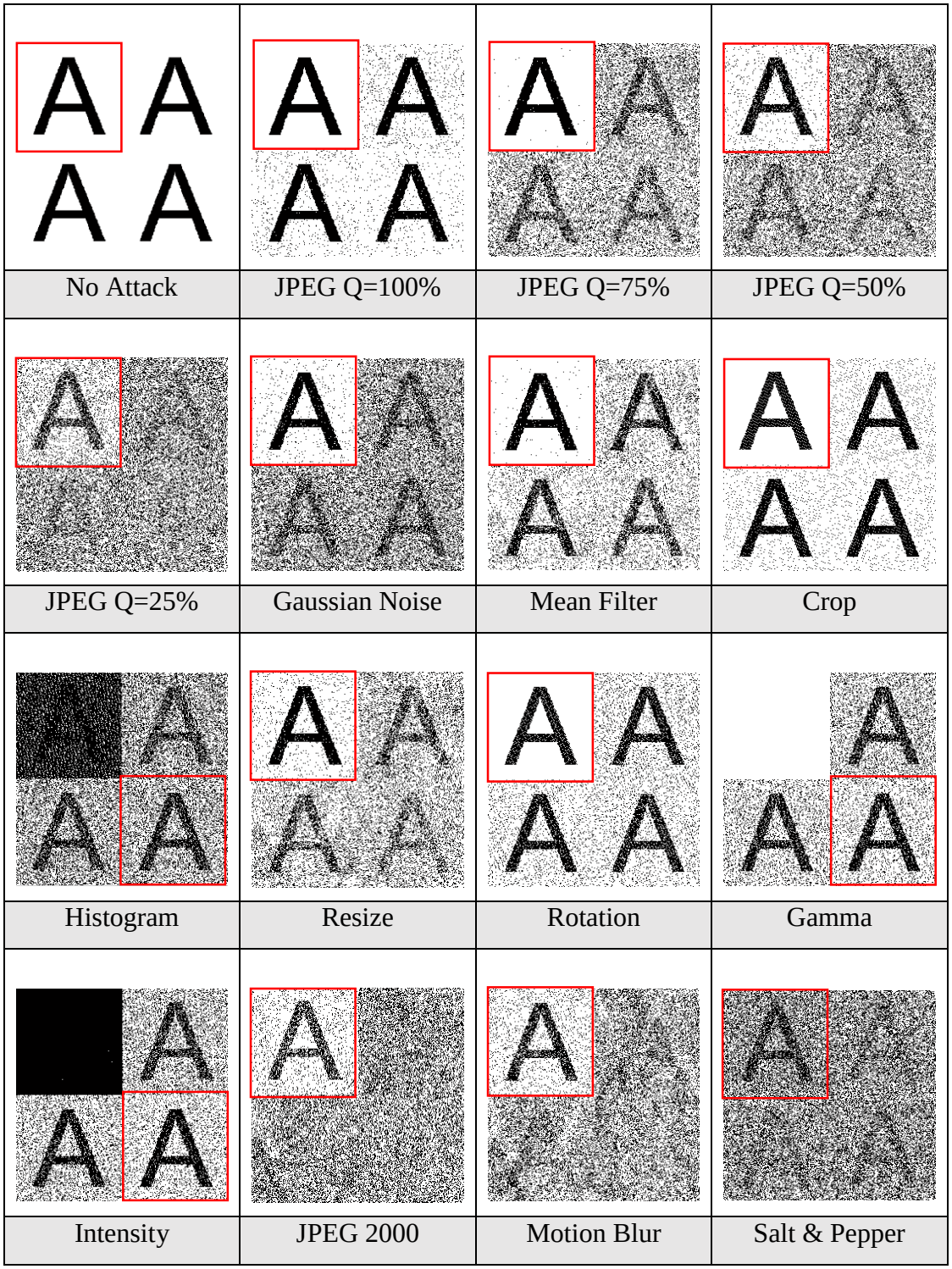


Figure 5.62: Green Channel Third Efficiency Test Algorithm Extractions

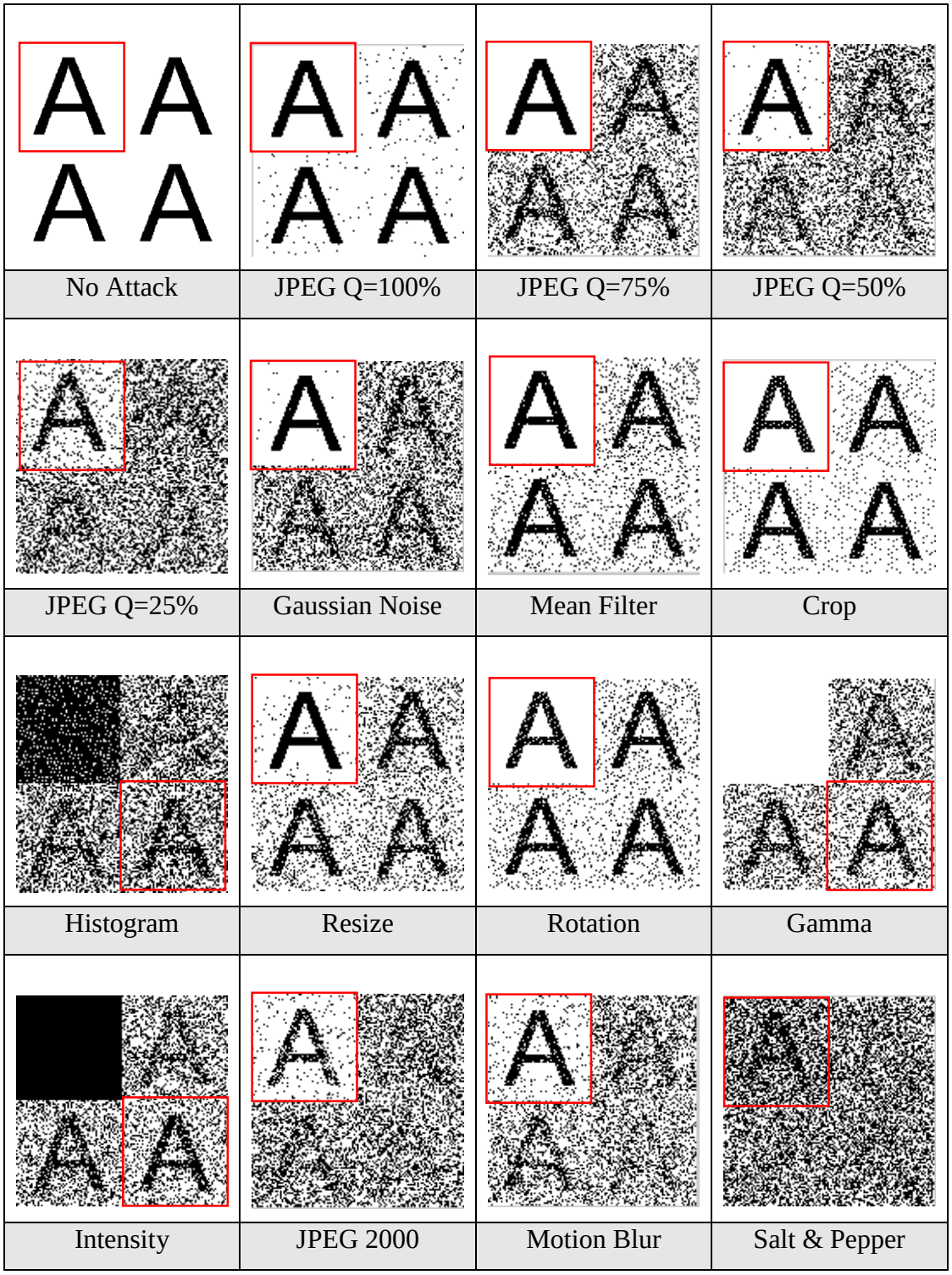


Figure 5.63: Green Channel Fourth Efficiency Test Algorithm Extractions

The above figures can be used for subjective assessment purposes.

Below the Figure (5.64) presents how the correlation coefficient value varies through the fourth efficiency test algorithms with both cases without and with attacks.

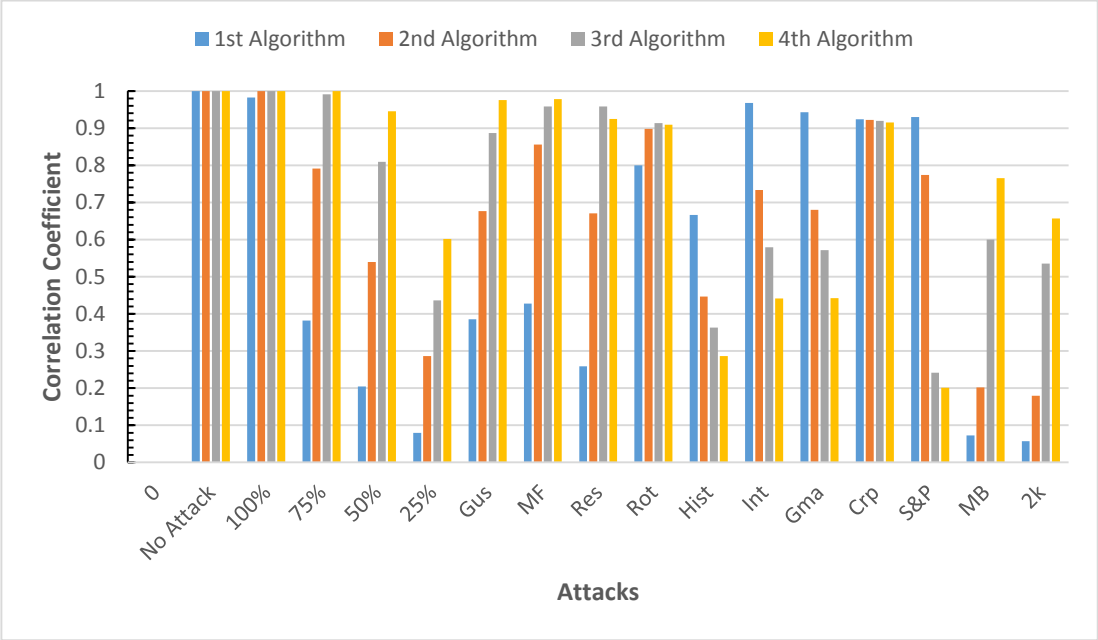


Figure 5.64: Extracted Watermarks Correlations of all Efficiency Test Algorithms with Attacks

The figure above shows the same behavior noticed in Figure (5.31).

5.2.2 RGB - blue channel efficiency test algorithms results

- First Efficiency Test Algorithm Embedding Results:

The Figures (5.65), (5.66) next show the level of decomposition used (1st level) and the watermarked image respectivly.

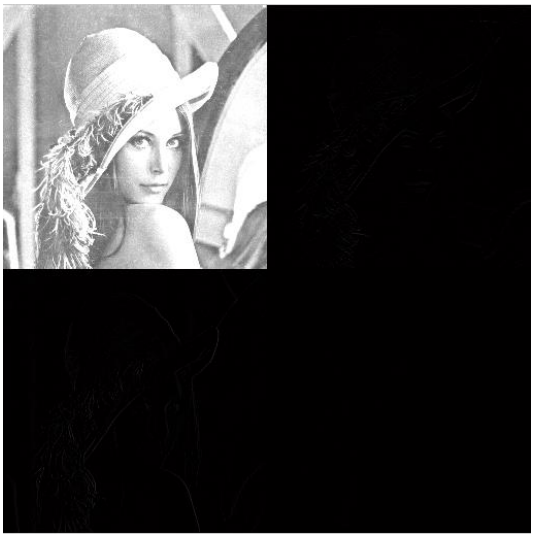


Figure 5.65: First level decomposition of Blue Channel

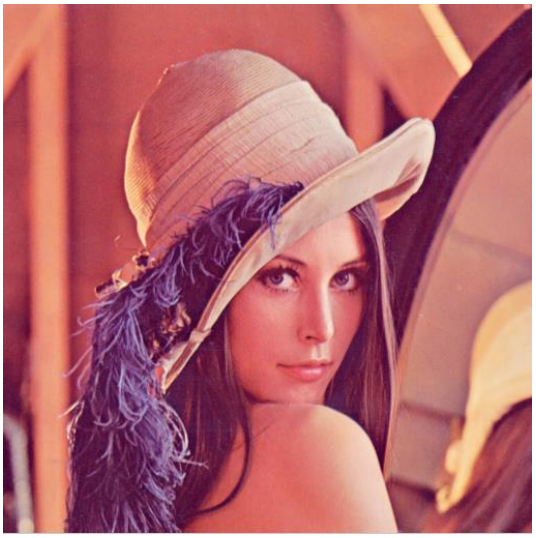


Figure 5.66: Blue Channel First Algorithm Watermarked Image, PSNR=45.2616 dB

- Second Efficiency Test Algorithm Embedding Results:

The Figures (5.67), (5.68) below show the level of decomposition used (2^{nd} level) and the watermarked image respectivly.

Figure 5.67: Second level Decomposition of Blue Channel

Figure 5.68: Blue channel Second Algorithm Watermarked Image, PSNR=46.4652 dB

- Third Efficiency Test Algorithm Embedding Results:

The Figures (5.69), (5.70) next show the level of decomposition used (3rd level) and the watermarked image respectivly.

Figure 5.69: 3rd level decomposition of Blue Channel

Figure 5.70: Blue Channel Third Algorithm Watermarked Image, PSNR=48.7566 dB

- Fourth Efficiency Test Algorithm Embedding Results:

The Figures (5.71), (5.72) next show the level of decomposition used (4^{th} level) and the watermarked image respectivly.

Figure 5.71: Fourth level Decomposition of Blue Channel

Figure 5.72: Blue Channel Fourth Algorithm Watermarked Image, PSNR=52.3074 dB

Below the Table (5.5) shows the PSNR values for all efficiency test algorithms in both cases without and with attacks.

Table 5.5: PSNR in dB of all the Efficiency Test Algorithms with Attacks

No.	Case	1st Alg.	2nd Alg.	3rd Alg.	4th Alg.
1	No Attack	45.2616	46.4652	48.7566	52.3074
2	Blue Channel	40.4904	41.6940	43.9853	47.5362
3	JPEG, Q=100	43.4975	43.2509	43.6598	44.2937
4	JPEG, Q=75	37.0601	37.0054	36.9813	37.0698
5	JPEG, Q=50	35.5989	35.5778	35.5506	35.5920
6	JPEG, Q=25	33.6041	33.5946	33.5977	33.6097
7	Gaussian Noise	29.8840	29.9162	29.9541	29.9841
8	Mean Filter	36.9804	36.9021	36.9586	37.0674
9	Resizing 50%	37.7751	37.6996	37.7394	37.8768
10	Rotation 20^0	11.1773	11.1772	11.1774	11.1780
11	Histogram Equalization	14.1936	14.1948	14.2023	14.2057
12	Intensity Adjustment	18.2099	18.2206	18.2409	18.2650
13	Gamma Correction	18.2990	18.2930	18.2784	18.2590
14	Cropping	14.4645	14.4653	14.4663	14.4671
15	Salt & Pepper Noise,	25.0867	25.1672	25.1483	18.2134
16	Motion Blur	32.6675	32.6608	32.6629	32.6879
17	JPEG 2000	35.5089	35.4779	35.4702	35.5343

The Figure (5.73) next, presents how the PSNR value varies through the fourth efficiency test algorithms with both cases without and with attacks.

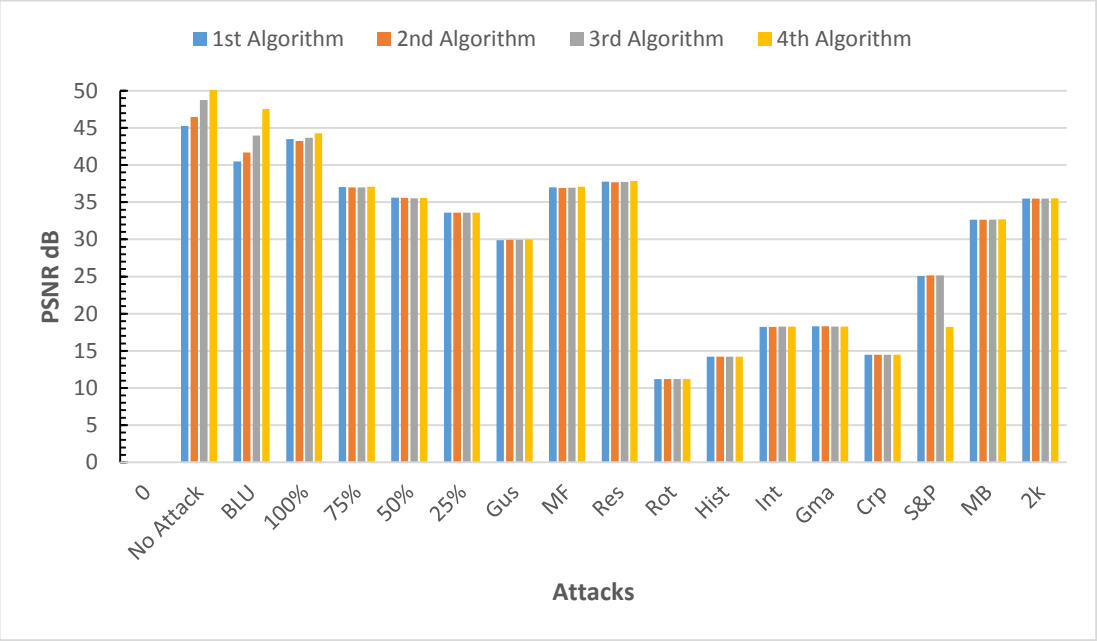


Figure 5.73: PSNR in dB of all Efficiency Test Algorithms with Attacks

The results in the Figure (5.73) again indicating that the deeper the level of DWT decomposition, the higher the PSNR value with respect to the scaling factor.

Next the Table (5.6) presents the correlation coefficients values of watermarks extractions in all efficiency test algorithms with both cases without and with attacks.

Table 5.6: Extracted Watermarks Correlations of all the Efficiency Test Algorithms

No.	Case	LL	HL	LH	HH	Level
1	No Attack	1	1	1	1	***1st***
		1	1	1	1	***2nd***
		1	1	1	1	***3rd***
		1	1	1	1	***4th***
2	JPEG, Q=100%	0.6261	0.0679	0.0590	0.0875	***1st***
		0.9512	0.2924	0.2319	0.2068	***2nd***
		0.9960	0.5414	0.4965	0.4633	***3rd***
		1	0.6835	0.6173	0.7034	***4th***
3	JPEG, Q=75%	0.0479	0.0033	0.0053	0.0028-	***1st***
		0.1984	0.0177	0.0163	0.0118	***2nd***
		0.6557	0.0688	0.0569	0.0225	***3rd***
		0.8783	0.1948	0.1727	0.1000	***4th***
4	JPEG, Q=50%	0.0271	0.0015	0.0043	9.0706e-004	***1st***
		0.1030	0.0057	0.0200	0.0061	***2nd***
		0.3277	0.0385	0.0298	0.0152	***3rd***
		0.5474	0.0813	0.0775	0.0382	***4th***
5	JPEG, Q=25%	0.0117	0.0011	0.0037	2.2636e-004	***1st***
		0.0528	0.0095	0.0074	0.0012-	***2nd***
		0.1434	0.0199	0.0188	0.0019-	***3rd***
		0.2684	0.0438	0.0316	0.0199	***4th***
6	Gaussian Noise	0.3852	0.1111	0.1094	0.1037	***1st***
		0.6826	0.1466	0.1425	0.1423	***2nd***
		0.8870	0.2046	0.2197	0.2066	***3rd***
		0.9659	0.2858	0.2894	0.2687	***4th***
7	Mean Filter	0.3655	0.0020	0.0253-	0.0012	***1st***
		0.8615	0.1444	0.1135	0.0740	***2nd***
		0.9652	0.4792	0.4233	0.3395	***3rd***
		0.9731	0.7130	0.6454	0.6484	***4th***
8	Crop	0.9236	0.8708	0.8477	0.9231	***1st***
		0.9218	0.8206	0.8034	0.8292	***2nd***
		0.9199	0.8101	0.7875	0.8223	***3rd***
		0.9148	0.8098	0.7651	0.8070	***4th***
9	Histogram Equalization	0.0712	0.4482	0.4135	0.5876	***1st***

Table 5.6 continued.

		0.0658	0.2471	0.2070	0.2932	***2nd***
		0.0495	0.2171	0.2031	0.2746	***3rd***
		0.0252	0.1639	0.1218	0.2281	***4th***
10	Resizing 50%	0.2167	0.0090	0.0046	0.0012	***1st***
		0.6755	0.0881	0.0694	0.0413	***2nd***
		0.8847	0.2934	0.2517	0.1787	***3rd***
		0.9559	0.5608	0.4804	0.4481	***4th***
11	Rotation -20^0	0.7609	0.3367	0.3726	0.3006	***1st***
		0.9030	0.3735	0.2994	0.2634	***2nd***
		0.9121	0.6518	0.6067	0.5829	***3rd***
		0.9093	0.7070	0.6675	0.6831	***4th***
12	Gamma Correction	NaN	0.9503	0.9212	0.9964	***1st***
		NaN	0.7588	0.6839	0.8505	***2nd***
		NaN	0.6694	0.5868	0.7612	***3rd***
		NaN	0.5258	0.4176	0.6373	***4th***
13	Intensity Adjustment	NaN	0.8870	0.8318	0.9952	***1st***
		NaN	0.5957	0.5056	0.6975	***2nd***
		NaN	0.5108	0.4459	0.6018	***3rd***
		NaN	0.3877	0.3010	0.4914	***4th***
14	JPEG 2000	0.0685	0.0237	0.0305	0.0208	***1st***
		0.1832	0.0576	0.0563	0.0264	***2nd***
		0.5292	0.0321	0.0390	0.0229	***3rd***
		0.6948	0.1498	0.1475	0.1316	***4th***
15	Motion Blur	0.0675	0.0422	0.0444	0.0482-	***1st***
		0.2134	0.0407	0.0343	0.0794-	***2nd***
		0.6418	0.1005	0.0752	0.0335-	***3rd***
		0.8195	0.2716	0.2134	0.1318	***4th***
16	Salt & Pepper	0.9297	0.9295	0.9297	0.9296	***1st***
		0.7622	0.7593	0.7651	0.7620	***2nd***
		0.5861	0.4413	0.4432	0.4539	***3rd***
		0.2742	0.0934	0.0850	0.0855	***4th***

Next the Figures (5.74), (5.75), (5.76) and (5.77) show the watermarks extracted images in all efficiency test algorithms with both cases without and with attacks.

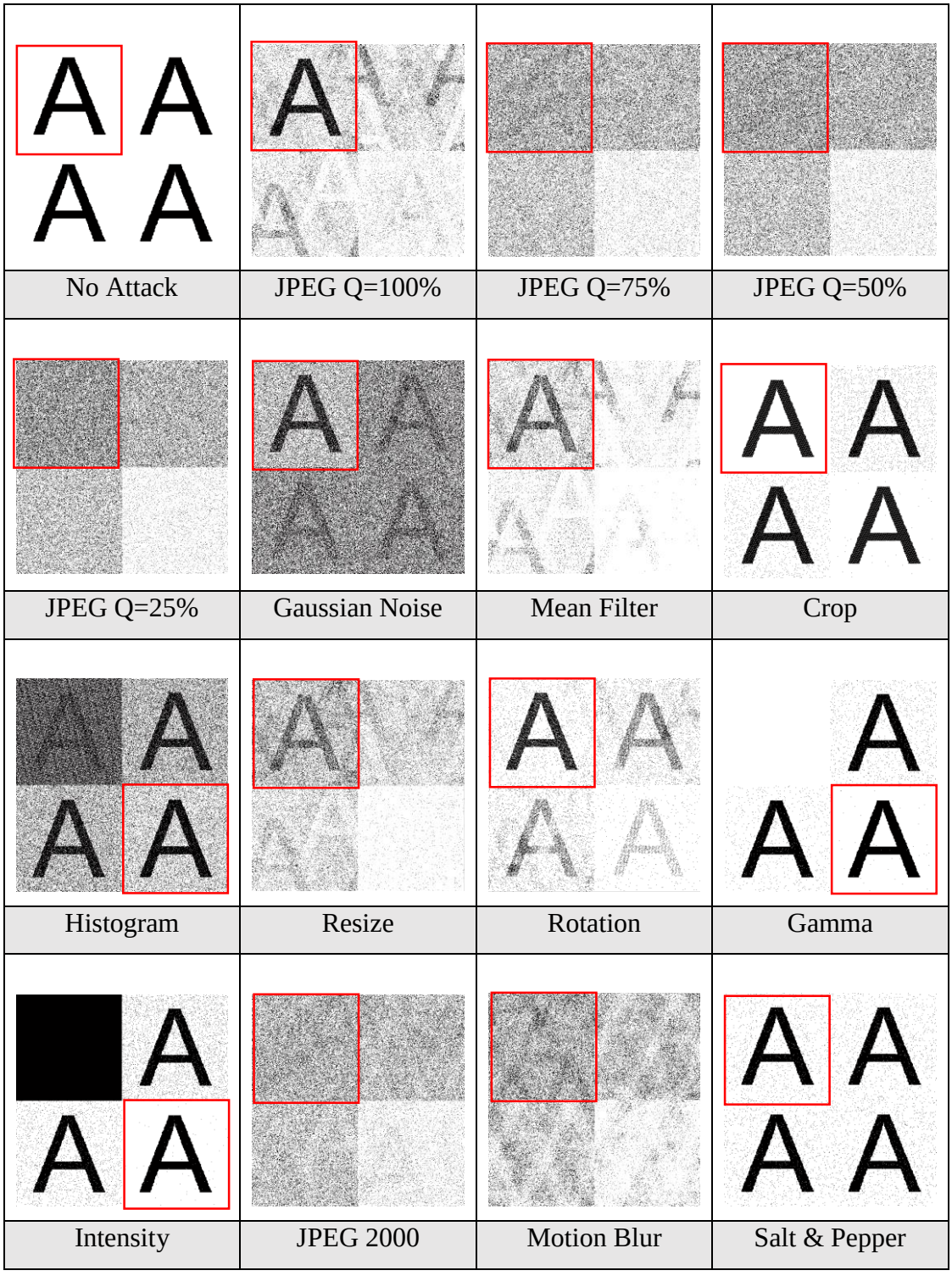


Figure 5.74: Blue channel First Efficiency Test Algorithm Extractions

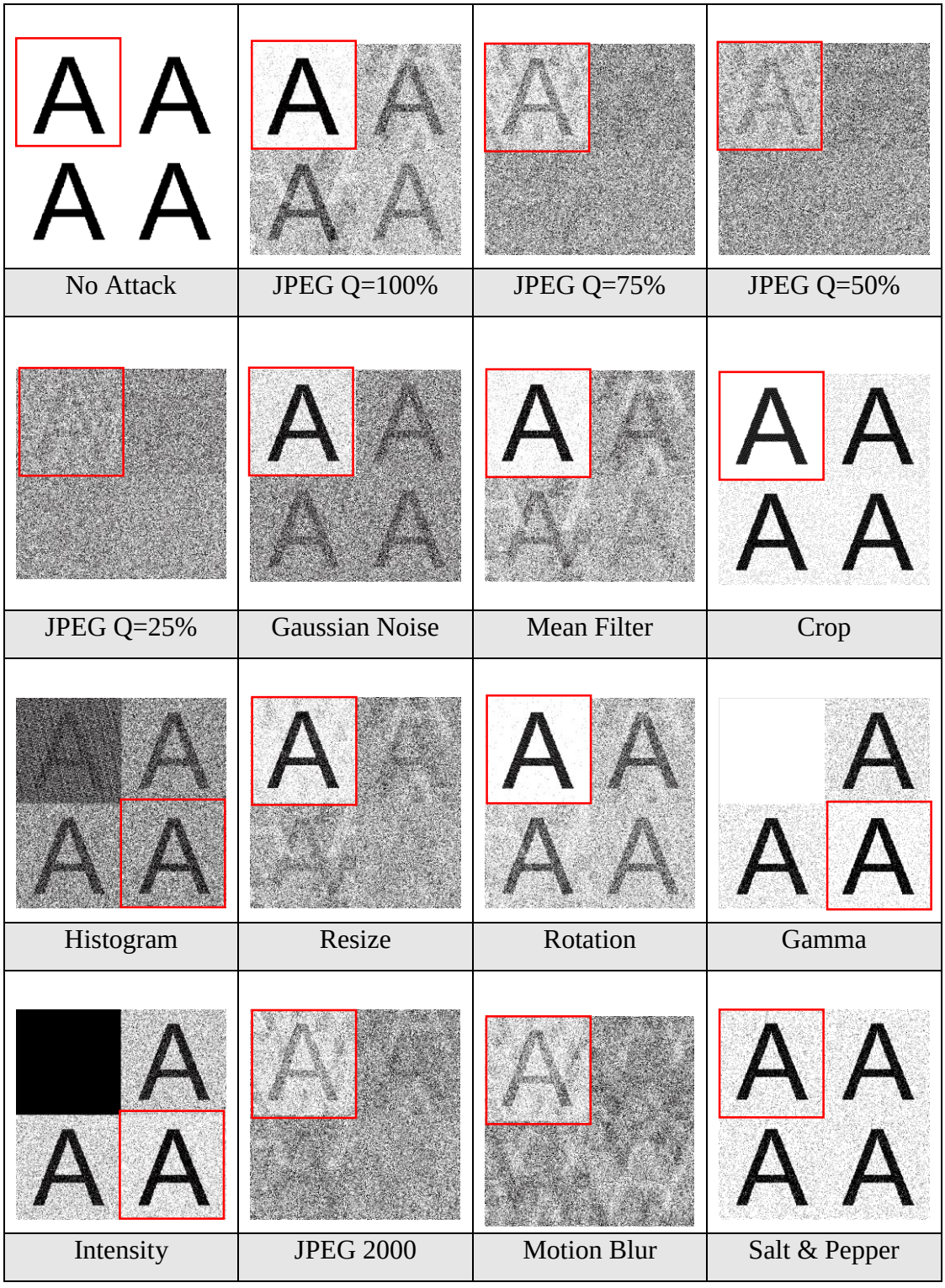


Figure 5.75: Blue Channel Second Efficiency Test Algorithm Extractions

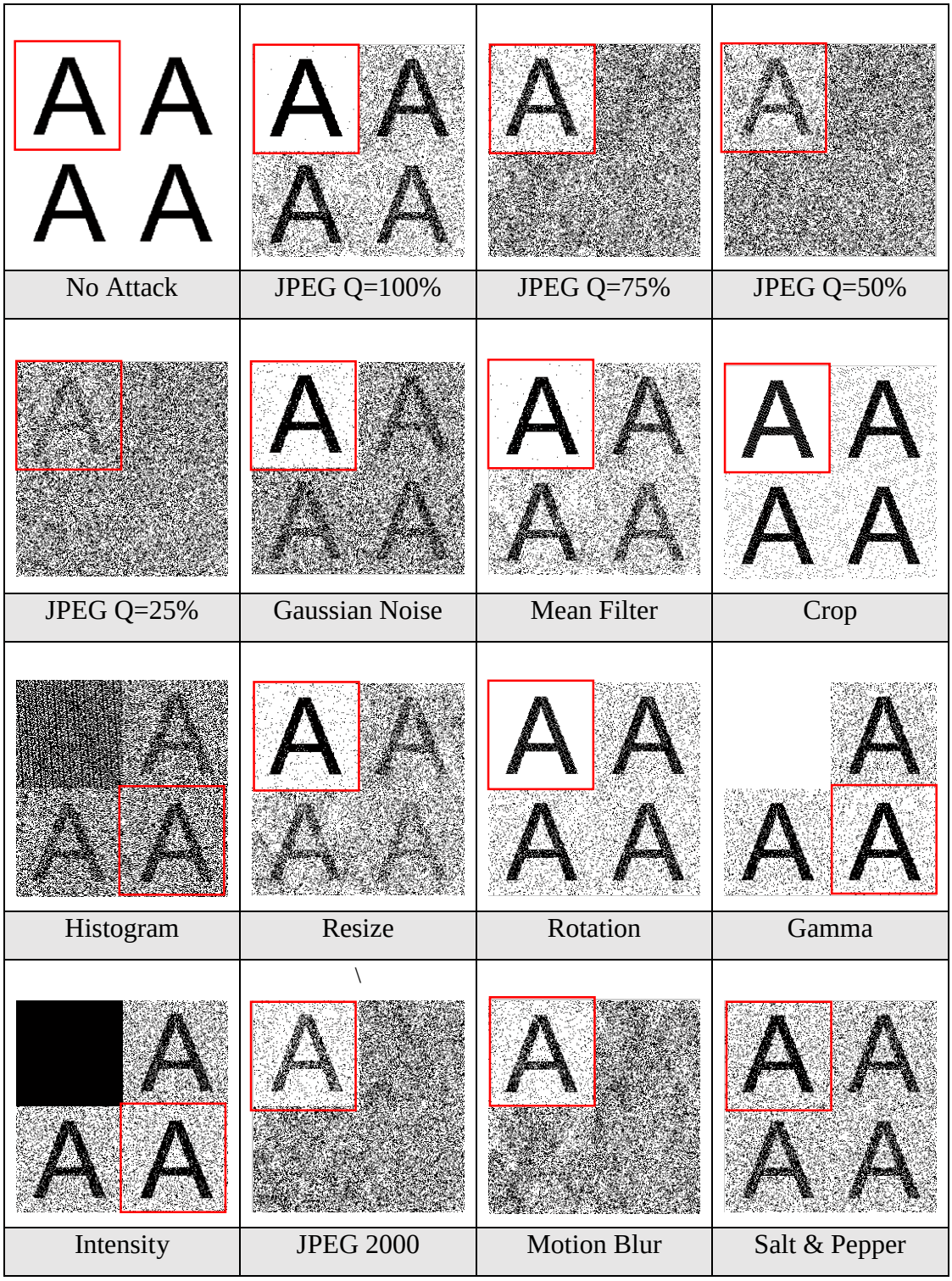


Figure 5.76: Blue Channel Third Efficiency Test Algorithm Extractions

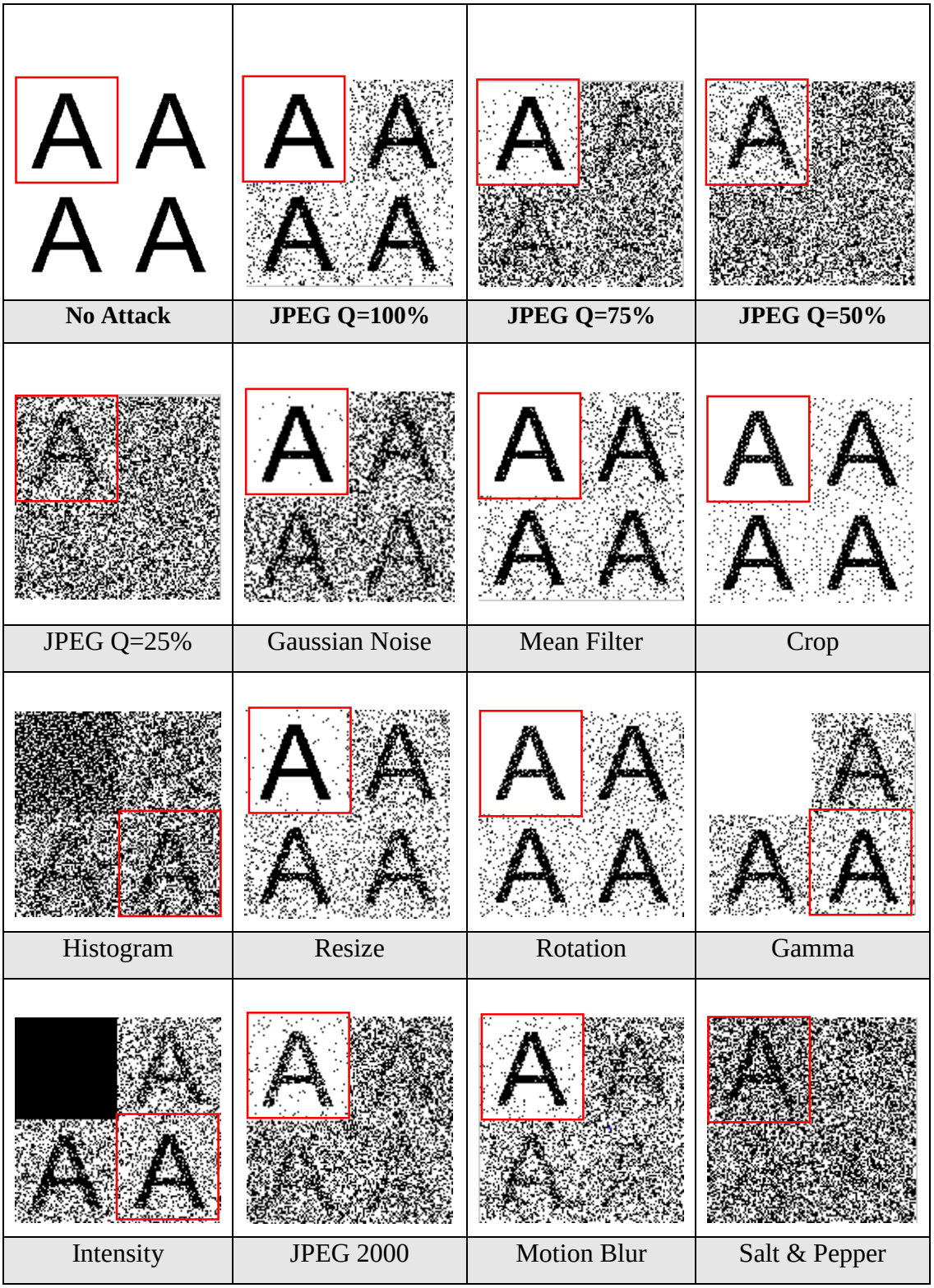


Figure 5.77: Blue Channel Fourth Efficiency Test Algorithm Extractions

Below the Figure (5.78) presents how the correlation coefficient value varies through the fourth efficiency test algorithms with both cases without and with attacks

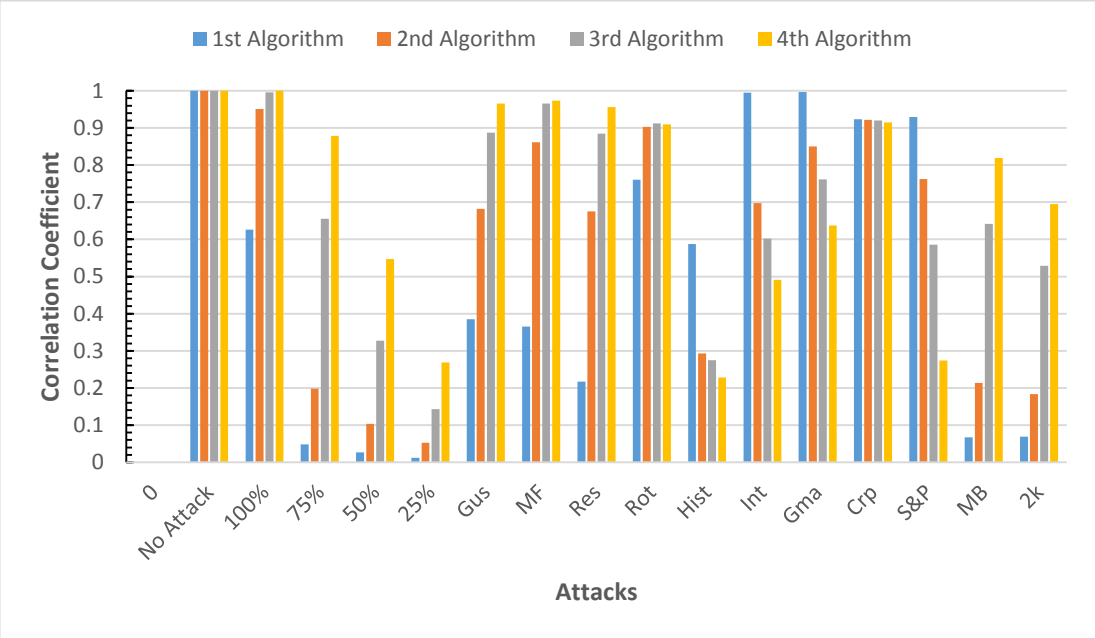


Figure 5.78: Extracted Watermarks Correlations of All the Efficiency Test Algorithms with Attacks

The figure above illustrates again that some attacks destroy high frequencies and other destroy low ones, and watermarks must be embedded in the lowest and highest frequencies possible. Also it shows that blue channel is less robust against the JPEG attack unlike the green channel.

5.2.3 Ycbcr luminance channel (Y) efficiency test algorithms results

- First Efficiency Test Algorithm Embedding Results:

The Figures (5.79), (5.80) next show the level of decomposition used (1st level) and the watermarked image respectivly.

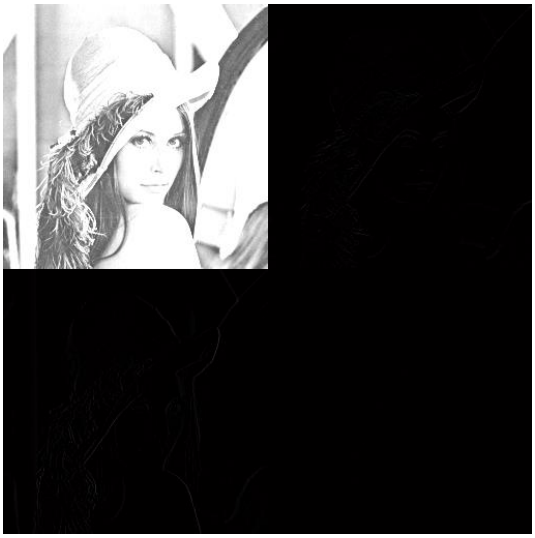


Figure 5.79: First level Decomposition of Y Luminance Channel

Figure 5.80: Y Channel First Algorithm Watermarked Image, PSNR=43.4232 dB

- Second Efficiency Test Algorithm Embedding Results:

The Figures (5.81), (5.82) next show the level of decomposition used (2^{nd} level) and the watermarked image respectivly.

Figure 5.81: Second level Decomposition of Y Luminance Channel

Figure 5.82: Y Channel Second Algorithm Watermarked Image, PSNR=44.3791 dB

- Third Efficiency Test Algorithm Embedding Results:

The Figures (5.83), (5.84) next show the level of decomposition used (3rd level) and the watermarked image respectivly.

Figure 5.83: Third level Decomposition of Y Luminance Channel

Figure 5.84: Y Channel Third Algorithm Watermarked Image, PSNR= 45.1978 dB

- Fourth Efficiency Test Algorithm Embedding Results:

The Figures (5.85), (5.86) next show the level of decomposition used (4^{th} level) and the watermarked image respectivly.

Figure 5.85: Fourth level Decomposition of Y Luminance Channel

Figure 5.86: Y Channel Fourth Algorithm Watermarked Image, PSNR= 46.1773 dB

Below the Table (5.7) shows the PSNR values for all efficiency test algorithms in both cases without and with attacks.

Table 5.7: PSNR in dB of all Efficiency Test Algorithms with Attacks

No.	Case	1st Alg.	2nd Alg.	3rd Alg.	4th Alg.
1	No Attack	43.4232	44.3791	45.1978	46.1773
2	Ycbcr Version	50.1449	51.2753	52.2784	53.5568
3	Y channel	45.3737	46.5041	47.5072	48.7856
4	JPEG, Q=100	41.2496	41.8608	42.3004	42.7828
5	JPEG, Q=75	36.6566	36.5936	36.6565	36.7848
6	JPEG, Q=50	35.3528	35.2748	35.3050	35.3839
7	JPEG, Q=25	33.5219	33.4408	33.4203	33.4737
8	Gaussian Noise	29.8184	29.8543	29.8843	29.9101
9	Mean Filter	36.9378	36.8312	36.7858	36.8332
10	Resizing 50%	37.6407	37.5500	37.4583	37.5117
11	Rotation 20^0	11.1771	11.1767	11.1764	11.1773
12	Histogram Equalization	14.1952	14.1976	14.2012	14.2064
13	Intensity Adjustment	18.1511	18.1658	18.1736	18.1880
14	Gamma Correction	18.3559	18.3460	18.3416	18.3291
15	Cropping	14.4629	14.4638	14.4645	14.4651
16	Salt & Pepper Noise,	25.1315	25.1709	25.1529	25.1284
17	Motion Blur	32.6509	32.6432	32.6109	32.6110
18	JPEG 2000	35.4620	35.4148	35.3381	35.3573

The Figure (5.87) next, presents how the PSNR value varies through the fourth efficiency test algorithms with both cases without and with attacks.

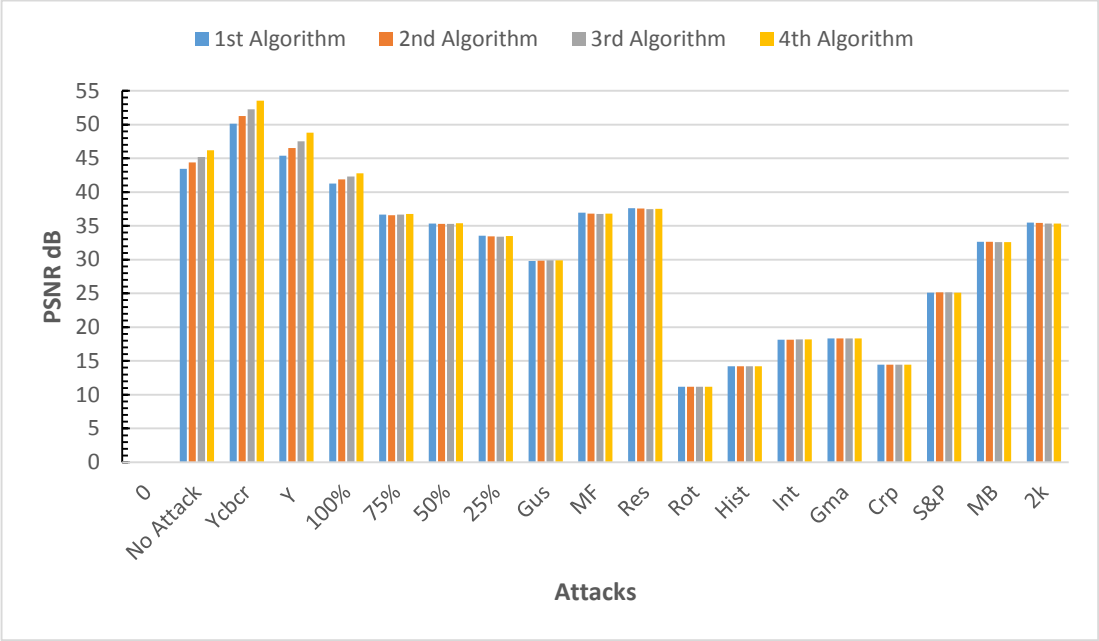


Figure 5.87: PSNR in dB of all Efficiency Test Algorithms with Attacks

The results in the Figure (5.87) again indicating that the deeper the level of DWT decomposition, the higher the PSNR value with respect to the scaling factor.

Next the Table (5.8) presents the correlation coefficients values of watermarks extractions in all efficiency test algorithms with both cases without and with attacks.

Table 5.8: Extracted Watermarks Correlations of all Efficiency Test Algorithms

No.	Case	LL	HL	LH	HH	Level
1	No Attack	1	0.9998	0.9998	0.9998	***1st***
		1	0.9998	0.9998	1	***2nd***
		1	1	1	1	***3rd***
		1	0.9991	1	1	***4th***
2	JPEG, Q=100%	0.9997	0.9308	0.9083	0.9274	***1st***
		1	0.9921	0.9864	0.9914	***2nd***
		1	0.9998	0.9989	0.9991	***3rd***
		1	0.9973	0.9964	0.9964	***4th***
3	JPEG, Q=75%	0.6331	0.0642	0.0529	0.0090	***1st***
		0.9926	0.3559	0.3380	0.2040	***2nd***
		1	0.6496	0.5984	0.5483	***3rd***
		1	0.5522	0.5324	0.5550	***4th***
4	JPEG, Q=50%	0.3064	0.0316	0.0258	0.0027	***1st***
		0.8034	0.1655	0.1655	0.0593	***2nd***
		0.9991	0.3103	0.3245	0.2650	***3rd***
		1	0.3045	0.2891	0.2930	***4th***
5	JPEG, Q=25%	0.1097	0.0074	0.0132	7.8255-e-004	***1st***
		0.3930	0.0493	0.0656	0.0115	***2nd***
		0.6159	0.1224	0.1445	0.0717	***3rd***
		0.8989	0.1462	0.1681	0.1505	***4th***
6	Gaussian Noise	0.3735	0.1252	0.1261	0.1267	***1st***
		0.6778	0.1902	0.1857	0.1819	***2nd***
		0.9518	0.2671	0.2434	0.2569	***3rd***
		0.9973	0.2530	0.2560	0.2577	***4th***
7	Mean Filter	0.3446	0.0060	0.0101-	9.1888-e-004	***1st***
		0.7803	0.2048	0.1790	0.1071	***2nd***
		0.9433	0.5116	0.4523	0.3803	***3rd***
		0.9767	0.6011	0.5316	0.5031	***4th***
8	Crop	0.9236	0.8737	0.8455	0.9210	***1st***
		0.9218	0.8273	0.8129	0.8488	***2nd***
		0.9199	0.8171	0.7898	0.8332	***3rd***
		0.9148	0.7923	0.7733	0.8139	***4th***
9	Histogram Equalization	0.0448	0.5635	0.5080	0.7044	***1st***
		0.0436	0.3725	0.3192	0.4705	***2nd***

Table 5.8 continued.

		0.0460	0.3095	0.2522	0.3639	***3rd***
		0.0307	0.1762	0.1251	0.2377	***4th***
10	Resizing 50%	0.2299	0.0091	0.0075	0.0036	***1st***
		0.5838	0.1234	0.1129	0.0645	***2nd***
		0.7899	0.3081	0.2710	0.2037	***3rd***
		0.8878	0.4296	0.3388	0.3422	***4th***
11	Rotation -20^0	0.7237	0.3141	0.3328	0.2552	***1st***
		0.8726	0.4666	0.4155	0.3724	***2nd***
		0.9098	0.6479	0.5918	0.5854	***3rd***
		0.9093	0.6465	0.6048	0.6240	***4th***
12	Gamma Correction	NaN	0.8145	0.7509	0.9376	***1st***
		NaN	0.6419	0.5755	0.7544	***2nd***
		NaN	0.5329	0.4459	0.6293	***3rd***
		NaN	0.3538	0.2402	0.4370	***4th***
13	Intensity Adjustment	NaN	0.7667	0.6914	0.9170	***1st***
		NaN	0.5512	0.4800	0.6965	***2nd***
		NaN	0.4625	0.3662	0.5496	***3rd***
		NaN	0.2884	0.1958	0.3357	***4th***
14	JPEG 2000	0.0453	0.0168	0.0202	0.0108	***1st***
		0.1414	0.0485	0.0470	0.0247	***2nd***
		0.5081	0.0258	0.0389	0.0115	***3rd***
		0.8083	0.1351	0.1091	0.0961	***4th***
15	Motion Blur	0.0587	0.0448	0.0450	0.0395-	***1st***
		0.1565	0.0581	0.0477	0.0735-	***2nd***
		0.5759	0.1030	0.0913	0.0447-	***3rd***
		0.7705	0.2070	0.1400	0.0954	***4th***
16	Salt & Pepper	0.8187	0.8116	0.8163	0.8118	***1st***
		0.6903	0.5105	0.5129	0.5093	***2nd***
		0.6621	0.2678	0.2775	0.2734	***3rd***
		0.8041	0.1708	0.1630	0.1561	***4th***

Next the Figures (5.88), (5.89), (5.90) and (5.91) show the watermarks extracted images in all efficiency test algorithms with both cases without and with attacks.

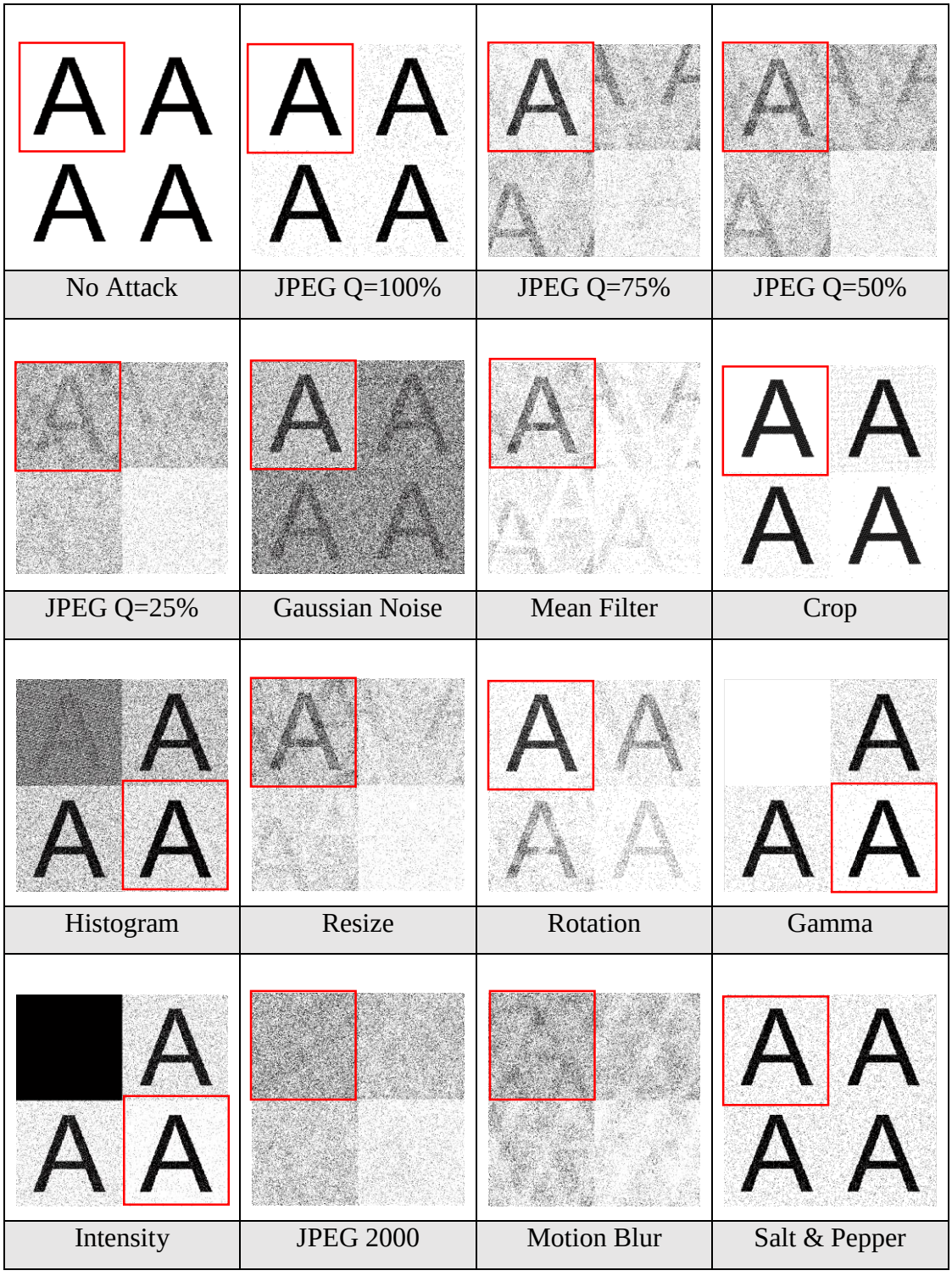


Figure 5.88: Y Channel First Efficiency Test Algorithm extractions

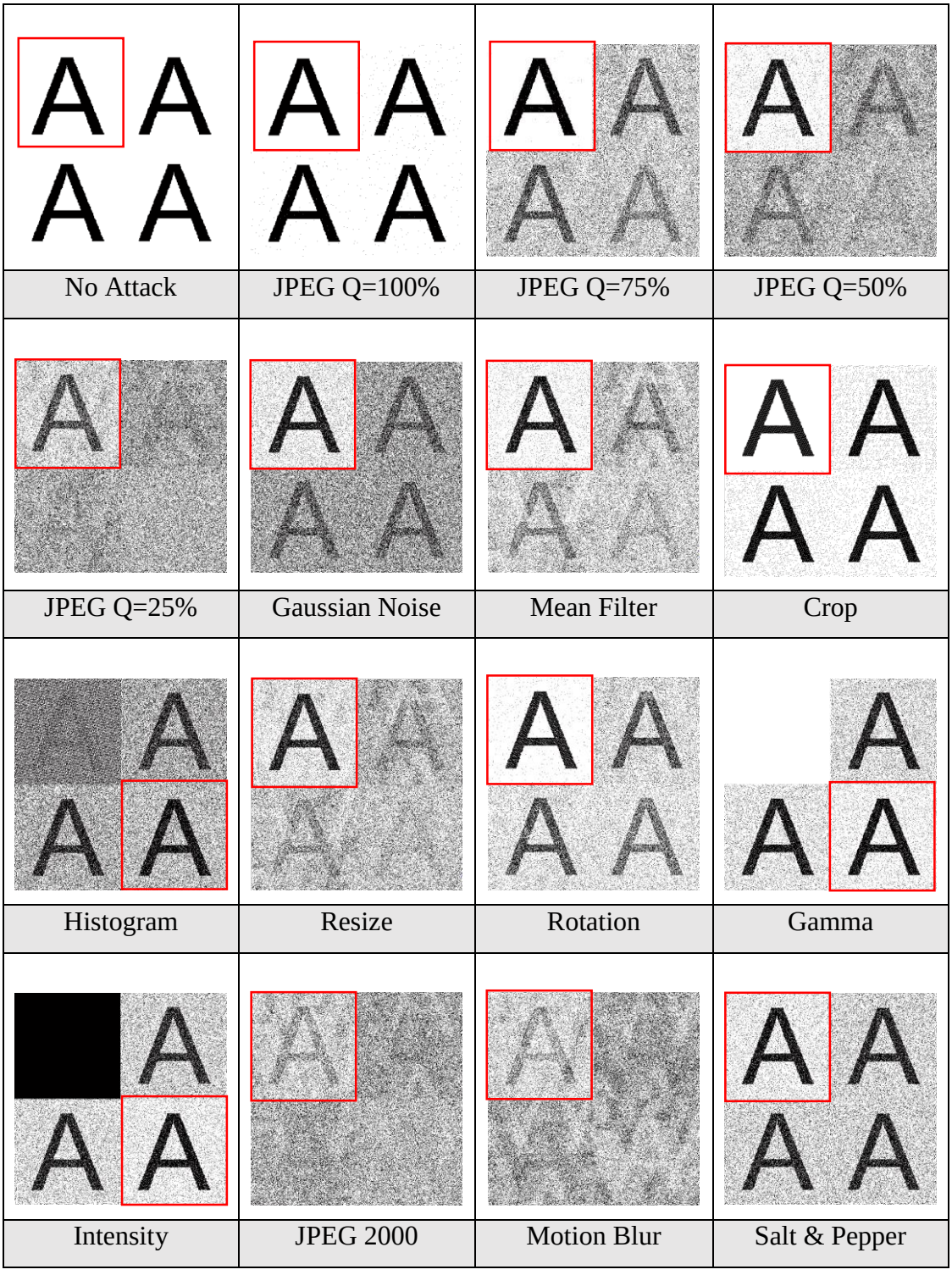


Figure 5.89: Y Channel Second Efficiency Test Algorithm Extractions

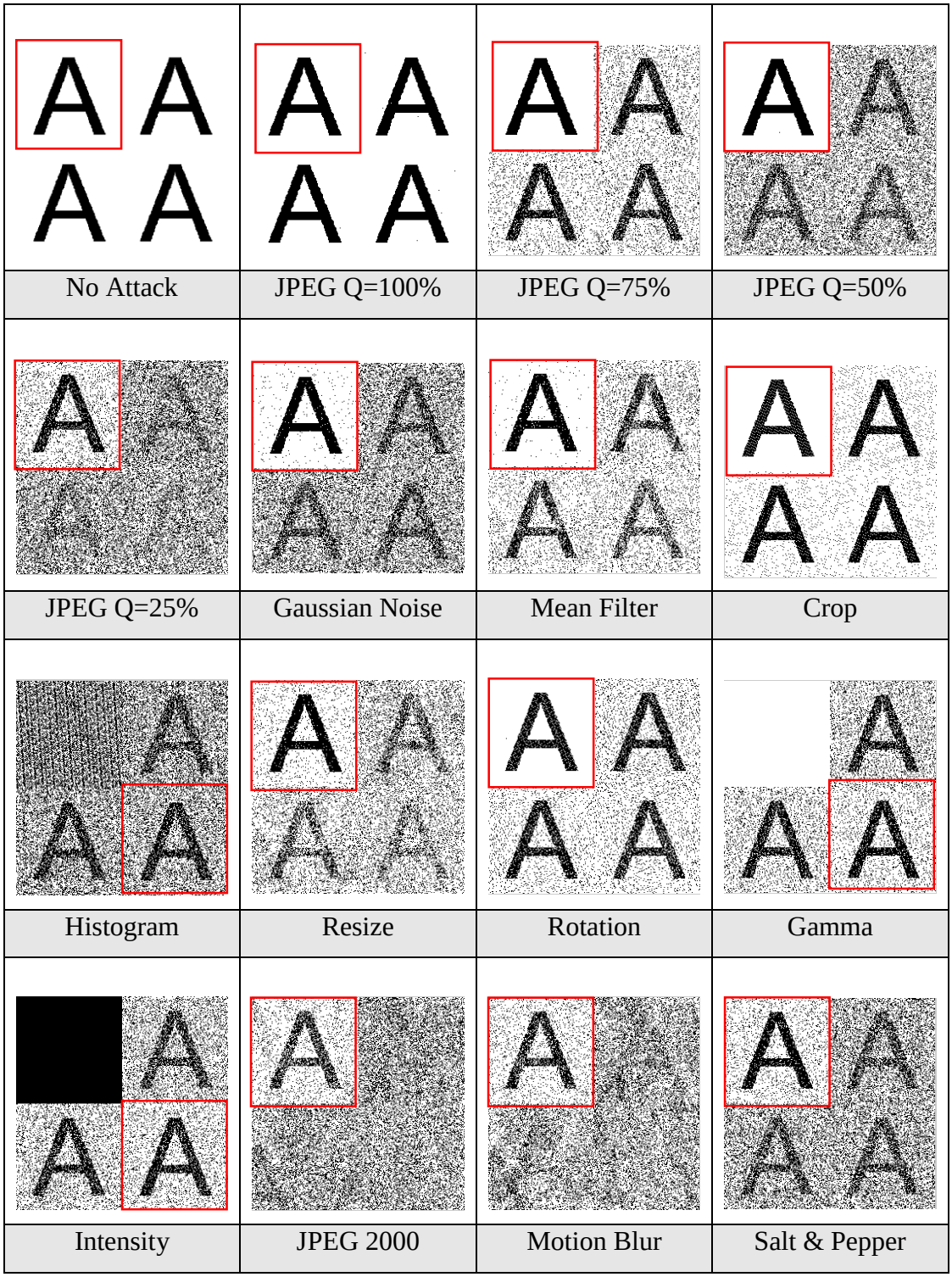


Figure 5.90: Y Channel Third Efficiency Test Algorithm Extractions

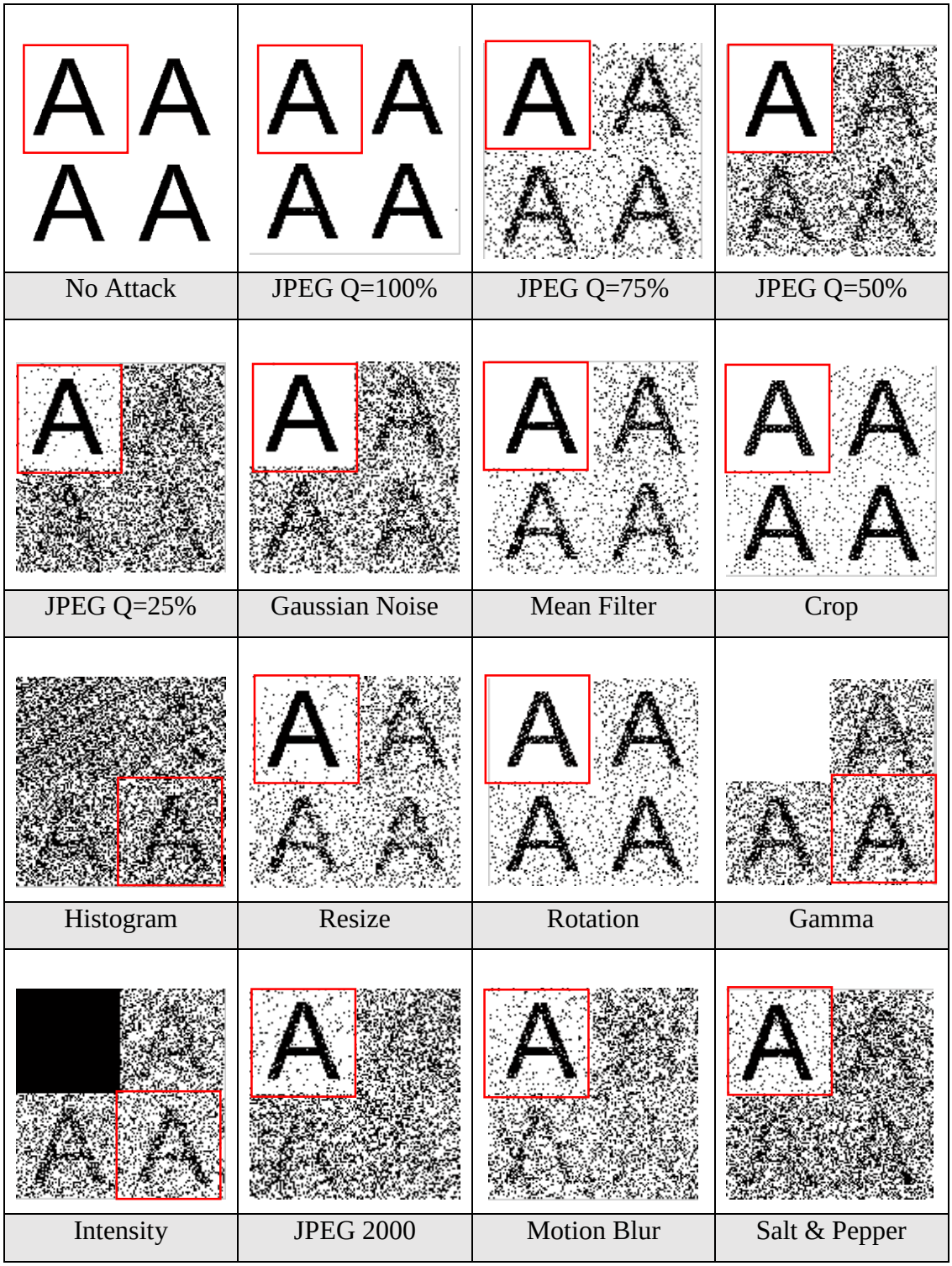


Figure 5.91: Y Channel Fourth Efficiency Test Algorithm Extractions

Below the Figure (5.92) presents how the correlation coefficient value varies through the fourth efficiency test algorithms with both cases without and with attacks

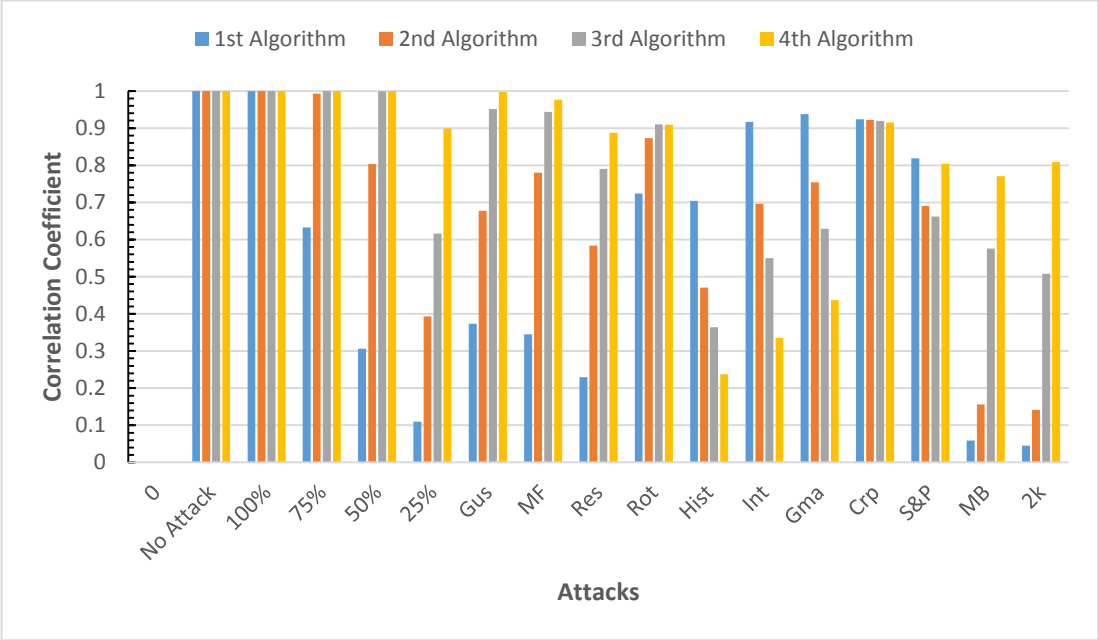


Figure 5.92: Extracted Watermarks Correlations of all Efficiency Test Algorithms with Attacks

The figure above illustrates again that some attacks destroy high frequencies and other destroy low ones, and watermarks must be embedded in the lowest and highest frequencies possible. Also it shows that Y channel is more robust against the JPEG attack than both of green and blue channels and the reason for that is in JPEG the down sampling step only applied on cb and cr channels while the Y channel is not down sampled.

5.3 Optimum Algorithm Results

Below the Figures (5.93), (5.94) and (5.95) show the levels of decompositions used (1st & 2nd levels) and the watermarked image respectively.

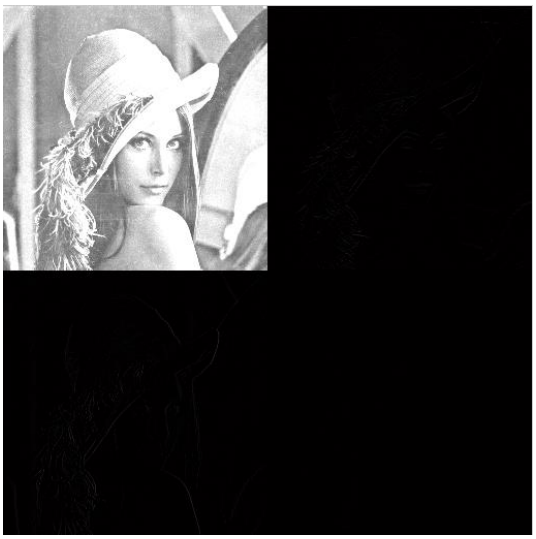


Figure 5.93: First level Decomposition of Blue Channel

Figure 5.94: Fourth level Decomposition of Blue Channel

Figure 5.95: Optimum Algorithm Watermarked Image, PSNR= 46.7582 dB

Next, the Table (5.9) shows the PSNR values of the optimum algorithm without and with attacks.

Table 5.9: PSNR in dB of the Optimum Algorithm with Attacks

No.	Case	Optimum Alg.
1	No Attack	46.7582
2	Blue Channel	41.9870
3	JPEG, Q=100	42.8978
4	JPEG, Q=75	36.7632
5	JPEG, Q=50	35.3635
6	JPEG, Q=25	33.4703
7	Gaussian Noise	29.9213
8	Mean Filter	36.7799
9	Resizing 50%	37.5020
10	Rotation 20^0	11.1773
12	Histogram Equalization	14.1959
13	Intensity Adjustment	18.2181
14	Gamma Correction	18.2966
15	Cropping	14.4654
16	Salt & Pepper Noise,	25.1573
17	Motion Blur	32.5936
18	JPEG 2000	35.3414

Next, Figure (5.96) show how the PSNR value varies among different attacks.

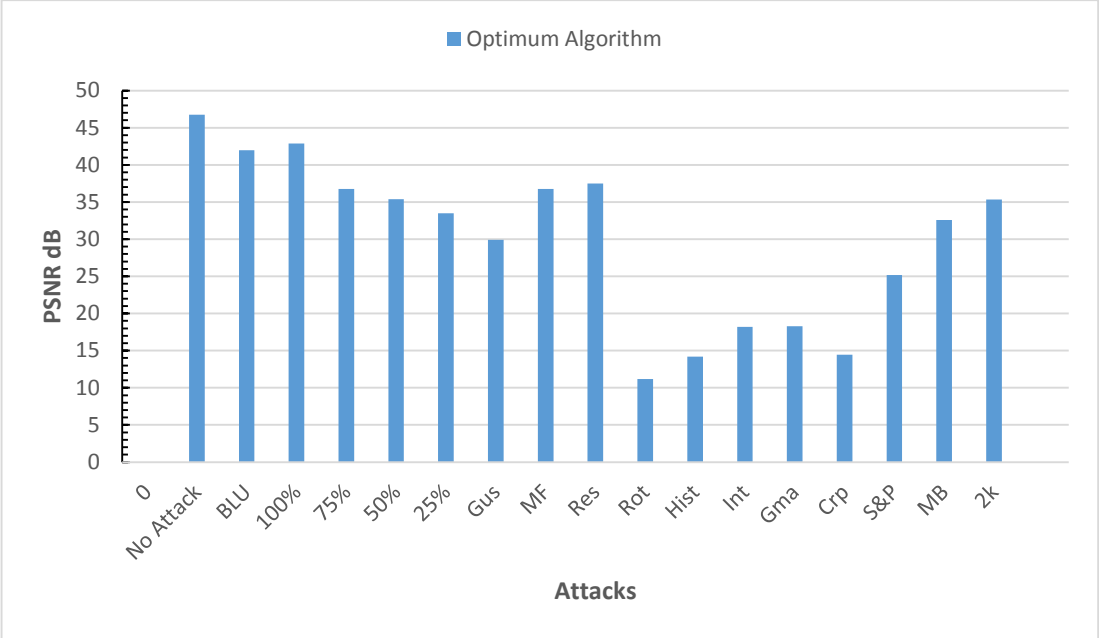


Figure 5.96: Optimum Algorithm PSNR in dB with Attacks

The figure above shows that the PSNR value before attacks is (46.7582 dB) and that is a high value, it also means that there is no distortion in the watermarked image and the embedded watermarks are totally invisible.

Below the Table (5.10) show the correlation coefficient values of the extracted watermarks of the optimum algorithm without and with attacks.

Table 5.10: Optimum Algorithm Extracted Watermarks Correlations with Attacks

N0.	case	LL	HL	LH	HH
1	No Attack	**1**	1	1	1
2	JPEG, Q=100%	**1**	0.0491	0.0866	0.0916
3	JPEG, Q=75%	**1**	0.0096	-0.0067	0.0487
4	JPEG, Q=50%	**0.9729**	0.0195	-0.0167	0.0192
5	JPEG, Q=25%	**0.5320**	0.0183	-0.0231	0.0162
6	Gaussian Noise	**1**	0.1195	0.1196	0.1294
7	Mean Filter	**0.9884**	0.0312	0.0069	-0.0170
8	Cropping	**0.9148**	0.5152	0.4626	0.6603
9	Histogram Equalization	0.0592	0.4821	0.4202	**0.6535**
10	Resizing 50%	**1**	0.0410	-0.0093	0.0175
11	Rotation -20^0	**0.9148**	0.0232	-4.0641e-004	0.0127
12	Gamma Correction	NAN	1	0.9982	**1**
13	Intensity Adjustment	NAN	0.9799	0.9442	**1**
14	JPEG 2000	**0.9803**	0.0326	-0.0140	0.0163
15	Motion Blur	**0.9357**	0.0839	0.0411	0.0745
16	Salt & Pepper	**0.9714**	0.9351	0.9309	0.9215

The Figure (5.97) below shows the extracted watermarks images.

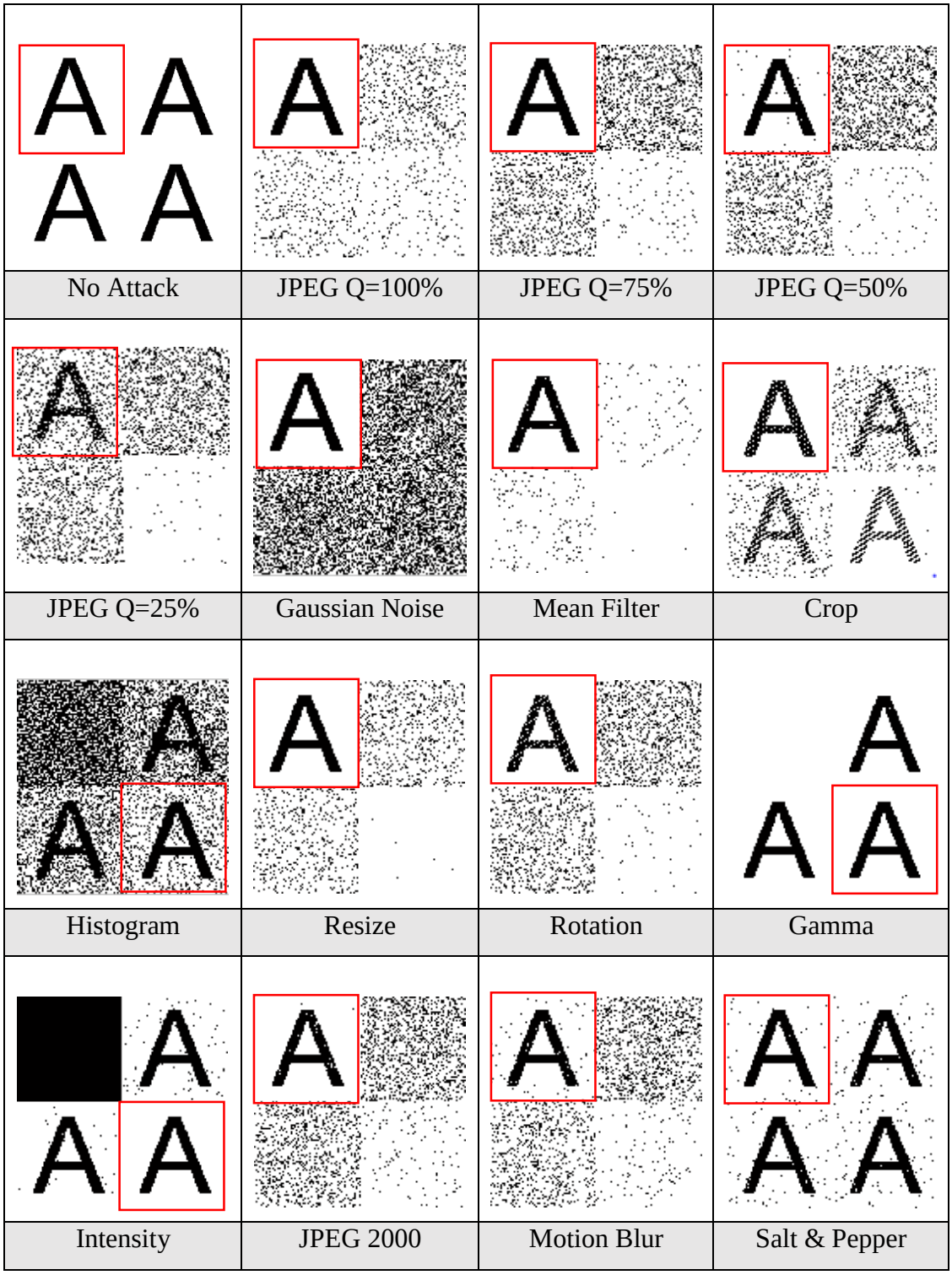


Figure 5.97: Optimum Watermarks Extractions

The Figure (5.98) below shows how the correlation coefficient value varies among different attacks.

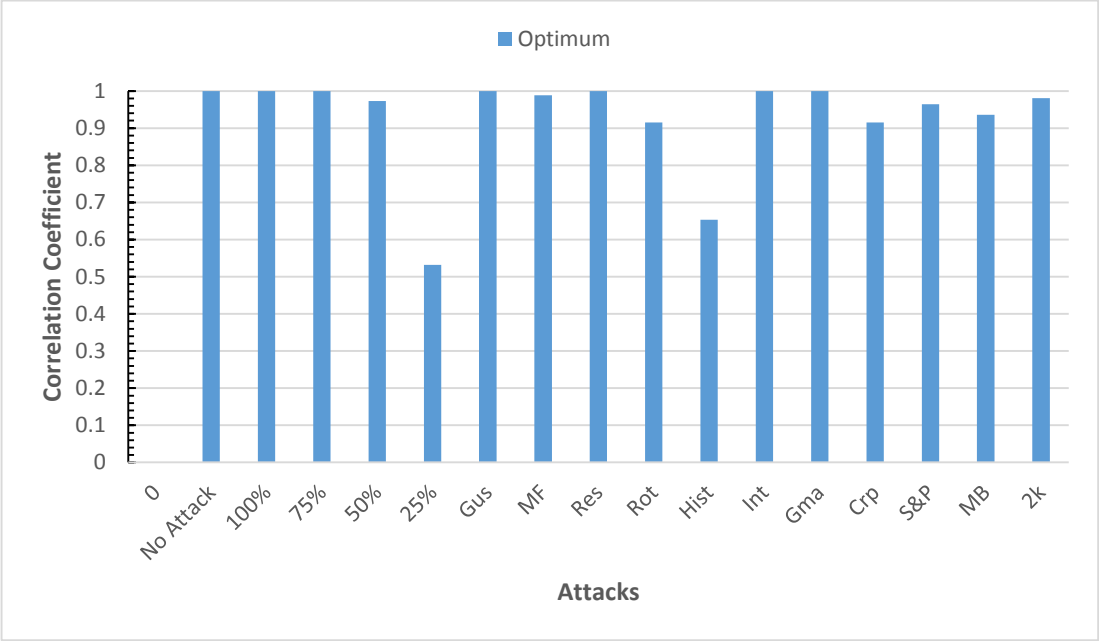


Figure 5.98: Optimum Watermarks Correlations with Attacks

The figure above illustrates that all the correlation coefficient values are above the 0.9 after each attack except for the JPEG 25% and Histogram equalization attacks.

The Table (5.11) shows the PSNR values of different colored images watermarked by the optimum algorithm.

Table 5.11: Optimum Algorithm PSNR in dB for Different Images

Image	**PSNR in dB**
Lena	46.7582
Mandrill	46.6208
Girl	46.7766
Splash	46.5164
Peppers	46.4461
Airplane	46.3395

- Now the Optimum algorithm will be put to harder tests by increasing the effect of two important attacks and those are (Crop attack, Gaussian noise attack). See Figure (5.99), (5.100), (5.101), (5.102), (5.103), (5.104), (5.105) and (5.106) for different attacks and extractions.

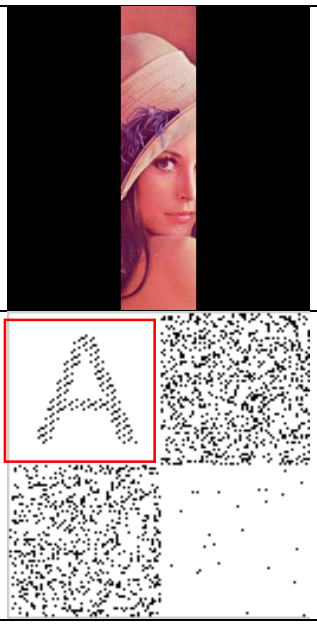
Crop PSNR= 14.4654 dB	Crop at 50% PSNR= 8.3324 dB	Crop at 75% PSNR= 6.5845 dB
		
Correlation= 0.9148	Correlation= 0.6633	Correlation= 0.4450

Figure 5.99: Crop Attack at Different Rations

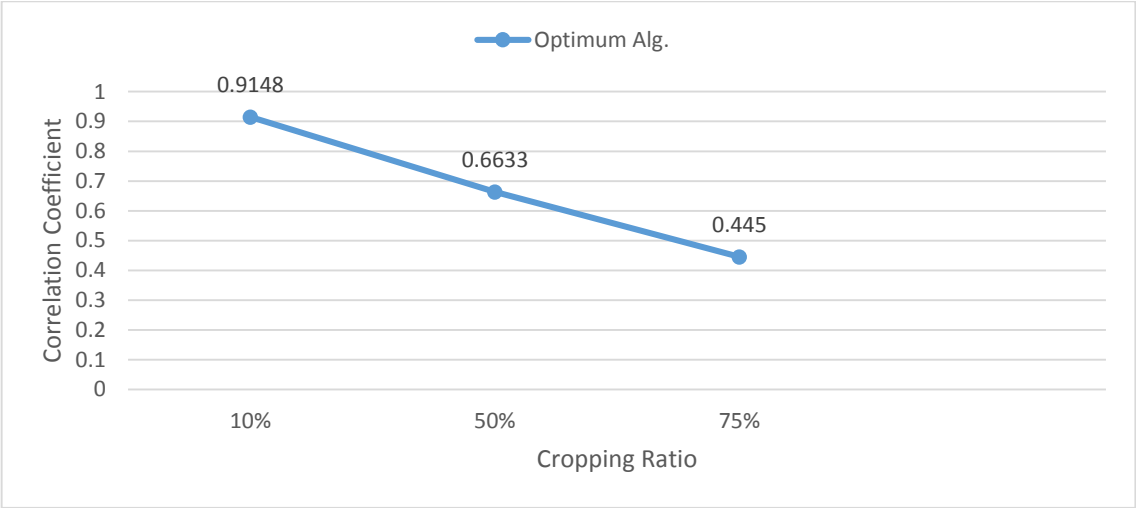


Figure 5.100: Correlation vs. Cropping Ratio

Figure 5.101: Hard Crop 1, PSNR= 5.6567 dB

Figure 5.102: Extracted Watermarks, Correlation of Selected Watermark= 0.6096

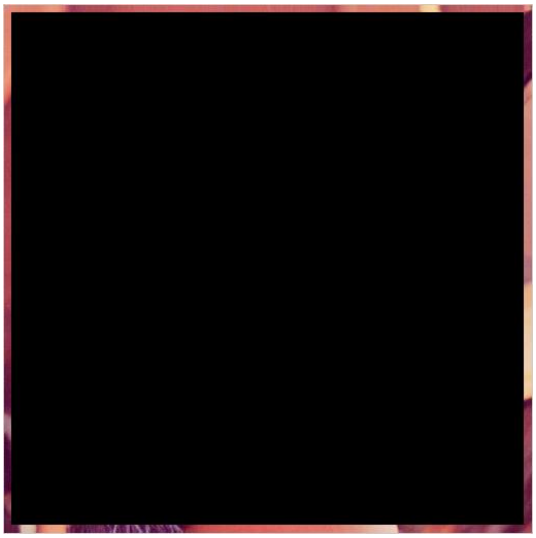


Figure 5.103: Hard Crop 2, PSNR= 5.3887 dB

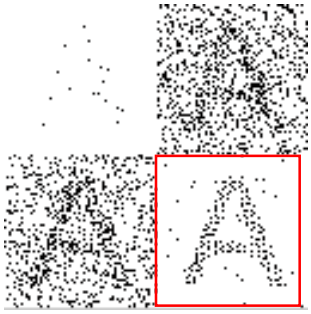


Figure 5.104: Extracted Watermarks, Correlation of Selected Watermark= 0.4230

From the above figures of different cropping attacks, the optimum algorithm managed to keep the watermarks even when there is a large loss of information (pixels)

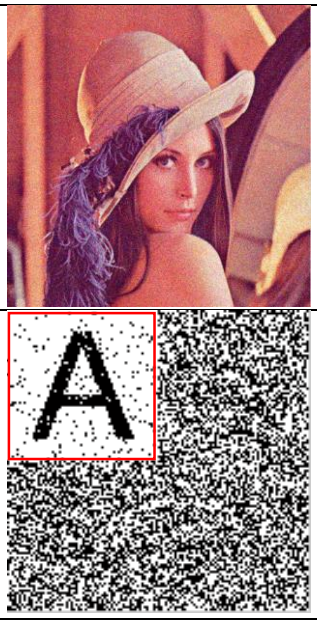
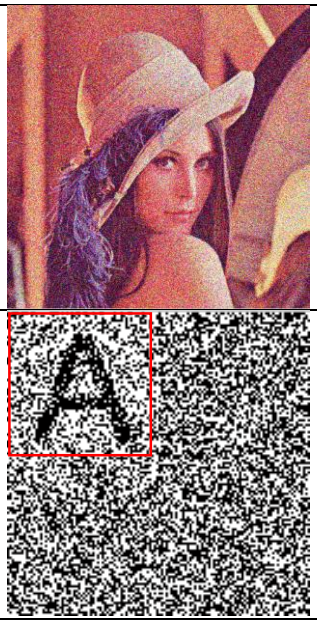
Mean=0; Variance= 0.001 PSNR= 29.9213 dB	Mean=0; Variance= 0.01 PSNR= 20.1925 dB	Mean=0; Variance= 0.05 PSNR= 13.8458 dB
		
Correlation= 1	Correlation= 0.8141	Correlation= 0.3558

Figure 5.105: Gaussian Nosie Attack with Different Variances

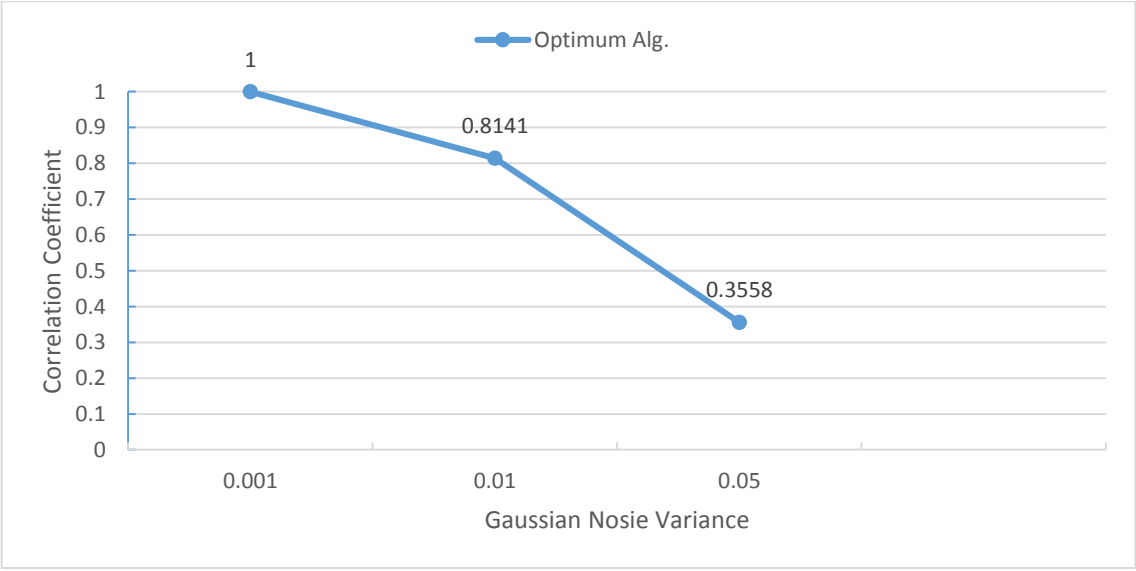


Figure 5.106: Correlation vs. Gaussian Nosie variance

5.3.1 Optimum algorithm vs. dual attacks

This is the final section of this work which presents the results of dual attacks applied on the optimum algorithm, the attacks are a combination of some of the previous attacks each with a Gaussian noise added. See the Figure (5.107) below.

Figure 5.107: Optimum Algorithm Noisy Watermarked Image, Mean=0, Variance=0.01, PSNR= 20.1961 dB

As shown in the above figure the Gaussian noise (with Mean=0, Variance=0.01) added to the watermarked image before applying the attacks, so after applying each attack the result will be a multi-attack or as called in this work a dual attack which is the attack itself plus the Gaussian noise added previously to the watermarked image.

This procedure will test the optimum algorithm robustness. Next the Figures (5.108),(5.109),(5.110), (5.112), (5.112), (5.113), (5.114) and (5.115) show the attacks (JPEG with Q=25%, JPEG 2000, Mean Filter, Resizing, Rotation, Crop, Salt & Pepper, and Motion Blur) respectively.

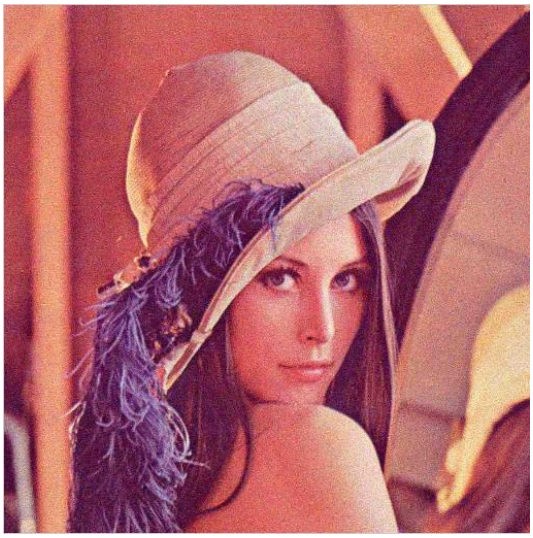


Figure 5.108: JPEG, Q=25%, PSNR= 26.3874 dB

Figure 5.109: JPEG 2000, PSNR= 18.4732 dB

Figure 5.110: Salt & Pepper, PSNR= 19.0360 dB

Figure 5.111: Resizing at 50%, PSNR= 31.4692 dB

Figure 5.112: Mean Filter, PSNR=28.8921 dB

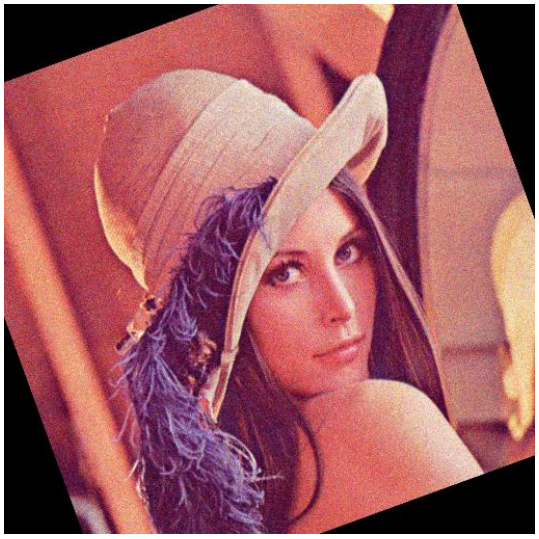


Figure 5.113: Rotation -20 Degrees, PSNR=10.9991 dB

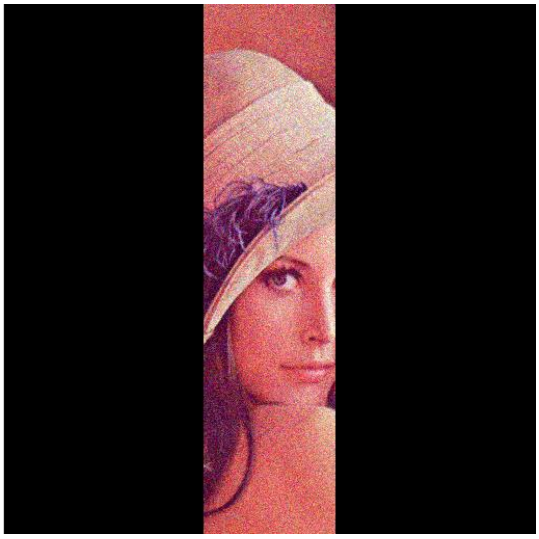


Figure 5.114: Cropping at 75%, PNSR= 6.5377 dB

Figure 5.115: Motion Blurred, PSNR=29.1967 dB

The Figure (5.116) below shows the extracted watermarks images with their correlation values after the dual attacks.

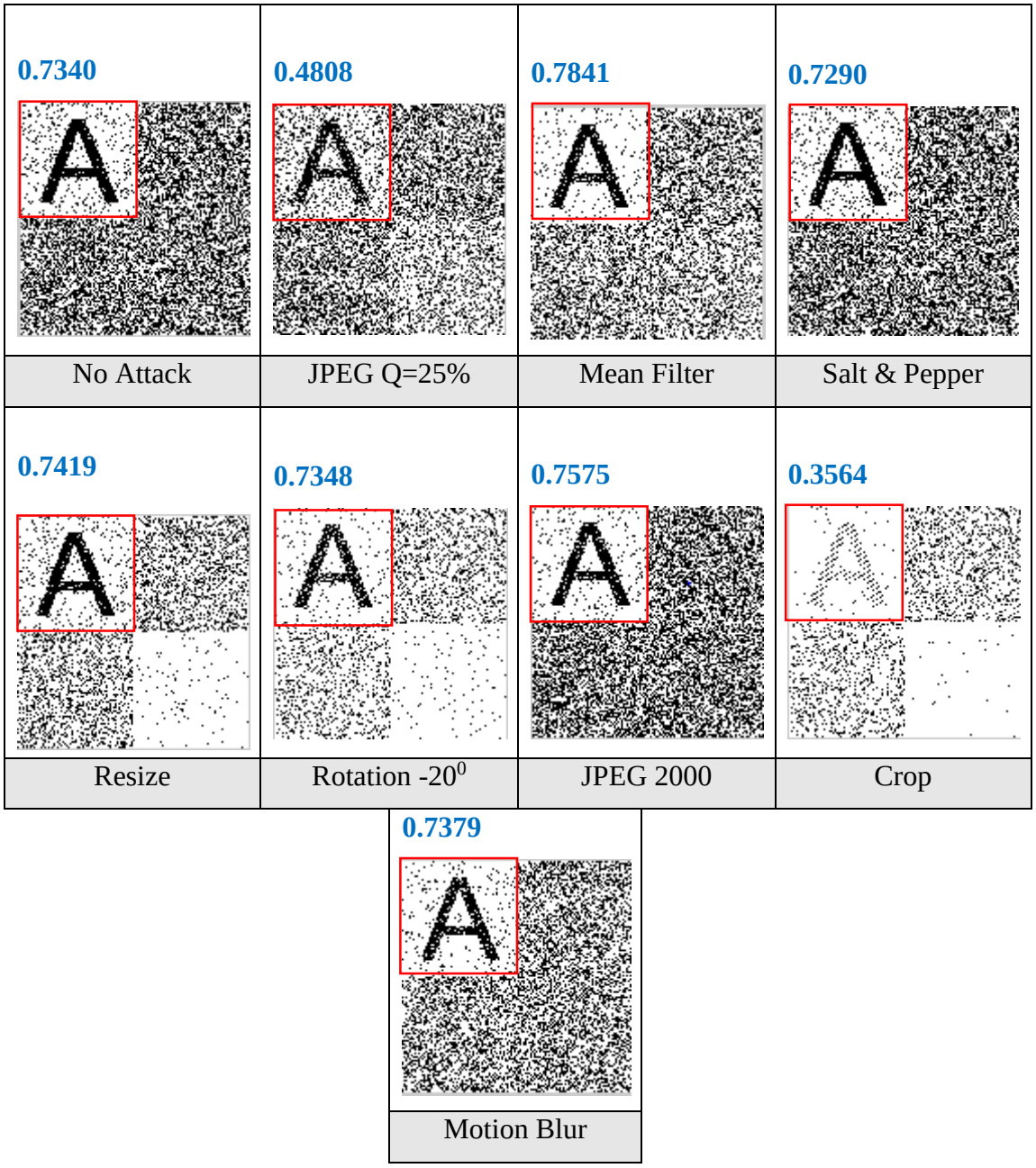


Figure 5.116: Optimum Algorithm Multiple Dual Attacks Extractions with Correlations Values In Blue Color

CHAPTER SIX

CONCLUSIONS AND FUTURE WORK

6.1 Conclusions

The need for digital watermarking as electronic distribution of copyright material becomes more prevalent. Various applications of watermarks have been introduced and necessary requirements of such watermarks have also been introduced. An overview of existing watermarking techniques and attacks has been given in this work. In this thesis also mentioned that the discrete wavelet transform (DWT) resembles the human visual system and allows a better image adaptation than the Discrete Cosine Transform (DCT). In this work fifteen important attacks were applied over the whole algorithms. The attacks were used for the purpose of robustness test.

From the results of all the efficiency test algorithms applied, several and important conclusions were conducted:

- The deeper the DWT level of decomposition in which the watermarks are embedded into, the higher the PSNR value gets between the original and the watermarked image with respect to scaling factor.

- The watermarks embedded in middle and high frequencies of the first efficiency test algorithm (1^{st} level of DWT decomposition) proved high robustness against the attacks (Histogram equalization, Gamma correction, and Intensify Adjustment) and recorded their higher correlation values across the four test algorithms.

- The watermarks embedded in the low frequency of the fourth efficiency test algorithm (4^{th} level of DWT decomposition) proved high robustness against the Attacks (JPEG, JPEG 2000, Gaussian Noise, Salt & Pepper Noise, Mean Filter,

Resizing, Rotation, and Motion Blur) and recorded their higher correlation values across the four test algorithms.

- Some attacks destroy the middle and high frequency components of the image and others destroy the low frequency components. And that lead us to think of an algorithm that embeds the 4 watermarks in the lowest and highest frequency components of the image and it can be done by using more than one level of DWT decomposition in the same algorithm, and that's our optimum algorithm.

- the Optimum algorithm watermark extractions in figure (5.98) show that the Optimum algorithm gave at least one successful watermark extraction with correlation value of more than 0.9 after each attack except for the JPEG with Quality factor of 25% and the Histogram Equalization attacks where the correlations of the extracted watermarks were under 0.9.

- The Dual attacks and the hard crop attack are two new attacks and never been used as far as we checked, and the watermark extractions after these attacks proved the algorithm robustness and reliability against vicious attacks even if there was a huge loss of information (pixels).

- The Optimum algorithm criteria which focused on the multi-selection of the frequency sub-bands from more than one level of DWT decomposition (LL4, HL1, LH1 and HH1), and the four watermarks embedding as an extraction alternatives besides the use of the Arnold's cat map scrambling of the watermarks proved to be as an efficient and reliable watermarking system.

Comparing the optimum algorithm with the works in the literature review, the comparison table is below:

Table 6.1: Optimum Algorithm PSNR in dB of Lena Image vs. Some Other Publications

#	Algorithm	PSNR in dB
1	Optimum Algorithm (Colored Lena)	46.7582
2	P. Kumhom et al. [15] (Gray scale Lena)	46.77
3	Nagaraj Dharwadkar and B.B.Amberker [16] (Colored Lena)	57.71
4	Nasseer M. Basheer and Shaymaa S. Abdulsalam [21] (Gray scale Lena)	45.47
5	YiweiWang et al. [11] (Gray Scale Lena)	42.5

6.2 Future Work

According to the results of this study, the optimum algorithm presented in this work is a non-blind watermarking technique. It may be useful to extend it straightforwardly to video data. But with a blind watermarking* technique that doesn't require the original cover data for extracting the watermarks.

REFERENCES

[1] **RAMANA, K. V.** et. al."A Randomized Secure Data Hiding Algorithm Using File Hybridization for Information Security," *International Journal on Computer Science and Engineering (IJCSE),* vol. Vol. 3, pp. 1878-1889, 2011.

[2] **ALAM, F. I., BAPPEE F. K. AND KHONDKER**, **F. U. A.** "An Investigation into Encrypted Message Hiding Through Images Using LSB," *International Journal of Engineering Science and Technology (IJEST),* vol. 3 No. 2, pp. 948-960, 2011.

[3] **LEE, C.W. AND TSAI**, **W.H.** "A Lossless Large-volume Data Hiding Method Based on Histogram Shifting Using an Optimal Hierarchical Block Division Scheme," *Journal of Information Science and engineering,* vol. 27, pp. 1265-1282, 2011.

[4] **PERWEJ, Y., PARWEJ, F. AND PERWEJ**, **A.** "An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection," *The International Journal of Multimedia & Its Applications (IJMA),* Vols. 4,No.2, pp. 21-38, 2012.

[5] **HUANG, HC. AND FANG**, **WC.** "Techniques and applications of intelligent multimedia data hiding" *Springer Science,* vol. 44, pp. 241-251, 2010.

[6] **PARTHIBAN, V., GANESAN**, **R.** "Hybrid Watermarking Scheme for Digital Images" *Journal of Computer Applications,* pp. 85-95, 2012.

[7] **TANAKA, K., NAKAMURA, Y. AND MATSUI**, **K.** "Embedding Secret Information Into a Dithered Multilevel Image," *In Proc. of IEEE Military Communications Conference,* vol. 1, pp. 216- 220, 1990.

[8] **TRIKLE, A., RANKIN, G. AND SCHYDEL, R.** "Electronic Watermark," *In Proc. DICTA 93, Australia,* 1993.

[9] **KUNDUR, D. AND HATZINAKOS**, **D.** "Digital Watermarking Using Multiresolution Wavelet Decomposition," *Acoustics, Speech and Signal Processing,*

1998. Proceedings of the 1998 IEEE International Conference on, vol. 5, pp. 2969-2972 , 1998.

[10] **LOO, P. AND KINGSBURY**, **N.** "Digital Watermarking Using Complex Wavelets," *Image Processing, 2000. Proceedings. 2000 International Conference on,* vol. 3, pp. 29-32, 2000.

[11] **YIWEIWANG, D., DOHERTY, J. F. AND DYCK**, **R. E. V.** "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images," *IEEE Transactions on Image Processing,* vol. 11, 2002.

[12] **GILANI, S.A.M., KOSTOPOULOS, I. AND SKODRAS**, **A.N.** "Color Image-Adaptive Watermarking," *Digital Signal Processing, 2002. DSP 2002. 2002 14th International Conference on* , vol. 2, pp. 721 -724, 2002.

[13] **HUANG Z. Q. AND JIANG**, **Z.** "Image Ownership Verification Via Private Pattern and Watermarking Wavelet Filters," *Digital Image Computing: Techniques and Applications Sun C., Talbot H., Ourselin S. and Adriaansen T. (Eds.), Sydney,* 2003.

[14] **TAOA, P. AND ESKICIOGLU**, **A. M.** "A robust multiple watermarking scheme in the Discrete Wavelet Transform domain," *Internet Multimedia Management Systems V. Edited by Smith, John R.; Zhang, Tong; Panchanathan, Sethuraman. Proceedings of the SPIE,* vol. 5601, pp. 133-144, 2004.

[15] **KUMHOM, P. AND CHAMNONGTHAI**, **K.** "Image Watermarking Based on Wavelet Packet Transform With Best Tree," *ECTI TRANSACTIONS ON ELECTRICAL ENG., ELECTRONICS, AND COMMUNICATIONS,* vol. 2, 2004.

[16] **DHARWADKAR, N. V. AND AMBERKER**, **B.B.**"Watermarking Scheme for Color Images using Wavelet Transform based Texture Properties and Secret Sharing," *International Journal of Information and Communication Engineering,* pp. 94-101, 2010.

[17] **AYUBI, J.** et. al., "A Chaos Based Blind Digital Image Watermarking in The Wavelet Transform Domain," *IJCSI International Journal of Computer Science Issues,* vol. 8, pp. 192-199, 2011.

[18] **KHALIFA , A. AND HAMAD**, **S.** "A Robust Non-blind Algorithm for Watermarking Color Images using Multi-resolution Wavelet Decomposition," *International Journal of Computer Applications,* vol. 37, 2012.

[19] **KUMAR.P, K., REDDY, M.Y. AND OMPRAKASH**, "Digital image watermarking using wavelet technique," *World Journal of Science and Technology,* pp. 6-9, 2012.

[20] **GUPTA**, **T.** "Image Watermarking Using discrete Wavelet Transform," *International Journal of Data & Network Security,* vol. 1, 2012.

[21] **BASHEER, N. M. AND ABDULSALAM**, **S. S.** "Digital Image Watermarking Scheme Using Discrete Wavelet Transform Domain Quantization and Genetic Algorithm," *Fifth Scientific Conference Information Technology,* 2013.

[22] **HSIEN, E. F.**, "Literature Survey on Digital Image Watermarking," *EE381K-Multidimensional Signal Processing,* 1998.

[23] **JOHNSON,**, **N.** "Information Hiding: Steganography and Watermarking-Attacks and Countermeasure," *Kluwer Academic Publishers,* 2000.

[24] **LOO**, **P.** "Digital Watermarking Using Complex Wavelets," *Ph. D. Thesis, University of Cambridge,* vol. 3, 2002.

[25] **KARZENBEISSER, P. F. S.**, "Information Hiding Techniques for Steganography and Digital Watermarking," *Artech House,* 2000.

[26] **COX, I. J. , MILLER, M. AND BLOOM**, **J.** "Watermarking Applications and their Properties," *Information Technology: Coding and Computing, 2000. Proceedings. International Conference on* , pp. 6-10, 2000.

[27] **SU, J. K., HARTUNG, F. AND GIROD**, **B.** "Digital Watermarking of Text Image, and Video Documents," *Elsevier Preprint,* 1999.

[28] **BENDER, W.** et. al. ,"Techniques for Data Hiding" *IBM Systems Journal,* vol. 35, 1996.

[29] **BUSCH, C., FUNK, W. AND WOLTHUSEN, S.**, "Digital Watermarking: From Concepts to Real-time Video Applications," *Computer Graphics and Applications, IEEE* , vol. 19, pp. 25-35, 1999.

[30] **SOWERS, S. AND YOUSSEF**, **A.** "Testing Digital Watermark Resistance to Destruction," *Springer-Verlag Berlin Heidelberg,* pp. 239-257, 1998.

[31] **QIAO, L. AND NAHRSTEDT**, **K.** "Watermarking Schemes and Protocols for Protecting Rightful Ownership and Customer Rights," *National Science Foundation Career Grant,* 1999.

[32] **J. FRIDRICH**, "Methods for detecting Changes in Digital Images," *In Proc. of IEEE Signal Processing,* 1998.

[33] **KUNDUR, D. AND HATZINAKOS**, **D.** "Towards a Telltale Watermarking Techniques for Tamper-Proofing," *Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on ,* vol. 2, pp. 409- 413 , 1998.

[34] **REY, C. AND DUGELAY**, **J.L.** "Blind detection of Malicious Alteration in Still Images using Robust Watermarks," *IEE, Savoy Place, London WCPR OBL, UK,* 2000.

[35] **DARMSTAEDTER, V.,** et. al. , "Low Cost Spatial Watermarking," 2001.

[36] **SHOEMAKER**, **C.** "Hidden Bits: A Survey of Techniques for Digital Watermarking," 2002.

[37] **HERNANDEZ, J. AND GONZALEZ**, **F.** "Shedding More Lights on Image Watermarks," *Springer,* pp. 191-207, 1998.

[38] **TZENG, J., HWANG, W.L. AND CHERN**, **I.L.** "Enhancing Image Watermarking Methods with/without Reference Images by Optimization on Second-Order Statistics," *IEEE Transaction on Image Processing,* vol. 11, pp. 771-782 , 2002.

[39] **NIKOLAIDIS, N. AND PITAS**, **I.** "Robust Image Watermarking in the Spatial Domain," *Elsevier Science B.V.,* pp. 385-403, 1998.

[40] **HARTUNG, F., SU, J. AND GIROD**, **B.** "Spread Spectrum Watermarking: Malicious Attacks and Counterattacks," *Signal Processing (Special Issue on Watermarking),* 1999.

[41] **SOLACHIDIS, V. AND PITAS**, **I.** "Circularly Symmetric Watermark Embedding in 2-D DFT Domain," *IEEE TRANSACTIONS ON IMAGE PROCESSING,* vol. 10, 2001.

[42] **BARNI, M. ,** et. al. "A DCT-domain system for robust image watermarking," *Elsevier Science B.V., Signal Processing,* pp. 357-372, 1998.

[43] **GONZALEZ R**., **W. R.** Digital Image Processing, Prentice-Hall, 2002.

[44] **TAN, L. AND JIANG**, **J.** Digital Signal Processing : Fundamentals and Applications, second ed., Academic Press, Elsevier Inc., 2013.

[45] **C. J. G. N. GEORGE M.**, "Spread Spectrum Spatial and Spectral Watermarking for Images and Video," *in Proc. 1999 IEEE Can.Workshop in Information Theory,* 1999.

[46] **GEORGE, M., CHOUINARD, J.Y. AND GEORGANAS**, **N.** "Digital Watermarking of Images and Video Using Direct Sequence Spread Spectrum Techniques," *Proceedings of the 1999 IEEE Canadian Conference on Electrical and Computer Engineering,* 1999.

[47] **COX, I. J.** et. al., "Secure Spread Spectrum Watermarking for Multimedia," *IEEE TRANSACTIONS ON IMAGE PROCESSING,* vol. 6, pp. 1673-1687, 1997.

[48] **SWANSON, M., ZHU, B. AND TEWFIK**, **A.** "Transparent Robust Image Watermarking," *Image Processing, 1996. Proceedings., International Conference on ,* vol. 3, pp. 211- 214, 1996.

[49] **KOCH , E. AND ZHAO**, **J.** "Towards Robust and Hidden Image Copyright Labeling," *IEEE Workshop on Nonlinear Signal and Image Processing,* 1995.

[50] **ZHAO, J. AND KOCH**, **E.** "Embedding Robust Labels into Images for Copyright Protection," *In: Proc. of the Int. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, Vienna,* 1995.

[51] **WAH**, **W.** "Image Watermarking and Data Hiding Techniques," *Ph. D., Thesis,Hong Kong University,* 2003.

[52] **HSU, C.T., AND WU**, **J.L.**"Hidden Digital Watermarks in Images," *Image Processing, IEEE Transactions on ,* vol. 8, pp. 58- 68 , 1999.

[53] **SUHAIL, M. AND OBAIDAT**, **M.** "Digital Watermarking-based DCT and JPEG Model," *IEEE Transaction on Instrumentation and measurement,* vol. 52, pp. 1640-1647, 2003.

[54] **MALLAT**, **S.** A Wavelet Tour of Signal Processing, Third Edition ed., S. G. Mallat, 1998.

[55] **PINSKY**, **A.** "Introduction to Fourier Analysis and Wavelets," *Brooks/Cole*, 2000.

[56] **POLIKAR**, **R.**"The Wavelet Tutorial," 2002.

[57] **XIA, X.G., BONCELET, C. G. AND ARCE**, **G. R.** "Wavelet transform based watermark for digital images," *The International Online Journal of Optics*, vol. 3, pp. 497-511, 1998.

[58] **GONZALEZ,R. AND WINTZ P.**, Digital Image Processing, Addison-Wesley Publishing Co., 1977.

[59] **ABDULAZIZ, N. AND PANG**, **K.** "Robust Data Hiding for Images," *Communication Technology Proceedings, 2000. WCC - ICCT 2000. International Conference on*, vol. 1, pp. 380- 383, 1998.

[60] **MECHOLSKY**, **N.** "Cat Map," Chaos @ UMD, 2009. [Online]. Available: http://www.chaos.umd.edu/misc/catmap.html.

[61] **WANG, H.Q., HAO, J.C. AND FU-MING**, **CUI, F.M.** "Color Image Watermarking Algorithm Based on the Arnold Transform," *Communications and Mobile Computing (CMC), International Conference on* , vol. 1, pp. 66 - 69, 2010.

[62] **FRIDRICH**, **J.** "Applications of Data Hiding in Digital Images," *Tutorial for the ISPACS'98 Conference in Melbourne, Australia,* 1998.

[63] **LACY, J.** et al. "Intellectual Property Protection Systems and Digital Watermarking," *Springer-Verlag Berlin Heidelberg*, 1998.

[64] **KUTTER, M. , JORDAN, F. AND BOSSEN**, **F.** "Digital signature of Color Images Using Amplitude Modulation," *in Proc. SPIE Electronic Imaging 97, Storage and Retrieval for Image and Video Databases*, pp. 518-526, 1997.

CURRICULUM VITAE

Surname, Name: Mohammed, Ahmed
Nationality: Iraqi
Date and Place of Birth: 24 January 1988, Baghdad
Marital Status: Married
Phone: +9647702944867
Email: eng_47@yahoo.com

EDUCATION

Degree	Institution	Year of Graduation
BS	Al-Hadbaa University College	2009
High School	Al-Mansour High School	2005

WORK EXPERIENCE

Year	Place	Enrollment
2009-Present	Al-Hadbaa University College / Tech. Comp. Eng. Dept.	Lab Instructor
2007	Al-Akmaar Company	Programming and Operating GPS devices
2005-2006	Al-Tayf Company / Internet Provider	Programmer

FOREIGN LANGUAGES

Fluent American-English, little French.

HOBBIES

Soccer, Swimming, BJJ, Cars