UNIVERSITI PUTRA MALAYSIA

DESIGN OF ROBUST AND FRAGILE IMAGE WATERMARKING SYSTEM FOR COPYRIGHT PROTECTION AND AUTHENTICATION USING LIFTING WAVELET TRANSFORM AND BIVARIATE EMPIRICAL MODE DECOMPOSITION TECHNIQUES

NIDAA HASAN ABBAS

FK 2017 47

DESIGN OF ROBUST AND FRAGILE IMAGE WATERMARKING SYSTEM FOR COPYRIGHT PROTECTION AND AUTHENTICATION USING LIFTING WAVELET TRANSFORM AND BIVARIATE EMPIRICAL MODE DECOMPOSITION TECHNIQUES

By

NIDAA HASAN ABBAS

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Doctor of Philosophy

April 2017

DEDICATION

To my lovely husband, my dearest parents, sisters and brothers for their endless support and encouragement.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the Degree of Doctor of Philosophy

DESIGN OF ROBUST AND FRAGILE IMAGE WATERMARKING SYSTEM FOR COPYRIGHT PROTECTION AND AUTHENTICATION USING LIFTING WAVELET TRANSFORM AND BIVARIATE EMPIRICAL MODE DECOMPOSITION TECHNIQUES

By

NIDAA HASAN ABBAS

April 2017

Chairman : Associate Professor Sharifah Mumtazah bt Syed Ahmad Abdul Rahman, PhD
Faculty : Engineering

In this thesis, a dual purpose watermarking system is designed that satisfy both robustness and fragility, and thus combining copyright protection and tamper proofing simultaneously without significantly degrading each other. The proposed copyright scheme is new and effective. Two transforms which are; lifting wavelet transform (LWT) and bivariate empirical mode decomposition (BEMD), are used to decompose the original image to provide flexibility in choosing the robust frequency subband of the original image. LWT, is chosen as it is fast and keeps the integrity of the retrieved watermark. While BEMD could sift the image from the most robust to the least sensitive (fragile) frequency bands. This property is exploited in this thesis to embed the watermark in the robust part of BEMD which is the residue (*r*).

To ensure the integrity and authenticity of digital images, a wide variety of authentication schemes have been proposed in the literature to detect image tampering. However, most of the existing schemes either fail to address this issue or use inaccurate method to evaluate the system performance. For this reason, a procedure to generate a new type of fragile watermark that can detect any tampering is developed in this thesis. The most sensitive subbands of the BEMD which are Intrinsic Mode Function (*IMFs)* are used to derive and embed the watermark bits in the frequency domain and further processed to increase the security and the ability to detect any alteration. Another watermark is generated and embedded in the spatial domain using block wise method and the Least Significant Bits (LSBs) insertion.

The dual-purpose scheme is obtained by combining both the copyright protection and image authentication schemes and has been subjected to robust and fragile attacks. The results demonstrated that the performance of the scheme remains at par or only degrade at an acceptable level after inserting the dual watermarks. The obtained visual quality, Peak Signal to Noise Ratio (*PSNR*), is greater than 48dB and the Normalised Cross Correlation (*NCC*) is greater than 0.97 while the tampering detection rate (*AV*) is greater than 94%.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk Ijazah Doktar Fasafah

REKABENTUK SISTEM *WATERMARKING* IMEJ YANG TEGUH DAN RAPUH UNTUK PERLINDUNGAN HAKCIPTA DAN PENGESAHAN DENGAN MENGGUNAKAN TEKNIK LIFTING *WAVELET TRANSFORM* DAN *BI EMPIRICAL MODE DECOMPOSITION*

Oleh

NIDAA HASAN ABBAS

April 2017

Pengerusi : Profesor Madya Sharifah Mumtazah bt Syed Ahmad Abdul Rahman, PhD
Fakulti : Kejuruteraan

Kebanyakkan sistem *watermarking* imej sejenis bertujuan untuk mencapai satu matlamat sahaja, samaada untuk pengesanan pemalsuan atau perlindungan hak cipta. Namun bagi sesetengah aplikasi yang kritikal seperti perdagangan elektronik, pembeli mahu memastikan bahawa imej yang diterima adalah asli dihasilkan oleh pemilik dan tidak diubahsuai. Ini telah membawa kepada pengenalan algoritma pelbagai tujuan *watermark*, dengan objektif utama untuk mencapai kedua-dua matlamat perlinduangan hakcipta dan pengesanan pengubahsuaian pada masa yang sama.

Di dalam tesis ini, dua tujuan sistem *watermarking* telah direkabentuk yang memenuhi kedua-dua keteguhan dan kerapuhan, seterusnya mengabungkan perlindungan hak cipta dan pengesanan pengubahsuaian pada masa yang sama tanpa melemahkan satu sama lain. Skema *watermarking* yang dicadangkan adalah baru dan berkesan. Dua jelmaan iaitu; *lifting wavelet transform (LWT)* dan *bivariate empirical mode decomposition (BEMD*), telah digunakan untuk menguraikan imej asli bagi memberikan fleksibiliti memilih frekuensi subjalur yang teguh di dalam imej asli. *LWT* dipilih kerana ia cepat dan mengekalkan integriti *watermark* yang diperolehi. Manakala Jelmaan *BEMD* boleh menapis imej daripada jalur frekuensi yang paling teguh kepada yang paling sensitif (rapuh). Ciri ini dieksploitasikan di dalam tesis ini untuk membenamkan *watermark* di dalam bahagian *BEMD* yang teguh iaitu pada bakinya (*r*).

Untuk memastikan integriti dan ketulenan imej digital, pelbagai skema pengesahan telah dicadangkan di dalam kajian untuk mengesan mengubahsuaian imej. Namun, kebanyakkan skema yang sedia ada gagal untuk menyelesaikan isu ini atau

menggunakan cara yang tidak jitu untuk menilai prestasi sistem. Di atas sebab inilah, satu prosedur untuk menghasilkan *watermark* rapuh yang baru yang boleh mengesan sebarang pengubahsuaian telah dibangunkan di dalam tesis ini. Subjalur Jelmaan *BEMD* yang paling sensitif iaitu Fungsi Mod yng Intrinsik (*IMF*s) telah digunakan untuk menghasilkan dan membenamkan bits *watermark* di dalam domain frekuensi dan di proses seterusnya untuk meningkatkan keselamatan dan kebolehan bagi mengesan sebarang pengubahsuaian. *Watermark* yang lain dihasilkan dan dibenamkan pula di dalam domain ruang dengan menggunakan kaedah blok dan kemasukkan pada Bit yang Paling Kurang Kepentingan (LSBs).

Skema dua tujuan diperolehi dengan menggabungkan kedua-dua skema perlinduangan hakcipta dan pengesahan imej dan telah menjalani pelbagai serangan keteguhan dan kerapuhan. Keputusan menunjukkan prestasi skema ini kekal atau hanya berkurang pada kadar yang dibenarkan setelah dimasukkan kedua-dua *watermark* (i.e. pengurangan hanya $\leq$ 5%). Kualiti visual yang diperolehi; Nisbah Puncak Isyarat kepada Hingar (*PSNR*) adalah melebihi 48dB dan Norma Kolerasi Silang (*NCC*) adalah melebihi 0.97, manakala Kadar Pengesanan Pengubahsuaian (*AV*) adalah melebihi 94%.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank almighty ALLAH (S.W.T), the Most Beneficent and the Most Merciful for giving me the strength, courage, and his blessed guidance during my post graduate period.

I would like to thank my mother for her supportive prayers, calls, and blessings. I am also thankful to my husband, sisters, brothers, friend and many others for their support.

I am grateful to my supervisor, **Dr. Sharifah Mumtazah bt Syed Ahmad Abdul Rahman** for giving me the opportunity to embark on this research. Her consistent motivation, support, and guidance have been very crucial in the completion of my research.

I would like to express my sincere gratitude to my supervisory committee members, **Dr. Wan Azizun bt. Wan Adnan** and **Dr. Abd Rahman Bin Ramli** for their constructive suggestions during my research period and for dedicating their time in reviewing this thesis. Their valuable suggestions and comments have been very helpful in modifying the thesis.

This thesis was submitted to the Senate of the Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Sharifah Mumtazah bt Syed Ahmad Abdul Rahman, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Wan Azizun bt. Wan Adnan, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Abdul Rahman b. Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) were adhered to.

Signature: _____
Name of Chairman of Supervisory Committee: Associate Professor Dr. Sharifah Mumtazah bt Syed Ahmad Abdul Rahman

Signature: _____
Name of Member of Supervisory Committee: Associate Professor Dr. Wan Azizun bt. Wan Adnan

Signature: _____
Name of Member of Supervisory Committee: Associate Professor Dr. Abdul Rahman b. Ramli

TABLE OF CONTENTS

		Page
ABSTRACT		i
ABSTRAK		iii
ACKNOWLEDGEMENTS		v
APPROVAL		vi
DECLARATION		viii
LIST OF TABLES		xiii
LIST OF FIGURES		xvii
LIST OF ABBREVIATIONS		xix
CHAPTER		
1	**INTRODUCTION**	1
	1.1 Background	1
	1.2 Problem statement	2
	1.3 Objectives of the study	3
	1.4 Scope of the study	4
	1.5 Thesis layout	4
2	**LITERATURE REVIEW**	5
	2.1 Robust watermarking systems	5
	2.1.1 Properties of Robust Watermarking	6
	2.1.2 Attacks on The Robust Watermarking	8
	2.1.3 Robust Watermarking Techniques	10
	2.2 Fragile watermarking systems	16
	2.2.1 Properties of Fragile Watermarking	18
	2.2.2 Typical Counterfeiting Attacks	19
	2.2.3 Fragile watermarking techniques	20
	2.3 Dual purpose in Image Watermarking	25
	2.3.1 Requirements and properties of dual purpose watermarking	25
	2.3.2 Dual purpose watermarking algorithms	25
	2.4 Theoretical Background of Frequency Domain Transforms	32
	2.4.1 Discrete Wavelet Transform (DWT)	32
	2.4.2 Integer Wavelet Transform	34
	2.4.3 Two-dimensional Empirical Mode Decomposition	36
	2.5 Chapter Summary	38
3	**RESEARCH METHODOLOGY**	40
	3.1 Robust Watermarking System Architecture	40
	3.1.1 Experimental Setup	40
	3.1.2 Process for Watermark Embedding	41
	3.1.3 Watermark extraction procedure	44
	3.2 Fragile Watermarking System Architecture	47

		3.2.1 Fragile watermark generation and embedding process	47
		3.2.2 The Tamper Detection Procedure	53
	3.3	Dual purpose watermarking system architecture	57
		3.3.1 The dual-purpose watermarking embedding procedure	57
		3.3.2 The Dual Purpose Watermarking Detection Procedure	60
	3.4	Evaluation Procedure	62
		3.4.1 Evaluation for Robust Watermarking Algorithm	62
		3.4.2 Evaluation for Fragile Watermarking Algorithm	66
		3.4.3 Evaluation for Dual Purpose Watermarking Algorithm	66
	3.5	Chapter Summary	66
4	**RESULTS AND DISCUSSION**		68
	4.1	The Experimental Results of the Robust Image Watermarking Scheme	68
		4.1.1 The Robust Watermarking Scheme Results without Attacks	68
		4.1.2 The Robust Watermarking Scheme Results under nongeometric Attacks	70
		4.1.3 The Robust Watermarking Scheme Results under Geometric Attacks	82
		4.1.4 Benchmarking The Robust Watermarking Scheme	88
	4.2	Experimental Results of a Fragile Watermarking Image Scheme	92
		4.2.1 The Fragile Watermarking Scheme Results without Attacks	93
		4.2.2 The Fragile Watermarking Scheme Results under Deletion Attack	94
		4.2.3 The Fragile Watermarking Scheme Results under Copy-Paste Attack	96
		4.2.4 Benchmarking the Fragile Watermarking Scheme	99
	4.3	The Experimental Results of the Dual-Purpose Image Watermarking Scheme	101
		4.3.1 Verifying the Algorithm Performance under Nongeometric attacks	103
		4.3.2 Verifying the Algorithm Performance under Geometric attacks	118
		4.3.3 Verifying the Algorithm Performance under Deletion attack	120
		4.3.4 Verifying the Algorithm Performance under Copy-Paste attack	121
	4.4	Chapter Summary	126
5	**CONCLUSION AND FUTURE WORKS**		127
	5.1	Conclusion	127
	5.2	Thesis Contribution	129
	5.3	Recommendation for Future Work	129

REFERENCES 130
APPENDICES 138
BIODATA OF STUDENT 152
LIST OF PUBLICATIONS 153

LIST OF TABLES

Table		Page
2.1	Comparison of the various existing robust watermarking methods	15
2.2	Comparison of the various existing fragile watermarking methods	24
2.3	Comparison of the various existing dual purpose watermarking methods	31
4.1	Embedding binary watermark for Lena image in the four subbands without attack	69
4.2	Embedding grey scale watermark for Lena in the four subbands without attack	70
4.3	Lena watermarked image and the extracted watermark under median filter attack.	72
4.4	Lena watermarked image and the extracted watermark under Wiener filter attack.	73
4.5	Lena watermarked image and the extracted watermark under Gaussian filter attack	74
4.6	Lena watermarked image and the extracted watermark under gamma correction attack	75
4.7	Lena watermarked image and the extracted watermark under Gaussian noise attack	77
4.8	Lena watermarked image and the extracted watermark under speckle noise attack..	78
4.9	Lena watermarked image and the extracted watermark under salt & pepper noise attack.	79
4.10	Lena watermarked image and the extracted watermark under JPEG	81
4.11	Lena watermarked image and the extracted watermark under rotation attack	83
4.12	Lena watermarked image and the extracted watermark under translation attack	84
4.13	Lena watermarked image and the extracted watermark under scaling attack.	85

4.14	Lena watermarked image and the extracted watermark under cut	87
4.15	Lena watermarked image and the extracted watermark under shearing attack.	88
4.16	Fragile watermark embedding process	92
4.17	PSNR value of the watermarked images	93
4.18	Fragile watermarking	93
4.19	Tampered Lena image with the bit error matrix	94
4.20	Tamper detection rate values for deletion attacks	95
4.21	Tampered Tank image with the bit error matrix	97
4.22	Tampered Lena image with the bit error matrix	98
4.23	Comparison of the proposed algorithm with three others in terms of average detection rate for copy–paste attack	100
4.24	Robust and fragile watermark extraction for the dual purpose	102
4.25	Single-purpose and dual-purpose systems comparison	102
4.26	Dual-purpose system performance under median filter	104
4.27	Dual-purpose system performance under Wiener filter	105
4.28	Dual-purpose system performance under Gaussian filter	106
4.29	Dual-purpose system performance under Gaussian noise	107
4.30	Dual-purpose system performance under Speckle noise	108
4.31	Dual-purpose system performance under Salt and pepper noise	109
4.32	Dual-purpose system performance under JPEG compression	110
4.33	Robustness evaluation of the dual purpose under median filter attack	111
4.34	Robustness evaluation of the dual purpose under Wiener filter	112
4.35	Robustness evaluation of the dual purpose under Gaussian filter attack	113
4.36	Robustness evaluation of the dual purpose under Gaussian noise attack	114

4.37	Robustness evaluation of the dual purpose under under speckle noise	115
4.38	Robustness evaluation of the dual purpose under salt &pepper	116
4.39	Robustness evaluation of the dual purpose under JPEG compression attack	117
4.40	Robustness evaluation of the dual purpose under translation attack	118
4.41	Robustness evaluation of the dual purpose under cut attack	119
4.42	Robustness evaluation of the dual purpose under shearing attack	119
4.43	Deletion attack on dual purpose	120
4.44	Copy paste attack on dual purpose watermark	122
4.45	Detection rate (*AV*) for 10% tampering attack	123
4.46	Detection rate (*AV*) for 20% tampering attack	123
4.47	Detection rate (*AV*) for 30% tampering attack	124
4.48	Detection rate (*AV*) for 40% tampering attack	124
4.49	Detection rate (*AV*) for 50% tampering attack	125
A.1	Benchmarking the proposed scheme in case of salt & pepper noise attacks	138
A.2	Benchmarking the proposed scheme in case of speckle noise attack	139
A.3	Benchmarking the proposed scheme in case of Gaussian noise attack	140
A.4	Benchmarking the proposed scheme in case of Gaussian filter attack	141
A.5	Benchmarking the proposed scheme in case of Median filter attack	142
A.6	Benchmarking the proposed scheme in case of Wiener filter attack	143
A.7	Benchmarking the proposed scheme in case of Gamma correction attack	144

A.8	Benchmarking the proposed scheme in case of JPEG compression attacks	145
A.9	Benchmarking the proposed scheme in case of rotation attack	146
A.10	Benchmarking the proposed scheme in case of scaling attack	147
A.11	Benchmarking the proposed scheme in case of Translation attack	148
A.12	Benchmarking the proposed scheme in case of cut attack	149
A.13	Benchmarking the proposed scheme in case of shearing attack	150
A.14	Determining of k and T values of robust watermarking algorithm	151

LIST OF FIGURES

Figure		Page
2.1	A generic watermarking system	6
2.2	Kundur and Hatzinakos's DWT watermark embedding process	11
2.3	Authentication watermark embedding	17
2.4	Watermarking extraction and verification model	17
2.5	The general procedure to publicly authenticate digital content with the LSB replacement	21
2.6	Multipurpose watermark embedding scheme (1)	26
2.7	partitioning original image and one-level DWT for 4xx4 block	27
2.8	Hybrid embedding system in (F. Deguillaume et al2003)	28
2.9	Multipurpose watermark embedding scheme (2)	29
2.10	One level of decomposition of two-dimensional	33
2.11	DWT decomposition of an image using 3-level pyramid	33
2.12	One level DWT transform	34
2.13	Three different phases in the lifting scheme	34
2.14	IMF sifting process	38
3.1	Block diagram of the robust watermarking embedding process	42
3.2	Block diagram of watermark detection process	46
3.3	General procedure of the fragile watermark generation process	48
3.4	Secret key generation	49
3.5	The key embedding process	50
3.6	Example of spatial domain fragile watermark construction	51
3.7	Procedure of the frequency fragile watermark embedding	52
3.8	Proposed authentication flowchart	54

3.9	Bit error matrix without tampering	55
3.10	Example of alteration one bit in the Spatial domain fragile	57
3.11	Procedure of dual purpose watermarking embedding algorithm	59
3.12	Procedure of dual purpose watermarking detection	61
3.13	Robust watermarking attacks classification	63
3.14	Robust watermarking algorithms proposed by: (a) Makbol et al. (b) this thesis	65
4.6	Comparison of the proposed algorithm with three others in terms of average detection rate for 30% tampering rate	101

LIST OF ABBREVIATIONS

NCC	Normalized Cross Correlation
FP	False Positive
FN	False Negative
HVS	the Human Visual System
RMSE	Root Mean Square Error
RST	Rotation, Scaling, and Translation
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
DFT	Discrete Fourier Transform
JND	Just Noticeable Distortion
FHT	Fast Hadamard Transform
SVD	Singular Value Decomposition
SVR	Support Vector Regression
NWT	Non-separable Wavelet Transform
HD	Hamming Distance
LWT	Lifting Wavelet Transform
EMD	Empirical Mode Decomposition
IMF	Intrinsic Mode Function
r	Residue
SD	Standard Deviation
FABEMD	Fast and Adaptive BEMD
VQ	Vector Quantisation
LSB	Least Significant Bit

MSB	Most Significant Bit
ST	Slant Transform
QIM	Quantization Index Modulation
ROI	Regions Of Interest
DDWT	Distributed Discrete Wavelet Transform
BEMD	Bivariate Empirical Mode Decomposition
SFFF	Self-Fractional Fourier Function
BVQ	Blind Vector Quantization
ECC	Error Correction Codes
LS	Lifting Scheme
IWT	Integer Wavelet Transform
T	Threshold
RDWT	Redundant Discrete Wavelet Transform
PST	Pinned Sine Transform

CHAPTER 1

INTRODUCTION

1.1 Background

Recently, Internet products that make daily lives easier have grown drastically, such as images, video and audio. At the same time, they have led to the possibility of illegal reproduction, dissemination; and the important issue of copying intellectual property (You, 2009) (Zheng, Shi, & Lv, 2009). Consequently, the 'copyright infringement' problem has led to the need of research in this area. According to (Zhao, 2009), film and music industries lose millions of dollars per annum due to copyright infringement.

In addition to copyright protection, another important issue relates to the authentication and verification of the integrity of an image or other digital content. It is widely recognised that digital contents; especially images, can be manipulated and altered with ease. With the enormous availability of image editing software, like Corel Paint Shop and Adobe Photoshop, even novice users have the ability to modify or manipulate the contents of digital products. Accordingly, for some feasible applications, like news reporting, medical archiving and legal applications, it is particularly essential to verify image integrity where it is required to be certain that the image in question really returns what the scene seems to be at the moment of capture. In order to ensure image integrity, it is not merely necessary to prove that photographic verification remains authentic and unchanged, but in addition, any tampered regions should be localised to identify untrusted image parts (Wong & Memon, 2001) (Zhao, 2009).

Several approaches have to be adopted to ensure controlled manipulation and copyright protection (Gu & Gao, 2012). Two widely used approaches to ensure the security of transferring the digital content over the Internet include data encryption (Baptista, 1998) and digital watermarking (Bender, Gruhl, Morimoto, & Lu, 1996). Data encryption is a traditional mechanism used to protect data from illegitimate use by transforming the data into meaningless code. Cryptography has its drawback, because it does not ban or track digital products against illegal reproduction after it has been decrypted (Zhao, 2009). As a consequence, digital watermarking techniques are an adequate solution, as they can track digital contents after decryption.

Digital watermarking conceals the existence of secret data by embedding additional information into a meaningful host multimedia data file to distract the attention of observers; without introducing perceptual changes (Sukumar, Hemalatha, & Soman, 2009). Watermarking was first introduced at the beginning of the 1990s as a second generation of technical security protection after encryption (K. Loukhaoukha, 2009). This mechanism can be applied to different media formats, such as images, video and audio. Different techniques are used to embed different kinds of watermarks into multimedia contents to achieve various goals. Digital watermarking algorithms are

classified as either robust, semi-fragile, or fragile; and they are employed depending on the application to be used. A robust watermark is used for copyright protection. For this purpose, the embedded watermark must be robust and resistant towards deliberate attacks(Avila & Miyatake, 2010). Semi-fragile watermarks are designed to allow an acceptable level of alteration, such as slight contrast adjustment or low-level lossy compression in images (Jessica Fridrich, 2002). Meanwhile, fragile watermarks, which are used for tampering detection, do not require the same level of robustness as those used for copyright protection; mainly because it needs the capability to detect even the slightest modification to the media (Yeun & Mintzer, 1997). As a result, this type of watermarking is suitable for authentication and tamper localisation applications (P. Lin, Lee, & Chang, 2009).

Most digital watermarking systems perform a single task; either for copyright protection or tampering detection. However, for high-valued applications, such as military satellite images and e-commerce, it is necessary to verify that the image received is in fact authentic and possibly to confirm actual ownership. This trend has driven the launch of multi-purpose watermarking (Yang & Zhang, 2008). Research in this domain has attracted tremendous interest in recent years; mainly due to its challenging nature in effectively satisfying both aims without degrading one another.

1.2 Problem statement

As stated previously, copyright protection watermarking algorithms should be robust under various attacks. Among these geometric and non-geometric attacks which are described in the next chapter. Several watermarking techniques were recently proposed by embedding robust watermark into digital images. In general, most of the algorithms focus only on limited attacks to determine the watermark robustness (Cox, Kilian, Leighton, & Shamoon, 1997); (Kundur & Dimitrios, 1997); (S. Lee, Yoo, & Kalker, 2007); (Senthilkumar & Sarkar, 2012) . In addition, the size of the employed watermark in majority of literature is quite small when compared to that of the host image (Kundur & Dimitrios, 1997); (Raval & Rege, 2003); (Bi, Sun, Huang, Yang, & Huang, 2007). However, the algorithms proposed by Makbol et al., (Makbol & Khoo, 2013) which based on Redundant Discrete Wavelet Transform (RDWT) with the SVD (RDWT–SVD) and Makbol et al., (Makbol & Khoo, 2014) which used the integer wavelet transform based on the Lifting Wavelet Transform with the SVD transform (LWT-SVD) have accomplished a good watermarked imperceptibility with high watermark capacity and are also able to be robust against many forms of attacks; geometric and non-geometric attacks. In this regard, they are used for benchmarking the robust watermarking algorithm proposed in this thesis. The only drawback of Makbol et al. works that the Normalised Cross Correlation (*NCC*) values of the extracted watermarks under the translation attack, scaling attack, JPEG compression attack, wiener attack and median attack, were 0.601, 0.467, 0.732,0.715 and 0.715, respectively, which are less than the acceptable values. In general, an *NCC* value is accepted if it is $\geq$0.75 (Al-Haj, 2007).

Based on the above-mentioned points, the algorithm proposed in this study would try to overcome some of the limitations seen in the published reports. This work focuses primarily on transparency, robustness and high capacity approaches, which are described in the next few chapters.

To ensure the integrity and authenticity of digital images, a wide variety of authentication schemes have been proposed in the literature to detect image tampering. However, most of the existing schemes either fail to address this issue (Yeun & Mintzer, 1997); (Jessica Fridrich, 2002); (X. Zhang, Wang, Qian, & Feng, 2011);(Mandal & Ghosal, 2012) or use inaccurate method to evaluate the system performance (Walton, 1995); (Jessica Fridrich, 2002); (X. Zhang et al., 2011); (Mandal & Ghosal, 2012). For this reason, a procedure to generate an effectual and secure fragile watermarking scheme is developed in this thesis which is able to detect tampering and inculcate localisation without affecting image quality. Moreover, precise and impartial methods are utilised in evaluating and benchmarking the recommended fragile watermarking system against others in terms of critical forging attacks.

The multipurpose system is a new challenging area of research in digital watermarking. It mainly focuses on combining dual watermarks; robust and fragile to achieve content authentication and also copyright protection. However, in most of the recent works only one function has been achieved: either the robustness function has been done at the expense of the fragility or vice versa due to shortcomings in the technique employed for copyright protection or tamper detection (Avila & Miyatake, 2010); (Schlauweg, Pröfrock, Zeibich, & Müller, 2006); (Sharma, Sharma, & Sahula, 2013); (Deguillaume, Voloshynovskiy, & Pun, 2003). In this thesis, a new effective dual purpose watermarking system is proposed. It has been devised to meet the criteria of fragility as well as robustness, while combining the processes of copyright protection and proofing tampering at the same time without significant degradation of each other.

1.3 Objective of the study

The main objective of this thesis is to design a dual purpose image watermarking system that can satisfy both robustness and fragility simultaneously.

The main objective can be broken into several sub-objectives as follows:

i. To design an effective robust image watermarking system that is comparable to or outperforms current robust watermarking techniques.
ii. To design an effective fragile image watermarking system that is comparable to or outperforms current fragile watermarking techniques.
iii. To design an effective mechanism to combine both robust and fragile image watermarking systems designed in item (1) and (2), where the performance remains at par or only degrades at an acceptable level after inserting the dual watermarks.

1.4 Scope of the study

The evaluation of the proposed systems is performed by using the following methods:

i. The proposed robust watermarking system was evaluated in terms of robustness and perceptuality. The critical attacks used to test the robustness of the algorithm are intentional and nonintentional attacks. The parameter used to evaluate the robustness of the proposed algorithm accurately is Normalized Cross Correlation (*NCC*), and represents the correlation between the original and extracted watermarks after the system has been subjected to all possible attacks. The quality of the watermarked image is evaluated using the Peak Signal to Noise Ratio (*PSNR*) and describes the quality of the image after adding the watermark. Furthermore, the proposed algorithm was benchmarked against existing algorithms and was able to outperform them with respect to watermarked image quality and robustness.

ii. The tamper detection ability of the proposed fragile watermark algorithm is evaluated by applying several tampering attacks such as copy paste and deletion attacks. False positive (F_P), False negative (F_N), and Average of detection rate (*AV*) are used to evaluate the tampering detection ability of the authentication algorithm. It is clear that the proposed system can detect even a slight percentage of tampering by achieving a low false positive value with a high detection rate. Furthermore, the system was compared to the existing fragile watermark systems and was able to outperform them with respect to image quality and the ability to detect tampered area.

iii. The proposed dual purpose algorithm was evaluated in terms of robustness and fragility and was subjected to all possible attacks that critically affect the performance of the robustness and fragility algorithms. Furthermore, the performance of the algorithm was compared to the proposed single purpose robust watermark and single purpose fragile watermark in terms of imperceptibility, robustness and fragility. The values of *NCC, PSNR* and *AV* are still high and degrade at an acceptable level after inserting the dual watermarks.

1.5 Thesis layout

The thesis is comprised of five chapters. Chapter one introduces the background and significance of the study, accompanied by the problem statement, objectives and scope of the study. Chapter two presents a review and analysis of previous researches related to the present study. It also covers a review of the literature on robust and fragile watermarking algorithms, including their advantages and disadvantages. Chapter three presents the proposed system and explains the utilized methodologies in detail. Chapter four provides the experimental results and discusses the analysis of the results achieved. Finally, Chapter five reports the most promising research trends along with the conclusions of this thesis.

REFERENCES

Abbasi, A., Woo, C. S., & Shamshirband, S. (2015). Robust image watermarking based on Riesz transformation and IT2FLS. *Measurement*, *74*, 116–129.

Agreste, S., Andaloro, G., Prestipino, D., & Puccio, L. (2007). An image adaptive, wavelet-based watermarking of digital images. *Journal of Computational and Applied Mathematics*, *210*(1), 13–21.

Al-jaber, A., & Aloqily, I. (2003). High Quality Steganography Model with Attacks Detection. *Image (Rochester, N.Y.)*, *2*(2), 116–127.

Alomari, R. S., & Al-jaber, A. (2004). A Fragile Watermarking Algorithm for Content Authentication. *International Journal of Computing & Information Sciences*, *2*(1), 27–37.

Amirmazlaghani, M., Rezghi, M., & Amindavar, H. (2015). A novel robust scaling image watermarking scheme based on Gaussian Mixture Model. *Expert Systems with Applications*, *42*(4), 1960–1971.

Avila, C. S., & Miyatake, M. N. (2010). Multipurpose Image Watermarking Scheme Based on Self-Embedding and Data Hiding into Halftone Image. In *proceeding of IEEE Conference on Electronics, Robotics and Automotive Mechanics* (pp. 394–398).

Baptista, M. S. (1998). Cryptography with chaos. *Physics Letters A*, *240*(1), 50–54.

Barreto, P. S. L. M., Kim, H. Y., & Rijmen, V. (2002). Toward secure public-key blockwise fragile authentication watermarking. *IEE Proceedings-Vision, Image and Signal Processing*, *149*(2), 57–62.

Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal*, *35*(3.4), 313–336.

Bhuiyan, S. M. a, Adhami, R. R., & Khan, J. F. (2008). Fast and Adaptive Bidimensional Empirical Mode Decomposition Using Order-Statistics Filter Based Envelope Estimation. *EURASIP Journal on Advances in Signal Processing*, *2008*(1), 1–19.

Bi, N., Sun, Q., Huang, D., Yang, Z., & Huang, J. (2007). Robust image watermarking based on multiband wavelets and empirical mode decomposition. *IEEE Transactions on Image Processing*, *16*(8), 1956–1966.

Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, *6*(12), 1673–1687.

Craver, S., Memon, N., Yeo, B.-L., & Yeung, M. M. (1998). Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications. *IEEE Journal on Selected Areas in Communications, 16*(4), 573–586.

Dadkhah, S., Manaf, A. A., & Sadeghi, S. (2012). Efficient Digital Image Authentication and Tamper Localization Technique Using 3Lsb Watermarking. *International Journal of Computer Science*, *9*(1), 1–8.

Dadkhah, S., Manaf, A. A., & Sadeghi, S. (2014). Efficient image authentication and tamper localization algorithm using active watermarking. In *Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations* (pp. 115–148). Springer.

Daubechies, I., & Sweldens, W. (1998). Factoring wavelet transforms into lifting steps. *Journal of Fourier Analysis and Applications*, *4*(3), 247–269.

Deguillaume, F., Voloshynovskiy, S., & Pun, T. (2003). Secure hybrid robust watermarking resistant against tampering and copy attack. *Signal Processing*, *83*(10), 2133–2170.

Elbaşı, E. (2012). Robust MPEG Watermarking in DWT Four Bands. *Journal of Applied Research and Technology*, *10*(2), 87–93.

Fridrich, J. (2002). Security of fragile authentication watermarks with localization. *Electronic Imaging*, *10*(2), 691–700.

Fridrich, J., Goljan, M., & Baldoza, A. C. (2000). New fragile authentication watermark for images. In *proceeding of 8th IEEE International Conference on Image Processing* (pp. 446–449).

Fridrich, J., Goljan, M., & Memon, N. D. (2000). Further attacks on Yeung-Mintzer fragile watermarking scheme. In *proceeding of International Society for Optics and Photonics in Electronic Imaging* (pp. 428–437).

Gadicha, A. B., & Gadicha, V. B. (2013). Multi-Dimensional Empirical Mode Decomposition based Watermarking Scheme using Signal to Noise Concept. In *Proceedings of National Conference on New Horizons in IT-NCNHIT* (p. 58).

Ganic, E., & Eskicioglu, A. M. (2005). Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition. *Journal of Electronic Imaging*, *14*(4), 43004.

Gu, Q., & Gao, T. (2012). A novel reversible watermarking scheme based on block energy difference for medical images. In *the proceeding of 13th IEEE International Symposium on Advanced Intelligence Systems* (pp. 232–237).

Gui, X. I. E., & Hong, S. (2006). A new fusion based blind logo-watermarking algorithm. *IEICE Transactions on Information and Systems*, *89*(3), 1173–1180.

Gunjal, B. L. (2016). Robust, Secure and High Capacity Watermarking Technique based on Image Partitioning-Merging Scheme. *International Journal of Information Technology and Computer Science (IJITCS)*, *8*(4), 74.

Haotian, W. U. (2007). Information Hiding for Media Authentication and Covert Communication. *Philosophy*, (September).

Himaja, G., Reddy, B. M. K., & Raju, K. V. P. (2012). Blind and Robust Watermarking for Self-Authentication of Images Using Integer Wavelet Transform. *International Journal of Computer Technology and Electronics Engineering (IJCTEE)*, *2*(3), 61–64.

Ho, A. T. S., Zhu, X., & Woon, W. M. (2005). A semi-fragile pinned sine transform watermarking system for content authentication of satellite images. In *proceeding of Symposium in International Geoscience and Remote Sensing (IGARSS)* (Vol. 2, pp. 737–740).

Hossaini, E., El Arab, A., El Aroussi, M., Jamali, K., Mbarki, S., & Wahbi, M. (2014). A new robust blind watermarking scheme based on Steerable pyramid and DCT using Pearson product moment correlation. *Journal of Computers*, *9*(10), 2315–2327.

Huang, N. E., Shen, Z., Long, S. R., Wu, M. C., Shih, H. H., Zheng, Q., … Liu, H. H. (1998). The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, *454*(1971), 903–995.

Huang, W. H. W., & Sun, Y. S. Y. (2007). A New Image Watermarking Algorithm Using BEMD Method. In *proceeding of IEEE International Conference on Communications, Circuits and Systems* (pp. 588–592).

Jabade, V. S., & Gengaje, D. S. R. (2011). Literature review of wavelet based digital image watermarking techniques. *International Journal of Computer Applications*, *31*(1), 28–35.

K. Loukhaoukha, J. Y. C. (2009). A new image watermarking algorithm based on wavelet transform. In *proceeding of IEEE Canadian Conference on Electrical and Computer Engineering* (pp. 229–234).

Kiani, S., & Moghaddam, M. E. (2011). A multi-purpose digital image watermarking using fractal block coding. *Journal of Systems and Software*, *84*(9), 1550–1562.

Kundur, D., & Dimitrios, H. (1997). A robust digital image watermarking method using wavelet-based fusion (1997). In *Proceeding of IEEE Int. Conf. on Acoustics, Speech and Sig. Proc* (Vol. 5, pp. 544–547).

Kutter, M. (1999). Watermarking resistance to translation, rotation, and scaling. *SPIE Multimedia Systems and Applications*, *3528*, 423–431.

Kutter, M., & Petitcolas, F. a P. (1999). A fair benchmark for image watermarking systems. In *International society for optics and pohonics* (Vol. 3657, pp. 25–27).

Langelaar, G. C., Setyawan, I., & Lagendijk, R. L. (2000). Watermarking digital image and video data. A state-of-the-art-overview. *IEEE Signal Processing Magazine*, *17*(5).

Lee, S., Yoo, C. D., & Kalker, T. (2007). Reversible image watermarking based on integer-to-integer wavelet transform. *IEEE Transactions on Information Forensics and Security*, *2*(3), 321–330.

Lee, T.-Y., & Lin, S. D. (2008). Dual watermark for image tamper detection and recovery. *Pattern Recognition*, *41*(11), 3497–3506.

Lee, Y.-P., Lee, J.-C., Chen, W.-K., Chang, K.-C., Su, J., & Chang, C.-P. (2012). High-payload image hiding with quality recovery using tri-way pixel-value differencing. *Information Sciences*, *191*, 214–225.

Liang, L., & Ping, Z. (2008). Information Hiding Based on Empirical Mode Decomposition. In *proceeding of IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application* (Vol. 1, pp. 561–565).

Lin, C.-H., Li, Y.-C., Wu, M.-N., Yang, S.-S., & Chen, K.-J. (2009). Multipurpose Watermarking Method Based on Blind Vector Quantization. In *proceeding of Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 636–639).

Lin, E., Delp, E., Lin, E. T., & Delp, E. J. (2001). A Review of Fragile Image Watermarks. In *Proceedings of IEEE Workshop on the Multimedia and Security* (pp. 25–29).

Lin, E. T., Podilchuk, C. I., & Delp III, E. J. (2000). Detection of image alterations using semifragile watermarks. In *proceeding of IEEE international conference society for optics and phonics* (pp. 152–163).

Lin, P., Lee, J., & Chang, C. (2009). Dual Digital Watermarking for Internet Media Based on Hybrid Strategies. *IEEE Transactions on Circuits and Systems for Video Technology*, *19*(8), 1169–1177.

Linderhed, A. (2002). 2D empirical mode decompositions in the spirit of image compression. In *International Society for Optics and Photonics AeroSense* (pp. 1–8).

Liu, B., Riemenschneider, S., & Xu, Y. (2006). Gearbox fault diagnosis using empirical mode decomposition and Hilbert spectrum. *Mechanical Systems and Signal Processing*, *20*(3), 718–734.

Liu, R., & Tan, T. (2002). An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia*, *4*(1), 121–128.

Loukhaoukha, K., & Chouinard, J.-Y. (2009). Hybrid watermarking algorithm based on SVD and lifting wavelet transform for ownership verification. In *In proceeding of 11th IEEE Canadian Workshop on Information Theory* (pp. 177–182).

Lu, C.-S., & Liao, H.-Y. M. (2001). Multipurpose watermarking for image authentication and protection. *IEEE Transactions on Image Processing*, *10*(10), 1579–1592.

Makbol, N. M., & Khoo, B. E. (2013). Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *AEU-International Journal of Electronics and Communications*, *67*(2), 102–112.

Makbol, N. M., & Khoo, B. E. (2014). A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. *Digital Signal Processing*, *33*, 134–147.

Mallat, S. (2009). *A wavelet tour of signal processing*. Academic press.

Mandal, J. K., & Ghosal, S. K. (2012). A Fragile Watermarking based on Separable Discrete Hartley Transform for Color Image Authentication (FWSDHTCIA). *Signal & Image Processing*, *3*(6), 23.

Miller, M. L., Cox, I. J., Ton, J. M. G. L., Philips, K., Prof, R., & Eindhoven, a a. (1999). A review of watermarking principles and practices. *Methods*, (February 1997), 461–485.

Minghui, D., & Jingbo, Z. (2009). Robust Image Watermarking Algorithm against Geometric Attack Based on BEMD. In *proceeding of IEEE International Conference on Computer and Communications Security* (pp. 36–39).

Mintzer, F., & Braudaway, G. W. (1999). If one watermark is good, are more better? In *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing* (Vol. 4, pp. 2067–2069).

Moreno, O., Tirkel, A., van Schyndel, R., & Parampalli, U. (2010). New Families of 2D & 3D Arrays for Sub-image Watermarking. In *proceeding of Fourth International Conference on Network and System Security* (pp. 340–344).

Nezhadarya, E., Wang, Z. J., & Ward, R. K. (2011). Robust image watermarking based on multiscale gradient direction quantization. *IEEE Transactions on Information Forensics and Security*, *6*(4), 1200–1213.

Nunes, J. C., Bouaoune, Y., Delechelle, E., Niang, O., & Bunel, P. (2003). Image analysis by bidimensional empirical mode decomposition. *Image and Vision Computing*, *21*(12), 1019–1026.

Qin, C., Chang, C.-C., & Chen, K.-N. (2013). Adaptive self-recovery for tampered images based on VQ indexing and inpainting. *Signal Processing*, *93*(4), 933–946.

Raja, A., & Ahmed, A. (2004). A fragile watermarking algorithm for content authentication. *International Journal of Computing & Information Sciences*, *2*(1), 27–37.

Raval, M. S., & Rege, P. P. (2003). Discrete wavelet transform based multiple watermarking scheme. In *proceeding of IEEE Conference on Convergent Technologies for the Asia-Pacific Region* (Vol. 3, pp. 935–938).

SABRI, A., KAROUD, M., TAIRI, H., & AARAB, A. (1796). Image Watermarking Using the Empirical Mode Decomposition. LESSI, Department of physics, Faculty of Science, Dhar El mahraz BP.

Schlauweg, M., Pröfrock, D., Palfner, T., & Müller, E. (2005). Quantization-based semi-fragile public-key watermarking for secure image authentication. In *International Society for Optics and Photonics* (p. 591506).

Schlauweg, M., Pröfrock, D., Zeibich, B., & Müller, E. (2006). Dual watermarking for protection of rightful ownership and secure image authentication. In *Proceedings of the 4th ACM international workshop on Contents protection and security* (p. 59).

Senthilkumar, K., & Sarkar, S. (2012). A Highly Secured Digital Watermarking Algorithm for Binary Watermark Using Lifting Wavelet Transform and Singular Value Decomposition. In *proceeding of 3rd international conference on Sustainable Energy and Intelligent Systems* (Vol. 3, pp. 109–113).

Sharma, J. B., Sharma, K. K., & Sahula, V. (2013). Digital image dual watermarking using self-fractional fourier functions, bivariate empirical mode decomposition and error correcting code. *Journal of Optics*, *42*(3), 214–227.

Shen, H., & Chen, B. (2012). From single watermark to dual watermark : A new approach for image watermarking q. *Computers and Electrical Engineering*, *38*(5), 1310–1324.

Shivani, S., Patel, A. K., Kamble, S., & Agarwal, S. (2011). Image Authentication and Restoration using Block-Wise Fragile Watermarking based on k-Medoids Clustering Approach. In *2nd Int. Conf. Work. Emerg. Trends Technol* (pp. 44–51).

Sukumar, K., Hemalatha, T., & Soman, K. P. (2009). Multi Image-Watermarking Scheme Based on Framelet and SVD. In *proceeding of International Conference on Advances in Recent Technologies in Communication and Computing* (pp. 379–383).

Sweldens, W. (1996). The lifting scheme: A custom-design construction of biorthogonal wavelets. *Applied and Computational Harmonic Analysis*, *3*(2), 186–200.

Sweldens, W. (1998). The lifting scheme: A construction of second generation wavelets. *SIAM Journal on Mathematical Analysis*, *29*(2), 511–546.

Taghia, J., Doostari, M. A., & Taghia, J. (2008). An image watermarking method based on bidimensional empirical mode decomposition. In *CISP Congress on Image and Signal Processing* (Vol. 5, pp. 674–678).

Tao, H., Chongmin, L., Zain, J. M., & Abdalla, A. N. (2014). Robust image watermarking theories and techniques: A review. *Journal of Applied Research and Technology*, *12*(1), 122–138.

Verma, B., Jain, S., Agarwal, D. P., & Phadikar, A. (2006). A New color image watermarking scheme. *Infocomp, Journal of Computer Science*, *5*(2), 37–42.

Walton, S. (1995). Image authentication for a slippery new age. *Dr Dobb's Journal-Software Tools for the Professional Programmer*, *20*(4), 18–27.

Wang, L. J., & Syue, M. Y. (2013). A wavelet-based multipurpose watermarking for image authentication and recovery. *International Journal of Communications*, *2*(4).

Watson, A. B., & Poirson, A. (1986). Separable two-dimensional discrete Hartley transform. *JOSA A*, *3*(12), 2001–2004.

Weber, G. (1993). *USC-SIPI report image database: Version 4*.

Wong, P. W. (1998). A public key watermark for image verification and authentication. In *Proceedings of IEEE International Conference on Image Processing* (Vol. 1, pp. 455–459).

Wong, P. W., & Memon, N. (2001). Secret and public key image watermarking schemes for image authentication and ownership verification. *IEEE Transactions on Image Processing*, *10*(10), 1593–1601.

Xie, G., & Shen, H. (2005). Toward improved wavelet-based watermarking using the pixel-wise masking model. In *proceeding of IEEE International Conference on Image Processing* (Vol. 1, pp. I–689).

Xin, X. (2010). A Singular-Value-Based Semi-Fragile Watermarking Scheme for Image Content Authentication with Tampering Localization. *Journal of Visual Communication and Image Representation*, *30*, 312–327.

Yang, H., & Zhang, T. (2008). A New Algorithm of Compound Image Watermarking Based on DDWT. In *proceeding of IEEE International Conference on MultiMedia and Information Technology* (pp. 268–271).

Yeo, D.-G., & Lee, H.-Y. (2012). Block-based image authentication algorithm using reversible watermarking. In *Computer Science and Convergence* (pp. 703–711). Springer.

Yeun, M. M., & Mintzer, F. (1997). An invisible watermarking technique for image verification. In *Proceedings of IEEE International Conference on Image Processing* (Vol. 2, pp. 680–683).

You, X. (2009). An image watermarking scheme using new wavelet filter banks. In *proceeding of 3rd IEEE International Conference on Anti-counterfeiting, Security, and Identification in Communication* (pp. 148–151).

Yousefi, S., Rabiee, H. R., Yousefi, E., & Ghanbari, M. (2007). Reversible date hiding using histogram sorting and integer wavelet transform. In *proceeding of IEEE conference in Digital EcoSystems and Technologies* (pp. 487–490).

Zhang, C., Cheng, L. L., Qiu, Z., & Cheng, L.-M. (2008). Multipurpose watermarking based on multiscale curvelet transform. *IEEE Transactions on Information Forensics and Security*, *3*(4), 611–619.

Zhang, X., & Wang, S. (2007). Statistical fragile watermarking capable of locating individual tampered pixels. *Signal Processing Letters, IEEE*, *14*(10), 727–730.

Zhang, X., Wang, S., Qian, Z., & Feng, G. (2011). Self-embedding watermark with flexible restoration quality. *Multimedia Tools and Applications*, *54*(2), 385–395.

Zhao, X. (2009). *Robust and Semi-fragile Watermarking Techniques for Image Content Protection*. Department of Computing, University of Surrey.

Zhao, X., Bateman, P., & Ho, A. T. S. (2011). Image authentication using active watermarking and passive forensics techniques. In *Multimedia Analysis, Processing and Communications* (pp. 139–183). Springer.

Zheng, Q., Shi, G., & Lv, X. (2009). A robust digital watermarking scheme based on integer wavelet using compound encryption. In *proceeding of 4th IEEE International Conference on Computer Science & Education* (pp. 716–719).