ENHANCED LSB WATERMARKING METHODS BASED ON SCANNING PATTERNS FOR AUTHENTICATION OF MEDICAL IMAGES

SYIFAK IZHAR HISHAM

Thesis submitted in fulfilment of the requirements for the award of the degree of Doctor of Philosophy (Computer Science)

Faculty of Computer System and Software Engineering
UNIVERSITI MALAYSIA PAHANG

January 2016

ABSTRACT

This thesis investigated the trend in the current watermarking technology of medical images which features authentication, tamper localization, and recovery. Nowadays the information system is used widely in hospitals and clinical departments globally. It is able to help the clinical professionals doing diagnosis, smoothen the transmission process, and store the patients' data and medical images. Since the system handles thousands of crucial medical data, a security and authentication method is seen as imperative to protect the data. Three watermarking techniques were proposed to enhance the fragile watermarking algorithm aiming at improving the numbering technique before embedding the watermark data. They are Authentication Watermarking for Grey-Scale Medical Images Using Spiral Manner Numbering (SPIRAL-LSB), Authentication Watermarking for Grey-Scale Medical Images Using Hilbert Manner Numbering (HILBERT-LSB) and Authentication Watermarking for Color Medical Images Using Hilbert Manner Numbering (HILBERT-LSB-C). All proposed methods used unique styles of numbering and mapping pixels to guarantee a good performance of the authentication system. This can be done by spreading the numbered original data as far as possible from the original locations. The watermark generating and embedding phases used the same processes in all schemes. They produced the authentication data by using simple operations, which were parity bits check and comparison between average intensity data. The schemes embedded the authentication data in the least significant bit (LSB). The embedded authentication data in the same host image were utilized to localize any tamper using block-wise approach. The method is effective since it only required a secret key and a public, chaotic mixing algorithm to recover the attacked image.

ABSTRAK

Tesis ini mengkaji perkembangan dalam teknologi watermark untuk imej-imej perubatan yang merangkumi ciri pengesahan keaslian, penjejakan kerosakan dan pemulihan. Kini, sistem maklumat telah pun digunakan secara meluas di hospital-hospital dan pusat-pusat klinikal pada peringkat global. Ia mampu membantu golongan perubatan profesional dalam melakukan diagnosis, memudahkan proses peralihan maklumat dan menyimpan data pesakit dan imej perubatan. Oleh kerana sistem maklumat ini mengendalikan ribuan data-data penting, sistem keselamatan dan kaedah-kaedah pengesahan keaslian dilihat sangat penting demi melindungi data-data perubatan. Terdapat tiga teknik penghasilan watermark yang telah diketengahkan demi meningkatkan keutuhan pencapaian algoritma watermark rapuh, justeru menambah baik teknik penomboran sebelum diterapkan data watermark. Tiga teknik yang diketengahkan adalah Authentication Watermarking for Grey-scale Medical Images Using Spiral Manner Numbering (SPIRAL-LSB), Authentication Watermarking for Grey-scale Medical Images Using Hilbert Manner Numbering (HILBERT-LSB) dan Authentication Watermarking for Color Medical Images Using Hilbert Manner Numbering (HILBERT-LSB-C). Setiap kaedah di atas menggunakan cara yang unik dalam menomborkan dan memetakan pixel demi menjamin hasil yang baik dalam sistem pengesahan keaslian. Hal ini dilakukan dengan meletak dan menyebar data asli yang sudah dinomborkan sejauh mungkin dari lokasi asal. Fasa penghasilan watermark dan penerapan ini melalui proses yang serupa, iaitu dengan menghasilkan data pengesahan keaslian melalui operasi yang mudah seperti semakan keseimbangan bit dan perbandingan antara data purata keamatan. Penerapan data watermark kemudian dilakukan pada bit terkurang penting (LSB) . Data pengesahan yang diterapkan dalam imej hos yang sama digunakan untuk menjejak sebarang kerosakan pada imej dengan menggunakan pendekatan berblok (block-wise approach). Kaedah ini tidak rumit malahan efektif kerana ia hanya memerlukan kunci rahsia dan algoritma kucaran terbuka untuk memulihkan imej yang rosak.

TABLE OF CONTENTS

		Page
SUPERVISOR'S DECLARATION		ii
STUDENT'S DECLARATION		iii
DEDICATION		iv
ACKNOWLEDGEMENTS		v
ABSTRACT		vi
ABSTRAK		vii
TABLE OF CONTENTS		viii
LIST OF TABLES		xiii
LIST OF FIGURES		xiv
LIST OF SYMBOLS		xviii
LIST OF ABBREVIATIONS		xix
CHAPTER 1	**INTRODUCTION**	
1.1	Introduction to Security of Information System	1
1.2	Background of Research Problem	2
	1.2.1 Integrity and Authentication of Digital Image	2
	1.2.2 The Numbering in Watermarking	4
	1.2.3 Medical Image Watermarking and Motivation	5
1.3	Problem Statement	8
1.4	Research Questions	9
1.5	Research Objectives	10
1.6	Research Expected Outcome	10
1.7	Research Scope	10
1.8	Thesis Outline	11
1.9	Conclusion	12

CHAPTER 2 LITERATURE REVIEW

2.1 Introduction 13

2.2 General Concepts in the Information Security and The Popular Terminologies 13

2.3 Authentication in Digital Image 19

2.3.1 Technique in Authentication 20
2.3.1.1 Digital Signature Based Approach 20
2.3.1.2 Watermarking-based Approach 20
2.3.2 Digital Image Definition 21
2.3.3 Digital Image Structure 21
2.3.4 Digital Image Format 24
2.3.4.1 Portable Network Graphic (PNG) 24
2.3.4.2 Joint Photographic Experts Group (JPEG) 25
2.3.4.3 Bitmap (BMP) 25
2.3.4.4 Digital Imaging and Communications in Medicine (DICOM) 26

2.4 Fragile Watermarking 26

2.4.1 Features in Fragile Watermarking 28
2.4.1.1 Detection and Localization 28
2.4.1.2 Recovery 29
2.4.1.3 Reversible 30

2.5 Technique Classification of Image Watermarking 31

2.5.1 Spatial Domain 32
2.5.2 Transform Domain 32

2.6 Blind Watermarking 34

2.7 Requirement for Image Watermarking Methods 36

2.7.1 Perceptibility 36
2.7.2 Robustness / Fragileness 37
2.7.3 Capacity 37
2.7.4 Computational Complexity 37

2.8 Attacks to Digital Watermarking 38

2.8.1 Removal Attack 39
2.8.2 Geometry Attack 39
2.8.3 Cryptographic Attack 39
2.8.4 Protocol Attack 40
2.8.4.1 Copy Attack 40
2.8.4.2 Ambiguity Attack 40
2.8.4.3 Scrambling Attack 41

2.9 Performance Measurement Methods 41

	2.9.1	Mean-square error (MSE)	41
	2.9.2	Peak signal-to-noise ratio (PSNR)	41
	2.9.3	Structural similarity index measure (SSIM)	42
2.10	Least Significant Bits (LSB)		43
2.11	Medical Images and the Current Technology		45
	2.11.1	Authentication System in Medical Images	49
		2.11.1.1 Region of Interest (ROI) and Region of Non-Interest (RONI)	49
		2.11.1.2 Criteria to Measure Watermarking for Medical Images	50
2.12	Proposed Schemes of Digital Image Watermarking In Medical Image		55
	2.12.1	Localization Feature in Fragile Watermarking	55
	2.12.2	Reversible Feature in Fragile Watermarking	56
	2.12.3	Recovery Feature in Fragile Watermarking	57
	2.12.4	Block-based Algorithm in Fragile Watermarking	62
	2.12.5	Conclusion of Authentication of Medical Images	65
2.13	Scanning		66
	2.13.1	Spiral Scanning Pattern for Numbering	67
	2.13.2	Hilbert Scanning	68
2.13	Conclusion		70

CHAPTER 3 RESEARCH METHODOLOGY

3.1	Introduction		72
3.2	Research Strategy and Development		72
	3.2.1	Phase 1: Initial Planning	73
	3.2.2	Phase 2: Analysis	78
	3.2.3	Phase 3: Design and Testing	80
3.3	Research Datasets		82
3.4	Research Instrument		85
3.5	Research Analysis		85
3.6	Conclusion		86

CHAPTER 4 AUTHENTICATION WATERMARKING FOR GRAY SCALE MEDICAL IMAGES USING SPIRAL MANNER NUMBERING (SPIRAL-LSB)

4.1 Introduction 87

4.2 SPIRAL-LSB Watermarking 87

4.2.1 Block Numbering and Mapping 88
4.2.2 Watermark Data Generation and Embedding 90
4.2.3 Tamper Detection and Localization 93
4.2.4 Image Recovery 94

4.3 The Results and Discussions 95

4.4 Limitation of SPIRAL-LSB Scheme 107

4.5 Conclusions 108

CHAPTER 5 AUTHENTICATION WATERMARKING FOR GRAY SCALE MEDICAL IMAGES USING HILBERT MANNER NUMBERING (HILBERT-LSB)

5.1 Introduction 110

5.2 Hilbert Manner Numbering In Medical Image Authentication Watermarking (HIBERT-LSB) 110

5.2.1 Block Numbering and Mapping in Hilbert-Lsb 112
5.2.2 Process of Watermark Generation and Embedding in HILBERT-LSB 113
5.2.3 Process of Detection in HILBERT-LSB 115
5.2.4 Process of Recovery in HILBERT-LSB 116

5.3 The Results And Discussions Of HILBERT-LSB Scheme 117

5.3.1 The imperceptibility of HILBERT-LSB scheme 117
5.3.2 Embedding Capacity 123
5.3.3 Time Performance 125
5.3.4 Tamper Localization 127
5.3.5 Recovery Feature 131

5.4 Limitations Of Hilbert-LSB Scheme 135

5.5 Conclusion 137

CHAPTER 6 AUTHENTICATION WATERMARKING FOR COLOR MEDICAL IMAGES USING HILBERT MANNER NUMBERING (HILBERT-LSB-C)

6.1 Introduction 138

6.2 Proposed Hilbert Manner Numbering For Color Image 138

	Watermarking Scheme (HILBERT-LSB-C)	
	6.2.1 Block Division and Mapping	141
	6.2.2 Process of Watermark Generation and Embedding	141
	6.2.3 Process of Tamper Detection	143
	6.2.4 Process of Recovery	146
6.3	The Results and Discussions Of Hilbert-LSB-C Scheme	146
	6.3.1 Quality Evaluation	147
	6.3.2 Performance Evaluation on Different Attacks	150
	6.3.3 Performance Comparison.	159
6.4	Limitations of HILBERT-LSB-C	160
6.5	Conclusion	161

CHAPTER 7 CONCLUSIONS AND REFLECTIONS

7.1	Introduction	163
7.2	Summary of the Research	163
	7.2.1 Summary	164
	7.2.2 Problem Statement of the research	165
	7.2.3 Purpose of the research	165
7.3	Contributions And Limitations	166
7.4	Future Research	170
7.5	Conclusion	171

REFERENCES		173
APPENDICES		187
A	The Developed Programming for 3 Schemes	187
B	Copyright for SPIRAL-LSB	268
C	Copyright for HILBERT-LSB	270
D	List of Publications	273
E	Product Competition Achievement	274
F	System Built For The Schemes	275

LIST OF TABLES

Table No.	Title	Page
2.1	Spatial domain vs. transform domain	33
2.2	Example of LSB (adapted from Sutaone & Khandare (2008))	44
2.3	Summary of tamper localization and recovery watermarking for medical images	61
2.4	Hilbert Scan	70
3.1	Research datasets of grayscale and color images	83
4.1	Comparison with other used watermarking methods using block-based mechanism	97
4.2	The tampered area in yellow circle and the details of recovery performance	103
4.3	Spread block tamper and recovered image by Zain (2006)	106
4.4	Spread block tamper and recovered image by SPIRAL-LSB	107
5.1	Hilbert pattern	113
5.2	Comparison between the original and watermarked images with the PSNR value produced by HILBERT-LSB, SPIRAL-LSB and AW-TDR scheme	122
5.3	The average PSNR values of the recent proposed medical image watermarking schemes	122
5.4	Comparison between the recent block-wise watermarking schemes	124
5.5	The detection rate of HILBERT-LSB	131
6.1	The operating time of each scheme	161
7.1	The summary of contributions from three proposed schemes	170

LIST OF FIGURES

Figure No.	Title	Page
1.1	(a) Raster scan pattern, (b) Reverse raster scan pattern	4
1.2	The black area as the RONI of the image	6
2.1	Cryptography for secure communication	14
2.2	Steganography branches (Penumarthi and Subhash, 2006)	15
2.3	The classification of steganography as proposed by De Vleeschouwer et al. (2002)	16
2.4	A steganography system	16
2.5	Visible Watermarking	18
2.6	Embedder and Extractor of watermarking system	18
2.7	Structure of digital image	22
2.8	The 8-bit binary number, the bit positions and their decimal values.	23
2.9	Calculation example for 00101101 binary	24
2.10	Intensity of 00101101 binary	24
2.11	The mutual dependencies among the elements of the basic requirements in image watermarking (adapted from Langelaar et al., 2000)	38
2.12	Least Significant Bits (LSB)	43
2.13	Cranio-caudal (CC) view of mammogram	47
2.14	Ultrasound image	47
2.15	X-ray radiograph of teeth	47
2.16	Computed tomography of a human brain, from the base of the skull to top	48
2.17	MRI of brain	48
2.18	Tomographic view of a brain examination in transaxial view	48

2.19	(a) shows the watermarked medical images and (b) shows the ROI in white portion and RONI in the black portion of the images (adapted from Maity & Maity, 2012)	50
2.20	Sample of image that contains salt-and-pepper noise; (a) original image, (b) hidden data image with salt-and-pepper, (c) histogram of image	52
2.21	Multi slices of MRI	53
2.22	Several types of Scan: (a) Raster, (b) Spiral, (c) Zeta, (d) Diagonal, (e) Hilbert	67
2.23	Spiral numbering starting from the centre; showing the ring level	68
2.24	Hilbert Scanning Pattern: (a) 2 x 2 pixels, (b) 4 x 4 pixels, (c) 8 x 8 pixels	68
3.1	Research Framework of SPIRAL-LSB	73
3.2	(a) Spiral numbering of blocks, as recorded in Matlab software (b) mapping with k = 1193	77
3.3	Numbering by Zain (2006)	79
3.4	The flowchart of research structure	82
4.1	Functional block diagram for watermark numbering, mapping, generation and embedding in the proposed scheme	89
4.2	An example of spiral numbering from the centre for 5 x 5 block	89
4.3	Block of 8 x 8 pixels and sub-block of 4 x 4 pixels (represent by four colors)	91
4.4	Block of location of watermarked bits in cover object (the white region is the original data, and the orange region is the embedding bits)	92
4.5	The PSNR values of 70 datasets from embedding process	96
4.6	(left) the original MRI brain image; (centre) the watermarked bits; (right) the watermarked image	96
4.7	(from left) a) original image; b) watermarked image; c) removal attack at the centre; d) detected tamper in red	97
4.8	(from left) a) original image; b) watermarked image; c)	98

	removal attack at the centre; d) detected tamper in red	
4.9	a) The watermarked mammogram; b) tampered with unsharp mask filter; c) tampered with salt-and-pepper noise; (From bottom left) d) tampered with cloning; e) tampered with convolve filter; f) tampered with Gaussian blur filter	99
4.10	a) detecting unsharp mask filter area; b) detecting salt-and-pepper noise area; c) detecting cloning area; (From bottom left) d) detecting convolve filter area; e) detecting Gaussian blur filter area; f) recovered mammogram	99
4.11	(From left) A mammogram with a tamper; The recovered version of mammogram	101
4.12	Zoomed pixels of recovered image in Figure 4.6	101
4.9	Original mammogram and the watermarking data	108
5.1	The flow diagrams for proposed numbering technique	111
5.2	The flow diagrams for proposed embedding technique	111
5.3	A brain MRI and the embedded data in the LSB	114
5.4	A detected change in the MRI of brain in colored label	116
5.5	(a), (c), (e), (g), (i), (k) Original image; (b) watermarked image (58.9348 dB), (d) watermarked image (53.6794 dB), (f) watermarked image (58.8268 dB), (h) watermarked image (58.3968 dB), (j) watermarked image (55.4978 dB), (l) watermarked image (58.4014 dB),	121
5.6	PSNR value of the image after being embedded with watermark data	121
5.7	The operating time in embedding phase for mammogram, ultrasound, MRI, X-ray and CT scan images	126
5.8	The operating time in recovery phase for numerous tampers between SPIRAL-LSB and HILBERT-LSB	126
5.9	Block-based tamper localization; (a) mosaic effect; (b) 996 tamper blocks detected; (c) clone attack; (d) 1868 tamper blocks detected; (e) shade addition; (f) 1096 tamper blocks detected; (g) Gaussian blur attack; (h) 724 tamper blocks detected; (i) color paint; (j) 104 tamper blocks detected; (k) cut-and-paste attack; (l) 502 tamper blocks detected; (m) collage attack; (n) 576 tamper blocks detected	130

5.10	Zoom in figure 5.9 (l) and (n) respectively	130
5.11	Block-based recovery; (a) mosaic effect (b) recovered image (50.9309 dB); (c) clone attack (d) recovered image (51.6163 dB); (e) shadow addition (f) recovered image (69.2627 dB); (g) Gaussian blur attack; (h) recovered image (45.5714 dB); (i) color paint (j) recovered image (58.4551 dB); (k) cut-and-paste attack; (l) recovered image (75.5038 dB); (m) collage attack (n) recovered image (71.3960 dB)	135
5.12	HILBERT-LSB on color image; (a) work well for embedding; (b) tampered color image; (c) color image is not fully recovered	136
6.1	The Flow Diagram for Proposed Technique to Embed in Color Medical Images	140
6.2	The location of embedded bits in a color host object (white region is the original data and orange region is the embedding bits)	143
6.3	The flow diagram for proposed tamper detection and recovery in proposed watermarking scheme	145
6.4	Color cover images used in the simulation and their watermarked color images; (a) brain MRI, (b) watermarked MRI (PSNR: 57.1472) (c) cells PET, (d) watermarked PET (PSNR: 58.8429 dB) (e) brain DTI, (f) watermarked DTI (PSNR: 58.749 dB (g) 4-dimensional ultrasound, (h) watermarked ultrasound (PSNR: 58.7646 dB) (i) pelvis CT, (j) watermarked CT (PSNR: 54.089 dB (k) hand x-ray, and (l) watermarked x-ray (PSNR: 58.4788 dB)	150
6.5	Cut-and-paste attack; (a) tampered 'brain', (b) detected 'brain', (c) recovered 'brain' (PSNR: 64.35 dB), (d) tampered 'pelvis', (e) tamper detected 'pelvis', (f) recovered 'pelvis' (PSNR: 67 dB), (g) tampered 'fetus',(h) tamper detected 'fetus' (i) recovered 'fetus' (PSNR: 69 dB)	154
6.6	Collage attack; (a) tampered 'cells', (b) detected 'cells', (c) recovered 'cells' (PSNR: 61 dB), (d) tampered 'hand', (e) tamper detected 'hand', (f) recovered 'hand' (PSNR: 63.5 dB)	156
6.7	Filter attack; (a) tampered 'pelvis' with jitter filter, (b) detected 'pelvis', (c) recovered 'pelvis' (PSNR: 67.3 dB) (d) tampered 'brain tissue' with mosaic filter , (e) detected 'brain tissue', (f) recovered 'brain tissue' (PSNR: 65 dB)	158

LIST OF SYMBOLS

I	Image
μ_I	Luminance (photometric measure of the density)
σ_I	Standard deviation
C_I	Constant
dB	Decibel
B	Block
B_s	Sub block
N_b	Total number of blocks in the image
H	Hilbert scan pattern
V	Authentication watermark
P	Parity check bits
R	Recovery intensity
s	Spiral pattern

LIST OF ABBREVIATIONS

ASCII	American Standard Code for Information Interchange
AW-TDR	Authentication Watermarking with Tamper Detection and Recovery
BMP	Bitmap
CC	Cranio-caudal
CRC	Cyclic Redundancy Check
CT	Computed Tomography
DCT	Discrete Cosine Transform
DE	Difference Expansion
DFT	Discrete Fourier Transform
DICOM	Digital Imaging and Communications in Medicine
DTI	Diffusion tensor imaging
DWT	Discrete Wavelet Transform
EZW	Embedded zero-tree wavelet
HIS	Hospital information system
JPEG	Joint Photographic Experts Group
KeV	Kiloelectronvolt
LSB	Least Significant Bits
LUT	Look-up table
MRI	Magnetic Resonance Imaging
MSB	Most Significant Bits
MSE	Mean-square error
PACS	Picture Archiving and Communication System
PSNR	Peak signal-to-noise ratio

PNG	Portable Network Graphics
RAM	Random-access memory
RGB	Red, Green, Blue
ROA	Region of authentication
ROI	Region of interest
RONI	Region of non-interest
RSMA	ROI Segmentation and Multilevel Authentication
SSIM	Structural similarity index measure
SLT	Slantlet transform
TALLOR	Tamper localization and lossless recovery
VQ	Vector quantization
2D	Two dimensional
3D	Three dimensional

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION TO SECURITY OF INFORMATION SYSTEM

Nowadays, we are enjoying the technology of digital multimedia which offers so many new advantages compared to the one provided by old analog counterpart. We are free to transmit the digital data, edit any part of the digital content, copy a digital content with the same quality as original, and many more. The technology becomes more superior with the existence of speedy Internet and wireless applications. The distribution and use of multimedia data are much easier and faster with the growth of Internet technology.

The technology comes with great problems too, besides its significant advantages. The great facility in copying a digital content rapidly, perfectly and without limitations on the number of copies has resulted in the problem of copyright protection (Koz, 2002). There always has been a problem in creating the identification of the original owner. Therefore, the security of information field has been a very active research area in recent years. Among the technology invented in this area are watermarking, steganography and cryptography.

The digital watermarking for integrity verification is called fragile watermarking as compared to robust watermarking for copyright protection. Robust is designed to survive malicious and non-malicious modifications, which aim at removing or distorting the watermark. While in a fragile watermarking scheme, the embedded watermark should be fragile to modifications so as to detect and localize any modification in the presence of different attacks. While, semi-fragile watermarks are designed to detect any unauthorized modification at the same time allowing some image- processing operations (Zain, 2007; Kuang et al., 2009; Halder et al., 2010; Liew, 2011; Zhou & Lv, 2011).

1.2 BACKGROUND OF RESEARCH PROBLEM

For the purpose of understanding the research problem easier and clearer, this section is divided into three parts, which will lead to the problem statements of the thesis. First, we will find out what are the concepts of image authentication and the problem in security of medical images. Second, to limit the problem to a smaller scope, we will review the current numbering in watermarking and its flaw in the system. With that, the third section will discuss the implementation of security technology in them to cater the stated problems, with the approach of digital watermarking.

1.2.1 Integrity and Authentication of Digital Images

Among the methods to protect the security of digital data, digital watermarking has gained more and more interest from researchers and users attributable to its versatility and its potential to preserve integrity and authentication of digital images. By the Oxford Dictionary, integrity means the state of being whole and undivided. To this point, the integrity of image is defined as the state of not being attacked or changed. Whereas, authentication means proving or showing (something) to be true, genuine, or valid, which in this case, the authentic image is found to be original or genuine. Among the method to prove authentication of images is the localization of tamper.

Together with it, digital watermarking can, theoretically, distinguish the kinds of manipulations and attacks from the third party. In this case, manipulations consist of allowed and not allowed one (Caldelli et al., 2006).

As mentioned in the previous section, three approaches are applied in watermarking. They are fragile watermarking, robust watermarking, and the other one is semi-fragile watermarking which is a combination of fragile and robust elements.

Authentication through fragile watermarking is accomplished by embedding a watermark within the image itself, which the watermark is easily changed or ruined once the watermarked image experiences any manipulations or attacks. The modification or deletion of the watermark is detected when comparing with the actual content of an image (Caldelli et al., 2006). A mismatch allows the receiver or the holder of the image to find out that the image is not authentic anymore. The accurate recovery process is done by retrieving the hidden data that able to pertain to the origin (Zain, 2006; Fridrich et al., 2000; Holliman & Memon, 2000; Liew, 2011). Some popular techniques localize and recover the altered areas in a block-wise (Fridrich & Goljan, 1999; Kim et al., 2012; Zain & Afifah, 2007). Some schemes also insert information about the image while embedding (Giakoumaki et al., 2004; Manaf et al., 2010).

While in contrast, schemes which based on robust watermarking (Fridrich, 1998; Fu and Shen, 2008; Kuang and Chen 2010; Sun & Bo, 2010) suppose that a good watermark is not affected by any image manipulations or attacks. A robust watermark should be able to survive from any process of additive Gaussian noise, compression, printing and scanning, rotation, scaling, cropping and many other operations. The ability to survive leads to the meaning of substantial integrity of an image.

Nowadays, the usage of the digital image is everywhere, in formal business and informal business in the life of people. This revolution helps the pirates to exploit these features for their intended purpose illegally (Cox et al., 2002). Therefore, the demand for the authentication methods of digital media becomes a significant issue to ensure that work has not been tampered with, especially for critical cases like national security, medical safety, internet banking and transfer of military information and forensic investigations.

The prime advantage of digital watermarking is that the authentication information is directly embedded into the image data. Consequently, the authentication information survives, although the watermarked image undergoes format conversion and the retrieving process is stated as easier and less complicated (Zain, 2006). Embedding the authentication code in the image will also make it less sensitive to attack than appending the information on a medical image (Manaf et al., 2010; Boucherkha & Benmohamed, 2005).

1.2.2 The Numbering in Watermarking

In block-wise method of authentication watermarking, pixels or blocks of images need to be numbered before being embedded in the host image. Most of the developed watermarking use raster pattern of numbering, as shown in Figure 1.1. Chang (2007) claims that modification to some blocks would be done effortlessly if malicious attackers know the block mapping sequence in advance, which in this case when we use the typical raster pattern.

Block numbering process is seen as critical as it also decides the location of the embedded watermark data when mapping. With the probability of getting the tamper in the middle of medical images is high, a unique numbering system is seen as helpful to protect the region of interest in the middle (Zain, 2005).

Reconstruction is achieved by embedding the recovery bits in a block some distance away from the original block as suggested by Fridrich and Goljan (1999). From the experimental results, it showed that the recovery bits were not embedded in blocks situated in the same column, but with some percentage in the same row. Those in the same row must have odd blocks distance from the original because the way we spread the tamper was by using the same size, as the block use for embedding and the distance from each other were, at least, one block.

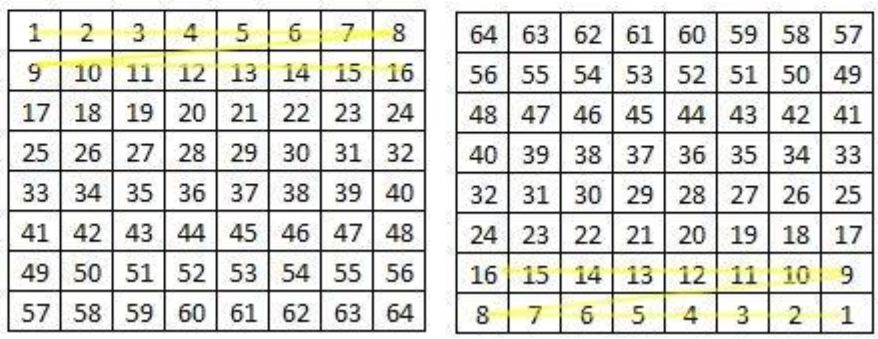

Figure 1.1: (a) Raster scan pattern, (b) Reverse raster scan pattern

1.2.3 Medical Image Watermarking and Motivation

The idea of using watermarking on medical data is a security issue in the sense that we want to ensure the critical medical data is authentic when the radiologist and doctor refer it. Nowadays, medical images are not printed anymore. Since many advantages of using digital medical images are discovered and it is frequently used in the medical domain, most hospitals are facing issues to manage a large amount of data storage such as administrative documents, patient's information and medical images. Therefore, it is important to handle those data accurately to avoid the problem of lost, tampering, manipulation and mishandling record at the hospital (Manaf et al., 2010). Thus, the digital watermarking is becoming a new research focus for medical documents, specifically medical images (Planitz & Maeder, 2005; Coatrieux et al., 2005; Feng et al., 2006; Wang et al., 2008; Coatrieux et al., 2013; Huang et al., 2012; Bouslimi et al., 2012; Rao and Kumari, 2011; Chen et al., 2010; Vellaisamy & Ramesh, 2013; Tripathi, 2013; El-Haj and Amer, 2014; Eswaraiah & Reddy, 2014).

Another advantage of having medical image watermarking is it can help the clinical staff to find or examine the old medical image in the Hospital Information System (HIS) collection because there are some cases that medical images and patient's records need to be verified for the integrity before use. Besides, images usually are the prime tool to discover new findings in the medical case. Thus, it is needed to protect the copyright and integrity of the medical image by digital watermarking for the sake of medical study (Boucherkha & Benmohamed, 2005).

Medical images are also compelling as there are used for jurisdiction proof and documents for insurance claim nowadays. Thus, watermarking is needed as to ensure all the attached documents and evidence are valid and not edited.

Various researches on the medical image watermarking have been done for copyright protection, authentication and patient management system. Furthermore, in future medical information database system, it is forecasted to be integrated with the watermarked scheme that is used to protect the security of each personal data and medical information (Liew, 2011; Ping et al., 2007; Babel et al., 2008; El-haj & Amer, 2014).

Regarding medical use, a primary concern among the clinical professionals is that the probability of being modified by attackers, thus, the demand for the authentication and originality is high (Coatrieux et al., 2000; Tan et al., 2011). Image authentication can assure receivers that the received image is from the authorized source and that the image content is identical to the one sent (Zain, 2005). Nowadays, even by using generic software for image elaboration, a medical image can be attacked by erasing or adding any sign of disease onto it. If this image were a critical piece of evidence in a legal case or police investigation, this form of tampering might pose a serious problem. Especially where the telemedicine technology is widely implemented, it is a serious call to start implementing the security system to medical images.

One of the requirements of an effective watermarking based authentication system as defined by Liu and Qiu (2002) is the ability to identify manipulated area or also known as localization where the authentication watermark should be able to detect the location of manipulated areas, and verify other areas as authentic. This feature is very useful to watermarking for medical images. The ability is not only saying there is a tamper mark but stating where the mark too. This feature can help validating whether the medical image is still up to be used for diagnosis or not. If the locality of the tamper is not in the region of interest, for an example, in the black areas of ultrasound and an x-ray (as shown in Figure 1.2), they will not give any misleading information to the doctors.

Figure 1.2: The black area as the RONI of the image

Many researches had been done in tampering localization field (Liew, 2012; Tan et al., 2011; Guo & Zhuang, 2009; Osamah & Khoo, 2011; Kim et al., 2011; Giakoumaki et al., 2004; Pushpita & Nigudkar, 2005; Zain & Abdul, 2006; Liu et al., 2008; Walia and Suneja, 2013; Coatrieux et al., 2013; Huang et al., 2012; Naskar and Chakraborty, 2012; Rao and Kumari, 2011; Liew and Zain, 2011; Chen et al., 2010). The challenge is whether it is reversible or can be recovered. Although these two schemes are alike, they are not same.

The reversible watermarking scheme can reverse from a watermarked image to original one. In some cases, modification of the original pixel value is often not approved by professionals and watermarking scheme used should be reversible (Coatrieux et al., 2000). Radiologist generally prefers the original image for diagnostic purposes (Tan et al., 2011).

Recovery of the tampered region is functional to know exactly what had tampered and the motive of the tampering. Liew (2012) defined recovery scheme as to recover tampered images that have been attacked. Removal attack is a crucial problem for medical images. This attack category includes compression, noising, sharpening and histogram equalization.

One popular mechanism to develop a fragile watermarking scheme that has tamper localization and recovery feature is the block-based mechanism. It is a popular mechanism introduced by Fridrich and Goljan (1999) and is well-known to explain the problem of collage attack, vector quantization (VQ) counterfeiting attack and cut-and-paste attack (Fridrich & Goljan, 1999; Holliman & Memon, 2000; Zain, 2006; Liu, 2012). The method is by separating the block independence to enable recovery data embedding in block by block. However, it is well-known that most introduced schemes which implementing block-based mechanism are using raster manner of numbering, which, ill-mannered attackers can just modify the watermarked image and cover it up if they manage to obtain the block-mapping sequence in advance (Chang et al., 2008).

Accordingly, Fridrich and Goljan (1999) stated that reconstruction is accomplished by embedding the recovery bits in a block far from the original block. From the experimental results done by Zain (2011), it showed that the recovery bits were not embedded in blocks situated in the same column, but with some percentage in the same row. Those in the same row must have an odd distance from the original because the way we spread the tamper was by using the same size, as the block used for embedding and the distance from each other were, at least, one block. If we change the tamper block size in the spread-tampered blocks, then we may have a different result.

For medical images, which usually have the region of interest at the centre (as shown in Figure 1.2), the way we embed recovery data at the centre is crucial. When pseudorandom mapping process takes place, the mapping will lead the important recovery data to the centre if the block data is numbered in raster path. Thus, the unique way of block numbering can help to further the location of recovery data.

Sun and Bo (2010) agreed that colour medical images are playing an important role in the future medical systems. Therefore medical image watermarking research should focus on colour medical images too. CT, MRI, ultrasound, PET and DTI are produced in grey-scale and colour version, and clinical professionals widely use both. Nevertheless, the schemes for colour images should have good transparency and high capacity too.

The trend shows that a lot of reviewed schemes focus on hiding the medical information of the patient in medical images (Engan et al., 2003; Li et al., 2007; Manaf et al., 2010). Nonetheless, some schemes introduce tamper detection for medical images to ensure only authentic image is valid to be used. Some current schemes for medical images had shown better functions by having all three ability to localize tampers, recover to the original image and can be reversed, yet, most tested image modalities are only gray-scale images of magnetic resonance imaging (MRI), ultrasound (US) and common x-ray. In this study, we aim to develop a tamper localization and recovery scheme of watermarking that suits most of the medical modalities.

1.3 PROBLEM STATEMENT

Due to the main concern expressed by clinical professionals about the probability of electronic medical images being modified by attacker, thus, the demand

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION TO SECURITY OF INFORMATION SYSTEM

Nowadays, we are enjoying the technology of digital multimedia which offers so many new advantages compared to the one provided by old analog counterpart. We are free to transmit the digital data, edit any part of the digital content, copy a digital content with the same quality as original, and many more. The technology becomes more superior with the existence of speedy Internet and wireless applications. The distribution and use of multimedia data are much easier and faster with the growth of Internet technology.

The technology comes with great problems too, besides its significant advantages. The great facility in copying a digital content rapidly, perfectly and without limitations on the number of copies has resulted in the problem of copyright protection (Koz, 2002). There always has been a problem in creating the identification of the original owner. Therefore, the security of information field has been a very active research area in recent years. Among the technology invented in this area are watermarking, steganography and cryptography.

The digital watermarking for integrity verification is called fragile watermarking as compared to robust watermarking for copyright protection. Robust is designed to survive malicious and non-malicious modifications, which aim at removing or distorting the watermark. While in a fragile watermarking scheme, the embedded watermark should be fragile to modifications so as to detect and localize any modification in the presence of different attacks. While, semi-fragile watermarks are designed to detect any unauthorized modification at the same time allowing some image- processing operations (Zain, 2007; Kuang et al., 2009; Halder et al., 2010; Liew, 2011; Zhou & Lv, 2011).

1.2 BACKGROUND OF RESEARCH PROBLEM

For the purpose of understanding the research problem easier and clearer, this section is divided into three parts, which will lead to the problem statements of the thesis. First, we will find out what are the concepts of image authentication and the problem in security of medical images. Second, to limit the problem to a smaller scope, we will review the current numbering in watermarking and its flaw in the system. With that, the third section will discuss the implementation of security technology in them to cater the stated problems, with the approach of digital watermarking.

1.2.1 Integrity and Authentication of Digital Images

Among the methods to protect the security of digital data, digital watermarking has gained more and more interest from researchers and users attributable to its versatility and its potential to preserve integrity and authentication of digital images. By the Oxford Dictionary, integrity means the state of being whole and undivided. To this point, the integrity of image is defined as the state of not being attacked or changed. Whereas, authentication means proving or showing (something) to be true, genuine, or valid, which in this case, the authentic image is found to be original or genuine. Among the method to prove authentication of images is the localization of tamper.

Together with it, digital watermarking can, theoretically, distinguish the kinds of manipulations and attacks from the third party. In this case, manipulations consist of allowed and not allowed one (Caldelli et al., 2006).

As mentioned in the previous section, three approaches are applied in watermarking. They are fragile watermarking, robust watermarking, and the other one is semi-fragile watermarking which is a combination of fragile and robust elements.

Authentication through fragile watermarking is accomplished by embedding a watermark within the image itself, which the watermark is easily changed or ruined once the watermarked image experiences any manipulations or attacks. The modification or deletion of the watermark is detected when comparing with the actual content of an image (Caldelli et al., 2006). A mismatch allows the receiver or the holder of the image to find out that the image is not authentic anymore. The accurate recovery process is done by retrieving the hidden data that able to pertain to the origin (Zain, 2006; Fridrich et al., 2000; Holliman & Memon, 2000; Liew, 2011). Some popular techniques localize and recover the altered areas in a block-wise (Fridrich & Goljan, 1999; Kim et al., 2012; Zain & Afifah, 2007). Some schemes also insert information about the image while embedding (Giakoumaki et al., 2004; Manaf et al., 2010).

While in contrast, schemes which based on robust watermarking (Fridrich, 1998; Fu and Shen, 2008; Kuang and Chen 2010; Sun & Bo, 2010) suppose that a good watermark is not affected by any image manipulations or attacks. A robust watermark should be able to survive from any process of additive Gaussian noise, compression, printing and scanning, rotation, scaling, cropping and many other operations. The ability to survive leads to the meaning of substantial integrity of an image.

Nowadays, the usage of the digital image is everywhere, in formal business and informal business in the life of people. This revolution helps the pirates to exploit these features for their intended purpose illegally (Cox et al., 2002). Therefore, the demand for the authentication methods of digital media becomes a significant issue to ensure that work has not been tampered with, especially for critical cases like national security, medical safety, internet banking and transfer of military information and forensic investigations.

The prime advantage of digital watermarking is that the authentication information is directly embedded into the image data. Consequently, the authentication information survives, although the watermarked image undergoes format conversion and the retrieving process is stated as easier and less complicated (Zain, 2006). Embedding the authentication code in the image will also make it less sensitive to attack

CHAPTER 3

RESEARCH METHODOLOGY

3.1 INTRODUCTION

This chapter starts with describing the strategy used and the followed subchapters are divided based on the objectives. The main discussion will be concentrated on the efficient and effective watermarking methods to be proposed for image tamper localization and recovery in this study. This chapter is structured as follows:

- Section 3.2 describes the strategy used to finish all the development in this project. It explains about a set of the methodology used to conduct research that consists of three phases.
- Section 3.3 describes the sample used for this method.
- Section 3.4 clarifies the instrument used for the method.
- Section 3.5 describes the method to evaluate the performance of the proposed scheme.
- Section 3.6 gives the summary of the chapter.

3.2 RESEARCH STRATEGY AND DEVELOPMENT

Three phases involved at this stage. Figure 3.1 shows the framework of SPIRAL-LSB development methodology, which was the first algorithm proposed in the thesis.

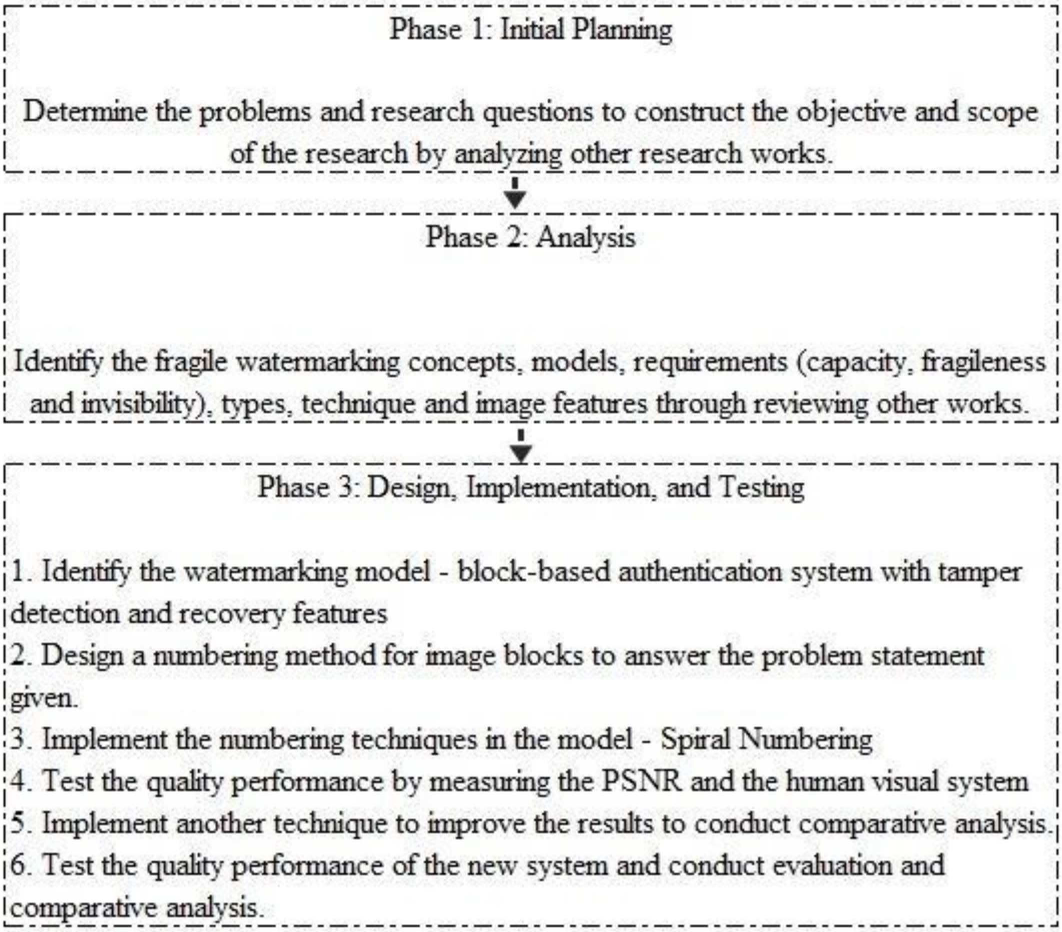

Figure 3.1: Research Framework of SPIRAL-LSB

In methodology phase, each activity that needed to do was identified to accomplish the objectives.

3.2.1 Phase 1: Initial Planning

In the initial planning stage, the study about the project was done. The problems faced by watermarking in medical imaging were determined by studying the previous works of other researchers. After obtaining the problems, the questions of the research were constructed followed by objectives that answered all the research questions. Also, the scope of the project was also identified to narrow down the boundary of the project.

We tried to answer these questions along the way completing the research;

- Will unique numberings make a difference in the distribution of blocks?

- Will unique numberings help to keep the recovery data safe from tamper?
- Are unique numberings suitable to be used when embedding a watermark in medical images?

Chang (2007) claims that modification to some blocks would be done effortlessly if malicious attackers know the block mapping sequence in advance, which in this case when we use the typical raster pattern. Hung (2013) also states that a unique scan pattern is known as the secure method of encryption for having great compression before embedding, which would be further investigated in this research whether it is also good in watermarking or not.

Block numbering process is seen as critical as it also decides the location of the embedded watermark data when mapping. With the probability of getting tamper attacks in the middle of the medical image is high, a unique numbering system is seen as helpful to protect the region of interest in the middle (Zain, 2005). However, as we aimed to develop schemes that are compatible with all types of modalities, we could not say that the ROI is definitely in the middle only. As an example, a scanned femur in MRI will have the ROI as from top to the bottom of the image as that part of a body is long.

Many patterns can be studied to investigate the ability of unique patterns to improve the performance of watermarking and its recovery feature. The spiral pattern is not complex, yet has a different way of arranging the pixel when comparing to raster pattern. The key to its specialty is because the pattern starts at the centre of the image. This specialty suits the mapping method which is pseudorandom, where the original location of the pixels at the central will be scattered far away from the central in the host image. The rest of the pixels will be following the principle, even though the farthest distance between the original and recovery data location will be the central pixels.

Other than the hypothesis that spiral numbering helps further the embedded bits from the original blocks, another advantage of spiral numbering technique is in the fact that a significant computational outcome is possible rather than using the full raster scan (Sims & Poularikas, 1990). After using the double function of the ring type spiral scan,