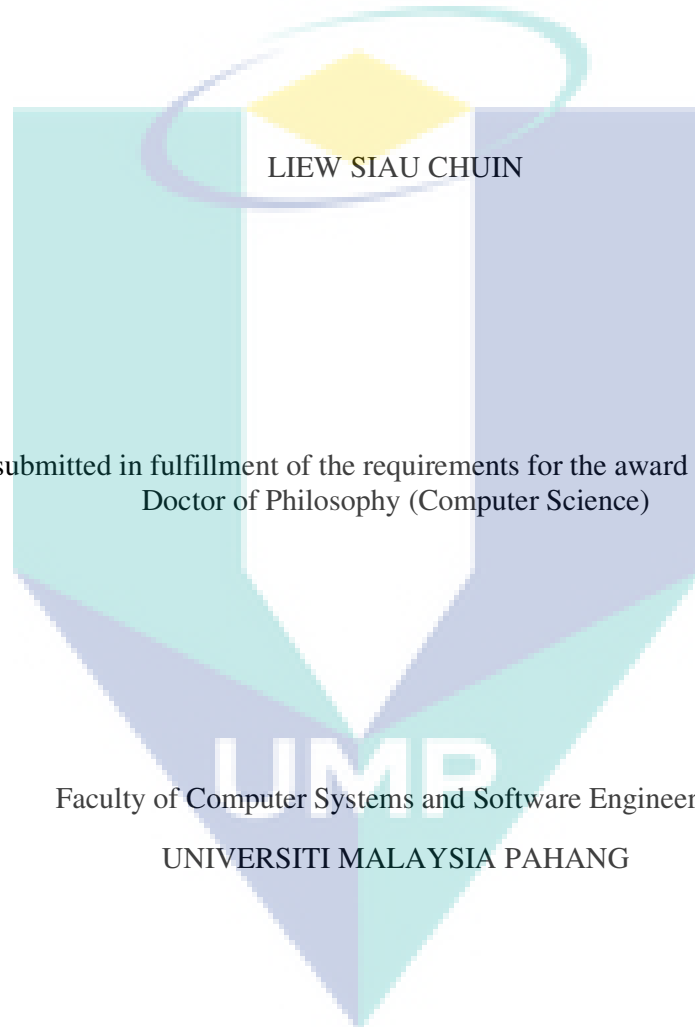


TAMPER LOCALIZATION AND RECOVERY WATERMARKING SCHEMES FOR
MEDICAL IMAGES IN PACS



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

Faculty of Computer Systems and Software Engineering

UNIVERSITI MALAYSIA PAHANG

JULY 2011

SUPERVISOR'S DECLARATION

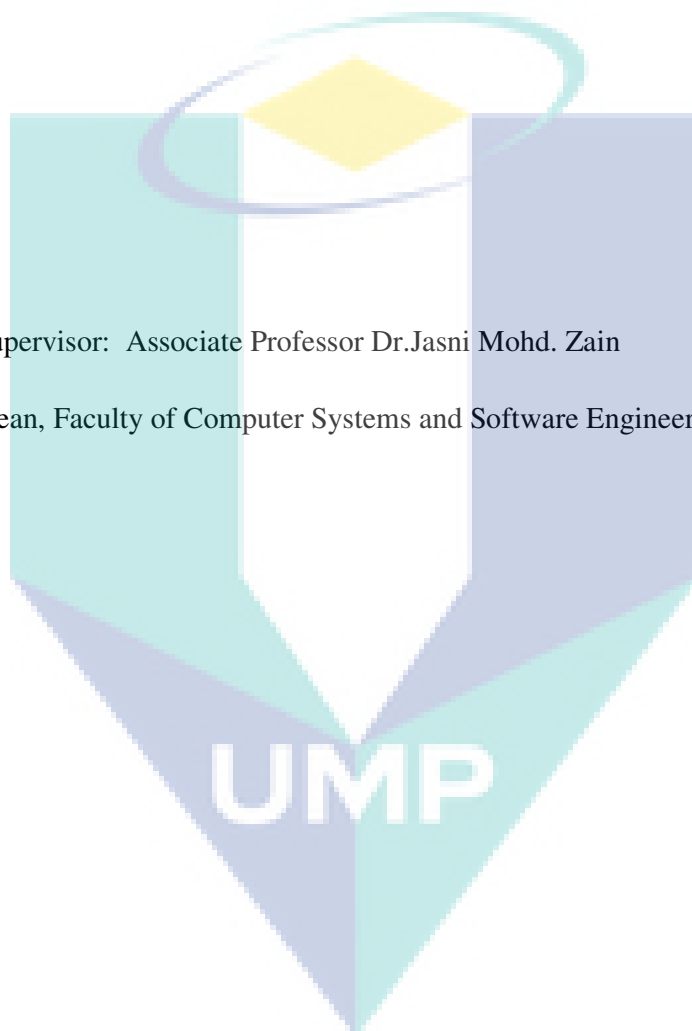
I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Doctor of Philosophy in Computer Science.

Signature

Name of Supervisor: Associate Professor Dr.Jasni Mohd. Zain

Position: Dean, Faculty of Computer Systems and Software Engineering

Date:



STUDENT'S DECLARATION

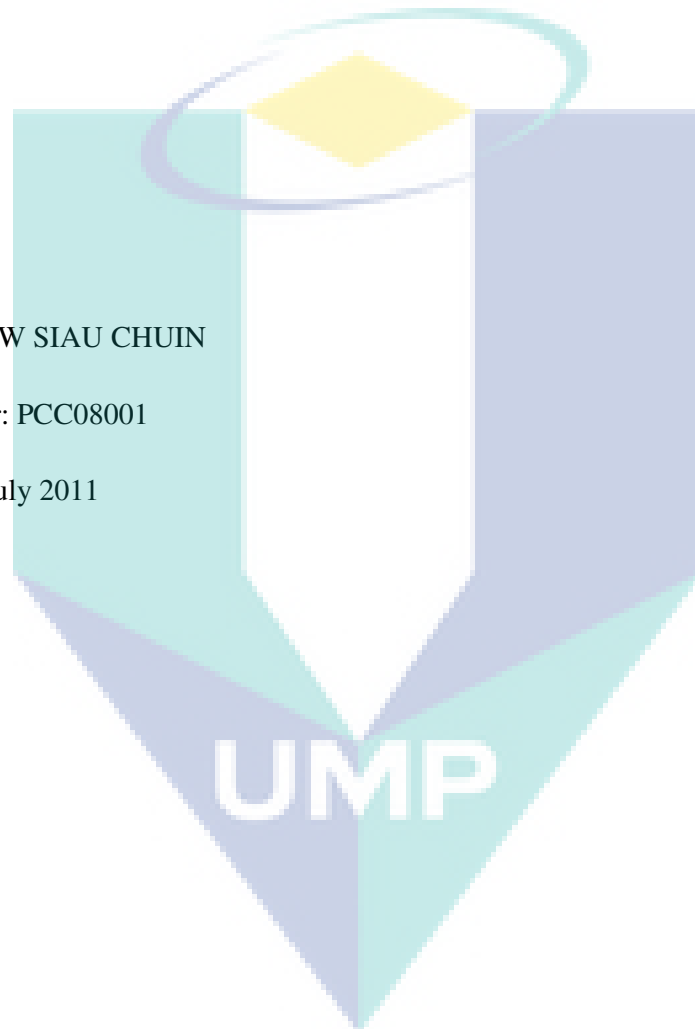
I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged. The thesis has not been accepted for any degree and is not concurrently submitted for award of other degree.

Signature

Name: LIEW SIAU CHUIN

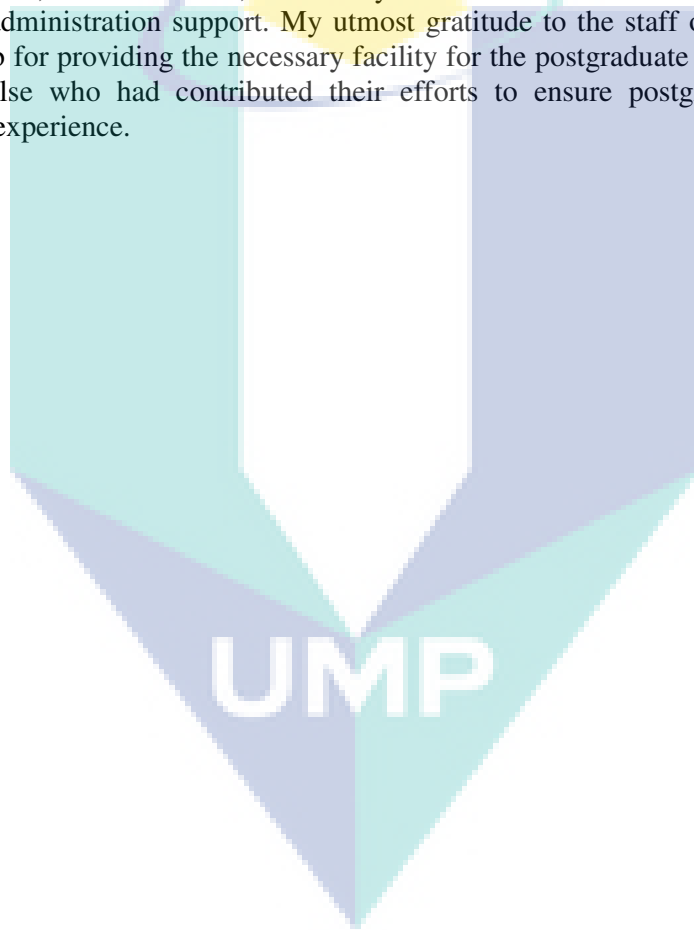
ID Number: PCC08001

Date: 6th July 2011



ACKNOWLEDGEMENTS

Firstly, I would like to thank my supervisor, Associate Prof. Dr. Jasni Mohd. Zain for her encouragement and support. My sincere thanks to my wife for her support and understanding as well as her endless love. To my two lovely princesses, thank you for the source of motivations and inspirations. Special thanks to my brother for his support and assistance. My greatest gratitude to my parents for being there for me. Not forgetting Dr. Tutut and Dr. Azhar for their valuable comments. I would also like to thank Ms. Rezita and also the CGS staffs for the support provided. Many thanks to Mdm. Fauziah, Mdm. Darwina, Ms. Rohaya and others in the faculty for providing the necessary administration support. My utmost gratitude to the staff of the postgraduate research lab for providing the necessary facility for the postgraduate students. Lastly, to everyone else who had contributed their efforts to ensure postgraduate studies an invaluable experience.



ABSTRACT

This thesis focuses on the implementation of medical image watermarking in Picture Archiving and Communications System (PACS). PACS is an important part of information technology infrastructure in a health institution. Medical images stored in PACS are vulnerable to malicious modifications. Watermarking can be used to authenticate medical images and provide the additional security needed on top of the existing security measures that were already in place. Watermarking methods applied to medical images should be reversible or if not, an area known as a region of interest (ROI) needs to be defined on the image to retain the original information. The watermarked image produced should have visual quality similar to its original version. Watermarking schemes should also be tested in a simulated operational environment for practicality verification. In this thesis, three watermarking schemes for medical image are proposed. All three watermarking schemes were tested by watermarking eight different samples. The PSNR of the watermarked images were measured. The watermarked images were tampered by cloning, salt and pepper noise, rotation and smoothing. The tampered images were recovered and the success rates were taken. The first proposed scheme, the reversible tamper localization and recovery scheme (R-TLR). The watermarked image can be reversed by restoring the least significant bits (LSBs) in a predefined region of interest (ROI) and regions of non-interest (RONI) to their original states. The watermarked images have an high average PSNR of 53.9 dB. The success rate of the tamper localization and recovery is close to 100%. Secondly, the tamper localization and lossless recovery (TALLOR) scheme uses compressed recovery information embedded outside of the ROI to achieve exact or lossless recovery after tampering is detected. Thirdly, an enhanced scheme, the tamper localization and lossless recovery with ROI segmentation (TALLOR-RS) is also proposed. It managed to reduce the tamper localization and recovery average processing time by approximately 53%. The average PSNR of the watermarked images for both schemes is high at 48.3 dB and 48.2 dB for TALLOR and TALLOR-RS respectively. The proposed schemes have 100% success rate for tamper localization and recovery. Both schemes also performed better than the scheme developed by Osamah and Khoo(2011). The proposed watermarking schemes were then tested in a simulated PACS environment with good results. A design of a watermark embedder and image authenticator (WEIA) to facilitate the implementation of watermarking in PACS is then proposed. In conclusion, watermarking schemes can be effectively implemented in practice to prevent fraud and improve information security.

ABSTRAK

Tesis ini tertumpu pada pelaksanaan tanda air untuk imej perubatan di dalam *Picture Archiving and Communications System (PACS)*. *PACS* adalah infrastruktur teknologi maklumat yang penting bagi sesuatu institusi kesihatan. Imej-imej perubatan yang disimpan di dalam *PACS* adalah terdedah kepada pengubahsuaian yang tidak dibenarkan. Tanda air boleh digunakan untuk pengesanan imej perubatan dan memberikan keselamatan tambahan yang diperlukan selain daripada langkah-langkah keselamatan yang sedia ada. Kaedah penandaan air yang digunakan untuk imej perubatan haruslah reversibel atau suatu bahagian yang dikenali sebagai *region of interest (ROI)* perlu ditakrifkan pada imej untuk mengekalkan maklumat asli. Imej yang telah melalui proses penandaan air mestilah mempunyai kualiti visual yang mirip dengan versi asal. Skim penandaan air juga harus diuji dalam simulasi persekitaran operasi untuk pengesanan. Di dalam tesis ini, tiga skim penandaan air untuk imej perubatan telah dicadangkan. Pertama, skim *reversible tamper localization and recovery (R-TLR)*. Imej yang telah melalui proses penandaan air boleh dipulihkan kepada versi yang asal dengan memulihkan *least significant bits (LSBs)* di dalam *ROI* dan *region of non-interest (RONI)*. Kedua, skim *tamper localization and lossless recovery (TALLOR)* yang menggunakan maklumat pemulihan yang disimpan di *RONI* untuk mencapai pemulihan yang *lossless* jikalau pengubahsuaian dikesan. Ketiga, skim *tamper localization and lossless recovery with ROI segmentation (TALLOR-RS)* juga dicadangkan. Tujuan skim ini adalah untuk mengurangkan masa pemprosesan untuk mengesan dan memulihkan sebarang pengubahsuaian. Skim penandaan air yang dicadangkan kemudian diuji dalam persekitaran *PACS* yang disimulasikan dengan keputusan yang baik. Aplikasi *watermark embedder and image authenticator (WEIA)* untuk memudahkan pelaksanaan penandaan air dalam *PACS* telah dicadangkan. Sebagai kesimpulan, skim penandaan air dapat dilaksanakan secara berkesan untuk mengelakkan penipuan dan meningkatkan keselamatan maklumat.

UMP

TABLE OF CONTENTS

	Page
SUPERVISOR’S DECLARATION	ii
STUDENT’S DECLARATION	iii
ACKNOWLEDGEMENTS	iv
ABSTRACT	v
ABSTRAK	vi
TABLE OF CONTENTS	vii
LIST OF TABLES	xii
LIST OF FIGURES	xiii
LIST OF ABBREVIATIONS	xxi
CHAPTER 1 INTRODUCTION	
1.1 Digital Imaging and Its Limitations	1
1.2 Security in Medical Records	3
1.3 Digital Watermarking	5
1.4 Medical Image Watermarking, PACS and Motivation	6
1.5 Research Aim	8
1.6 Research Objectives	8
1.7 Research Outcomes	9
1.8 Thesis Outline	9

CHAPTER 2 LITERATURE REVIEW

2.1	Introduction	11
2.2	General Watermarking Scheme	12
2.3	Types of Domain	13
	2.3.1. Spatial Domain	13
	2.3.2. Transform Domain	14
2.4	Requirements of Image Watermarking	14
	2.4.1. Perceptibility	14
	2.4.2. Robustness	15
	2.4.3. Capacity	16
	2.4.4. Computational Complexity	16
2.5	Reversible Watermark	16
	2.5.1. Fragile Watermarking Scheme	17
	2.5.2. Semi-Fragile Watermarking Scheme	20
	2.5.3. Summary of Reversible Watermarking	21
2.6	Region of Interest	21
2.7	Medical Image Watermarking	21
2.8	Tamper Localization	22
	2.8.1. Examples of Schemes	22
	2.8.2. Summary of Tamper Localization Schemes	25
2.9	Classification of Watermark Attack	28
	2.9.1 Removal Attack	28
	2.9.2 Geometry Attack	28
	2.9.3 Cryptographic Attack	28
	2.9.4 Protocol Attack	29
2.10	Hash Function	29
2.11	Compression in Image Watermarking	30
2.12	DICOM	31
2.13	PACS	32
2.14	Image Watermarking in PACS	32

CHAPTER 3 REVERSIBLE TAMPER LOCALIZATION AND RECOVERY(R-TLR)

3.1	Introduction	37
-----	--------------	----

3.2	Research Methodology	37
3.3	Reversible Tamper Localization and Recovery Watermarking	39
3.3.1	Authentication and Recovery Watermark	42
3.3.2	Image Preparation	43
3.3.3	Watermark Generation and Embedding	46
3.3.4	Tamper Localization and Recovery	49
3.3.5	Reversible Watermark	50
3.3.6	Experimental Results	50
3.4	Evaluation and Discussion	81
3.4.1	Image Quality and Fidelity	81
3.4.2	Tamper Localization and Recovery	81
3.4.3	Reversible Watermark and Hash Function	82
3.5	Conclusion	83
CHAPTER 4	TAMPER LOCALIZATION AND LOSSLESS RECOVERY(TALLOR)	
4.1	Introduction	84
4.2	Overview	84
4.2.1	Reversibility	85
4.2.2	Recovery	85
4.2.3	Authentication	86
4.3	Research Methodology	86
4.4	Compression	87
4.5	Tamper Localization and Lossless Recovery	91
4.5.1	Image Preparation	92
4.5.2	Watermark Generation and Embedding	92
4.5.3	Tamper Localization and Recovery	93
4.6	Tamper Localization and Lossless Recovery With ROI Segmentation	93
4.6.1	Image Preparation	94
4.6.2	Watermark Generation and Embedding	94
4.6.3	Tamper Localization and Recovery	95
4.7	Experimental Results	99
4.7.1	TALLOR	99
4.7.2	TALLOR-RS	127
4.8	Evaluation and Discussion	141

4.7.1	Image Quality and Fidelity	141
4.7.2	Tamper Localization and Recovery	141
4.7.3	Hash Function	143
4.7.4	Compression	144
4.7.5	Comparison	146
4.9	Conclusion	148

CHAPTER 5 MEDICAL IMAGE WATERMARKING IN PACS

5.1	Introduction	149
5.2	Overview	149
5.3	Research Methodology	150
5.4	PACS Test	151
5.5	Watermark Embedder and Image Authenticator(WEIA)	151
5.5.1	Requirements	152
5.5.2	User Interface Design	156
5.6	WEIA in PACS	159
5.6.1	Authentication Server	159
5.6.2	Watermark Embedding	160
5.6.3	Image Authentication	161
5.6.4	Reverse Watermark	162
5.7	Evaluation and Discussion	164
5.8	Conclusion	165

CHAPTER 6 CONCLUSIONS AND FUTURE WORK

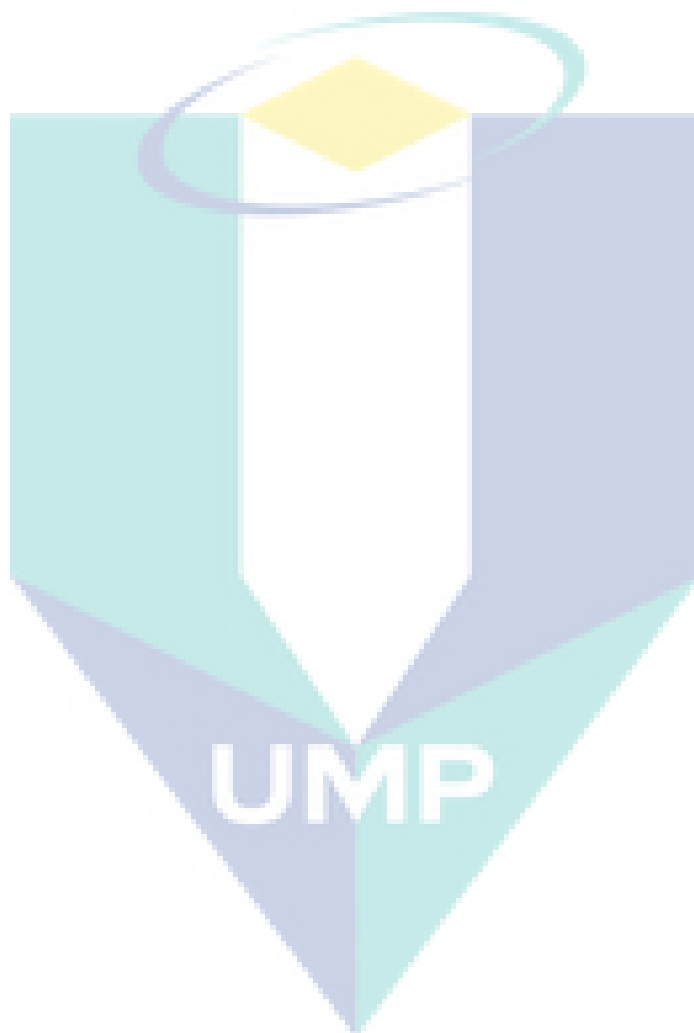
6.1	Introduction	166
6.2	Contributions and Limitations	166
6.3	Future Work	168
6.4	Summary	169

REFERENCES	171
-------------------	-----

APPENDICES

A	Publications	177
----------	--------------	-----

B1	Code Listing for R-TLR	Refer to CD
B2	Code Listing for TALLOR	Refer to CD
B3	Code Listing for TALLOR-RS	Refer to CD



LIST OF TABLES

Table No.	Title	Page
2.1	Summary of watermarking schemes	27
3.1	PSNR for each watermarked sample and the average PSNR	59
3.2	No. of undetected pixels and tamper detection rate for each sample	59
3.3	Pixel value comparison of selected pixels from the ROI	79
4.1	The details of the input, output and compression ratio using RLE	89
4.2	The details of input, output and compression ratio using JPEG	91
4.3	The experiment results for all samples using TALLOR	99
4.4	The experiment results for all samples using TALLOR-RS	127
4.5	Tamper localization and recovery processing time in seconds	143
4.6	ROI of Sample 1 applied with different lossy compression quality scale	145
4.7	Comparison of the proposed TALLOR and TALLOR-RS scheme	147
6.1	Summary of research contributions	170

LIST OF FIGURES

Figure No.	Title	Page
1.1	Original ultrasound image with a liver cyst	2
1.2	Tampered image using cloning tool	3
2.1	Image watermarking scheme	13
2.2	Generic PACS components and its data flow	34
2.3	Image security system in a PACS environment	35
2.4	The implementation of scheme by Tan et al. (2011) in PACS	36
3.1	Ultrasound images	41
3.2	Image divided into ROI and RONI	42
3.3	A block is divided into four sub-blocks	43
3.4	An ultrasound image is divided into ROI and RONI	44
3.5	An example of mapping sequence between blocks in ROI and RONI	45
3.6	Block x_1 is divided into sub-blocks with its computed average intensities to generate value for v and p	47
3.7	Recovery bits of y_1 s, avg_y_1 s is stored in x_1 s together with v and p generated from x_1 s	48
3.8	Block x_1 and block x_2	48
3.9	Original image	51
3.10	Watermarked image, PSNR=53.4 dB	51
3.11	Original image of Sample 2	52
3.12	Watermarked image of Sample 2, PSNR=54.1 dB	52
3.13	Original image of Sample 3	53
3.14	Watermarked image of Sample 3, PSNR=54.6 dB	53

3.15	Original image of Sample 4	54
3.16	Watermarked image of Sample 4, PSNR=53.4 dB	54
3.17	Original image of Sample 5	55
3.18	Watermarked image of Sample 5, PSNR=53.6 dB	55
3.19	Original image of Sample 6	56
3.20	Watermarked image of Sample 6, PSNR=53.7 dB	56
3.21	Original image of Sample 7	57
3.22	Watermarked image of Sample 7, PSNR=53.5 dB	57
3.23	Original image of Sample 8	58
3.24	Watermarked image of Sample 8, PSNR=54.1 dB	58
3.25	Sample 1 had been manipulated by cloning the highlighted area	60
3.26	The recovered image of Sample 1	60
3.27	The magnified recovered image of Sample 1	61
3.28	Sample 2 had been manipulated by cloning the highlighted area	62
3.29	The recovered image of Sample 2	62
3.30	The magnified recovered image of Sample 2	63
3.31	Sample 3 had been manipulated by cloning the highlighted area	64
3.32	The recovered image of Sample 3	64
3.33	The magnified recovered image of Sample 3 with undetected tampering highlighted	65
3.34	Sample 4 had been manipulated by cloning the highlighted area	66
3.35	The recovered image of Sample 4	66
3.36	The magnified recovered image of Sample 4 with undetected tampering highlighted	67
3.37	Sample 5 had been manipulated by cloning the highlighted area	68

3.38	The recovered image of Sample 5	68
3.39	The magnified recovered image of Sample 5	69
3.40	Sample 6 had been manipulated by cloning the highlighted area	70
3.41	The recovered image of Sample 6	70
3.42	The magnified recovered image of Sample 6 with undetected tampering highlighted	71
3.43	Sample 7 had been manipulated by cloning the highlighted area	72
3.44	The recovered image of Sample 7	72
3.45	The magnified recovered image of Sample 7 with undetected tampering highlighted	73
3.46	8 had been manipulated by cloning the highlighted area	74
3.47	The recovered image of Sample 8	74
3.48	The magnified recovered image of Sample 8 with undetected tampering highlighted	75
3.49	Magnified image with 1 pixel tampered	76
3.50	Magnified recovered image	76
3.51	Undetected pixels highlighted	77
3.52	The undetected area was painted in white and the rest of the tampered area is identical with Figure 3.34	77
3.53	The magnified recovered image	78
3.54	The RONI was tampered by modifying one pixel	80
3.55	(a) Hash_A which was embedded as watermark	80
	(b) Hash_B calculated from removed LSBs retrieved from the RONI	80
3.56	The authentication bit and parity check bit for the original block and tampered block	82
4.1	Image divided into ROI and RONI	86
4.2	Different images with ROI measuring 70 x 115 pixels	87
4.3	(a) Histogram for Sample 3	90

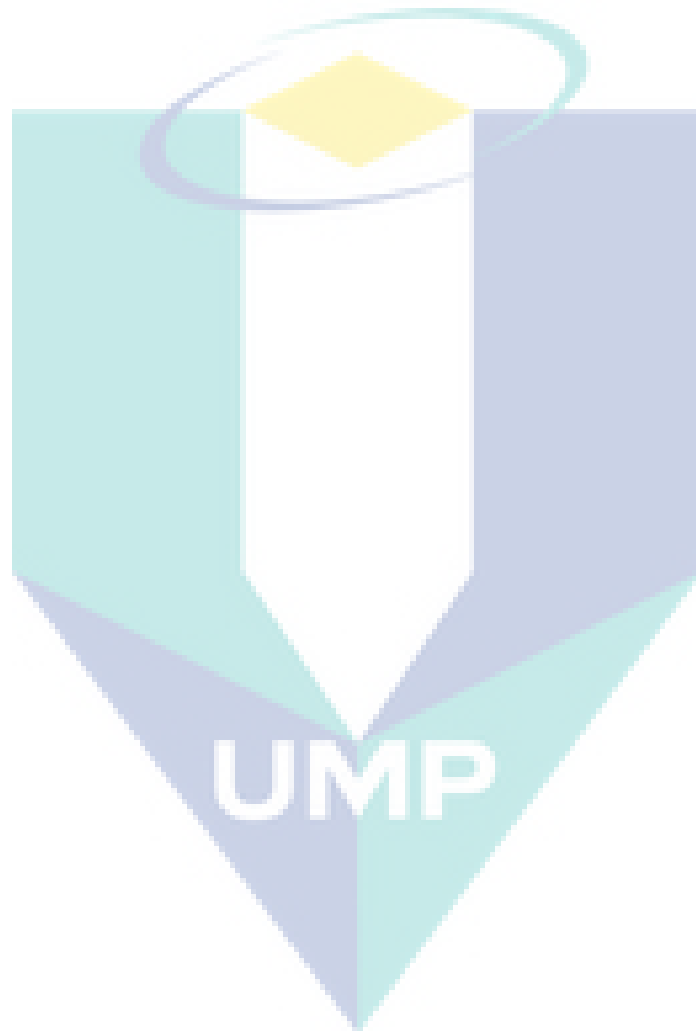
	(b) Histogram for Sample 4	90
4.4	Ultrasound image is divided into ROI and RONI	91
4.5	The watermark generation and embedding process for the authentication and recovery information	97
4.6	The tamper localization and recovery process for all 3 levels	98
4.7	Original image of Sample 1 with ROI highlighted	100
4.8	Watermarked image of Sample 1, PSNR= 48.1 dB	100
4.9	Original image of Sample 2 with ROI highlighted	101
4.10	Watermarked image of Sample 2, PSNR= 48.0 dB	101
4.11	Original image of Sample 3 with ROI highlighted	102
4.12	Watermarked image of Sample 3, PSNR= 48.9 dB	102
4.13	Original image of Sample 4 with ROI highlighted	103
4.14	Watermarked image of Sample 4, PSNR= 47.9 dB	103
4.15	Original image of Sample 5 with ROI highlighted	104
4.16	Watermarked image of Sample 5, PSNR= 48.8 dB	104
4.17	Original image of Sample 6 with ROI highlighted	105
4.18	Watermarked image of Sample 6, PSNR= 48.6 dB	105
4.19	Original image of Sample 7 with ROI highlighted	106
4.20	Watermarked image of Sample 7, PSNR= 48.6 dB	106
4.21	Original image of Sample 8 with ROI highlighted	107
4.22	Watermarked image of Sample 8, PSNR= 47.5 dB	107
4.23	(a) Magnified original ROI of Sample 1	108
	(b) Magnified ROI of Sample 1 that was cloned	108
4.24	(a) Magnified original ROI of Sample 5	109
	(b) Magnified ROI of Sample 5 that was cloned	109
4.25	(a) Recovered image of Sample 1	110
	(b) Magnified recovered ROI of Sample 1	110


4.26	(a) Recovered image of Sample 5	111
	(b) Magnified recovered ROI of Sample 5	111
4.27	(a) Magnified original ROI of Sample 2	112
	(b) Magnified ROI of Sample 2 tampered with salt and pepper noise as highlighted	112
4.28	(a) Magnified original ROI of Sample 6	113
	(b) Magnified ROI of Sample 6 tampered with salt and pepper noise as highlighted	113
4.29	(a) Recovered image of Sample 2	114
	(b) Magnified recovered ROI of Sample 2	114
4.30	(a) Recovered image of Sample 6	115
	(b) Magnified recovered ROI of Sample 6	115
4.31	(a) Magnified original ROI of Sample 3	116
	(b) Magnified ROI of Sample 3 tampered by rotating the highlighted area by 180°	116
4.32	(a) Magnified original ROI of Sample 7	117
	(b) Magnified ROI of Sample 7 tampered by rotating the highlighted area by 180°	117
4.33	(a) Recovered image of Sample 3	118
	(b) Magnified recovered ROI of Sample 3	118
4.34	(a) Recovered image of Sample 7	119
	(b) Magnified recovered ROI of Sample 3	119
4.35	(a) Magnified original ROI of Sample 4	120
	(b) Magnified ROI of Sample 4 tampered by smoothing the highlighted area	120
4.36	(a) Magnified original ROI of Sample 8	121
	(b) Magnified ROI of Sample 8 tampered by smoothing the highlighted area	121
4.37	(a) Recovered image of Sample 4	122
	(b) Magnified recovered ROI of Sample 4	122
4.38	(a) Recovered image of Sample 8	123
	(b) Magnified recovered ROI of Sample 8	123
4.39	RONI of Sample 1 painted in black	125
4.40	(a) JPEG_hash_A retrieved from the RONI	125
	(b) JPEG_hash_B computed from JPEG file retrieved from the RONI	125

4.41	ROI of Sample 1 compressed with different scales	126
4.42	Watermarked image of Sample 1, PSNR= 48.3 dB	128
4.43	Watermarked image of Sample 2, PSNR= 48.5 dB	128
4.44	Watermarked image of Sample 3, PSNR= 49.0 dB	129
4.45	Watermarked image of Sample 4, PSNR= 47.6 dB	129
4.46	Watermarked image of Sample 5, PSNR= 47.8 dB	130
4.47	Watermarked image of Sample 6, PSNR= 48.2 dB	130
4.48	Watermarked image of Sample 7, PSNR= 48.6 dB	131
4.49	Watermarked image of Sample 8, PSNR= 47.4 dB	131
4.50	Magnified ROI of Sample 1 that was cloned	132
4.51	Magnified ROI of Sample 5 that was cloned	132
4.52	Magnified recovered ROI of Sample 1	133
4.53	Magnified recovered ROI of Sample 5	133
4.54	Magnified ROI of Sample 2 that was tampered by adding salt and pepper noise as highlighted	134
4.55	Magnified ROI of Sample 6 that was tampered by adding salt and pepper noise as highlighted	134
4.56	Magnified recovered ROI of Sample 2	135
4.57	Magnified recovered ROI of Sample 6	135
4.58	Magnified ROI of Sample 3 that was tampered by rotating the highlighted area by 180°	136
4.59	Magnified ROI of Sample 3 that was tampered by rotating the highlighted area by 180°	136
4.60	Magnified recovered ROI of Sample 3	137

4.61	Magnified recovered ROI of Sample 7	137
4.62	Magnified ROI of Sample 4 that was tampered by smoothing the highlighted area	138
4.63	Magnified ROI of Sample 8 that was tampered by smoothing the highlighted area	138
4.64	Magnified recovered ROI of Sample 4	139
4.65	Magnified recovered ROI of Sample 8	139
4.66	Highlighted RONI of Sample 3 painted in black	140
4.67	(a) RONI1_hash_A retrieved from the RONI (b) RONI1_hash_B computed at the time of authentication	140 140
4.68	(a) RONI2_hash_A retrieved from the RONI (b) RONI2_hash_B computed at the time of authentication	141 141
4.69	Magnified RONI of Sample 1 (a) Original image (b) Watermarked image	142 142
4.70	Image for Sample 1 (a) Original ROI (b) Recovered ROI	143 143
4.71	Sample 1 (a) Lossless compressed ROI (b) Lossy compressed ROI (scale=90)	144 144
4.72	ROI of Sample 1 with an area of 480 x 360 pixels	146
5.1	Reverse watermark process for R-TLR using WEIA	154
5.2	Embedding process of TALLOR/TALLOR-RS using WEIA	155
5.3	Embedding function for WEIA	156
5.4	Panel to allow user to define ROI for compression	157
5.5	Authentication panel displaying processing in progress	158
5.6	WEIA panel for image transmission	159

5.7	Authentication server and workflow for the watermark embedding process	160
5.8	Centralized image authentication workflow	162
5.9	Centralized reverse watermark workflow	163



LIST OF ABBREVIATIONS

AET	Application Entity
CRC	Cyclic Redundancy Check
DICOM	Digital Imaging and Communications in Medicine
DE	Digital Envelope
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DS	Digital Signature
DWT	Discrete Wavelet Transform
HIS	Hospital Information System
JPEG	Joint Photographic Experts Group
LZW	Lempel-Ziv-Welch
LSB	Least Significant Bit
MD5	Message-Digest algorithm 5
PACS	Picture Archiving and Communications System
PSNR	Peak Signal-to-Noise Ratio
RLE	Run Length Encoding
ROA	Region of Authentication
ROI	Region of Interest
RONI	Region of Non-Interest
RSA	Rivest, Shamir and Adleman public key encryption
SCP	Storage Service Class Provider
SCU	Storage Service Class User
SHA	Secure Hash Algorithm
TCP/IP	Transmission Communication Protocol/Internet Protocol

CHAPTER 1

INTRODUCTION

1.1 DIGITAL IMAGING AND ITS LIMITATIONS

The existence of digital images can be traced back to the 1960s when computers were first used for space programs and also in medical research. Today, digital images can be produced without the need of being involved in a billion-dollar project by using devices as simple as a hand phone. The birth of the Internet had made it convenient for anyone with a computer to upload and download images. The advancements in digital image processing and computer graphics technology make it easy for an image to be manipulated. We sometimes read reports about images of important people that were intentionally doctored. The worst outcomes could be the victim was defamed and the person who committed the crime was charged in court. The Reuters news agency published a photo showing bombing damages in Beirut during the Lebanon war in 1996 and admitted that the photo had been doctored by a Lebanon freelancer who took the photo to exaggerate Israeli attack on the city (Lappin, 2006) using cloning tools provided by image editing software. This could lead to a more serious consequence compared to the former case such as causing unnecessary retaliation between parties involved that could cost more lives. The same tactic can be applied in a medical situation. Figure 1.1 shows an original image of an ultrasound image of a liver cyst. Figure 1.2 is the tampered image done by using easily available image editing software.

The cyst is removed by using the cloning tool to copy pixels around the targeted object and the brush tool to complete the modification. Suspicion might not arise if the images were not compared side by side. This tampered image might help someone to pass a medical examination without any problems. Tampered medical image can also be used as a counterfeit evidence for illegitimate medical claims in which a medical condition such as a tumor growth can be created or exaggerated.

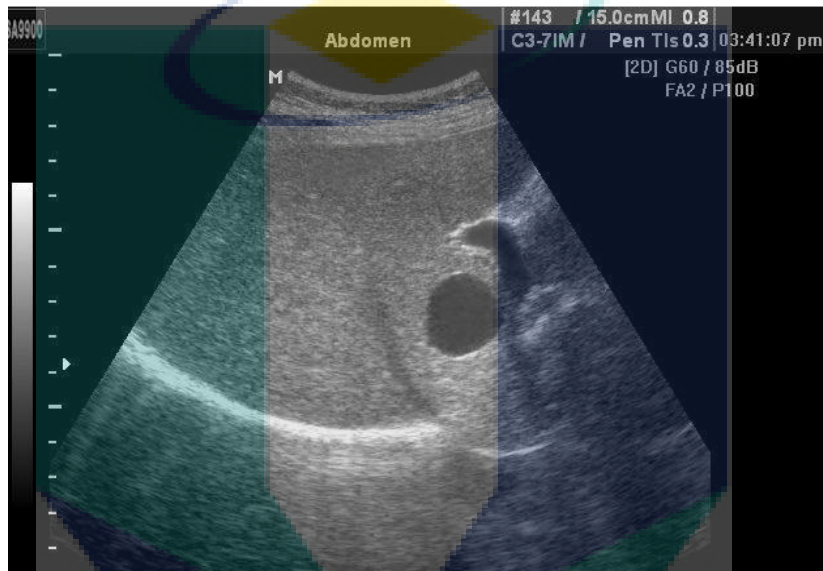


Figure 1.1: Original ultrasound image with a liver cyst

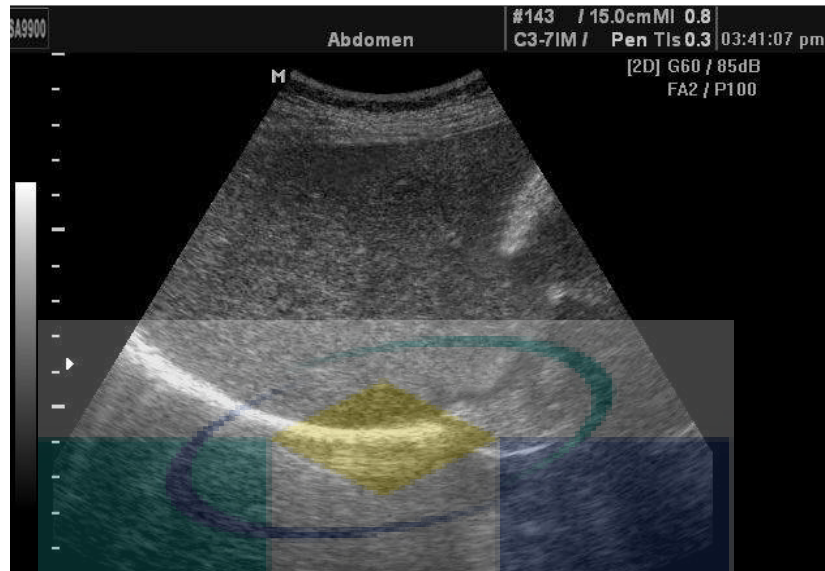


Figure 1.2: Tampered image using cloning tools

1.2 SECURITY IN MEDICAL RECORDS

In a modern health care environment, systems such as Hospital Information System (HIS) and Picture Archiving and Communications System (PACS) form the information technology infrastructure of a health institution. Advancements in medical information systems had changed the way patient records are stored, accessed and distributed. The convenience of data access and distribution in a health institution poses a great threat on privacy of patients' information (Li et al., 2005).

In the year 2005, nearly all health institution in United States need to comply with security standards adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 where part of its objective is to prevent fraud and abuse in health care (Department of Health and Human Services, 2007). The security standard includes access control measures such as unique user identification, automatic logoff and encryption had been implemented to prevent unauthorized access

to medical records. In order to ensure the integrity of medical records, requirements for digital signatures(DS) had been standardized.

Digital signature is an encrypted message digest extracted from electronic documents such as medical records. It is used to prove the source and integrity of a document. Any modifications done on the medical records can be detected by comparing the digital signatures. This security measure can be applied to an image. Friedman (1993) had first proposed the concept of using digital signature for image authentication by using a camera. An image file is used together with a private key in hashing to produce an encrypted digital signature. In order to authenticate the originality of the image, the digital signature is decrypted with a public key to obtain the hash value. A hash value is also calculated from the original image file at the time of authentication. These two hash values are then compared.

Medical images can be stored in a DICOM (Digital Imaging and Communications in Medicine) compliant format. DICOM standard was developed in 1982 by American College of Radiology and National Electrical Manufacturers Association. Its purpose is to facilitate the interoperability of medical imaging equipments. The standard covers issues such as network communications, media storages and file formats. Part 15 of the DICOM standard specifies security profiles and technical means for application entities involved in exchanging information to implement security policies. It also provides guidelines for the implementation of digital signature to ensure the integrity of medical images. Medical equipment manufactures like Siemens and GE Medical Systems had enhanced their modalities to allow the application of digital signature by the modality itself (Schutze et al., 2004).

Pizzi (2008) reported that approximately 70 current and former University of California, Los Angeles Medical Center employees who include physicians, had been accused of illegally viewing celebrity medical records. The most serious case is where an administrative personnel was accused of looking at the records of 61 patients. These are only examples of reported cases and it shows the vulnerability of medical records stored in a sophisticated health care information system. The patient and the imaging data, transmitted between imaging centers and other interested individuals using compact disc digital media, are also extremely vulnerable to alterations (Mcevoy and Svalastoga, 2007).

The existing security measures implemented might prevent unauthorized access but its effectiveness to prevent or detect abuse done by authorized user is questionable. Current technology is able to keep track specific user function when that authorized user is logged in into an information system such as to view a specific patient's medical images. The usage of digital signatures to ensure the integrity of medical records such as medical images does have its weakness. It might be able to detect whether that the integrity of the image had been compromised but it lacks of the ability to identify the area of tampering or also known as localization. Another problem with digital signature is that it needs to be transmitted together with the image in a separate file or in the image header. Encrypted files are very sensitive to bit errors occurring during transmission and proper error correction mechanism is needed (Coatrieux et al., 2000). The solution to these problems is digital watermarking which will be explained in the next section.

1.3 DIGITAL WATERMARKING

Watermarking had been widely applied to paper material since its invention such as to paper money, passports, postage stamps and other important documents to prevent counterfeiting. The watermark is usually hidden from normal view and only become visible when the watermarked paper is held against a light. Watermark carries information about the object in which it is hidden to indicate authenticity.

Digital watermarking is a technique where data is embedded into a digital content such as audio, video and images. The risk of losing the data for authentication purposes is eliminated since the data is embedded within the digital content itself (Cox et al., 2002). Watermarks can be categorized into visible and invisible types. A logo or pattern is an example of a visible watermark that is used for ownership identification of digital content such as image and video. An invisible watermark is closely related to the field of steganography where message is hidden within the digital content so that it can be retrieved later. Steganography has been used as a form of secret communication due to the difficulty in detecting the hidden message (Cobb, 2006). Invisible watermark can be used for content authentication where any modification on the digital content can be

detected. Invisible watermark is suitable in a situation where an image is watermarked and it is perceptually identical with the original version under a normal observation.

Watermark can be further categorized into fragile and semi-fragile types (Caldelli et al., 2010) which are suitable for the usage of content authentication. A fragile watermark can easily be destroyed and become undetectable after the watermarked image has been modified in anyway. If a fragile watermark is detected correctly, it can be assumed that the image had not been modified or tampered. A semi-fragile watermark is destroyed by illegitimate modification but unaffected by legitimate distortion such as compression. It is normally used for selective authentication. Both fragile and semi-fragile watermark types may have localization capability.

1.4 MEDICAL IMAGE WATERMARKING, PACS AND MOTIVATION

The purpose of medical image security is to maintain privacy of the patient information in the image and to assure data integrity that prevents the image from tampering (Cao et al., 2003). Watermarking can be used in medical images to prevent unauthorized modification by authenticating the content of the image. Tamper localization capable watermarking scheme can detect and locate modification of pixel values on the image. The tampered area can be recovered by retrieving the original pixel values that were stored on the image itself as a watermark. Tamper localization is useful for deducing the motive of the tampering and whether any modification is legitimate. One of the techniques used for watermark embedding is by inserting the watermark in the least significant bits (LSBs) of the image pixels. That also means that the embedding process of the watermark will cause the original pixel values of the image to be indiscernibly changed (Coatrieux et al., 2005).

The medical tradition is very strict with the quality of medical images that modification of the original pixel value is often not approved and watermarking scheme used should be reversible (Coatrieux et al., 2000) and original image is generally preferred by radiologist for diagnostic purposes (Tan et al.,2011). Thereby, the exact original pixel value must be recovered (Macq and Dewey, 1999) when the watermark is

removed from the image. Current medical image watermarking schemes that have tamper localization and recovery capability uses complex techniques to achieve reversibility. The complexity of the algorithm may require more computing resources and processing time. It may become an issue if thousands of medical images needs to be processed and may affect the operations of a health institution. The watermarked image should not have any noticeable distortions caused by the watermark embedding process to ensure that medical diagnoses are not affected. Another issue with the current schemes is that the recovery of the tampered area is in the form of approximate recovery that uses average intensity or lossy compression which has lower quality in terms of perception when being compared to the original non-tampered image. Further research on exact or lossless recovery which produces better quality image using minimum processing time is needed.

A PACS is a collection of network digital devices for acquisition, transmission, storage, display, and management of diagnostic imaging studies which is based on DICOM standards. It uses Transmission Communication Protocol/Internet Protocol (TCP/IP) for communication and allows system that uses DICOM standard to be interconnected through local network and the Internet. It also provides a mechanism for the interchange of DICOM images in PACS.

Medical images stored in PACS are in DICOM file format but DICOM does not provide standards for the usage of watermarking as a security measure. In a PACS, there might be hundreds or even thousands of medical images being stored at any given time. In watermarking these medical images, the process must not adversely affect the operation of the PACS. The tool needed to perform the job efficiently is non-existence. There are also no comprehensive guidelines on how image watermarking can be operated in a PACS.

Based on the motivations mentioned above, the following are the research questions:

- i. How to achieve reversibility by using simple watermarking technique and at the same time maintains tamper localization and recovery capability?

- ii. How to achieve exact recovery after tamper localization and uses minimum processing time?
- iii. How does medical image watermarking can be performed efficiently and what are the components needed?

1.5 RESEARCH AIM

The aim of this research is to facilitate the implementations of tamper localization and recovery watermarking schemes for medical images in PACS.

1.6 RESEARCH OBJECTIVES

There are four research objectives:

- i. To develop a reversible tamper localization and recovery watermarking scheme that uses simple technique.
- ii. To develop a tamper localization watermarking scheme that achieve exact recovery using minimum processing time.
- iii. To propose a tool to facilitate the process of watermarking and image authentication in PACS.
- iv. To propose necessary components needed to allow image watermarking to operate in PACS.

1.7 RESEARCH OUTCOMES

The following are the research outcomes:

- i. The development of a reversible tamper localization and recovery watermarking scheme for a chosen modality.
- ii. The development of a tamper localization and lossless recovery watermarking scheme for the chosen modality.
- iii. A design proposal of an application to facilitate the process of watermarking and image authentication in PACS.
- iv. A proposal of infrastructures and workflows needed to allow image watermarking to operate in PACS.

1.8 THESIS OUTLINE

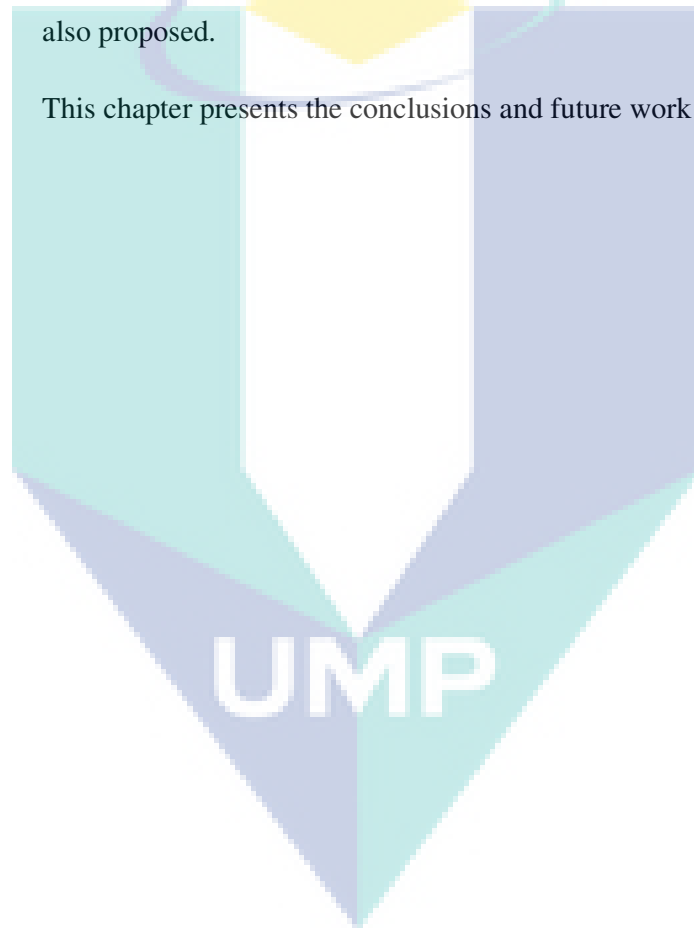
The thesis is divided into the following chapters:

- Chapter 1: This chapter presents the limitations of digital imaging and security issues in medical images. It also introduces watermarking as an alternative method for enhancing security in medical images. Tamper localization and recovery watermarking scheme will be the focus of the research.
- Chapter 2: The previous works on watermarking is reviewed in this chapter. It covers reversible watermarking schemes as well as tamper localization and recovery schemes for medical images.
- Chapter 3: This chapter proposes a reversible tamper localization and recovery(R-TLR) scheme for ultrasound images. It also discusses the experiments results obtained and evaluates the proposed scheme.

Chapter 4: This chapter proposes a tamper localization and lossless recovery (TALLOR) schemes for ultrasound images. An enhanced scheme that uses different technique is also proposed. It also discusses the experiments results obtained and evaluates the proposed schemes.

Chapter 5: The proposed schemes were tested in a PACS in a simulated environment in this chapter. The design of the watermark embedder and detector (WEIA) application is presented in this chapter. The necessary infrastructures and workflows to allow WEAI to operate in a PACS were also proposed.

Chapter 6: This chapter presents the conclusions and future work for the research.



CHAPTER 2



LITERATURE REVIEW

2.1 INTRODUCTION

This chapter introduces watermarking in details as well as its previous works. It consists of section 2.2 that introduces the components in a general watermarking scheme. Section 2.3 describes the classification of watermarking by domain. Section 2.4 presents the requirements in image watermarking. Section 2.5 introduces the concept of reversible watermarking and its previous works. Section 2.6 explains the concept of region of interest. Section 2.7 introduces the concept of medical image watermarking. Section 2.8 introduces the tamper localization and recovery schemes and its previous works. Section 2.9 describes the classification of watermark attacks. Section 2.10 describes hash function in image watermarking. Section 2.11 introduces the usage of compression in image watermarking. Section 2.12 explains the DICOM standard. Section 2.13 introduces PACS. Lastly, section 2.14 describes image watermarking in PACS and its previous work.

2.2 GENERAL WATERMARKING SCHEME

A general watermarking scheme consists of an encoder that embeds the information and a decoder for the detection of the information (Emad, 2009) as shown in Figure 2.1. The encoder embeds the watermark, W inside original image I by using embedding function, E as shown in Eq. (2.1).

$$E(I, W) = I_w \quad (2.1)$$

Information such as a logo, user information or information from the image itself can be embedded. An optional key may be used in order to protect the watermark. Watermark can be embedded in two image domains namely the spatial and transform domains (Cox et al., 2002 and Song et al., 2010) which will be explained in details in the next section. Watermarked images may be susceptible to attacks such as modification, fabrication or even lossy compression.

The output from this process is I_w , the watermarked image. The decoder, D detects or extracts the watermark, W from the original image as shown in Eq. (2.2). Some techniques allow the detection or extraction of watermark without the original image.

$$D(I, I_w) = W \quad (2.2)$$

Watermark detected or extracted is inspected in order to know whether the image had been modified in any form.

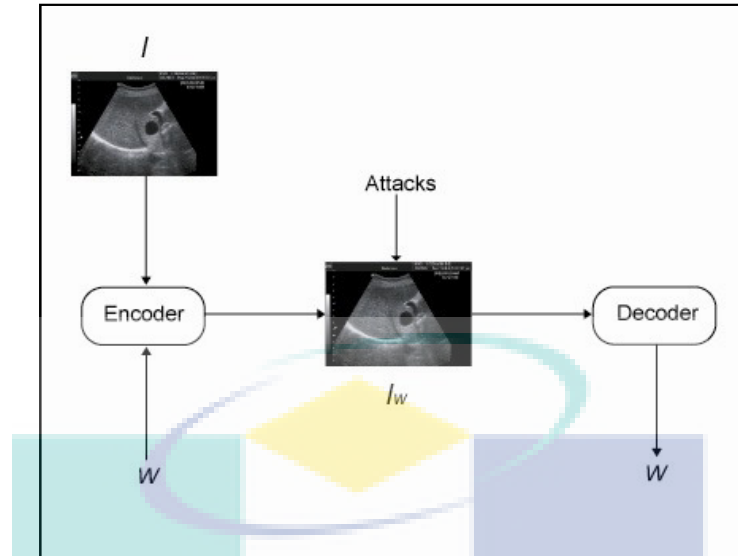


Figure 2.1: Image watermarking scheme

Source: (Emad, 2009)

2.3 TYPES OF DOMAIN

Watermarking techniques can be classified according to how the watermark is embedded namely within the spatial domain or the transform domain (Cox et al., 2002 and Song et al., 2010).

2.3.1 Spatial Domain

One of the most direct and simple technique is to embed the watermark information into the LSBs of the image. Since a change in LSB corresponds a change in one unit of image gray value, its modification is not perceivable by human eyes. This technique is not as robust as transform domain techniques and rarely survives various attacks. The types of watermark attack will be explained in the later section.

2.3.2 Transform Domain

Most of the transform domain techniques embed the watermark information into the transform coefficients of the cover image. The transform domain techniques produces spectral domains where watermarking can be applied. Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT) are the three popular techniques in this category. Techniques used needs a certain amount of computation but it can overcome possible compression and more robust against geometric transformation such as rotation, scaling, translation and cropping (Song et al., 2010).

2.4 REQUIREMENTS OF IMAGE WATERMARKING

Most image watermarking schemes try to meet the following requirements (Cox et al., 1999, Kutter and Hartung, 1999 and Meerwald and Uhl, 2001).

2.4.1 Perceptibility

The perceptibility of a watermarked image can be judged according to its fidelity and quality. Fidelity measures the similarity between images before or after watermarking (Cox et al., 2002). A reconstructed image that is very similar to the original has a high fidelity. A low fidelity reconstruction is dissimilar or distinguishable from the original. Watermarked images may bear visible or invisible distortion due to the embedding process. One way to quantify distortion is the mean-square error. This is defined as:

$$MSE = \frac{1}{n} \sum_i^n (I'_i - I_i)^2, \quad (2.3)$$

which is the average term by term difference between the original image, I , and the watermarked image, I' . If I and I' are identical, then $MSE(I', I) = 0$. A related distortion measure is the peak signal-to-noise ratio (PSNR), measured in decibels (dB). The problem with mean-square error is that it depends strongly on the image intensity scaling and while PSNR rectifies this problem by scaling the mean-square error according to the image range (Smitha and Navas, 2007). PSNR is defined as below:

$$PSNR(dB) = 10 \log_{10} \frac{\max I^2}{MSE}, \quad (2.4)$$

where $\max I$ is the peak value of the original image. If the signals are identical, then PSNR is equal to infinity. A high PSNR represents a high fidelity of a watermarked image. In this thesis, PSNR is used as a measurement for image fidelity.

A high quality watermarked image does not have any obvious noticeable distortion caused by the watermark embedding process. The assessment of quality is usually evaluated by human observers and is influenced by personal preferences which are subjective in nature.

2.4.2 Robustness

The watermark should be detectable by an authorized user after the image has undergone attacks such as compression, filtering and etc. For content authentication, a robust watermark may not be able to differentiate both compression and tampering.

Fragile watermarking can be an advantage for authentication purposes. If a fragile watermark is detected correctly in an image, it can be assumed that the image has not been altered or tampered with since the watermark has been embedded.

2.4.3 Capacity

Sufficiently useful amount of information must be allowed by a watermarking scheme to be embedded into an image. The amount of information embedded is subjected to the application. A reversible watermarking scheme may need to embed more information to allow image restoration, than a watermark scheme that embeds hash value of an image for authentication purposes.

2.4.4 Computational Complexity

The watermarking scheme should not be computationally complex especially for applications where real-time embedding is desired. In a hospital environment for instance, where thousands of medical image are produced daily, watermarking process needs to be less time consuming so that the operation of the hospital is not affected. Reducing the number of computations also means lower cost for computer hardware.

2.5 REVERSIBLE WATERMARK

In the process of watermarking an image for instance, a minor modification to the original content will be performed. The minor modification is needed so that watermarking information can be embedded but this introduces some amount of distortion onto the image. The amount of distortion should be minimal so that the perceptibility of the image is not affected. Depending on the applications of the watermarked image, minor distortion introduced may be acceptable. This cannot be

acceptable for some application scenarios such as digital images for military investigation and recognition (Fontani et al., 2010). In medical field, even a small modification is not allowed for legal reasons and a potential risk of a physician misdiagnoses an image (Fridrich et al., 2002). The watermarking scheme used on a medical image should be reversible (Coatrieux et al., 2000).

Reversible watermarking also referred as invertible watermarking is a technique where the watermark can be removed and the image is restored to its original form. Reversible watermark scheme can be divided into two main categories namely fragile and semi-fragile (Caldelli et al., 2010). Below are some examples of reversible watermarking scheme.

2.5.1 Fragile Watermarking Scheme

Fragile watermark embedded in an image is destroyed when modification is done on the watermarked image which may indicate that the integrity of the image had been compromised. It may not able to distinguish between malicious attacks and incidental manipulations like JPEG lossy compression (Piva et al., 2005). Below are some examples of fragile watermarking scheme.

Fridrich et al. (2002) proposes a technique by watermarking uncompressed image format based on embedding message bits in the status of groups of pixels. The statuses are singular, regular or unusable groups. The status can be obtained by using a flipping operation and discrimination function. The original status of the pixel groups is embedded together with the watermark in the image. In order to decrease the payload, the original status needs to be compressed before the embedding process. The watermark is extracted together with the original status. The original status is then used in the reversible process. Tian (2003) presents a reversible technique that calculates the difference of neighboring pixels values and then selects some of such differences to perform a difference expansion. This technique stores the original LSBs together with the watermark without the need of using compression by exploring the redundancy in digital content. A simple example, assume that $x = 206$, $y = 201$ and reversibly embed

one bit, $b=1$. The integer average denoted as z and the difference of x and y which is denoted as h is computed.

$$z = \left(\frac{206 + 201}{2} \right) = \left(\frac{407}{2} \right) = 203, h = 206 - 201 = 5$$

Next, the difference value, h is converted to binary representation $h=5=101_2$. The value of b is appended to h after the LSB and the new difference value h' is $h'=1011_2=11$. This is equivalent to

$$h' = 2 \times h + b = 2 \times 5 + 1 = 11$$

Finally, the new values based on the new difference value, h' and the original integer average value, z is computed.

$$x' = 203 + \left(\frac{11 + 1}{2} \right) = 209, y' = 203 - \left(\frac{11}{2} \right) = 198$$

The value of b , can be extracted from the embedded pair, x' and y' . The original value of x and y can be restored as well. The integer average and difference is computed.

$$z' = \left(\frac{209 + 198}{2} \right) = 203, h' = 209 - 198 = 11$$

The binary representation of $h'=11=1011_2$. The LSB is extracted, which is 1 in this case and leaves the original value of difference as $h=101_2=5$. This is equivalent to

$$b = LSB(h') = 1, h = \left(\frac{h'}{2} \right) = 5$$

The original value of x and y can be restored by using the integer average value, z' and restored difference value, h . From the above example, one bit is embedded by increasing the value bit length of the difference value, h from three bits to four bits. This method employs a simple algorithm to allow the watermark to be reversed but it involves two issues. The advantage of this technique is that not all LSBs need to be

stored and this reduces the watermark payload. However, this technique has two issues. The first issue is the perceptibility of the watermarked image. By referring to the example above, the values of a pair of pixel, x and y are 206 and 201 respectively. These pixel values were modified by three to 209 and 198 in order to embed one bit of information. It may not be suitable for the usage in medical images due to the importance of fidelity and quality of the watermarked image. The second issue is capacity. A pair of pixel is needed to embed one bit of information and theoretically, the embedding capacity is only at 0.5 bits per pixel.

Weng et al. (2007) uses prediction technique by using neighboring pixel to get its prediction error. A companding technique is introduced to increase the number of prediction errors than the threshold available for embedding and this technique decreases the watermark payload. Both Tian (2003) and Weng et al. (2007) techniques includes location map as part of the watermark to facilitate the extraction of watermark. Lou et al. (2009) proposed a multiple-layer watermarking technique that utilizes a reduced difference expansion method to embed the bit stream in the LSBs of the expanded differences. By using this method, a large amount of data can be embedded in a medical image and maintaining its quality. It was claim that this technique provides higher embedding capacity at the same level image quality compared with Tian (2003) difference expansion method. All four techniques mentioned above operates in the spatial domain which are well known to be vulnerable to many forms of attacks.

Yang et al. (2004) proposed a fragile watermark scheme that embeds the watermark in the transform domain which is more robust as compared to schemes proposed above. The reversibility is guaranteed by integer DCT, and using a lossless 8×8 block transform applied to the whole image. The algorithm exploits the principle of histogram modification. The integer DCT transform has the property of energy concentration which can be used to improve the capacity of histogram modification scheme. The original LSBs are embedded with watermark bits into the saved space from histogram modification technique. The watermark is extracted by reversing the 8×8 integer DCT and histogram modification.

2.5.2 Semi-Fragile Watermarking Scheme

Semi-fragile watermarks can survive certain degree of legitimate manipulation such as compression and cropping. Below are some examples of semi-fragile watermarking scheme.

Vleeschouwer et al. (2006) proposed a reversible semi-fragile watermark based on the identification of a robust feature of the luminance histogram for an image tile. The histograms of groups of pixels are mapped to a circle and the transform is chosen such that the histograms rotation of two groups of pixels is conveyed in one bit of information. It is a complicated scheme but the watermarked image can withstand some level of cropping and JPEG compression. This scheme is further improved by Ni et al. (2008) where a robust statistical quantity was employed to mitigate the effect of image compression and small incidental alteration for data embedding. The robustness against lossy modification like JPEG is slightly increased but with high compression rates, the results of the experiments are comparable to those presented by Vleeschouwer et al. (2006). Both techniques described above embed the watermark within the spatial domain.

As for transform domain watermarking scheme, Zou et al. (2006) proposed a semi-fragile reversible watermarking scheme based on integer wavelet transform integrated into JPEG2000 standard compression. The watermark is embedded into integer wavelet transform coefficient of a selected high frequency sub-band. In order to remove the embedded watermark and to retrieve the original image value, a fixed value is used to recover the original coefficients. The watermark is robust to lossy compression to a certain degree. Wu (2007) also proposed a scheme which embeds the watermark into the integer wavelet transform coefficients. The specialty of this scheme as compared to scheme proposed by Zou et al. (2006) is the usage of histogram shifting of integer wavelet coefficients which grants higher visual quality. Other than being reversible and robust against lossy compression at a low quality factor, this scheme is also able to localized tampering such as cropping and bit replacement.

2.5.3 Summary of Reversible Watermarking

Watermarking scheme with reversible capability can operate in the spatial and transform domain. The summary of the schemes are presented in Table 2.1. Different techniques were used such as flipping operation, difference expansion and usage of pixels histograms. Generally, the techniques used require some amount of computing time. This can be an issue if it is applied in real hospital environment where thousands of medical images need to be processed thus demanding extra computing resources. None of the schemes has tamper localization capability except for one. This capability will be explained in the next section. The watermarked images produced by the reviewed schemes have the PSNR of a low 16.5 dB to a high 53.1 dB but none of the schemes reviewed were designed for the usage in medical images.

2.6 REGION OF INTEREST (ROI)

Region of interest is an area of the image which is considered as important to the user. In medical images for instance, the ROI is the area which is used for diagnosis purposes. In the medical image watermarking, a ROI can be defined and often the watermark is being embedded in the region of non-interest (RONI) to maintain the originality of the ROI. In a situation where the ROI is used for watermark embedding, the process can be reversed by extracting the watermark and the original ROI information is restored.

2.7 MEDICAL IMAGE WATERMARKING

Coatrieux and Lecornu (2006) had identified three kinds of watermarking methods for medical images. The first method embeds the watermark within the RONI so it does not affect clinical diagnosis. The ROI is often used for diagnosis rather than the RONI which generally in black. The RONI sometimes can include gray-level portion of little interest (Shih and Wu, 2005). Since the watermark embedding in the

RONI causes no interference with the ROI, invisibility is less strict. However, distortions caused by the watermark embedding in the RONI may annoy physicians. Therefore, the level of distortion has to be kept low. The second method is the reversible watermarking. The watermark is embedded in the image but can be removed so that the image can be restored to its original state. However, this method more often has an issue with low storage capacity when being compared to non-reversible method. The last method focuses on minimizing the distortion caused by watermarking. The watermark replaces some image details such as LSBs of the image or details lost after lossy image compression.

2.8 TAMPER LOCALIZATION

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. Below are some examples of tamper localization watermarking scheme for medical images.

2.8.1 Examples of Schemes

Guo and Zhuang(2009) proposed a reversible scheme with tamper localization based on difference expansion. This scheme partitions an image into certain non-overlapping regions and appending the associated local authentication information directly into the watermark payload. The scheme also introduces the concept of region of authentication (ROA). ROA is a region used for integrity authentication or in other words, the area that needs to be protected. A ROA, which can be flexibly defined by the user, is partitioned into small regions as an image block or polygonal region in a multilevel hierarchical manner. The novelty of this scheme is that the information about the ROA is embedded as part of the watermark. The ROA will be used to reconstruct the ROA in the verification process. A hashing function is used to produce digital

signatures for each image block which are then added to the watermark payload. In order to verify the authenticity of the image, the process starts by comparing the signature for the whole image. If the initial verification process fails, the ROA will be reconstructed. The signatures for the ROA will be compared to detect any tampering. An interesting technique is used in the tamper localization process where an output image consist of shadings of the ROA is produced. The shading is used to reflect the level of confidence in the integrity of the ROA where light shadings corresponds to high confidence value and dark shadings corresponds to low confidence value. The tamper localization has the accuracy of up to 32 x 40 pixels. Ultrasound image was used in the experiment of this watermarking scheme and quality of the watermarked image is crucial especially for medical diagnoses. The perceptibility of the watermarked ultrasound image is not known as the measurement of the distortion level of watermarked image was not done in the experiment.

Tan et al. (2011) also proposed a tamper localization watermarking scheme that uses pixel value modification in order to allow the watermark to be reversible. The image is divided into 16 x 16 pixel blocks and Cyclic Redundancy Check (CRC) is computed for each block. Each CRC is embedded into its own block and in the event that the CRC cannot be embedded into its own block, the remaining bits will be carried over to the next block. The watermarked image can be verified by extracting the watermark and comparing the CRC of each block. Any mismatch of CRC values during comparison indicates tampering and the tampering localization accuracy is within 16 x 16 pixels. Medical images were watermarked and the PSNR of the watermarked images was between 34.0 to 35.0 dB. The disadvantage of this scheme is that in order to allow reversibility, all pixel value needs to be increased by four pixel values during the embedding process to prevent bit overflow and thus the maximum pixel value allowable in an image to be watermarked had been constrained.

Both schemes proposed by Guo and Zhang (2009) and Tan et al. (2011) operate in the spatial domain and have tamper localization and reversible capability. The schemes might be able to identify the area of tampering but tampered region cannot be recovered. Recovery of the tampered region is useful in order to know exactly what had been tampered and the motive of the tampering.

Chiang et al. (2008) proposed a reversible tamper localization scheme with tampered region recovery capability. This scheme is based on a difference expansion scheme proposed by Tian (2003). It was modified to allow the watermark to be embedded into the transform domain by using the integer Haar wavelet transform. The image is first divided into blocks. The recovery information is generated by taking the average pixel value of each block and embedded as watermark. The watermark is encrypted before the embedding process as a security feature. The whole image can be verified by comparing the retrieved average pixel value from the watermark with the current average pixel value of the image. Any mismatch indicates tampering and tampered region can be localized to an accuracy of 4×4 pixels. The tampered block is recovered using the average pixel value retrieved from the watermark. The advantage of this scheme is that it can be modified to allow applying the watermarking process to a defined ROI rather than to the whole image. The recovery information of the ROI is stored as the exact pixel value rather than average pixel values. Mammograms were watermarked and have the PSNR between 36.4 to 40.5 dB.

Osamah and Khoo (2011) proposed a scheme that consists of two types of watermark. The first watermark is embedded into spatial domain and the second watermark is embedded into transform domain. The image is first divided into 16×16 pixel blocks. The first watermark consists of patient's data and the hash value of the ROI and is embedded into the ROI itself by using a modified difference expansion technique. An embedding map of the ROI is produced to form a second watermark together with compressed recovery information of ROI and average value of each block in the ROI. The second watermark is compressed and embedded into the region of non-interest (RONI) using a DWT technique. Tamper localization is done by comparing the average value of each block in the ROI with the retrieved average value from the watermark. Tampered blocks can be recovered using the compressed ROI. It was claimed that this scheme is robust against salt and pepper attack and cropping. A watermarked ultrasound image has the PSNR of 36.7 dB.

Earlier research by Jasni and Abdul (2006) had also produced a tamper localization and recovery watermarking. It also uses block based technique where each block consists of 8×8 pixels. Each block is then divided into sub-blocks of 4×4 pixels. A three-tuple watermark embedded consists of a two-bit authentication watermark and a

seven-bit recovery watermark for other sub-block. Average intensity of a corresponding block and its sub-blocks is calculated to generate the authentication watermark. Average intensity of a sub-block is embedded as the seven-bit recovery watermark in another block which was predetermined in a mapping sequence. A parity bit is generated based on the seven-bit recovery watermark. Tamper localization is done by comparing the average intensity and parity bit. Blocks that were marked invalid are recovered using the embedded average intensity of the sub-block. The watermarked ultrasound image has a PSNR of 54.8 dB. This scheme was evaluated to know whether watermarked medical images affect clinical diagnoses. The study was done by Jasni et al. (2006) by adding an additional hash function to the existing watermarking scheme. Various types of medical images were watermarked and an ultrasound image has a PSNR of 54.2 dB with the total watermark bits of 480K. The watermarked images were assessed by radiologists and it was concluded that watermarked images did not alter clinical diagnoses. The disadvantage of this scheme is that it is not reversible. The original image is generally preferred by radiologist for diagnostic purposes (Tan et al., 2011). Although it has been clinically evaluated, an option should be given to allow the watermark to be removed and the original image to be restored by request.

Yang and Shen (2010) applied hash function to image blocks and embed the hash values into the LSBs of the corresponding blocks. They also used vector quantization to compress an image by producing an index table which can be used for image recovery. The index table is embedded into the second and third LSB of each pixel. Each block of the image is authenticated using the embedded hash value. Index table is used to reconstruct an image when tampering is detected. Tampered block is recovered using blocks from the reconstructed image. Non-medical image was watermarked with the PSNR of only 29.3 dB.

2.8.2 Summary of Tamper Localization Schemes

All schemes reviewed under this section were designed specifically for usage in medical images. All schemes have tamper localization capability and a majority has recovery capability as shown in Table 2.1. The watermarked images have the PSNR of

between 35.0 to 55.0 dB. The schemes that have recovery capability operate in the transform domain which is more robust against attack but requires more complex computation and this translates into more watermarking processing time. There are three schemes that operate in the spatial domain but scheme developed by Jasni and Abdul (2006) produces watermarked image that has the highest PSNR among the schemes reviewed in this literature but it lacks the reversible capability. It is the only scheme that was clinically evaluated.

Table 2.1 in the next page shows the summary of the watermarking schemes reviewed in this chapter

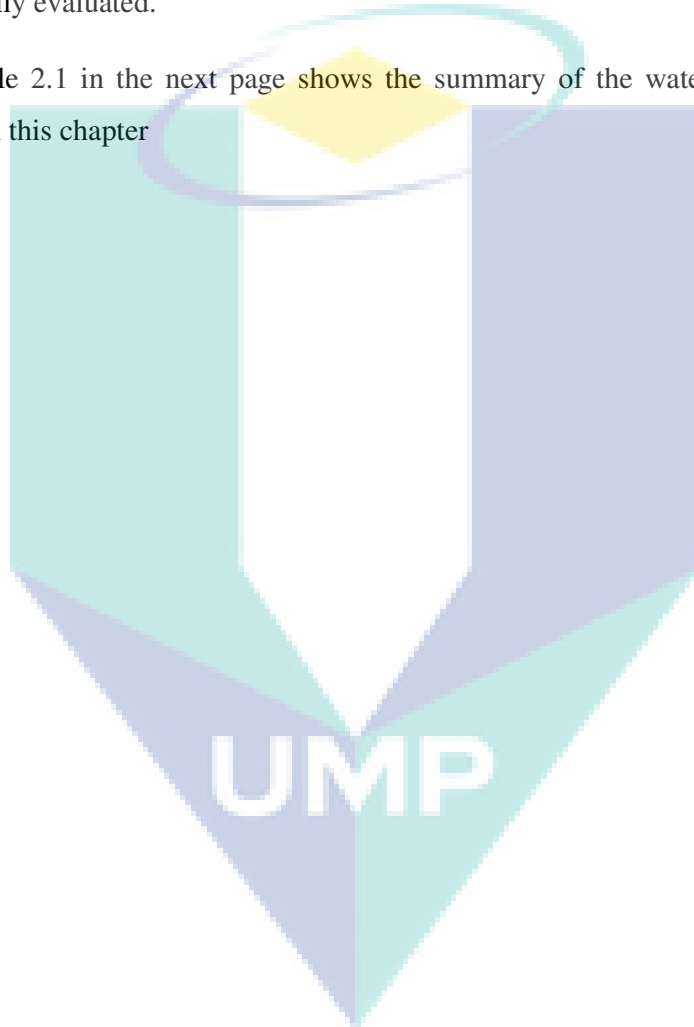


Table 2.1: Summary of watermarking schemes

Proposed by	Domain	Class	Reversible	Localization	Recovery	PSNR(dB)
Fridrich et al.(2002)	Spatial	Fragile	Yes	No	No	35.3 - 53.1
Tian(2003)	Spatial	Fragile	Yes	No	No	16.5 -44.2
Weng et al.(2007)	Spatial	Fragile	Yes	No	No	41
Lou et al.(2009)	Spatial	Fragile	Yes	No	No	21.6-48.9
Yang et al.(2004)	Transform	Fragile	Yes	No	No	44.6
Vleeschouwer et al. (2006)	Spatial	Semi-fragile	Yes	No	No	N/A
Ni et al.(2008)	Spatial	Semi-fragile	Yes	No	No	38.7-40.5
Zou et al.(2006)	Transform	Semi-fragile	Yes	No	No	40.1
Wu(2007)	Transform	Semi-fragile	Yes	Yes	No	43.4-44.5
Guo and Zhuang(2009)	Spatial	Fragile	Yes	Yes	No	N/A
Tan et al.(2011)	Spatial	Fragile	Yes	Yes	No	*34.7
Chiang et al.(2008)	Transform	Fragile	Yes	Yes	Yes	36.4-40.5
Osamah and Khoo(2011)	**Hybrid	Semi-fragile	Yes	Yes	Yes	*36.7
Jasni and Abdul(2006)	Spatial	Fragile	No	Yes	Yes	54.8
Yang and Shen(2010)	Spatial	Fragile	No	Yes	Yes	29.3

* Ultrasound image

**Spatial and transform

2.9 CLASSIFICATION OF WATERMARK ATTACK

Watermarked images may be vulnerable to various attacks as there is no watermarking scheme that can provide the perfect security protection needed. Voloshynovskiy et al. (2001) had classified watermark attacks into four categories as below.

2.9.1 Removal Attack

The aim of removal attacks is to remove the watermark signal from the watermarked image without breaking the security of the watermarking algorithm. It does not attempt to find out the encryption techniques applied or how the watermark is being embedded. This category includes compression, noising, sharpening and histogram equalization.

2.9.2 Geometry Attack

In geometry attack, the watermark signal is distorted rather than being removed from the image. It is possible to recover the original watermark if proper countermeasure is applied. Included in this category are skewing, image rotation and translation.

2.9.3 Cryptographic Attack

The aim of this kind of attack is to break the security measures applied in the watermarking schemes. Once the security measure is broken, the embedded watermark is removed or a misleading watermark is embedded. Brute-force search is one of the techniques in this category. This technique attempts to break the security of the watermark by using a large number of known possible measures to find meaningful secret information.

2.9.4 Protocol Attack

The last category is the protocol attack. It is aim at attacking the entire concept of watermarking application such as in copyright protection. The attacker adds its own watermark into an image and causes the true ownership of the image in question.

2.10 HASH FUNCTION

An example of a hash function is SHA-2. It is a set of hash functions that had been used in various applications. It was designed by the National Security Agency and consists of a set of four hash functions with hash value in length of 224, 256, 384 and 512 bits. A hash function takes a block of data as input and returns a fixed size string as an output. The output is known as the hash value. The modification of the input will cause a different hash value to be produced. It is also infeasible to find two different inputs with the same hash value. Hash function had been used widely in image watermarking for authentication and verification purposes. For example a block of pixels can be hashed and the hashed value is being embedded as part of the watermark. The hash value is retrieved and being compared with the hash value of the same block of pixels at the time of authentication. Kundu and Das (2010) applied SHA-256 hash function to the ROI of medical images for the usage of authentication. Tan et al. (2011) applied the same hash function to verify the success of watermark removal in an image.

MD5 is one in a series of hash function algorithms designed by Ronald Rivest in 1991. It produces a 128 bits hash value. MD5 hash function is not collision resistant and it had been demonstrated that it is possible to generate two inputs with different content but having the same hash value (Wang et al., 2004). Yang and Shen (2010) used MD5 hash function to hash image blocks and embeds the hash values into the LSBs of the corresponding blocks which is used for authentication purposes. Osamah and Khoo (2011) used the same hash function to authenticate the ROI. Fawad et al. (2010) developed their own hash function to be used for image authentication in a robust watermarking scheme. The disadvantage of using self developed hash function is that it may not be secure if proper testing is not performed.

2.11 COMPRESSION IN IMAGE WATERMARKING

Compression is the process of storing or packing data in a format that requires less space than the initial file. Lossless data compression is a category of data compression algorithm that allows the exact original data to be reconstructed from the compressed data. Lossless compression is suitable for the usage in medical image due to the importance of perceptibility in the process of diagnosis (Shih and Wu, 2005). Examples of lossless compression algorithm are Huffman coding, arithmetic coding, RLE and lossless JPEG.

Huffman coding was developed by David A. Huffman in 1952. Huffman coding is a predictive based compression technique where it removes the redundancy between successive pixels by encoding only the residual between actual and predicted values. Since the residue value usually has a much smaller dynamic range and leads to fewer encoding bits and causes a compression. Huffman coding is a variable output bit length encoding method in which the input bits are grouped together based on their bit probability in the signal.

Arithmetic coding is a very different algorithm from the Huffman algorithm. Arithmetic coding still uses the probabilities of source symbols. It successively subdivides the interval 0.0 to 1.0 into subintervals based on the probabilities of the source stream. These subintervals are again subdivided as each new source symbols in encountered. The sizes of the subintervals are proportional to the frequency of the symbols in the source stream. As the stream of symbols becomes longer, the interval representing it becomes finer and finer in precision. The number representing the whole stream can be found by choosing a number from this final interval. Arithmetic coding is more powerful than Huffman coding in terms of compression ratio but arithmetic coding is more complex and requires more computer resources.

RLE is a simple lossless data compression algorithm. It replaces the sequences of the same data values by a count number and a single value. In a more detailed example, binary data that contains 11111100000111111 is encoded as (6, 1), (5, 0) and (6, 1). This is interpreted as six 1's, five 0's and six 1's. The decimal number is then being converted to binary data that reads as (110, 1), (101, 0) and (110, 1). As a comparison, the original binary data has 17 bits and the compressed binary data has

only 12 bits. RLE has a very simple algorithm as compare to other compression techniques. But RLE will only work best if it is being applied to images that have large number of identical successive bits such as bitmap files.

JPEG standard is commonly used for lossy compression for digital images. A JPEG file can be created by specifying the degree of compression needed. The highest image quality has the largest file size and vice versa. JPEG has an option to allow lossless compression. JPEG2000 standard which is a wavelet based was developed in year 2000 to replace the original DCT based JPEG standard. JPEG 2000 has advantages over the original standard such as compression performance.

Compression algorithm can be applied in image watermarking. Chang et al. (2006) demonstrates the usage of RLE by encoding a bitmap file and embedding it into a gray-level image. Lin and Hu (2009) further improved this RLE based watermarking scheme to achieve higher embedding capacity by using an additional bit to represent the encoding. Osamah and Khoo (2011) had used lossy JPEG compression to compress the ROI for the same purpose. They had also compressed the average of block in the ROI for the usage of tamper detection using Huffman coding. Caldelli et al. (2006) proposed a system that permits to jointly compress and watermark remote sensing and medical images using a near-lossless JPEG compression algorithm. Weng et al. (2007) uses arithmetic coding to compress the location map used to facilitate the extraction of the watermark.

2.12 DICOM

The American College of Radiology and the National Electrical Manufacturers Association created a committee to develop a set of standards to serve as the common ground for various medical imaging equipment vendors. The set of standards will allow newly developed equipments to communicate and participate in sharing medical image information within the PACS environment. The standard is called DICOM or the current version known as DICOM 3.0, consist of 16 parts. Each DICOM document is identified by a title and standard number, which takes the form "PS 3.X-YYYY," where "X" is commonly called the part number and "YYYY" is the year of publication. For example, DICOM Part 1 has a title of "Introduction and Overview" and document

number PS 3.1-1996. Watermarking is not currently in the standard. It only provides guidelines for the implementation of digital signature to ensure the integrity of medical images.

2.13 PACS

A generic PACS infrastructure as described by Huang (2004) consist of patient data servers, imaging modalities, PACS controllers with database and archive and also display workstations connected by communication networks as shown in Figure 2.2. Application servers are where images and data are extracted from the PACS archive for various usages. Acquisition gateway acts as a buffer between imaging modalities and the PACS controllers. Its task are such as acquiring image from the imaging modalities, converting the data from manufacturer specifications to DICOM data formats and forwarding the image to PACS controller or display workstations. Other tasks such as image preprocessing, compression and data security are also performed here. PACS controllers and archive servers have more complicated functions such as image receiving, image stacking, image routing, image archiving, PACS database updating and RIS interfacing.

2.14 IMAGE WATERMARKING IN PACS

Fontani et al. (2010) described PACS in a hierarchical manner. The hierarchical structure can be viewed as a pyramid with hospitals at its bottom and the PACS at its top. Images are acquired in a hospital and are immediately stored in its PACS. The images are forwarded to a superior PACS and remain in this system for several hours and during this time the integrity of the images is not always strictly protected. The images are then forwarded to the hierarchically superior PACS, until they reach the top-PACS. The top-PACS will permanently store the images along with their hash signatures, encrypted using the private key of the PACS administrator. In order to implement watermarking in PACS, it was proposed by Fontani et al. (2010) that the images are watermarked after they were acquired by the imaging modalities.

Authentication of the images can be performed at every level of the hierarchy from bottom to top and vice versa.

Huang (2004) had proposed an image security system based on the digital envelope (DE) concept which is similar to watermarking. This concept is for ensuring data integrity, authenticity and privacy during image transmissions. DE consists of digital signature (DS) of the image and selected information from the DICOM image header. The method applies to both the sender and receiver sides. The sender side consists of the following four steps:

- *Image preprocessing*: The image is segmented from its background and relevant patient information is extracted from the DICOM image header.
- *Image hashing*: The segmented image is hashed using MD5 hashing algorithm.
- *Data encryption*: RSA public key encryption is used to produce DS by encrypting the image hash value. Data encryption standard is used to encrypt the DS and patient data to produce DE.
- *Data embedding*: The DE is embedded into the image or the background of the image. LSBs of a random pixel are replaced with DE bits.

The receiver side has the reversed process of the four steps that consist of data extraction and decryption. A mammogram was processed using the described method. A total of 6720 bits were embedded and the whole process took approximately 75 seconds. The disadvantage of this method is that tampering of an image can be detected but without tamper localization. It only provides protection for images during the transmission process. The DE method needs a different public key for a different user and thus requires intensive processing.

Huang (2004) had also proposed the implementation of this method in a PACS environment as shown in Figure 2.3. This implementation consists of a dedicated image authority server that was designed to solve the limitations of the DE method. All images from the modalities are digitally signed at the DICOM gateway using the authority server's public key instead of the individual user's key. Whenever a remote user needs to verify the origin authenticity or integrity of an image, a request can be made to the system authority and in this case, the PACS security server. The PACS security server

is the only one that has the private key which is used to extract and decrypt the DE embedded in the image.

The watermarking scheme proposed by Tan et al. (2011) described in the previous section had also applied public keys in its watermarking embedding. The watermark is encrypted using RSA public key system. Tan et al. (2011) had also proposed the implementation of the scheme in a PACS based on the image security system proposed by Huang (2004). In this implementation, the encryption and decryption of the watermark is done by the sender and the receiver as shown in Figure 2.4.

Both proposed implementations by Huang and Tan et al. (2011) has the disadvantage where the keys used for encryption and decryption needs to be properly managed. The issue of how medical images can be watermarked and authenticated efficiently without affecting the operation of the PACS was not addressed.

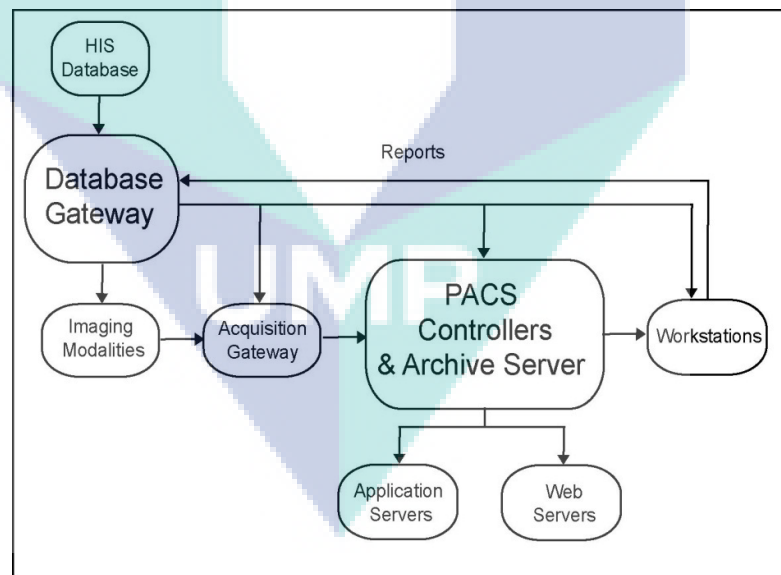


Figure 2.2: Generic PACS components and its data flow

Source: Huang (2004)

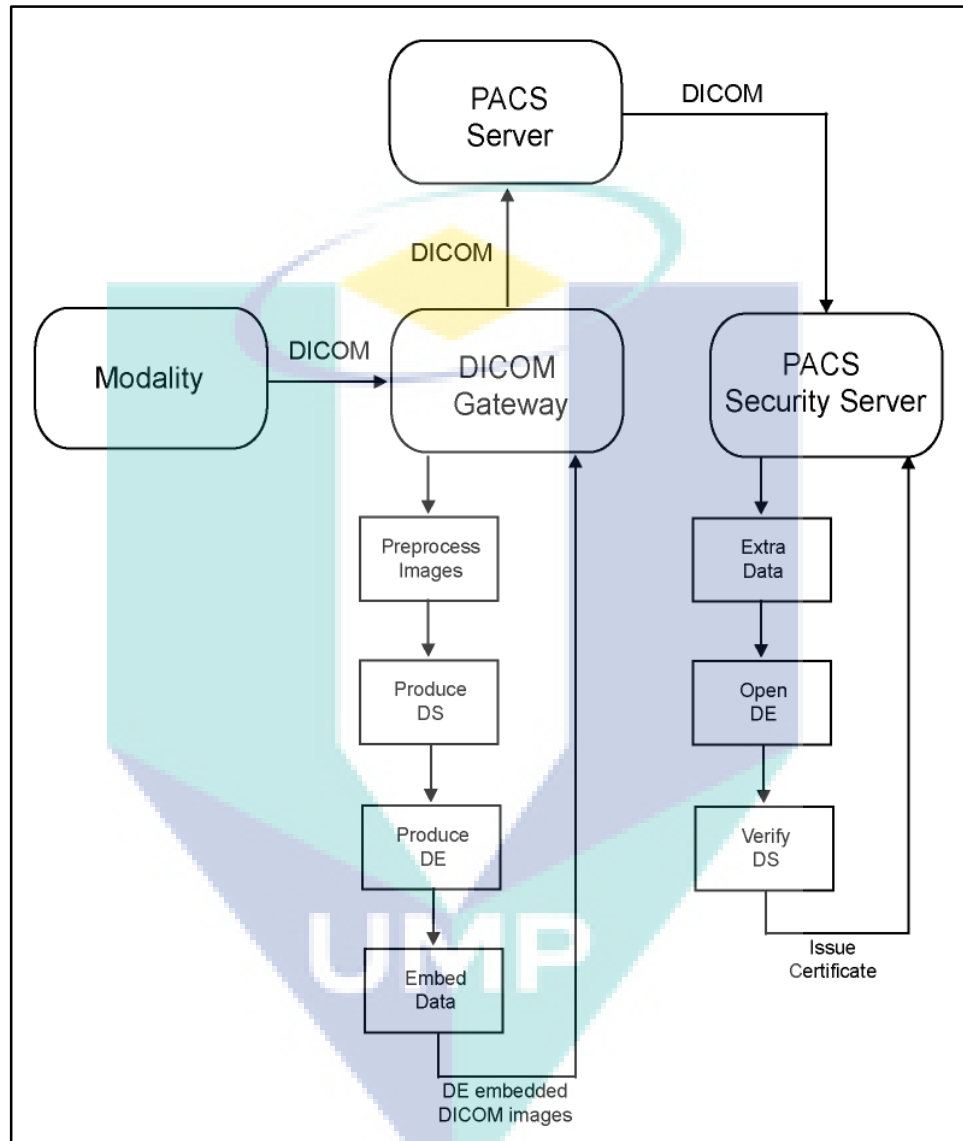


Figure 2.3: Image security system in a PACS environment

Source: Huang (2004)

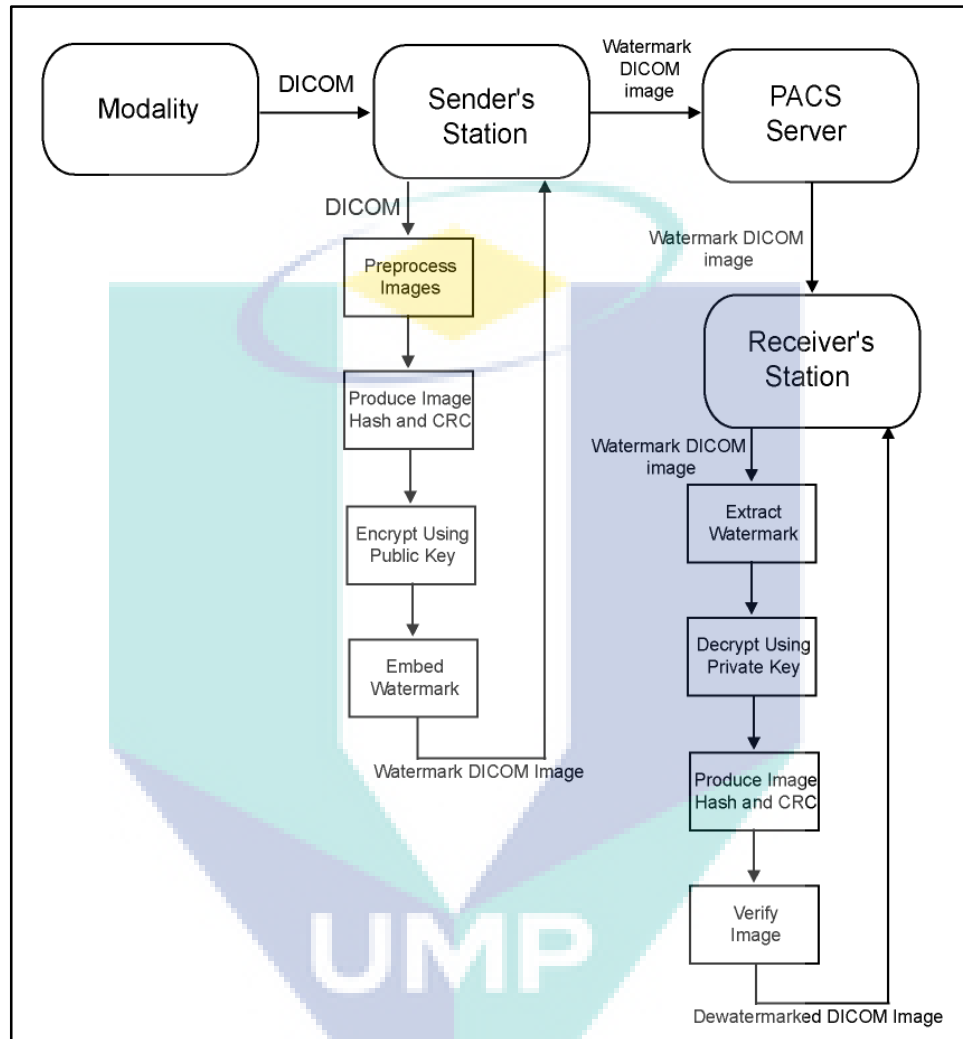


Figure 2.4: The implementation of scheme by Tan et al. (2011) in a PACS

Source: Tan et al. (2011)

CHAPTER 3

REVERSIBLE TAMPER LOCALIZATION AND RECOVERY(R-TLR)

3.1 INTRODUCTION

This chapter is starts with section 3.2 where it describes the research methodology used in this chapter. Section 3.3 proposes a reversible tamper localization and recovery watermarking scheme for ultrasound images. In this scheme, a ROI is defined and the watermark is embedded in the ROI. The watermark consists of authentication and recovery bits. The removed LSBs from the ROI are embedded in the RONI. Hash function is used to ensure the integrity of the RONI. Section 3.4 discusses the experiments results and evaluates the proposed scheme. Lastly, section 3.5 concludes the chapter.

3.2 RESEARCH METHODOLOGY

The first of part the research is to develop a reversible tamper localization and recovery watermarking for medical images. There are many medical image modalities that can be chosen for the purpose of this research such as ultrasound images, magnetic resonance images and radiographs. Ultrasound images are normally in monochrome grayscales and smaller in size thus is easier to work with compared to other modalities. They also have a special characteristic where the region of interest (ROI) is normally located in the center of the image and about two-third of the rest of image is normally

black. The black area could possibly be a good place to store the LSBs of the original pixel to allow the image to be restored to its original state. The ultrasound images that will be used for the experiments are acquired from the Internet.

There is an issue on the definition of the ROI and RONI. There is no existing guideline on how the ROI and RONI should be defined in medical image watermarking. The size and location of the ROI is subjected to the definition by the users or physicians. A proper study needs to be conducted in this area but it is not within the scope of the research. However, it has been observed that physicians will choose the center of the ultrasound images as the ROI. Therefore, for the purpose of being able to test the proposed watermarking schemes, the definition of ROI and RONI will be done by the watermarking scheme itself with the assumption that the ROI of the ultrasound images is located in the center of the image.

A reversible watermarking scheme allows the original pixel to be restored once the watermark had been removed. Thus it requires the removed or modified LSBs to be stored within the image before the watermark is embedded. The most direct technique is by embedding a watermark within the spatial domain had been used by Jasni and Abdul (2006) and Yang and Shen (2010). There is no mathematical calculation needed and this reduces the computation. The watermark is embedded directly into the LSBs of the image pixels. One bit of information can be embedded into the LSB of a pixel. For example, x has the value of 208 with the binary value of 11010000. In order to embed one bit of information with the value of 1 for instance, the new binary value of x is 11010001 which is equivalent to 209. This only causes a change of one pixel value in order to embed one bit of information in one pixel. The watermark is usually embedded in the RONI where most pixel values are zero. The embedded watermark can be retrieved and the LSB of the RONI is reset to zero. The second advantage of this method is the embedding capacity where it has a theoretical 1 bits per pixel as compare to only 0.5 bits per pixel in the difference expansion by Tian (2003) method.

Localization of a tampered image is useful for deducing the motive of the tampering or whether the modification is legitimate. An image is usually divided into blocks and localization accuracy depends on the block size. A block can be computed to produce a code or hash value and is embedded into the image itself. The code can be

retrieved and compared to current block code at the time of authentication. Difference in the comparison indicates that the particular block had been tampered.

Tampered image can be recovered by using embedded watermark that contains information of the original image. Approximate recovery is a concept to recover an image to approximately the original state. There would be a difference between the recovered image and the original image. The approximate recovery can be in the form of lossy compressed image as done by Osamah and Khoo (2011) where the quality of the recovered image depends on the compression rate applied to the original image. Another type of approximate recovery is by using average intensities of the image pixels as applied by Chiang et al. (2008). The image can be divided into blocks of 2 x 2, 4 x 4, 8 x 8 and so forth. The average intensity is calculated by dividing the total pixel values with the total number of pixels in a block. The quality of the recovered image is also depends on the block size used.

There is an issue of embedding capacity to be considered when deciding the size of the block to be used. The watermark payload consists of authentication and recovery watermark. A smaller block will result in a higher watermark payload and vice versa. The LSBs that will be removed to allow watermark embedding also needs to be considered in the total watermark payload. Therefore, it is crucial to ensure that the total watermark payload does not exceed the available embedding capacity in the image to allow reversibility, tamper localization and recovery.

Watermarked images will be measured in terms of PSNR. The watermarked image will be tampered by using ImageJ to know the effectiveness of the watermark scheme. ImageJ is a Java based software for image processing and analysis.

3.3 REVERSIBLE TAMPER LOCALIZATION AND RECOVERY(R-TLR) WATERMARKING

In this section, a reversible tamper localization and recovery(R-TLR) watermarking scheme is proposed. This scheme is an enhancement of the scheme proposed by Jasni and Abdul (2006) with reversible capability. The scheme proposed by Jasni and Abdul (2006) was chosen for further development for the following reasons:

- i. It operates in the spatial domain which is easier to be applied than schemes that operates in the transform domain that is more complex in terms of algorithm.
- ii. The watermarked image produced by the scheme has the highest PSNR among the schemes being reviewed. A high PSNR indicates low distortion in the watermarked image, which is an important factor to be considered in medical image watermarking. The issue with PSNR is that it is not correlating well with perceived quality measurement (Navas et al., 2007). In order to overcome this issue, the scheme had been clinically evaluated by Jasni et al. (2006). They showed that the watermarked medical images do not affect diagnoses done by the user which is crucial if the scheme is to be implemented in real operational environment. However, this scheme is not reversible.

The reversible methods used in the reviewed schemes in the previous chapter uses complex algorithm. This can be an issue if it is applied in operational PACS where thousands of medical images need to be processed and much computing resource is required.

In order to allow a watermarking scheme to be reversible, the original bits of the image needs to be restored once the watermark is being extracted from the image. In this proposed reversible scheme, a simple method where the information needed for image restoration is embedded in the RONI that requires very minimum processing was chosen. Grayscale monochrome ultrasound images are used as the modality to test this scheme as they are smaller in size thus easier to be work with as compare to other types of modalities. Figure 3.1 shows some examples of ultrasound images.

From the examples of the ultrasound images given in Figure 3.1, a common characteristic can be concluded. The important part of the image or also known as the ROI does not occupy the whole image. The ROI forms a triangle in the center of the image and the RONI is the black area outside of the triangle. The RONI usually contains descriptions for the image such as time, date and measurements display. The proposed scheme takes advantage of this characteristic by using the RONI to allow watermark reversibility. The image can be divided into ROI and RONI consist of rectangles as shown in Figure 3.2. The ROI consist of rectangles that form a pyramid. This method allows the ROI to be more accurately defined and results in having more space utilizable for defining the RONI. The authentication and recovery watermark will

be embedded in LSBs in the ROI. The LSBs that were removed from the ROI will be stored in the LSBs in the RONI. The process of embedding the removed LSBs does not use any compression or transformation method. This will minimize processing time and keep the distortion in the RONI at low.

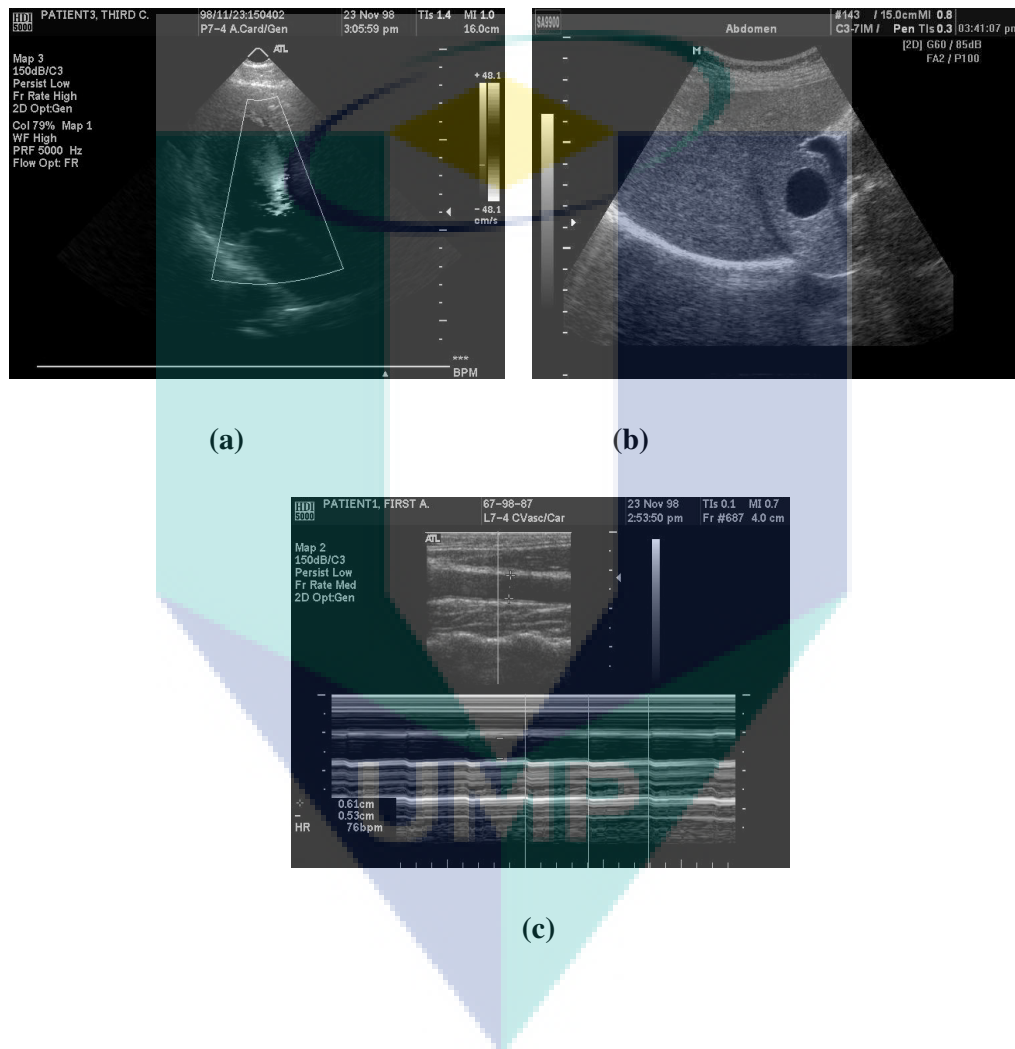


Figure 3.1: Ultrasound images

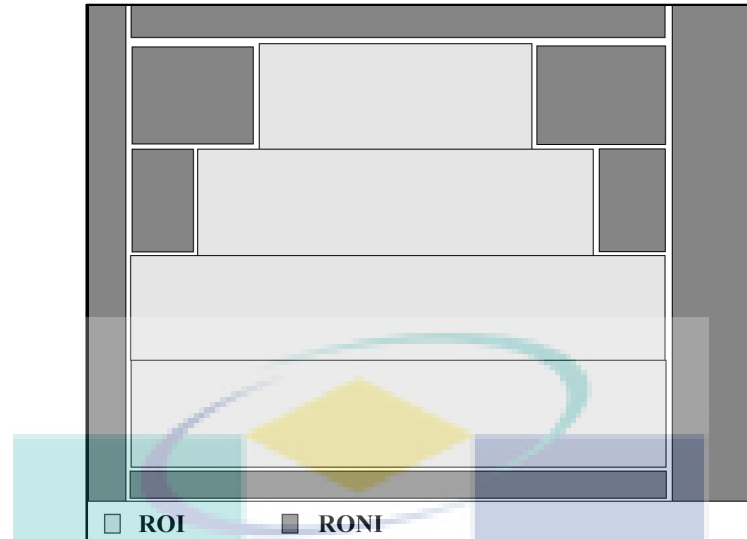


Figure 3.2: Image divided into ROI and RONI

3.3.1 Authentication And Recovery Watermark

This scheme divides an image into blocks and each block is further divided into sub-blocks as shown in Figure 3.3.

Average intensity of the block and its sub-blocks will be used in the authentication and recovery process. The average intensity of a block is calculated based on:

$$\text{Block average intensity} = \frac{(P_1+P_2+P_3\dots+P_{15}+P_{16})}{16} \quad (3.1)$$

where P_1 to P_{16} are the pixels intensity in a block. The average intensity of a sub-block is:

$$\text{Sub-block average intensity} = \frac{(P_1+P_2+P_5+P_6)}{4} \quad (3.2)$$

where P_1, P_2, P_5 and P_6 are the pixels intensity in a sub-block.

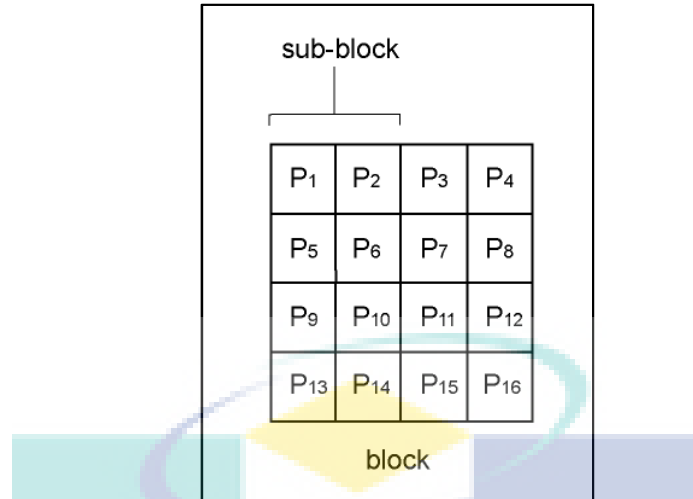


Figure 3.3: A block is divided into four sub-blocks

The average intensity of the sub-blocks will be used as the recovery information once tampering had been detected. If a block is being tampered locally, the pixel intensities will be changed and directly changes the average intensity of the concern block. To overcome this issue, a parity check is used. However, the parity check has a disadvantage whereby if more than one bit is changed, the parity check is ineffective. In order to ensure better security, an additional feature is used by comparing the average intensity of a block with its sub-blocks. The details of the algorithm will be explained in the later section.

3.3.2 Image Preparation

Image preparation is the key for this scheme to be reversible. The proposed scheme had taken a different approach by dividing an ultrasound image into ROI and RONI as shown in Figure 3.4.

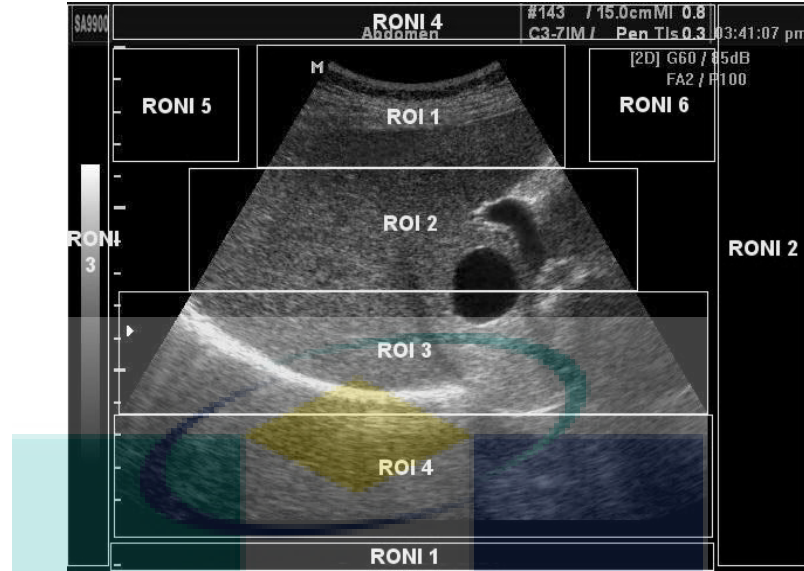


Figure 3.4: An ultrasound image is divided into ROI and RONI

In this scheme, four rectangles are used to form a pyramid boundary for the ROI and six rectangles in the RONI. The number of blocks in the ROI must not exceed the number of blocks in the RONI to ensure that the original LSBs that will be removed from the ROI for watermark embedding can be stored in the RONI without space constraints. Initial estimation based on the size of the ROI revealed that the optimal non-overlapping block size in the ROI is 8 x 8 pixels. The RONI is divided into non-overlapping blocks of 6 x 6 pixels for easy execution by matching the number of LSBs to be removed from each block in the ROI as shown in Figure 3.8.

One-to-one mapping sequence will be done based on Eq. (3.3) to create a unique and random mapping of the blocks.

$$\vec{B} = \left[(k \times B \bmod N_b) \right] + 1 \quad (3.3)$$

where $B, \vec{B}, k \in [1, N_b]$, k is a prime number, and N_b is the total number of blocks in the ROI. In this scheme, a unique integer is assigned $B \in \{1, 2, 3, \dots, N_b\}$ to each block in

the ROI. Number of blocks in the RONI is equal to the total number of blocks in the ROI. The maximum prime number $k \in \{1, N_b\}$ is picked. Eq. (3.3) is applied to each block number B where \bar{B} the number of its mapping blocks is obtained. All pairs of B and \bar{B} will form the block mapping sequence for ROI.

Blocks in the RONI were also assigned with a unique integer. Each block in RONI corresponds with the blocks in ROI. In this scheme, for example as shown in Figure 3.5, block x1 is mapped to block y1 in ROI by using Eq. (3.3). Block x1 in the ROI with unique integer “5” for example, is mapped with block x2 in the RONI with the same integer. The same algorithm is applied in mapping block y1 and block y2 and as well as the rest of the blocks.

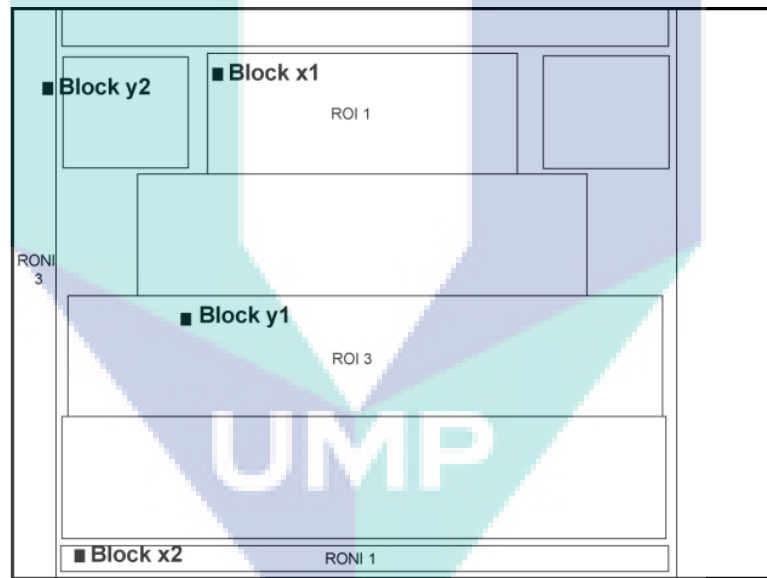


Figure 3.5: An example of mapping sequence between blocks in ROI and RONI

3.3.3 Watermark Generation And Embedding

i. Authentication and Recovery Watermark

Each block of 8 x 8 pixels in the ROI is divided into four sub-blocks of 4 x 4 pixels. The watermark in each sub-block is a block of 3 x 3 pixels where it contains one authentication bit, one parity check bit and a 7-bit recovery information.

This scheme has taken a different approach in the removal of LSBs significant bits. Only the LSBs for pixels which will be used for watermarking will be removed rather than the removal of LSBs for each pixel within the block as proposed by Jasni and Abdul (2006). In this scheme, only in the 3 x 3 pixels in each sub-block where the LSBs will be set to zero. This will minimize processing time needed and will ensure storage availability in the RONI for the LSBs which were removed from the ROI. The following algorithm describes how the one authentication bit, one parity check bit and a 7-bit recovery watermark are generated and embedded.

Step 1: The average intensity for block x_1 and its sub-blocks, x_{1s} will be computed, denoted by avg_x_1 and avg_x_{1s} respectively. As an example, the value for avg_x_1 is 85 and the values for avg_x_{1s} are 99, 84, 81 and 77 respectively as shown in Figure 3.6.

Step 2: Generate the authentication bit, v , of each sub-block as:

$$v = \begin{cases} 1 & \text{if } avg_x_{1s} \geq avg_x_1, \\ 0 & \text{otherwise,} \end{cases} \quad (3.4)$$

Step 3: Generate the parity check bit, p , of each sub-block as:

$$p = \begin{cases} 1 & \text{if num is odd,} \\ 0 & \text{otherwise,} \end{cases} \quad (3.5)$$

where num is the total number of 1s in the seven most significant bits of avg_x_{1s} .

Step 4: The value of v and p will be used to verify each sub-block, x_{1s} .

Step 5: From the mapping sequence generated in the image preparation step, block y_1 recovery information will be stored in block x_1 as shown in Figure 3.7. The average intensity of sub-blocks of block y_1 , denoted as avg_y_{1s} will be used for

recovery. Only the seven most significant bits of avg_y1s will be used as one bit is used for watermarking.

Step 6: The authentication bit and parity check bit for $x1s$ will be embedded in the LSBs of $x1s$ as shown in Figure 3.7. The recovery bits of block $y1$, avg_y1s will be embedded in the corresponding LSBs in $x1s$. The same process is applied to the rest of blocks.

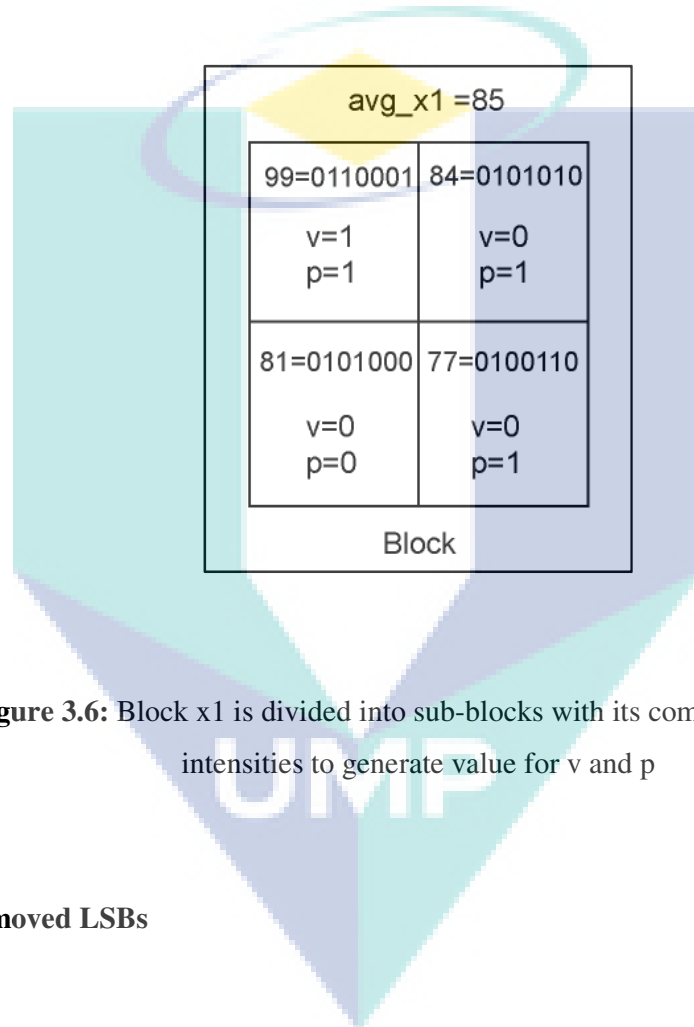


Figure 3.6: Block $x1$ is divided into sub-blocks with its computed average intensities UMP to generate value for v and p

ii. Removed LSBs

It is proposed that the LSBs that were removed during the watermark embedding process be stored in the RONI for restoring the ROI to its original state later. By using the example in Figure 3.8, LSBs of block $x1$ that were removed will be stored in LSBs of block $x2$ in the RONI. Each 3×3 pixel block in the RONI will store the nine LSBs that were removed from the corresponding sub-block in the ROI by matching the block number that were assigned in the preparation step. All removed LSBs will be collected to form a block of bits for hashing purposes which will be explained in the next section.

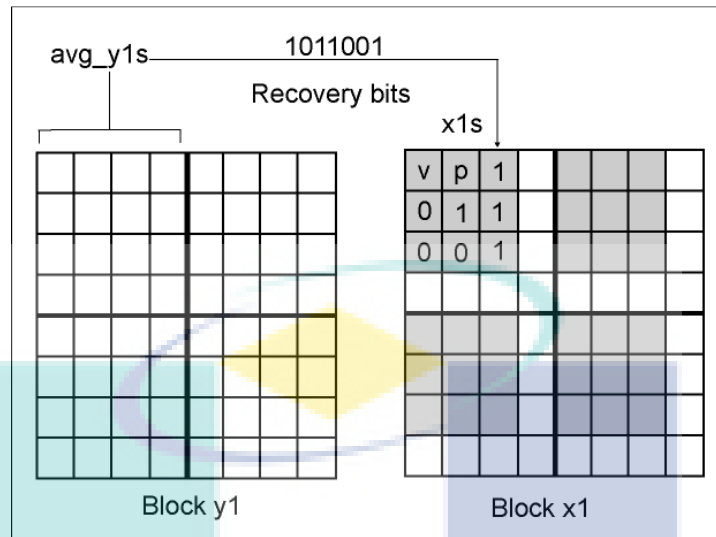


Figure 3.7 : Recovery bits of y1s, avg_y1s is stored in x1s together with v and p generated from x1s

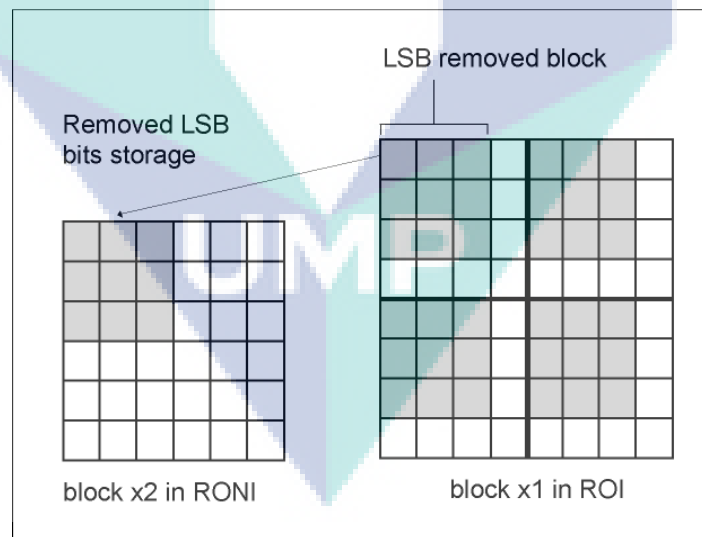


Figure 3.8: Block x1 and block x2

iii. Hash Function

The removed LSBs which were embedded in the RONI are vulnerable to malicious modification. In order to ensure its integrity, a hash function will be used. The hash value for the block of the removed LSBs, denoted as hash_A is calculated using SHA-256. SHA-256 is chosen due to its popular usage in medical image watermarking such as being applied by Kundu and Das (2010) and Tan et al. (2010). SHA-256 will produce a hexadecimal string which can be used to authenticate the removed LSBs. Other more secured hash function may be used. The hexadecimal string, hash_A is also embedded in the RONI.

3.3.4 Tamper Localization And Recovery

The ROI of the image is divided into non-overlapping blocks of 8 x 8 pixels and each block is further divided into 4 x 4 sub-blocks. The LSBs in the sub-block will be removed and to be specific, only 3 x 3 pixels out of the 4x4 pixels sub-block, same as in the embedding process. The tamper localization procedures are as below:

Step 1:The average intensity of the block y_1 is computed, denoted as avg_y_1 .

Step 2:For each sub-block of y_1 , denoted as y_{1s} , the authentication bit, v and parity check bit, p is extracted.

Step 3:Compute the average intensity for sub-block y_{1s} , denoted as avg_y_{1s} .

Step 4:The total number of 1s in avg_y_{1s} is counted and denoted it as p' .

Step 5:Set the parity check bit of y_{1s} , p' to 1 if p' is odd, otherwise, set it to 0.

Step 6: p' and p is compared and if they are not equal, mark y_{1s} as tampered .

Step 7:If avg_y_{1s} is more than or equal to avg_y_1 then set the authentication bit for y_{1s} , v' to 1, otherwise, set it to 0.

Step 8: v' and v is compared and if they are not equal, mark y_{1s} as tampered and complete the detection for y_{1s} .

Step 9:Block y_1 will be marked tampered if one of its sub-blocks is tampered.

Step 10: Tampered blocks will be recovered by locating its corresponding blocks by using the mapping sequence used in image preparation. In this example, block x_1 is mapped to block y_1 and with the assumption that block y_1 had been marked as tampered and its recovery bits were stored in block x_1 . The average intensity of each sub-block of block y_1 stored in sub-blocks of block x_1 will be obtained. Each sub-block of y_1 will be replaced with the recovered average intensity bits where the 7-bit recovery bit will be transformed to eight bits by padding a zero at the end.

3.3.5 Reversible Watermark

The embedded watermark can be reversed by restoring the removed LSBs during the watermark embedding process. Before the restoration process begins, the embedded LSBs in RONI are authenticated. The LSBs is retrieved and hashed using the same hash function used in the embedding process to produce a hash string denoted as $hash_B$. The embedded hash, $hash_A$ is retrieved and compared to $hash_B$. If the comparison result is equal, the embedded LSB in the RONI is considered as authentic and the process of restoring the ROI to its original state will begin.

Removed LSBs of block x_1 were stored in block x_2 in the RONI as shown in Figure 3.8. The LSBs of each sub-block x_1 will be replaced with its original bits that were stored in the 6×6 pixels of block x_2 . The same process is applied to every block in the ROI. The LSBs of each pixel in RONI will be set to zero.

3.3.6 Experimental Results

Experiments were carried out by watermarking 8 different ultrasound images. It was performed on a computer using Intel i3 2.93 GHz processor with 4 GB RAM. The ultrasound images are in 8-bit monochrome grayscale and 640×480 pixels in size. The ROI and RONI have a total of 173,056 and 107,784 pixels respectively. The total watermark payload is 194,944 bits. The watermarked images have the average PSNR of

53.9 dB as shown in Table 3.1. Figure 3.9 to Figure 3.24 shows the original images and watermarked images.

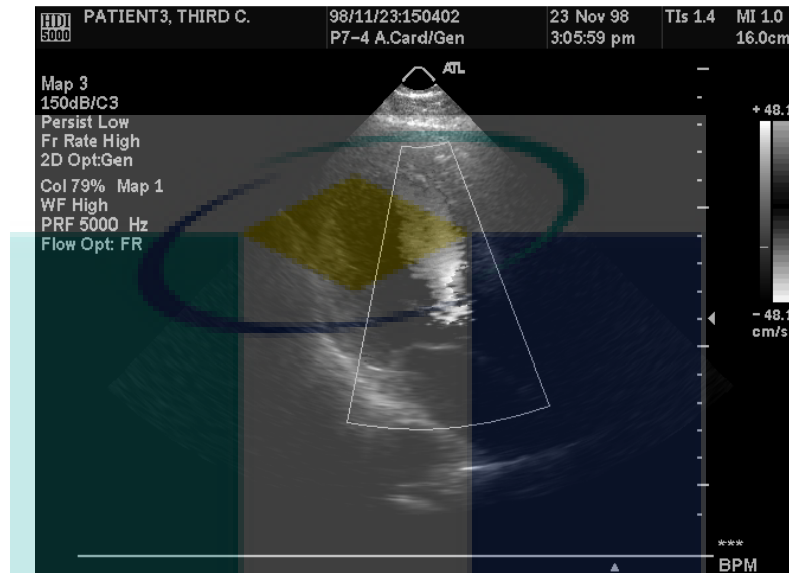


Figure 3.9: Original image of Sample 1

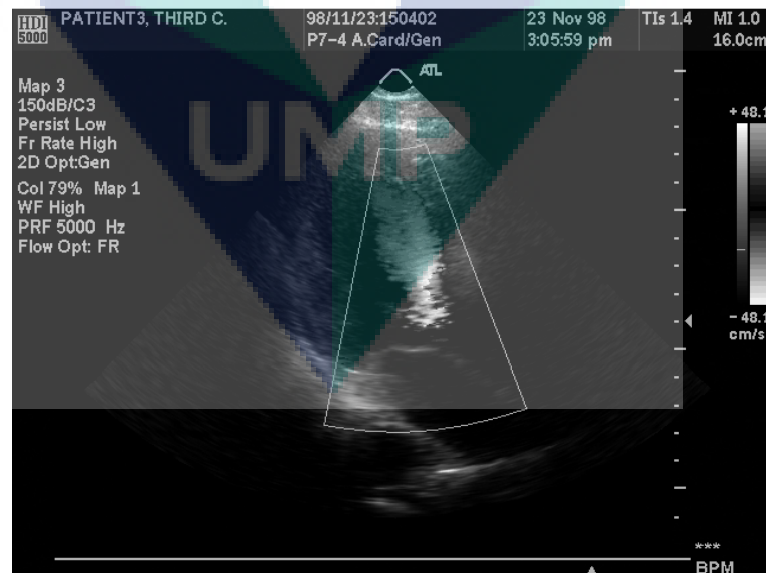


Figure 3.10 : Watermarked image of Sample 1, PSNR=54.1 dB

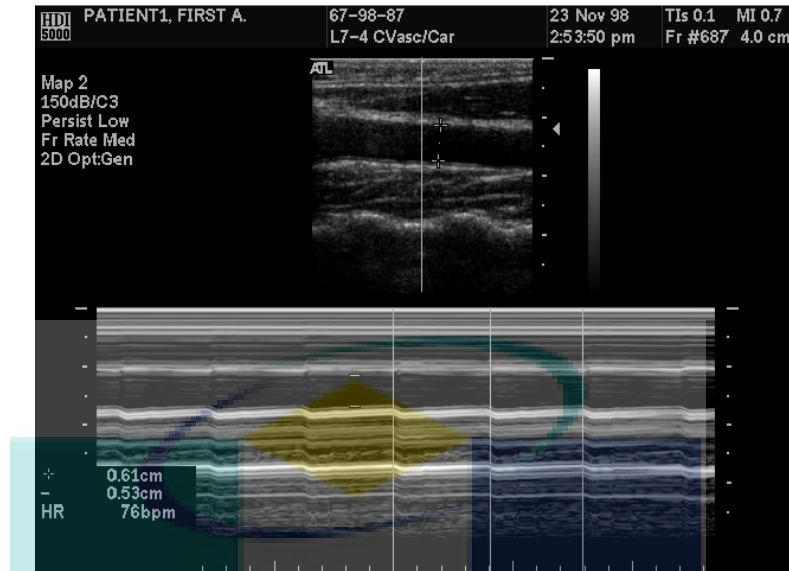


Figure 3.11: Original image of Sample 2

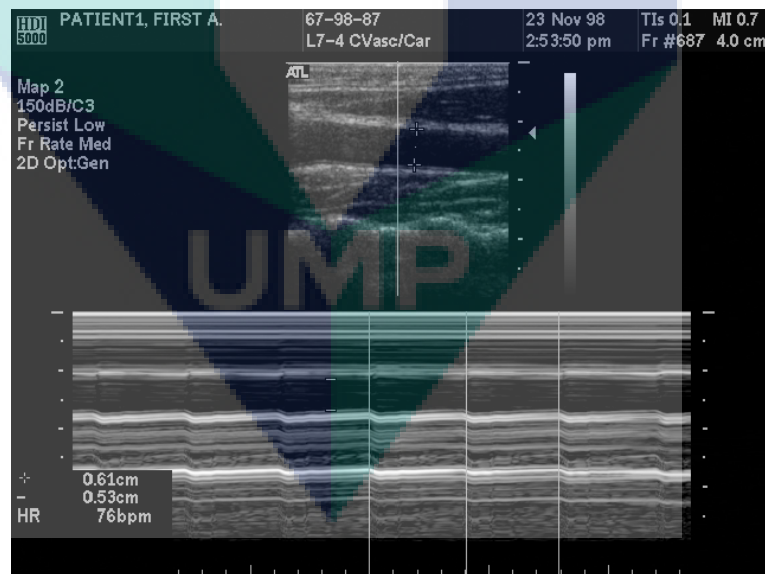


Figure 3.12 : Watermarked image of Sample 2, PSNR=54.1 dB

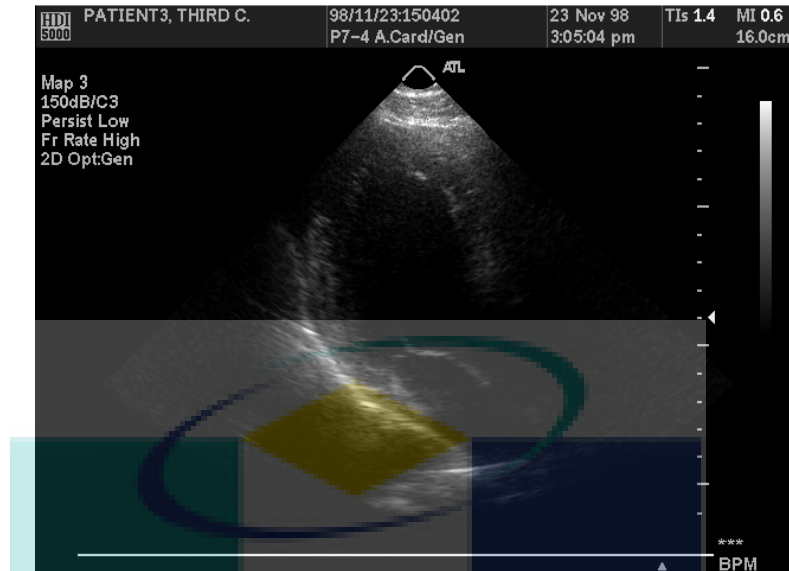


Figure 3.13: Original image of Sample 3

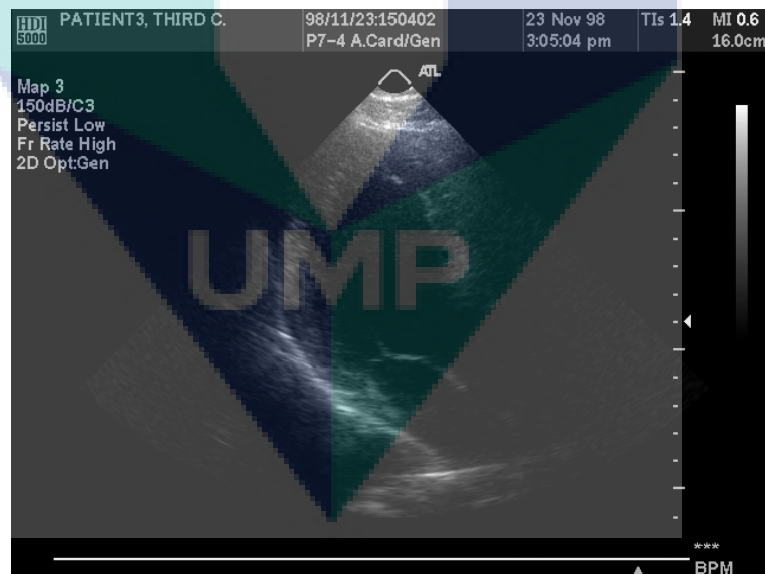


Figure 3.14 : Watermarked image of Sample 3, PSNR=54.6 dB

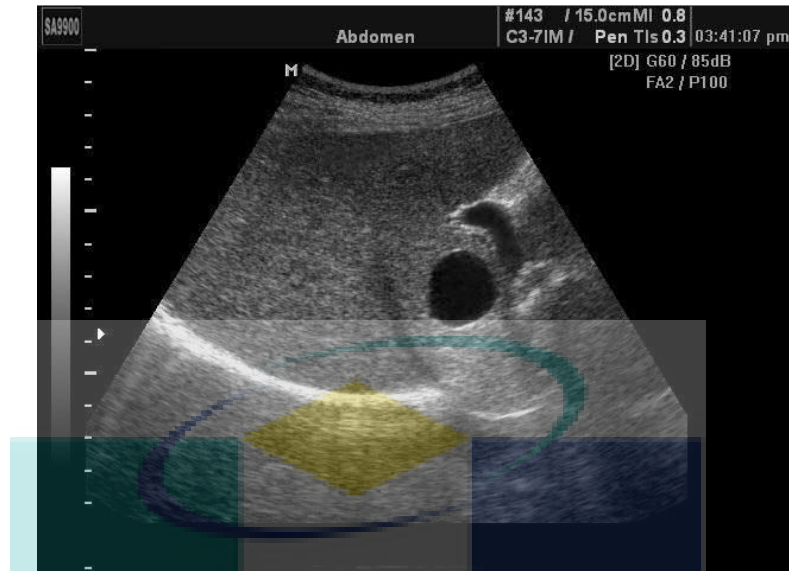


Figure 3.15: Original image of Sample 4

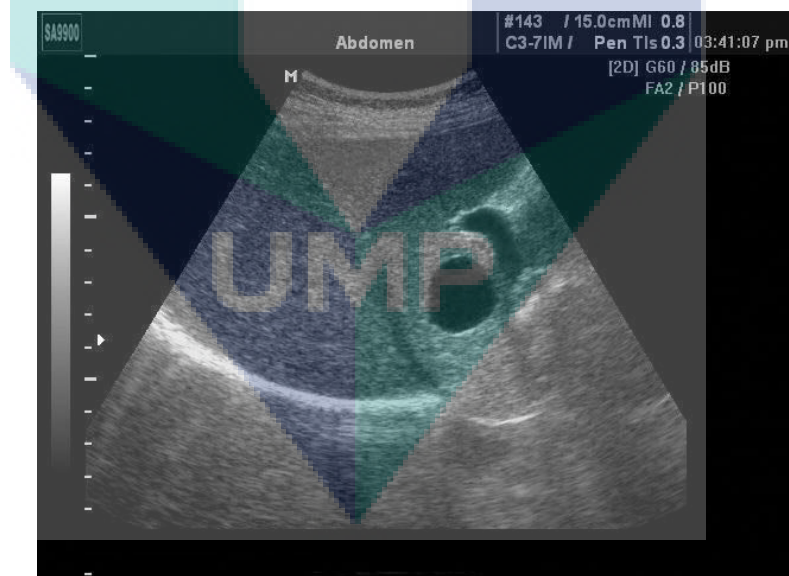


Figure 3.16 : Watermarked image of Sample 4, PSNR=53.4 dB

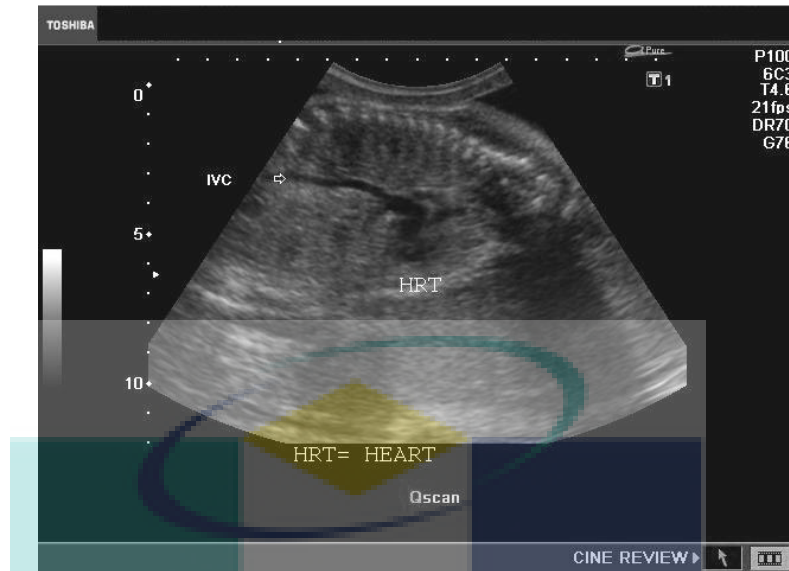


Figure 3.17: Original image of Sample 5

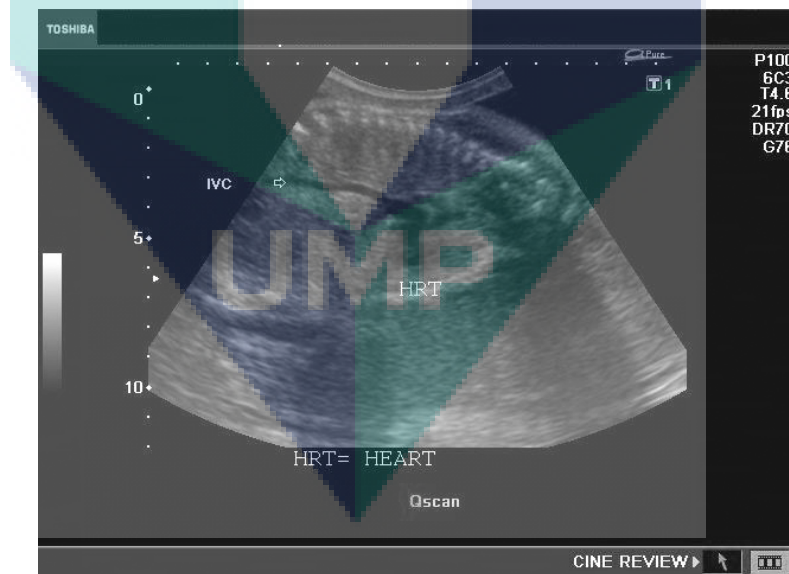


Figure 3.18 : Watermarked image of Sample 5, PSNR=53.6 dB

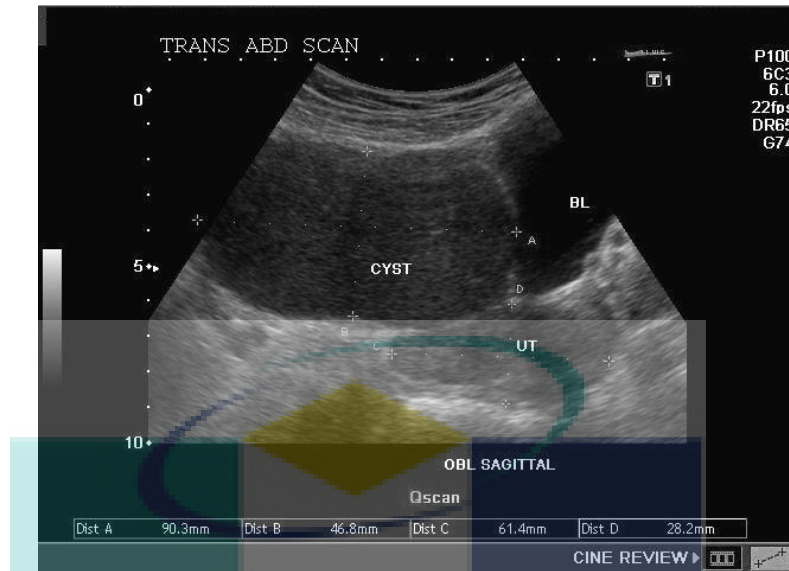


Figure 3.19: Original image of Sample 6

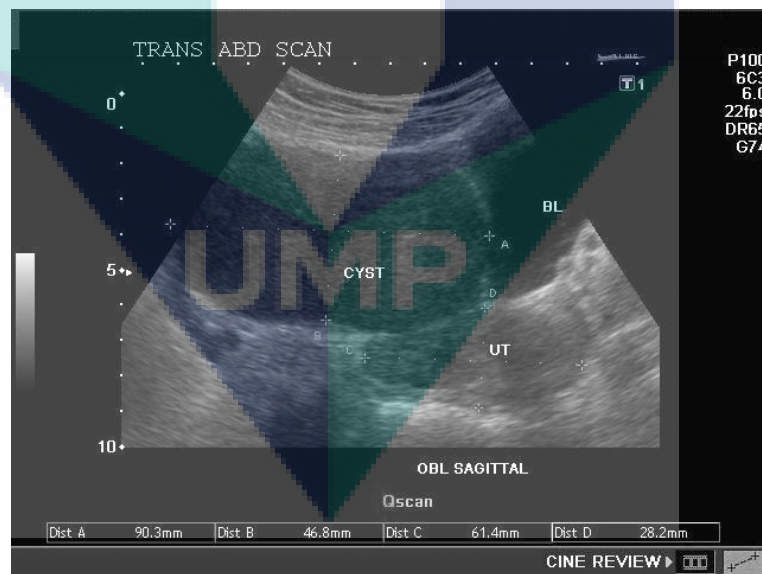


Figure 3.20 : Watermarked image of Sample 6, PSNR=53.7 dB

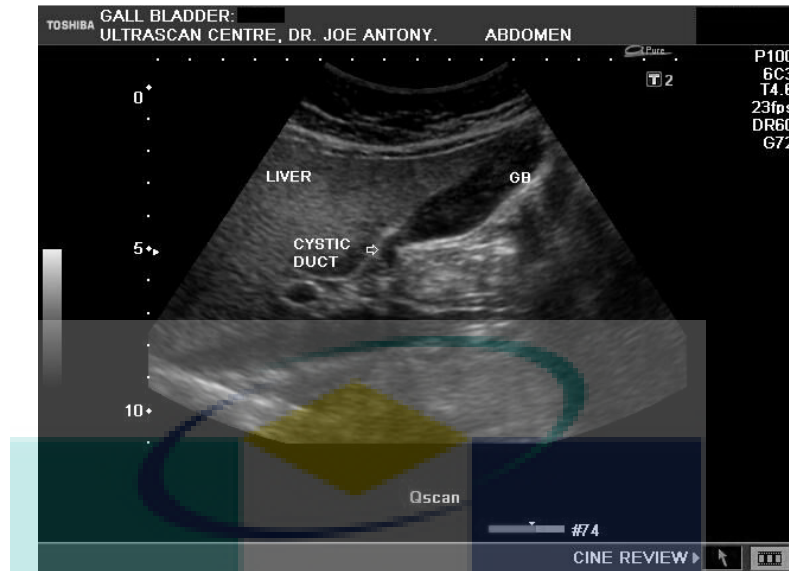


Figure 3.21: Original image of Sample 7

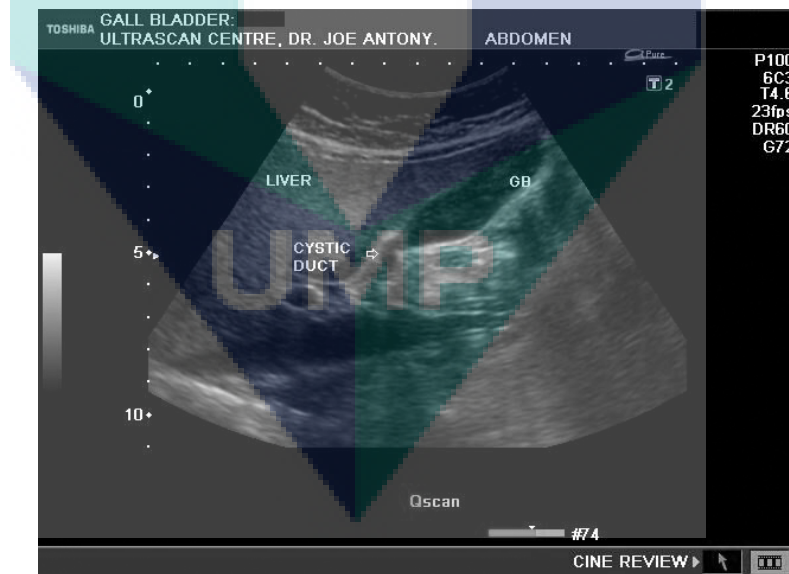


Figure 3.22 : Watermarked image of Sample 7, PSNR=53.5 dB

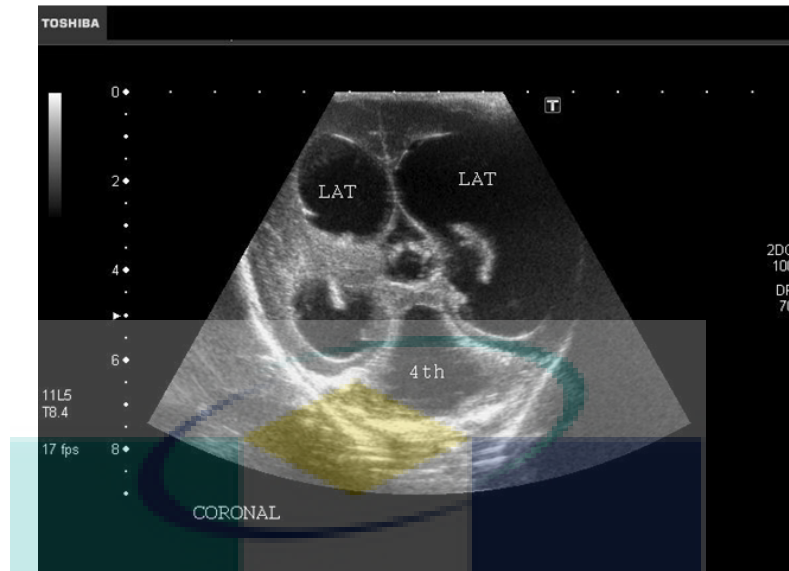


Figure 3.23: Original image of Sample 8

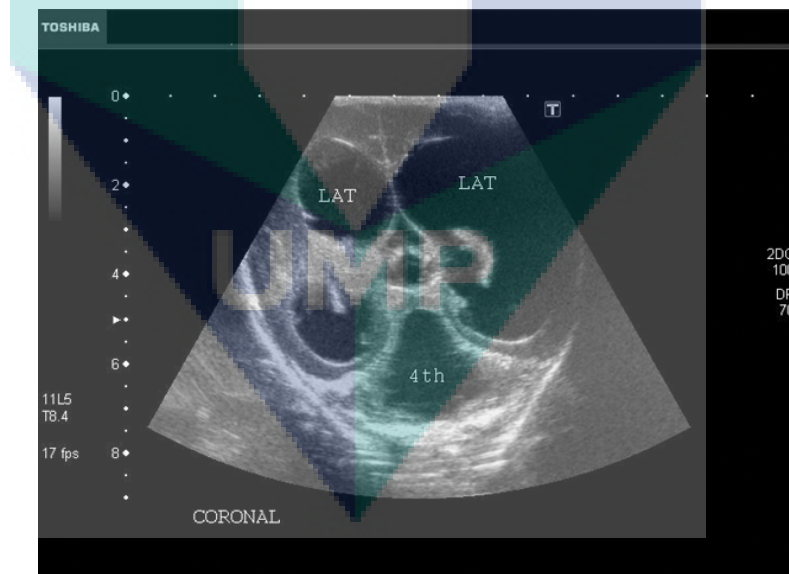


Figure 3.24 : Watermarked image of Sample 8, PSNR=54.1 dB

Table 3.1: PSNR for each watermarked sample and the average PSNR

	PSNR(dB)
Sample 1	54.1
Sample 2	54.1
Sample 3	54.6
Sample 4	53.4
Sample 5	53.6
Sample 6	53.7
Sample 7	53.5
Sample 8	54.1
Average	53.9

i. Tamper Localization And Recovery

The watermarked images were tampered by cloning an area measuring 50 x 30 pixels for each sample. The tampered and recovered images are shown in Figure 3.25 to Figure 3.48. Tampered pixels that were not detected are also highlighted. The number of undetected pixels and tamper detection rate for each sample is shown in Table 3.2. The average tamper detection rate is at 99.98%

Table 3.2: No. of undetected pixels and tamper detection rate for each sample

	1500 pixels tampered	
	No. of pixels undetected	Success Rate(%)
Sample 1	0	100
Sample 2	0	100
Sample 3	19	99.99
Sample 4	50	99.97
Sample 5	0	100
Sample 6	14	99.99
Sample 7	88	99.94
Sample 8	54	99.96
Average		99.98

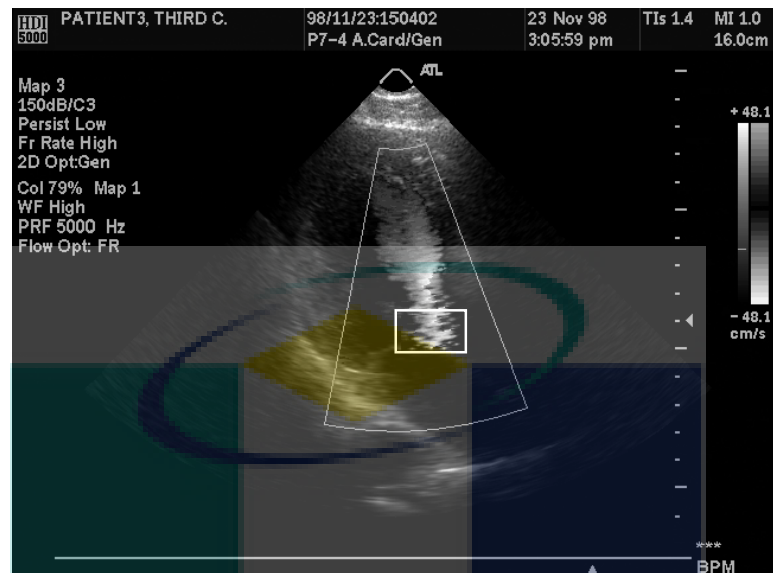


Figure 3.25 : Sample 1 had been manipulated by cloning the highlighted area

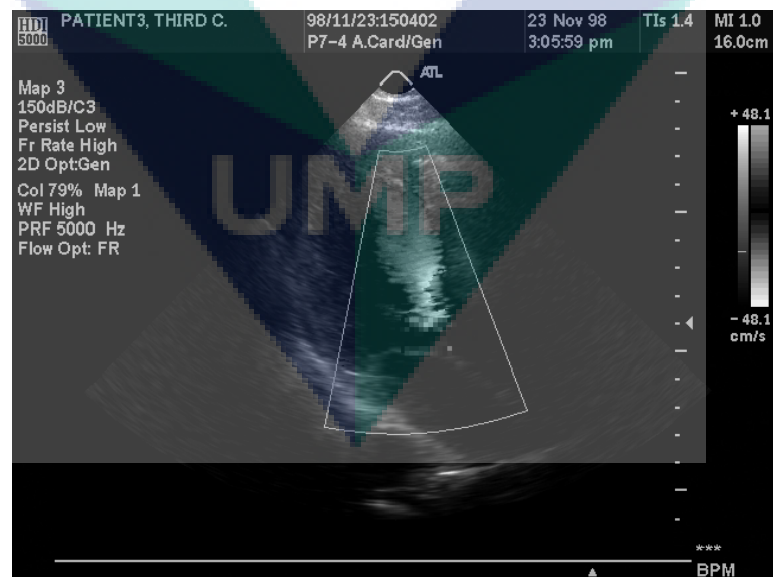


Figure 3.26 : The recovered image of Sample 1

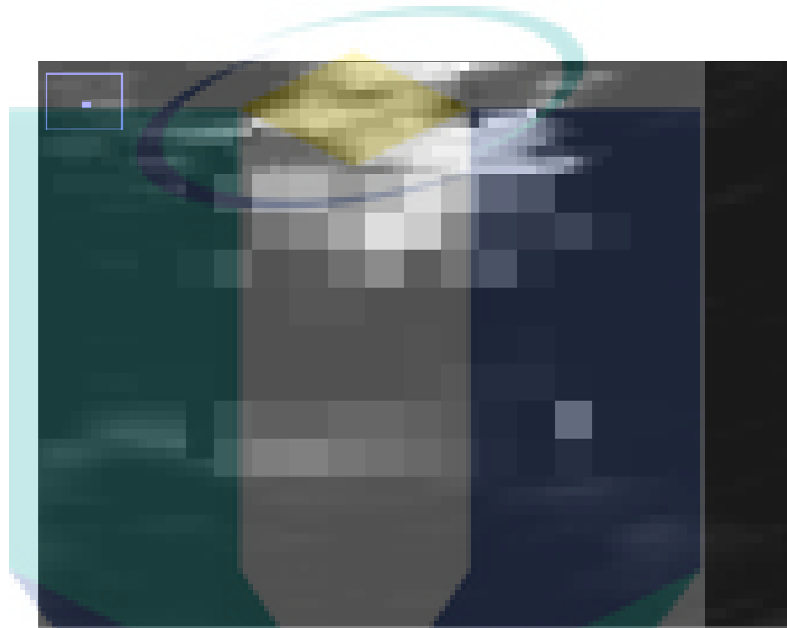


Figure 3.27 : The magnified recovered image of Sample 1

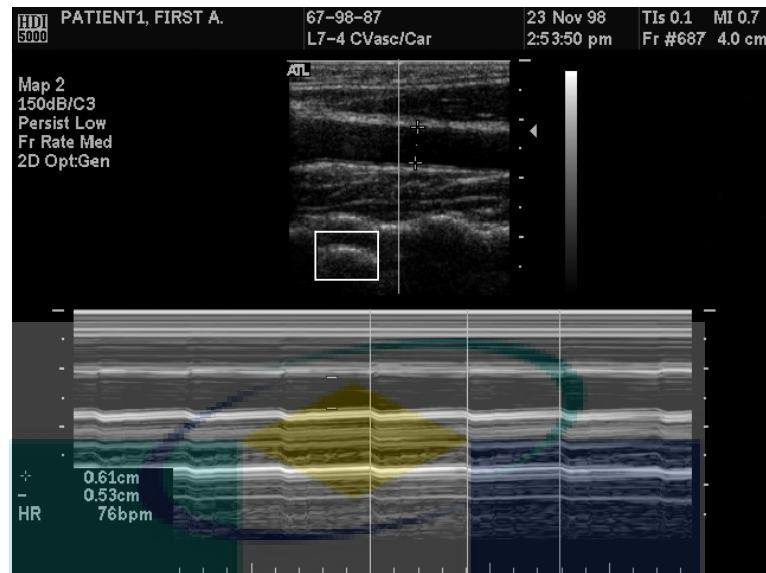


Figure 3.28 : Sample 2 had been manipulated by cloning the highlighted area

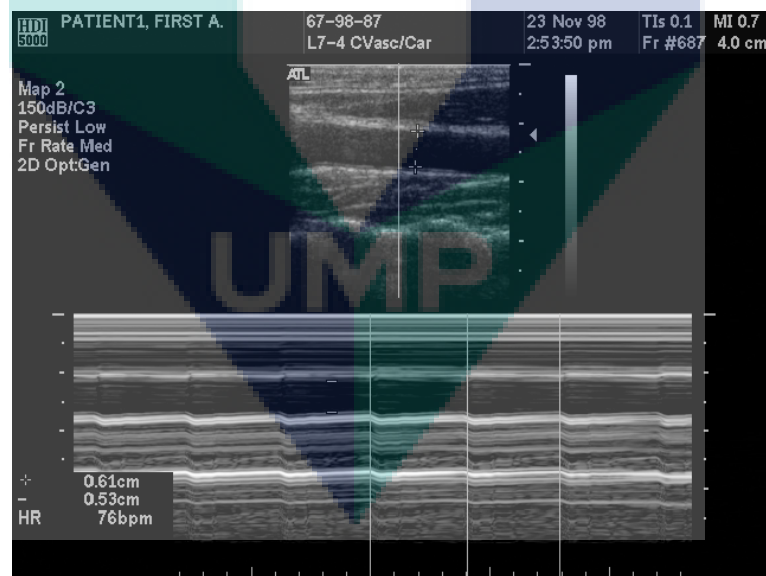


Figure 3.29 : The recovered image of Sample 2

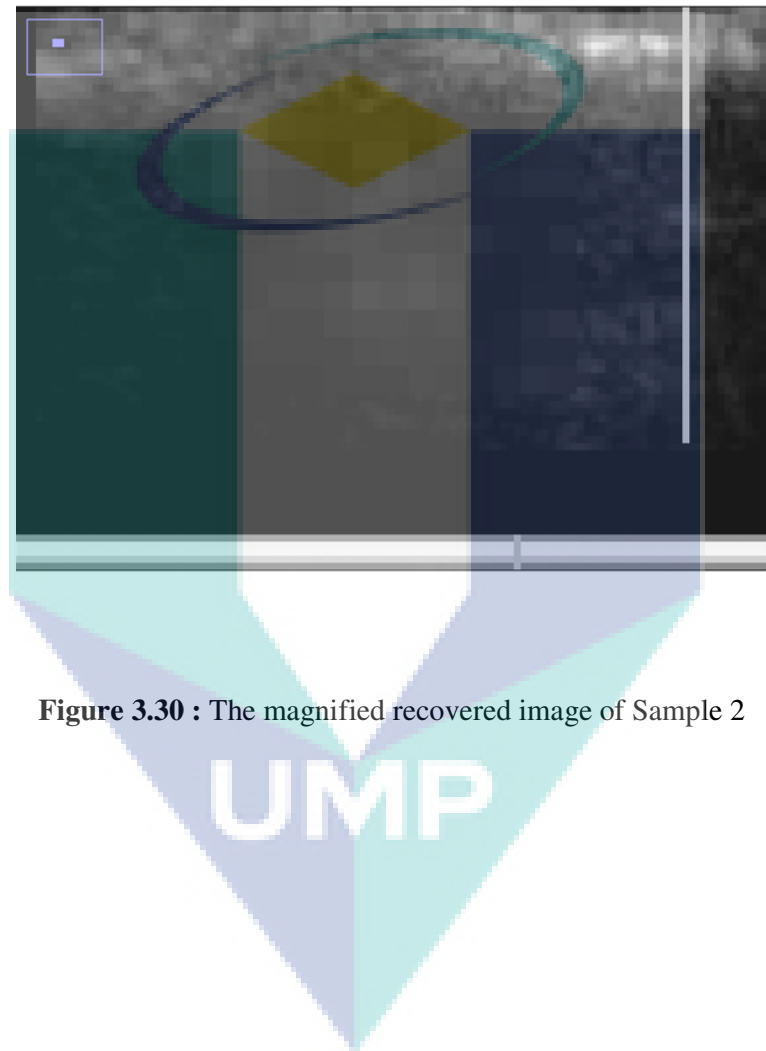


Figure 3.30 : The magnified recovered image of Sample 2

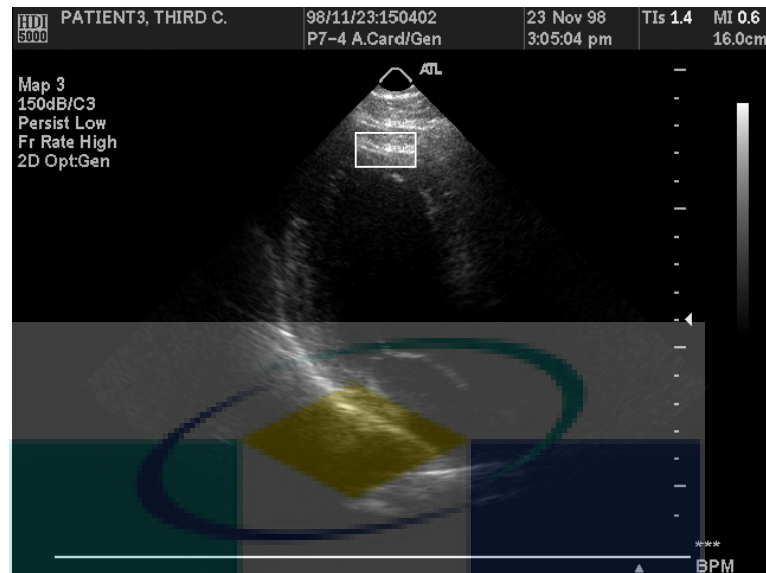


Figure 3.31 : Sample 3 had been manipulated by cloning the highlighted area

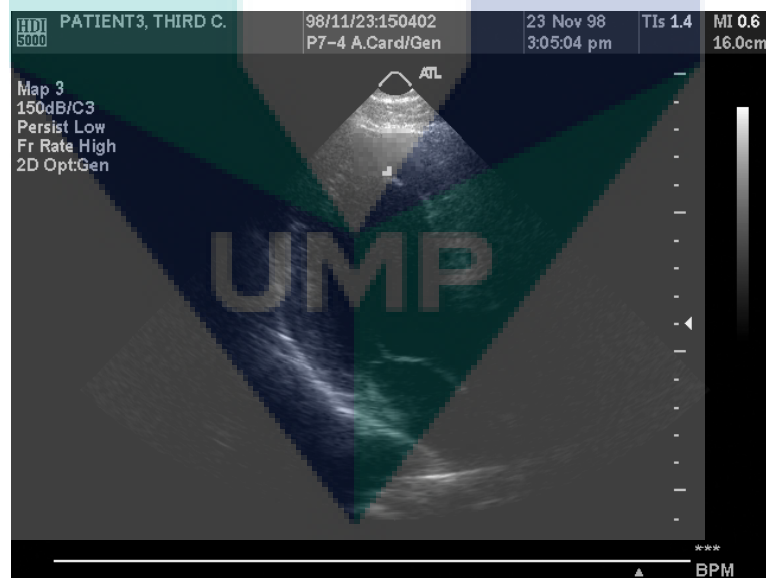


Figure 3.32 : The recovered image of Sample 3

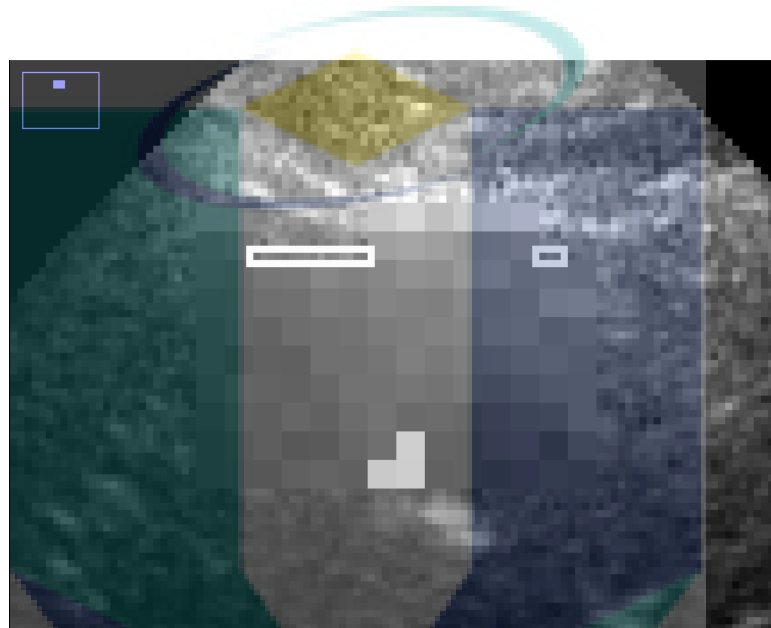


Figure 3.33 : The magnified recovered image of Sample 3 with undetected tampering highlighted

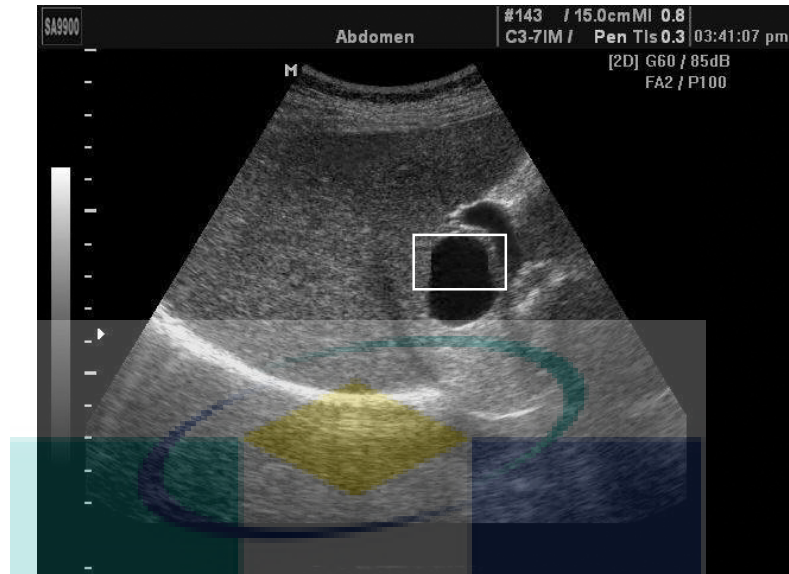


Figure 3.34 : Sample 4 had been manipulated by cloning the highlighted area

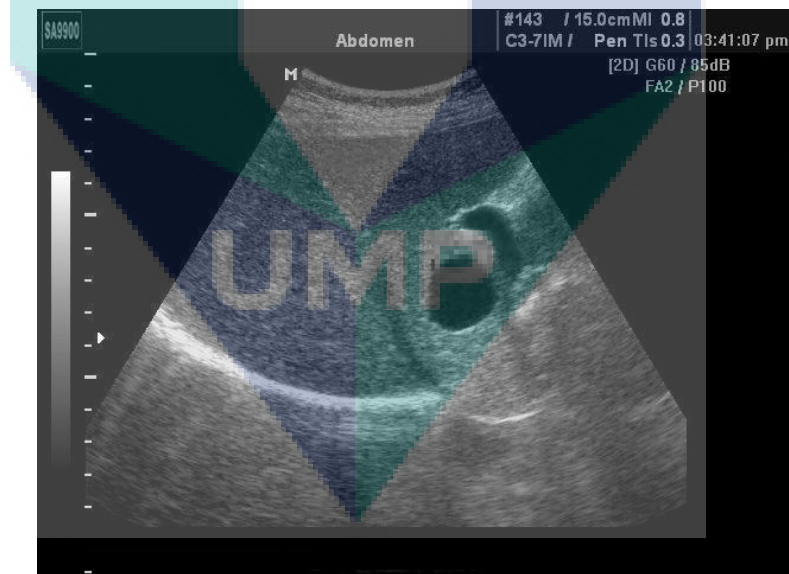


Figure 3.35: The recovered image of Sample 4



Figure 3.36 : The magnified recovered image of Sample 4 with undetected tampering highlighted

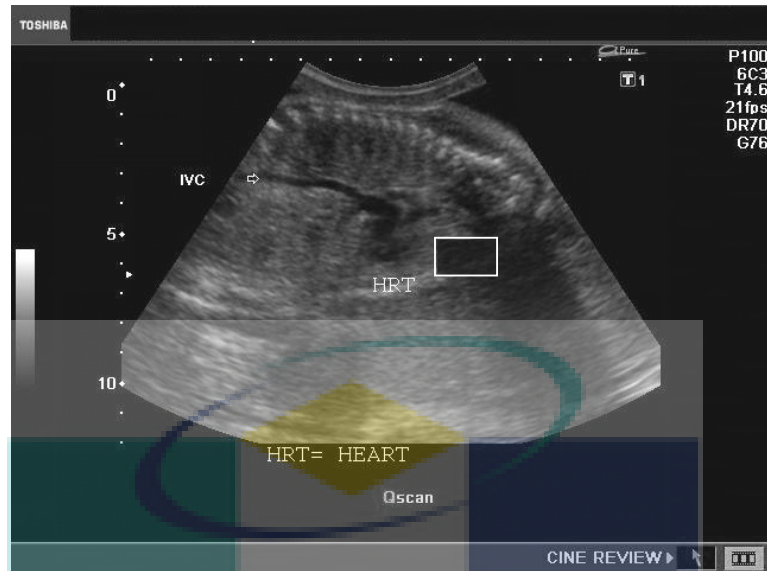


Figure 3.37 : Sample 5 had been manipulated by cloning the highlighted area

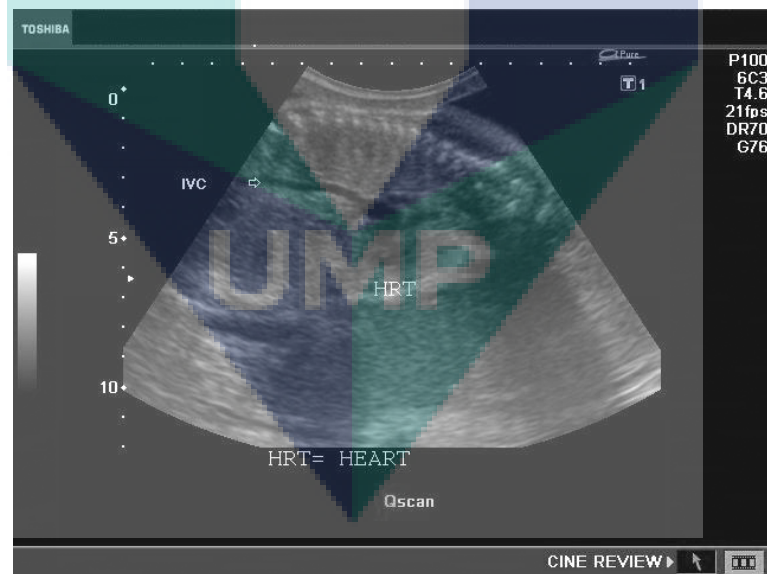


Figure 3.38: The recovered image of Sample 5

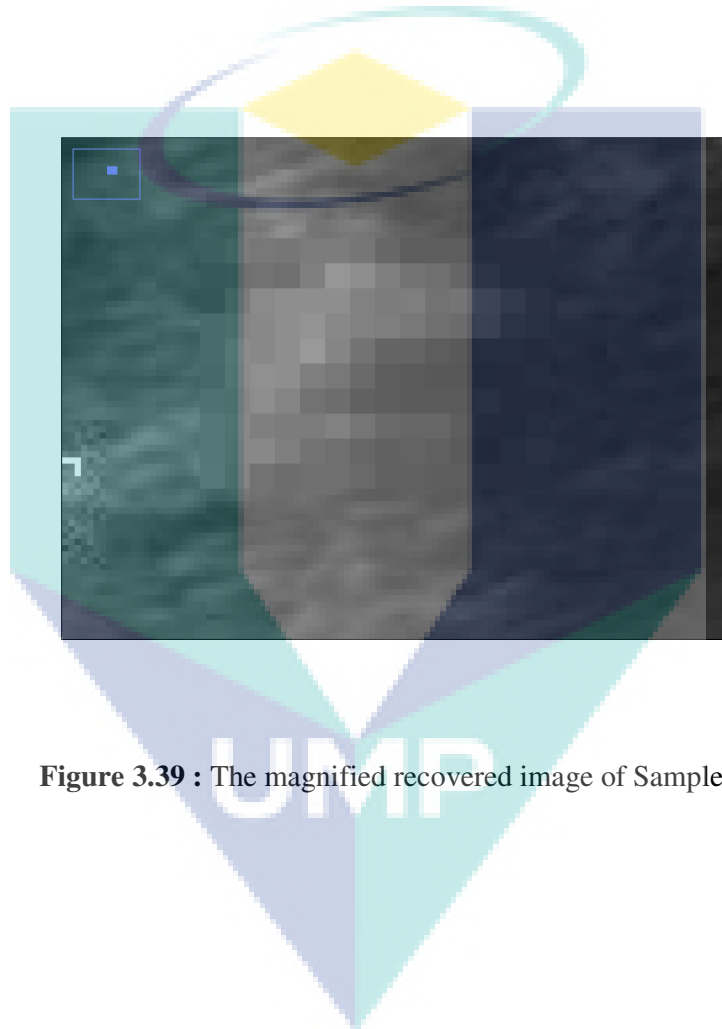


Figure 3.39 : The magnified recovered image of Sample 5

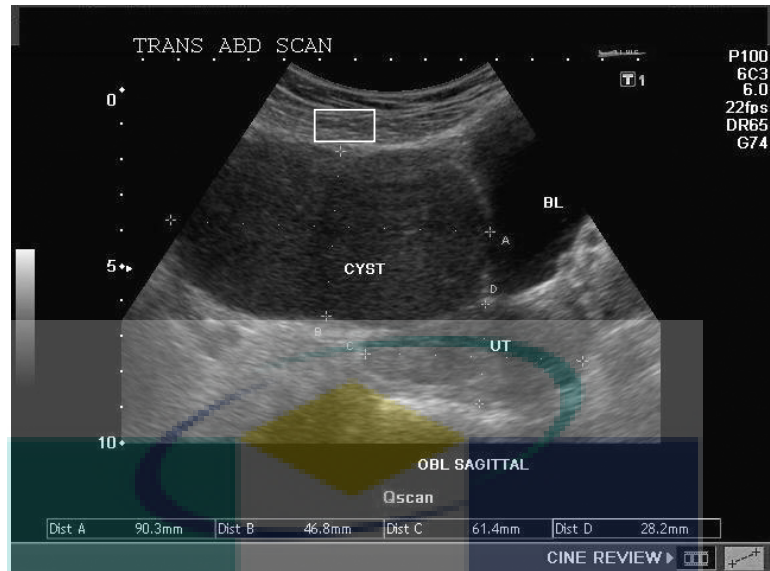


Figure 3.40 : Sample 6 had been manipulated by cloning the highlighted area

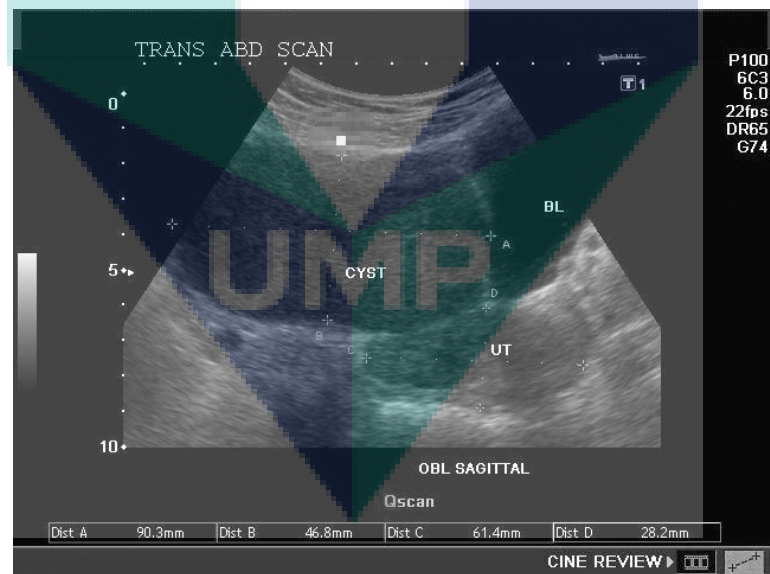


Figure 3.41: The recovered image of Sample 6

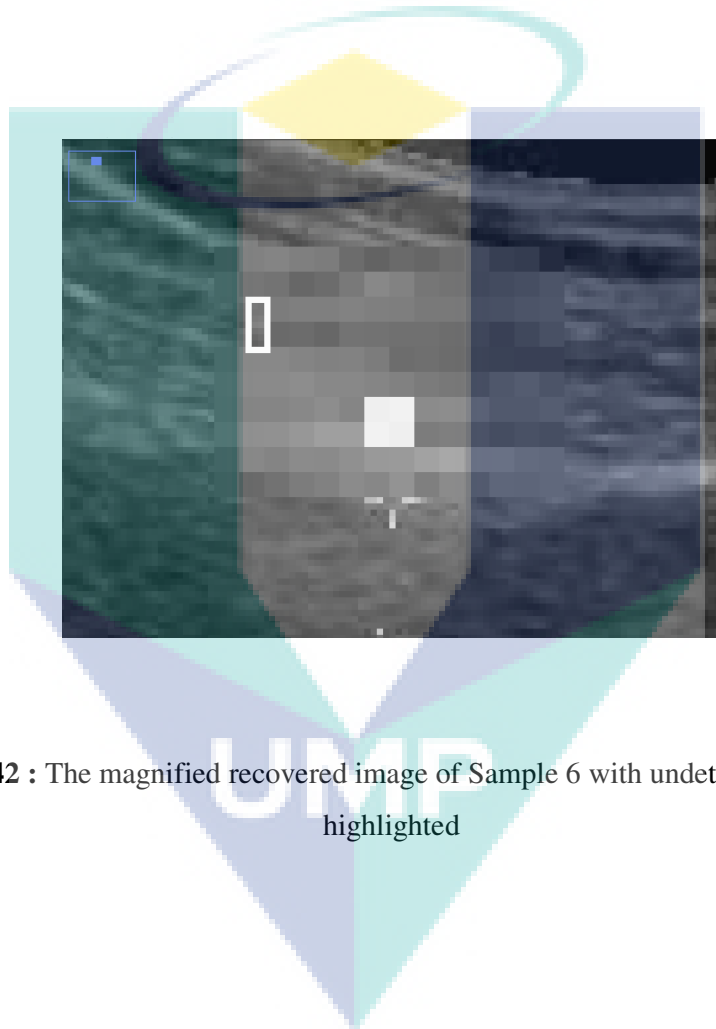


Figure 3.42 : The magnified recovered image of Sample 6 with undetected tampering highlighted

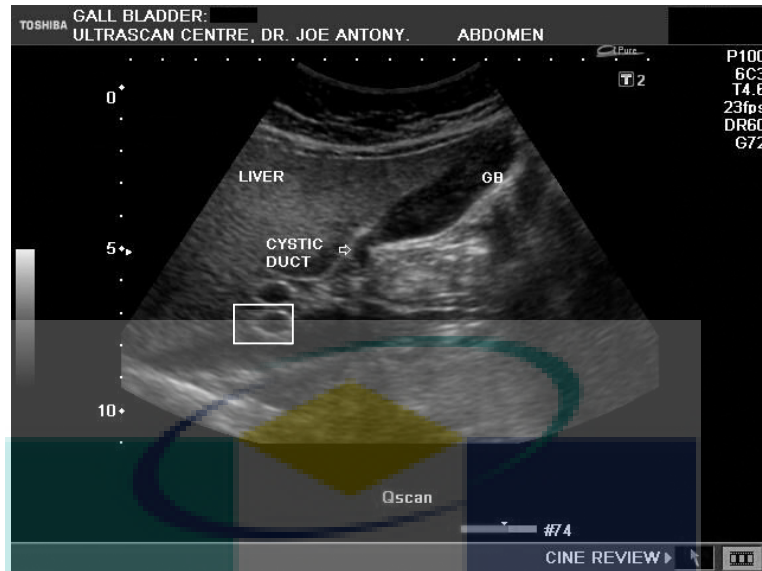


Figure 3.43 : Sample 7 had been manipulated by cloning the highlighted area

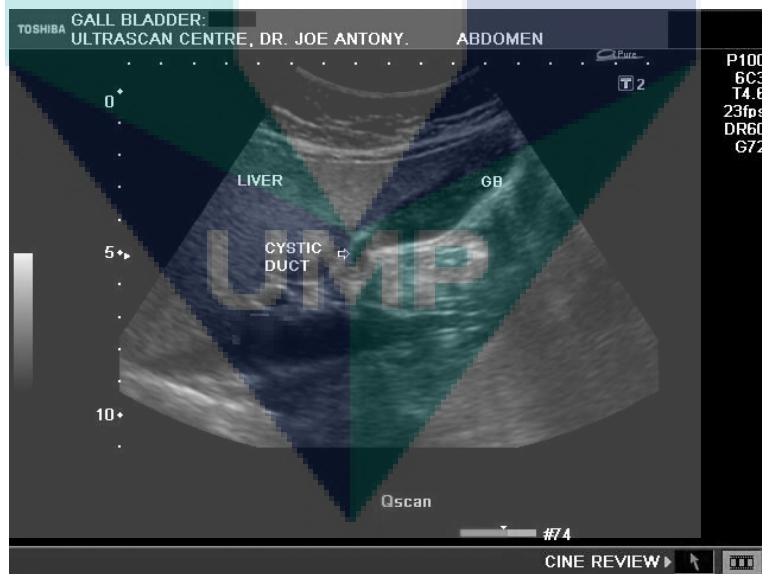


Figure 3.44: The recovered image of Sample 7

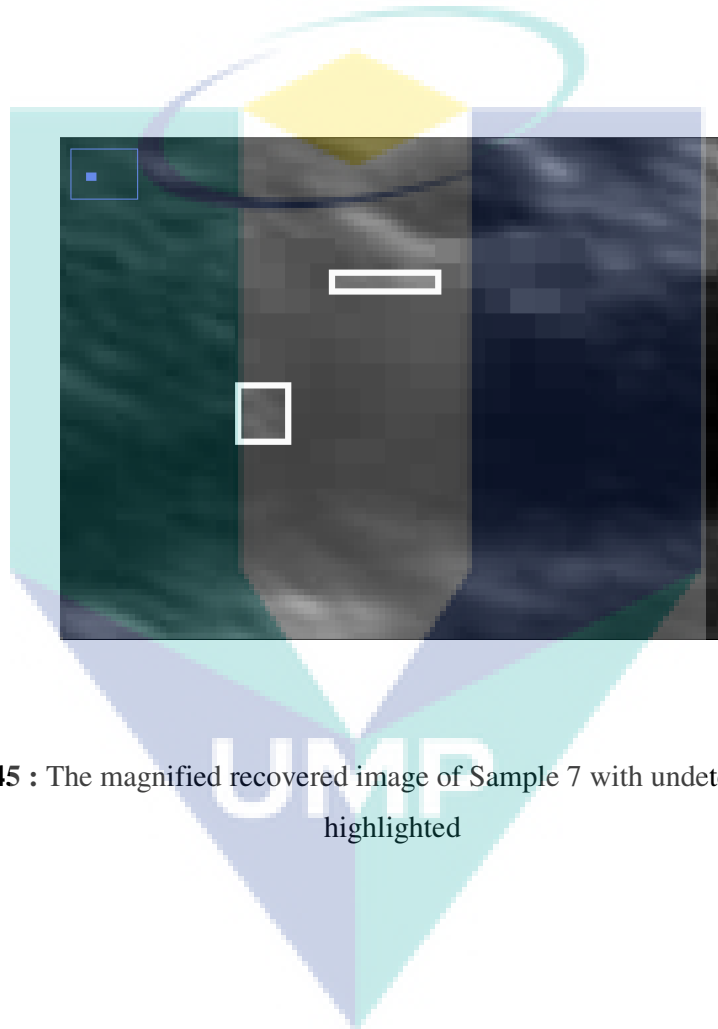


Figure 3.45 : The magnified recovered image of Sample 7 with undetected tampering highlighted

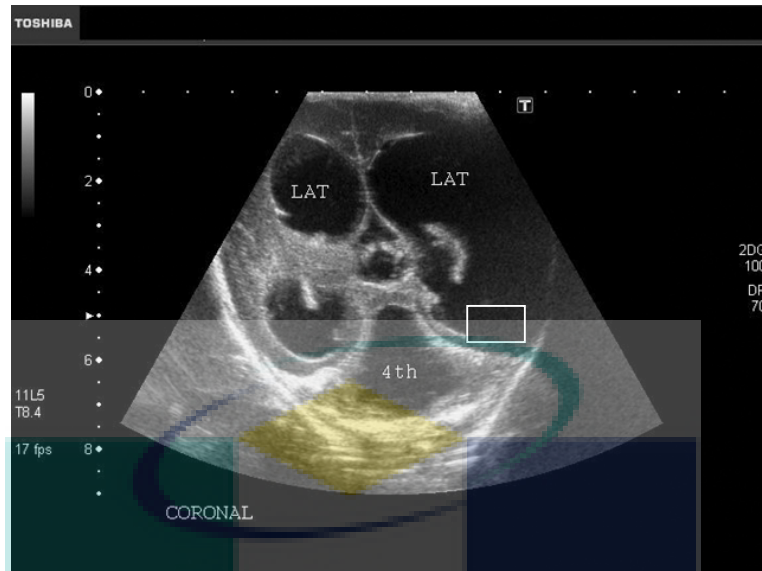


Figure 3.46 : Sample 8 had been manipulated by cloning the highlighted area

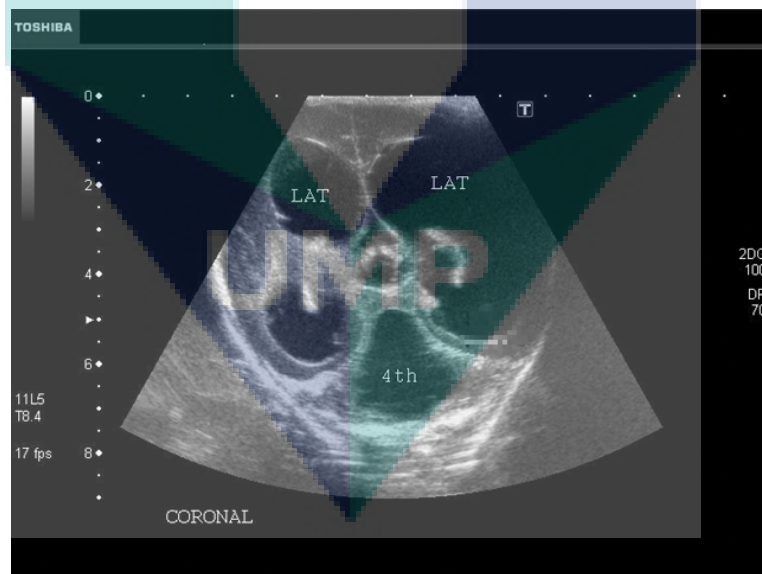


Figure 3.47: The recovered image of Sample 8

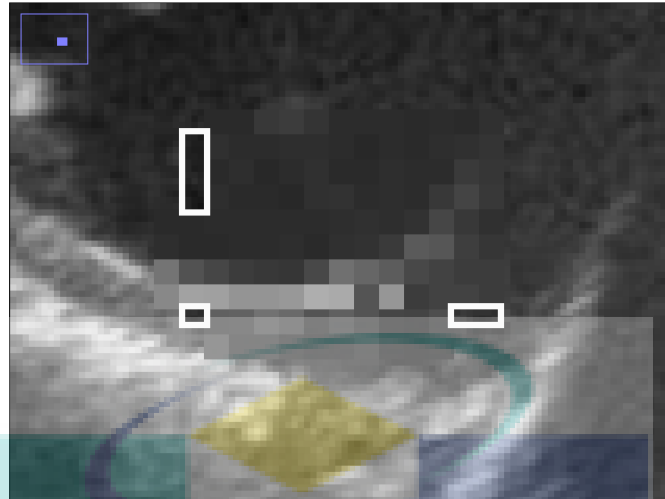


Figure 3.48 : The magnified recovered image of Sample 8 with undetected tampering highlighted

The watermarked image for Sample 4 was manipulated by changing a pixel value on the image. The magnified image is shown in Figure 3.49 and the recovered magnified image is in Figure 3.50. The manipulated pixels were detected and recovered.

There are some tampered pixels in Sample 4 which were undetected as shown in Figure 3.51. The watermarked image for Sample 4 is tested again by tampering one area which was previously undetected by painting it in white and the rest of the tampered area is identical with the previous tampering is shown in Figure 3.52. The recovered image in Figure 3.53 shows the area tampered in white which was previously undetected was successfully detected and recovered.

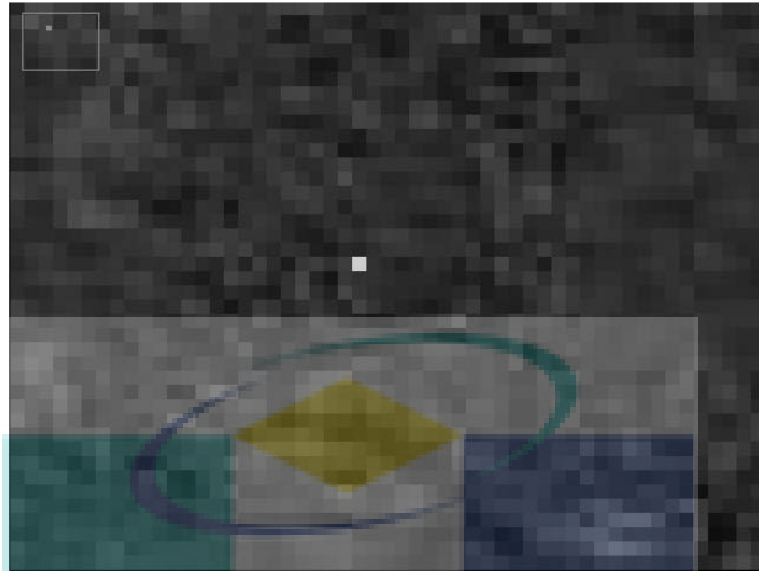


Figure 3.49 : Magnified image with 1 pixel tampered



Figure 3.50: Magnified recovered image

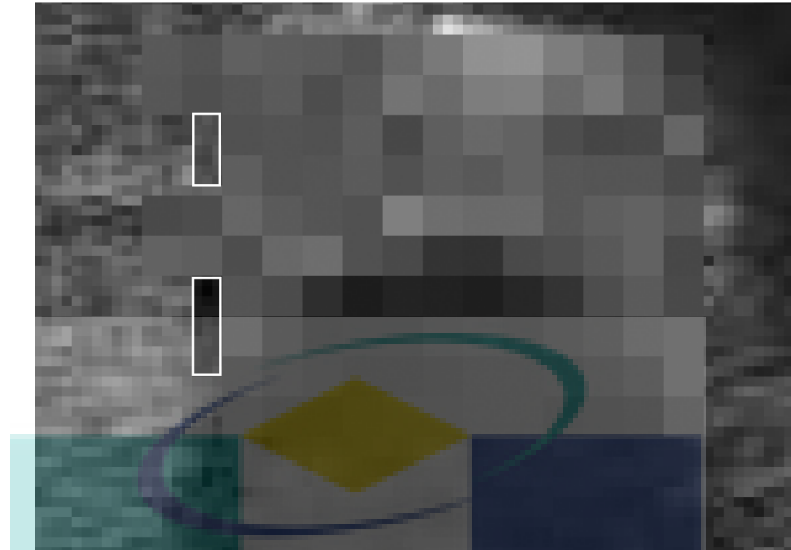


Figure 3.51: Undetected pixels highlighted



Figure 3.52 : The undetected area was painted in white and the rest of the tampered area is identical with Figure 3.34

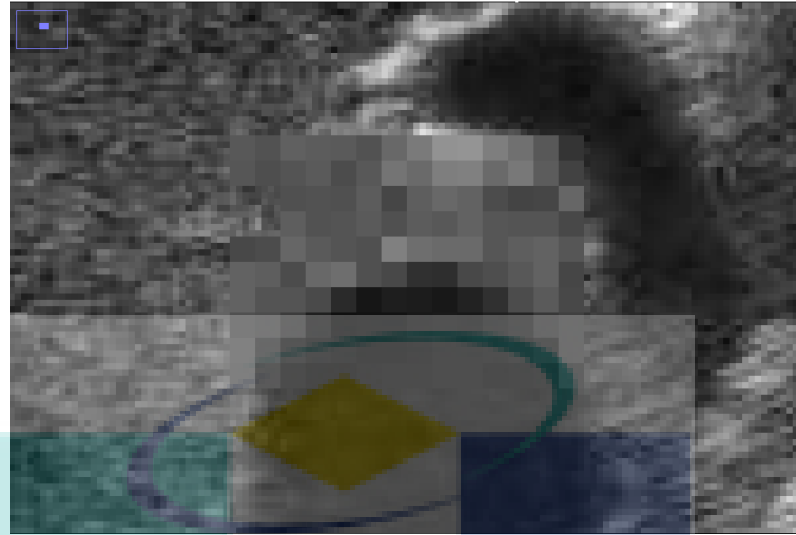


Figure 3.53: The magnified recovered image

ii. Reversible Watermark

After the tamper localization and recovery process, the original LSBs that were removed from the ROI during the embedding process were restored by retrieving it from the RONI. In order to verify that the ROI had been restored to its original state, some pixels from the ROI were selected for comparison. The pixel values were compared between the original image, watermarked image and restored image for Sample 4 as shown in Table 3.3. The pixel values in the restored image and original image are identical.

Table 3.3: Pixel value comparison of selected pixels from the ROI

Pixel coordinate(x,y)	Pixel value		
	Original image	Watermarked image	Restored image
(224,352)	72	73	72
(196,212)	48	49	48
(368,153)	92	93	92
(221,63)	28	29	28

iii. Hash Function Test

In order to verify the authenticity of the removed LSBs embedded in the RONI, the RONI was tampered by modifying the value of a pixel for Sample 4 as shown in Figure 3.54.

The removed LSBs embedded in the RONI were retrieved and hash value was calculated to produce hash_B as shown in Figure 3.55b. The embedded hash, denoted as hash_A was retrieved as shown in Figure 3.55a. The value of hash_A and hash_B are not equal.

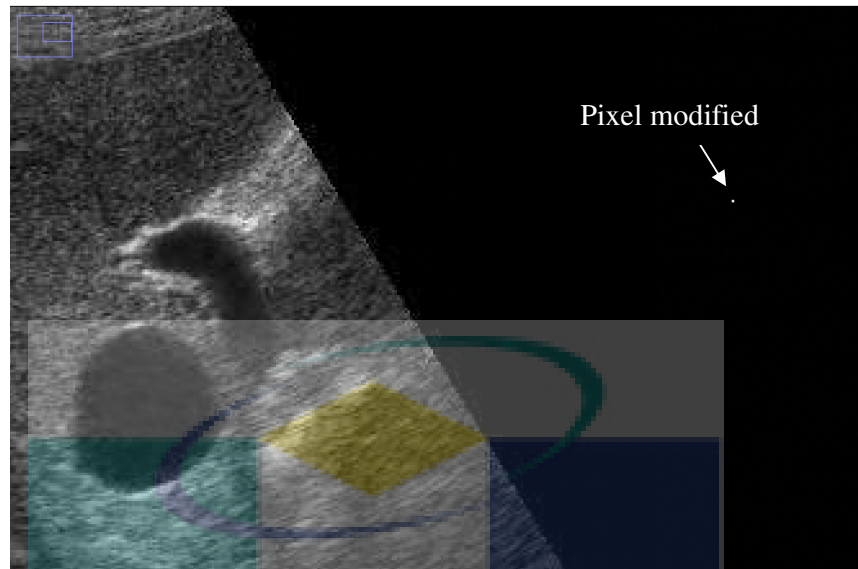


Figure 3.54: The RONI was tampered by modifying one pixel

d8ded8e4241cf297eba1c1681839de6e6f83642a16c4d382760628e4e363d83a

(a)

ab5bb4fba3500e26762e7fd4a88467f4b2bcedebb7631f29d6052f54154cf28e

(b)

Figure 3.55: (a) Hash_A which was embedded as watermark (b) Hash_B calculated from removed LSBs retrieved from the RONI

3.4 EVALUATION AND DISCUSSION

The analyses of the experiments performed are discussed as below:

3.4.1 Image Quality And Fidelity

The watermarked images are good in terms of quality with average PSNR of 53.9 dB which is close 54.8 dB as produced by Jasni and Abdul (2006). It is also among the highest when compared to other reversible watermarking schemes reviewed in the literature. Perception wise, the watermarked images and original images were similar with no noticeable distortion. The proposed scheme cannot be applied in a situation where modification is strictly not allowed in the ROI. However, the watermarked images may be acceptable for use since the distortion level introduced is minimal and imperceptible to the user.

3.4.2 Tamper Localization And Recovery

Based on the experiments performed, some tampered areas were not detected as shown in Figure 3.51 but it was detected when the same location was tampered with a different pixel value. It clearly shows that the authentication bit and parity bit check was ineffective. A further analysis was done based on the following Figure 3.56. As an example, the average intensity of the block, avg_x1 is 85. The average intensities for its sub-blocks are 99, 84, 81 and 77. The values of v and p were computed based on the average intensities and embedded as part of the watermark. The two sub-blocks in the first row were tampered where the average intensities had been changed to 101 and 82 respectively. The value of avg_x1 remains unchanged. During the tamper detection process, the authentication bit and parity check bit is computed, denoted as v' and p' . The values of v' and p' for the two sub-blocks in the first row remained unchanged. In

this situation, the tampered sub-block will pass the detection process and left unrecovered when the embedded v and p were retrieved for comparison.

The tampered areas that were detected were recovered successfully. The recovered image may not be usable for clinical diagnoses since the tampered blocks were recovered using only average intensities. However it is useful in investigations where the motive of the tampering can be implied.

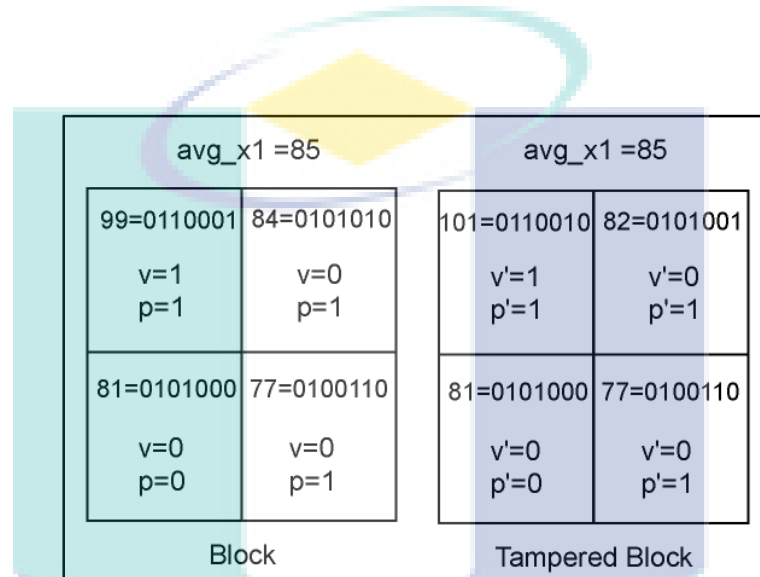


Figure 3.56 : The authentication bit and parity check bit for the original block and tampered block

3.4.3 Reversible Watermark And Hash Function

The watermark can be reversed by restoring the LSBs which were removed from the ROI for watermark embedding. The removed LSBs were retrieved from the RONI and needs to be authenticated before the restoration process begins. Experiment performed on Sample 4 showed that modifications as small as a pixel in the RONI can be detected as shown in Figure 3.49 and Figure 3.50. The RONI that was tampered causes the hash function to produce a different hash value. An identical hash value will indicate that the removed LSBs stored in the RONI as authentic.

The restoration of the ROI was successfully performed. This was verified by comparing pixel values between the original image, watermarked image and restored image as shown in Table 3.3. The LSBs in the RONI were reset to back to zero. The pixel values in the RONI of the original image were zero except for the image descriptions located at the top and left corner of the image. Excluding the image descriptions, an authenticated image was restored to its original state.

3.5 CONCLUSION

This chapter proposed a reversible tamper localization and recovery(R-TLR) watermarking scheme for application in ultrasound images. The watermarked images have an average PSNR value of 53.9 dB. The success rate of the tamper localization and recovery is close to 100%. The bits that were removed from the ROI for watermark embedding were authenticated by using hash function before being used in the restoration process. The watermarked image was reversed by restoring the LSBs in ROI and RONI to its original state. The method used to allow reversibility is simple and requires very minimum processing in comparison to complex methods used in other reversible schemes reviewed in the literature. The watermarked image has a low distortion level and can be reversed to its original state.

CHAPTER 4

TAMPER LOCALIZATION AND LOSSLESS RECOVERY (TALLOR)

4.1 INTRODUCTION

This chapter consists of section 4.2 where the weaknesses in the scheme proposed in the previous chapter are listed and possible solutions are described. Section 4.3 describes the research methodology used in this chapter. In section 4.4 two compression techniques are tested to choose the suitable technique. Section 4.5 presents a tamper localization and lossless recovery watermarking scheme for ultrasound images. This scheme compresses the pixel values from the ROI and embeds it in the RONI as part of the watermark. A hash function is used to ensure integrity of the compressed pixel values. Tampered ROI is recovered using decompressed pixel values from the RONI. Section 4.6 proposes an enhancement of the scheme presented in the previous section by using ROI segmentation to reduce the tamper localization and recovery processing time. Section 4.7 presents the results from the experiments performed for both schemes. Section 4.8 discusses the results from the experiments performed and evaluates the proposed schemes. Lastly, section 4.9 concludes the chapter.

4.2 OVERVIEW

In this chapter, two tamper localization and recovery watermarking schemes that uses different methods are proposed. These schemes attempt to solve the weaknesses that exist in the scheme proposed in the previous chapter. The weaknesses are:

- i. LSBs that were removed from the ROI to allow watermarked embedding needs to be stored to allow the image to be restored to its original state.
- ii. Tampered areas were recovered using average intensities embedded as part of the watermark. The recovered areas were only an approximate to the original image. The recovered image may not be usable for clinical diagnoses due to its lower quality.
- iii. The authentication and parity bit check be ineffective in certain conditions and causes some tampered areas left undetected.

The following sections are the proposed solutions.

4.2.1 Reversibility

For the new proposed schemes, ultrasound image remains the chosen modality. One of the methods identified by Coatrieux and Lecornu (2006) will be used. The ROI will maintain its originality without any modification since the watermark will be embedded in the LSBs of the RONI as show in Figure 4.1. Since the embedding region will be in the RONI, the ROI does not need any restoration. The majority of the RONI has the pixel value of zero and restoration in the RONI can be done by resetting the LSBs to zero.

4.2.2 Recovery

Another type of recovery is the exact or lossless recovery where the tampered image is being recovered to the original state. The recovered image is a perfect copy of the original image.

In these schemes, it is proposed that the tampered area will be recovered using the exact original pixel value. The original pixel value needs to be stored and embedded as part of the watermark in the RONI. There will be an issue of storage capacity available in the RONI. Every pixel defined in the ROI needs to be stored in the LSBs of the RONI and at the same time keep distortion at low level. In this situation, compression techniques are proposed where the pixels value from the ROI will be compressed before being embedded in the RONI. A lossless compression technique will

be suitable in this situation to ensure the recovered area has the highest quality as possible.

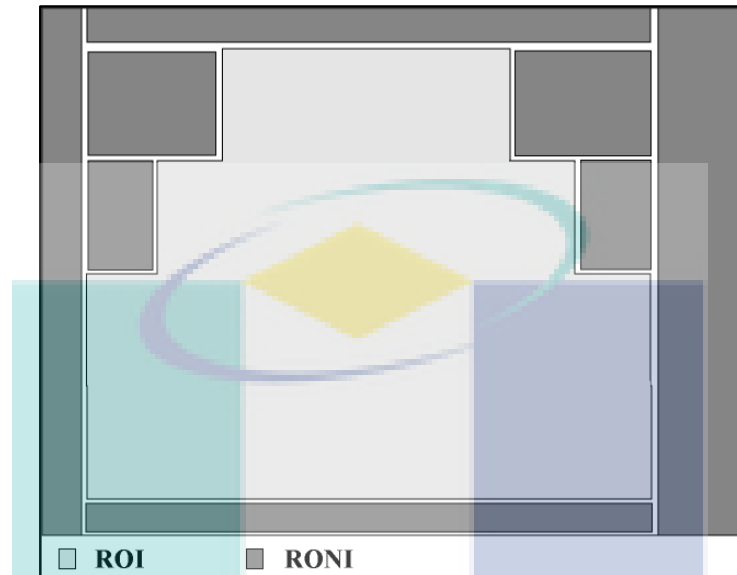


Figure 4.1: Image divided into ROI and RONI

4.2.3 Authentication

Since the recovery bits will be stored as in original pixel value, it can be used for authentication purposes. The ROI can be authenticated by comparing the pixel values from the ROI with the embedded original pixel values extracted from the RONI. The advantage of this is that no other authentication bit is needed. This reduces the watermark payload and computer resources. The embedded original pixel bits can be authenticated using a hash function.

4.3 RESEARCH METHODOLOGY

The research methods used in this chapter is similar to the methods used in the previous chapter in terms of the ultrasound images being used, PSNR to measure the

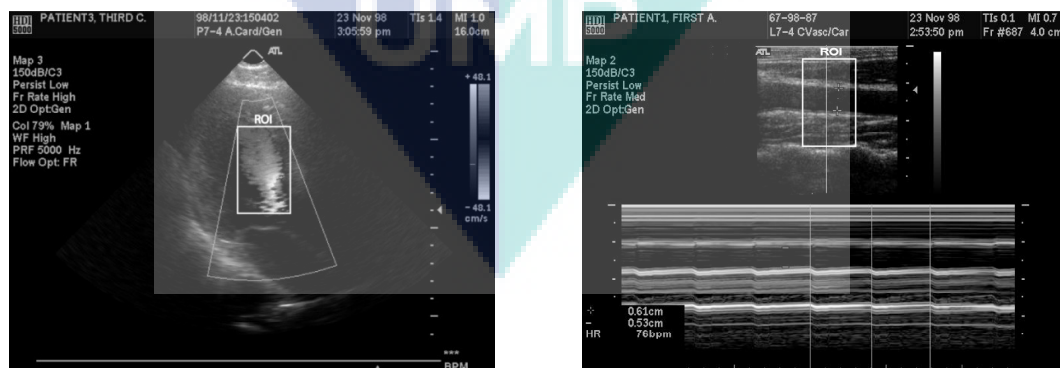
fidelity of watermarked images and tools used to test the effectiveness of the watermarked images.

As for this chapter, exact recovery for tampered images had been proposed. In order to achieve this, the suitable lossless compression technique will be chosen based on the compression ratio achieved. The definition of the size and location of the ROI is also based on the assumption stated in the previous chapter. But the size of the ROI defined will be depending on the compression ratio achieved. Therefore, the efficiency of different lossless compression technique will be tested.

The usage of compression may require additional processing time. Therefore, different method used to achieve exact recovery will be proposed. The methods will be compared in terms of processing time.

4.4 COMPRESSION

As for the proposed schemes, RLE and JPEG compression will be chosen due to its easy implementation. Testing is needed for deciding on the suitable compression technique for the usage in ultrasound images. In this test, 8-bit monochrome grayscale ultrasound images measuring 640 x 480 pixels will be used. A ROI measuring 70 x 115 pixels is defined in four different images as shown in Figure 4.2 below.



(a) Sample 1

(b) Sample 2

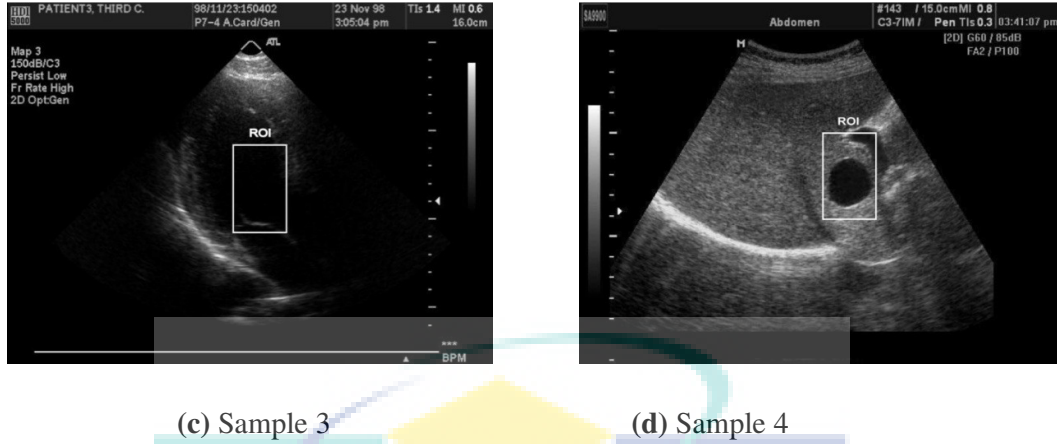


Figure 4.2: Different images with ROI measuring 70 x 115 pixels

RLE is used to compress the pixel values of the ROI. The compressed pixels consist of run value, RV and run count, RC. RV is represented by 8 bits and RC is represented by 3 bits. The pixel values of the ROI are gathered to form a single block by combining rows of pixel values. RLE algorithm is executed to compress the block. Table 4.1 shows the details of the input and output bits of RLE compression. The compression ratio indicates the efficiency of the compression algorithm which was calculated based on Eq. 4.1.

$$\text{Compression Ratio} = \frac{\text{Compressed Data}}{\text{Uncompressed Data}} \quad (4.1)$$

A compression ratio of more than 1.0 indicates that the output of the compression performed had expanded; a ratio closer to zero is preferred. Compression performed on Sample 2 and Sample 4 produced compression ratios of 1.22 and 1.26 respectively. Sample 1 and Sample 3 have the compression ratios of 0.73 and 0.67 respectively.

Table 4.1: The details of the input, output and compression ratio using RLE

Total input(ROI) bits=65320				
Figure	Sample 1	Sample 2	Sample 3	Sample 4
Total RV bits	34752	58040	31664	59896
Total RC bits	13032	21765	11874	22461
Total output(RV+RC) bits	47784	79805	43538	82357
Compression Ratio	0.73	1.22	0.67	1.26

Further investigation was performed on images that had been successfully compressed and images that failed in compression. For the purpose of comparison, histogram of a row of pixel values and count were produced for Sample 3 and Sample 4 is shown in Figure 4.3. It shows that RLE compression is effective if the ROI has high pixel counts within a narrow range of pixel values. Image ROIs that do not fit this criterion need to be processed using other compression techniques.

Based on the findings above, a different compression technique is used. The same images were compressed using JPEG compression. Lossless JPEG compression and lossy JPEG compression were applied to the ROI of the images. As for the lossy compression, compression that has the highest quality(100) was applied. The highest scale value applied will produce the highest image quality. The result is shown in Table 4.2 where ROI from all four images were successfully compressed. In this situation, lossless compression has better compression ratio as compare to lossy compression. Lossy compression may perform better at the lower quality. It is concluded that JPEG compression performed better than RLE compression in terms of compression ratio and reliability in successful compression.

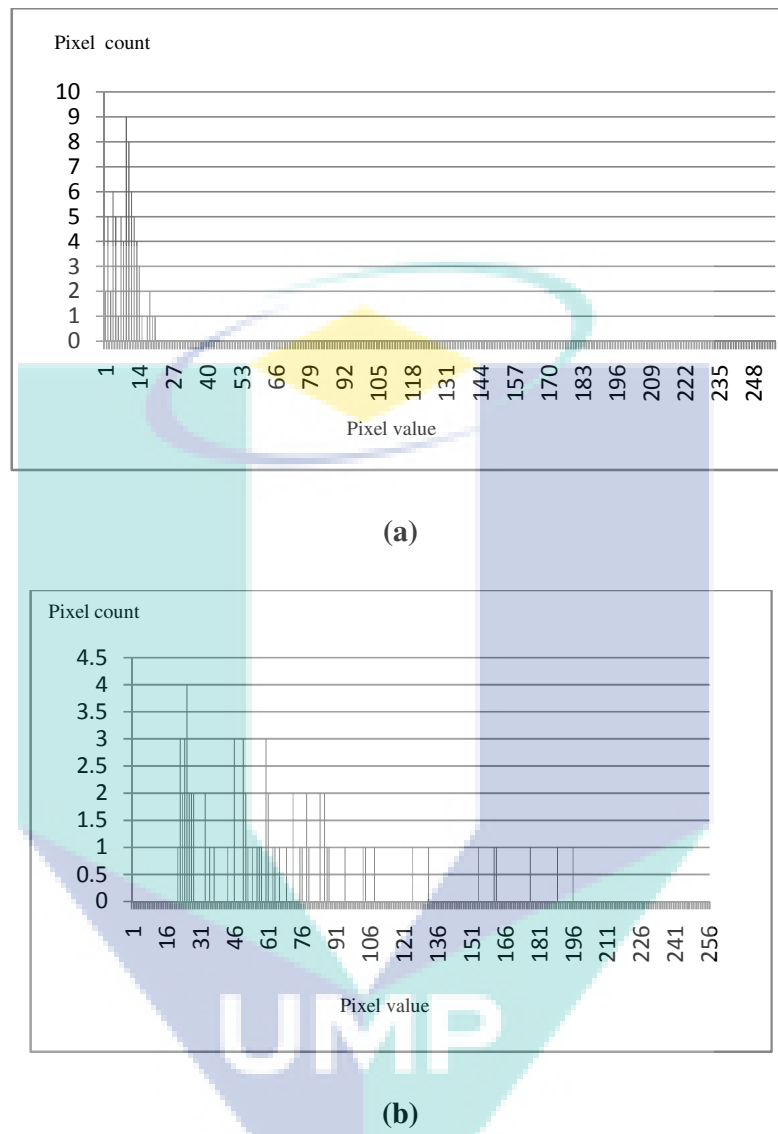


Figure 4.3: (a) Histogram for Sample 3, (b) Histogram for Sample 4

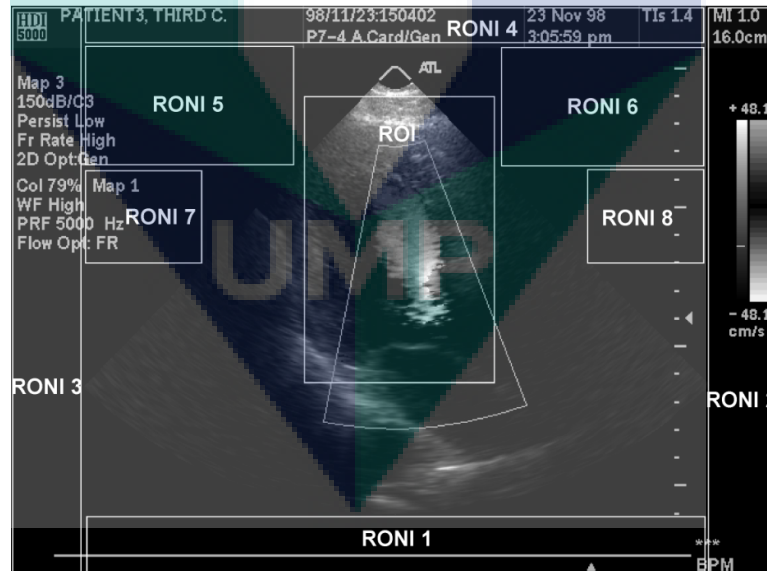
Table 4.2: The details of input, output and compression ratio using JPEG

Figure	Total input (ROI) bits = 65320			
	Lossless		Lossy(Quality=100)	
	Output Bits	Compression Ratio	Output Bits	Compression Ratio
Sample 1	31416	0.48	47552	0.73
Sample 2	47168	0.72	56200	0.86
Sample 3	22280	0.34	27200	0.42
Sample 4	47712	0.73	49576	0.76

4.5 TAMPER LOCALIZATION AND LOSSLESS RECOVERY(TALLOR)

4.5.1. Image Preparation

An ultrasound image is divided into ROI and RONI as shown as Figure 4.4.

**Figure 4.4:** Ultrasound image is divided into ROI and RONI

In this scheme, one rectangle is used for the ROI and eight rectangles in the RONI. The ROI is defined manually rather than automatically. This gives the flexibility

to the user for deciding on the location and the size of the ROI. This can be done with the assistance of an interface which will be explained in chapter 5. Based on the calculations, there are 143,400 pixels in the RONI. If only two bits per pixel are used for watermark embedding, the RONI can only store approximately 286,800 bits of watermark payload. Based on these limitations, the ROI can only be a portion of the non-black area in the image as shown in Figure 4.4. The ROI has the measurement of 160 x 240 pixels which equivalent to 307,200 bits. The final total bits from the ROI that needs to be embedded depends on the efficiency of the compression technique used. Based on the work done in the previous chapter, it is easier to process pixels in form of block rather than pixel by pixel. Therefore, the RONI is divided into non-overlapping blocks of 2 x 2 pixels.

4.5.2. Watermark Generation And Embedding

The watermark consist of compressed ROI pixels and its hash value. The watermark will be embedded in the LSB and second LSB of each pixel in the RONI.

i. Compressed ROI

The pixels from the ROI are compressed with JPEG compression available in MATLAB. The pixels were saved in a file with a JPEG extension. The file will be embedded in the RONI.

ii. Hash Function

SHA-256 is used to hash the JPEG file before it is being embedded in the RONI. The hash value can be used to authenticate the JPEG file and other more secure hash function may be use. The hexadecimal hash value, denoted as `JPEG_hash_A` will be embedded in the RONI together with the JPEG file.

4.5.3. Tamper Localization And Recovery

The RONI is divided into blocks of 2 x 2 pixels just as in the embedding process.

i. Tamper Localization

The ROI in the form of JPEG file that was embedded in the RONI is retrieved. The file is hashed using the same hash function used in the embedding process, producing a hash value, JPEG_hash_B. The embedded JPEG_hash_A is retrieved and compared with JPEG_hash_B. A positive result indicates that the JPEG file retrieved from the RONI is authentic or the RONI had not been tampered.

The retrieved JPEG file is decompressed to form a block of pixel values, denoted as ROI_A. The current pixel values of the ROI are gathered and denoted as ROI_B. ROI_A and ROI_B are compared and difference in value indicates tampering. The exact tampered pixel will be localized.

ii. Recovery

Tampered pixel in the ROI is being replaced with its corresponding pixel value from ROI_A. The LSBs in the RONI that were used for watermarking embedding are set to zero.

4.6 TAMPER LOCALIZATION AND LOSSLESS RECOVERY WITH ROI SEGMENTATION(TALLOR-RS)

Initial testing using the technique described above revealed that significant amount of time was taken to embed and retrieve the JPEG file. This directly slows down the process of watermarking and authentication. It can be an issue when a user of an image has to spend a significant amount of time waiting for the image to be authenticated and recovered.

A possible option is to further divide the ROI into segments. Only the segments that were tampered will be retrieved from the RONI for recovery purposes. Since the

ROI is to be divided into segments, each segments needs to be authenticated individually. The authentication can be performed in a multilevel manner where only suspected segments will be examined further for tampering. Theoretically, these techniques may reduce the processing time.

The JPEG file contributed a major portion to the total watermark payload. Therefore, additional payload from the authentication bits should be minimized and at the same time effective. Tan et al. (2011) had used a 16-bit CRC as the authentication bits for an image with non-overlapping blocks with the size of 16 x 16 pixels. CRC for each block is computed and embedded in its own block. As for the new proposed scheme, CRC can be used to authenticate the segments of the ROI individually.

4.6.1 Image Preparation

The division of the image is similar to the TALLOR scheme with a ROI and eight RONI. But in this scheme, the ROI is further segmented into non-overlapping blocks of 40 x 40 pixels and the RONI is divided into non-overlapping blocks of 2 x 2 pixels.

4.6.2 Watermark Generation And Embedding

The watermark consist of authentication and recovery information. The RONI is further divided into one area for authentication information embedding and one area for recovery information embedding. This will allow separate authentication for different types of information embedded in the RONI. The watermark will be embedded in the LSB and second LSB of each pixel in the RONI.

i. Authentication

Each of the 40 x 40 pixels segment in the ROI is assigned a segment number, $S_{no} \in \{1,2,3, \dots, N_s\}$ where N_s is the total number of segments. The authentication bits will be computed by producing 16-bit ITU-T CRC for each segment in the ROI denoted as CRC_A.

All of the CRC bits computed will be gathered to form a single block denoted as CRC_Block_A. A hash value for the ROI denoted as ROI_hash_A will be generated by hashing CRC_Block_A with SHA-256.

The authentication information will be embedded in the designated area in the RONI. The RONI will be hashed using SHA-256, producing a hash value denoted as RONI1_hash_A.

ii. Recovery

Each segment in the ROI will be saved in an individual JPEG file denoted as JPEG_A and identified by its segment number, S_{no} . The x and y coordinate, denoted as Seg_XY_ROI for each segment in the ROI will be saved. The x and y coordinate where each JPEG file will be embedded in the RONI, denoted as Seg_XY_RONI is also saved. Both Seg_XY_ROI and Seg_XY_RONI will be needed to allow speedy retrieval and recovery of ROI segments. The recovery information will be embedded in the designated area in the RONI. The RONI where the embedding process occurs is hashed using SHA-256 producing a hash value, RONI2_hash_A.

The summary of the process described above is shown in Figure 4.5.

4.6.3 Tamper Localization And Recovery

The ROI and RONI are divided in a manner similar in the watermark generation and embedding process.

i. Tamper Localization

The process of authentication begins by hashing the RONI where the authentication information was embedded using SHA-256, producing a hash value denoted as RONI1_hash_B. The embedded RONI1_hash_A will be retrieved and compared with RONI1_hash_B. A positive result will indicate that the RONI where the authentication information was embedded had not been tampered and the process of authenticating the ROI can begin. The ROI will be authenticated in 3 levels.

- **Level 1:** The ROI is divided into segments and numbered similar in the embedding process. CRC will be computed for each segment denoted as CRC_B. The CRC bits will be gathered as a block, CRC_{Block_B} and hashed using SHA-256 producing hash value, ROI_{hash_B}. ROI_{hash_A} will be retrieved and compared with ROI_{hash_B}. A positive result will indicate that the ROI is authentic and the process of authentication ends. If otherwise, the authentication process proceeds to the next level.
- **Level 2 :** In the level 2 authentication process, at least one segment of the ROI is expected to be tampered. Each segment will be authenticated by comparing its retrieved CRC_A from the RONI and the current CRC bits, CRC_B. The tampered segments will be recorded in a list denoted as Tampered_ S_{no} using segment number, S_{no}. In the next level, tampered pixel will be localized and recovered. The RONI where the recovery information is embedded will be hashed producing a hash value denoted as RONI2_{hash_B}. The embedded hash value, RONI2_{hash_A} will be retrieved and compared with RONI2_{hash_B}. If both hash values are equal then it can be concluded that the embedded recovery information is authentic.
- **Level 3:** Seg_{XY_RONI} that stores the location of the JPEG file for each segment will be retrieved. By knowing the location of each JPEG file and reference to Tampered_ S_{no}, direct retrieval of only the desired JPEG files can be performed. The exact location of the tampered segment in the ROI can be known by referring to the embedded Seg_{XY_ROI}. The retrieved JPEG file, JPEG_A will be decoded and compared with the tampered segment in the ROI pixel by pixel. The tampered pixels will be localized and recovered using the pixel values from JPEG_A.

The summary of the process described above is shown in Figure 4.6.

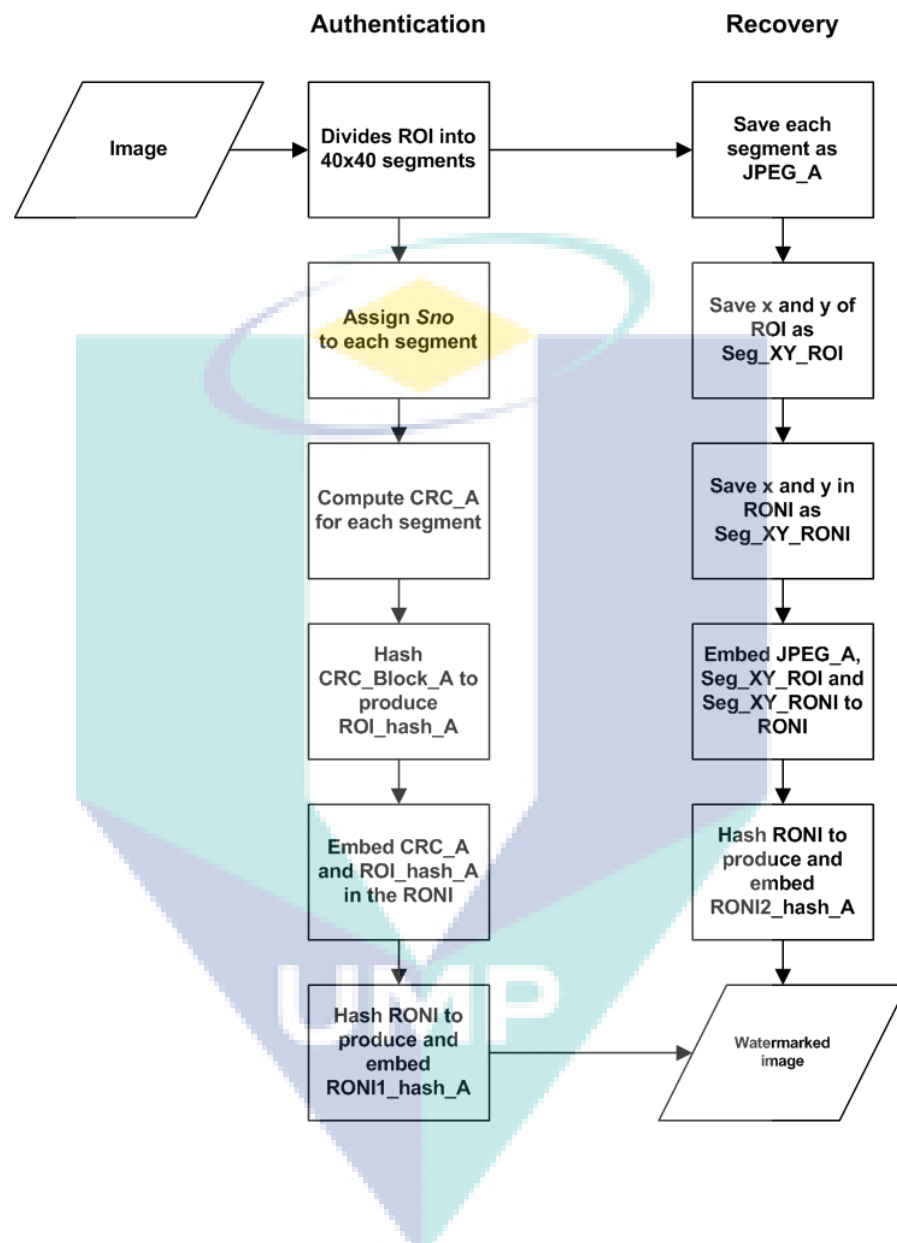


Figure 4.5 : The watermark generation and embedding process for the authentication and recovery information

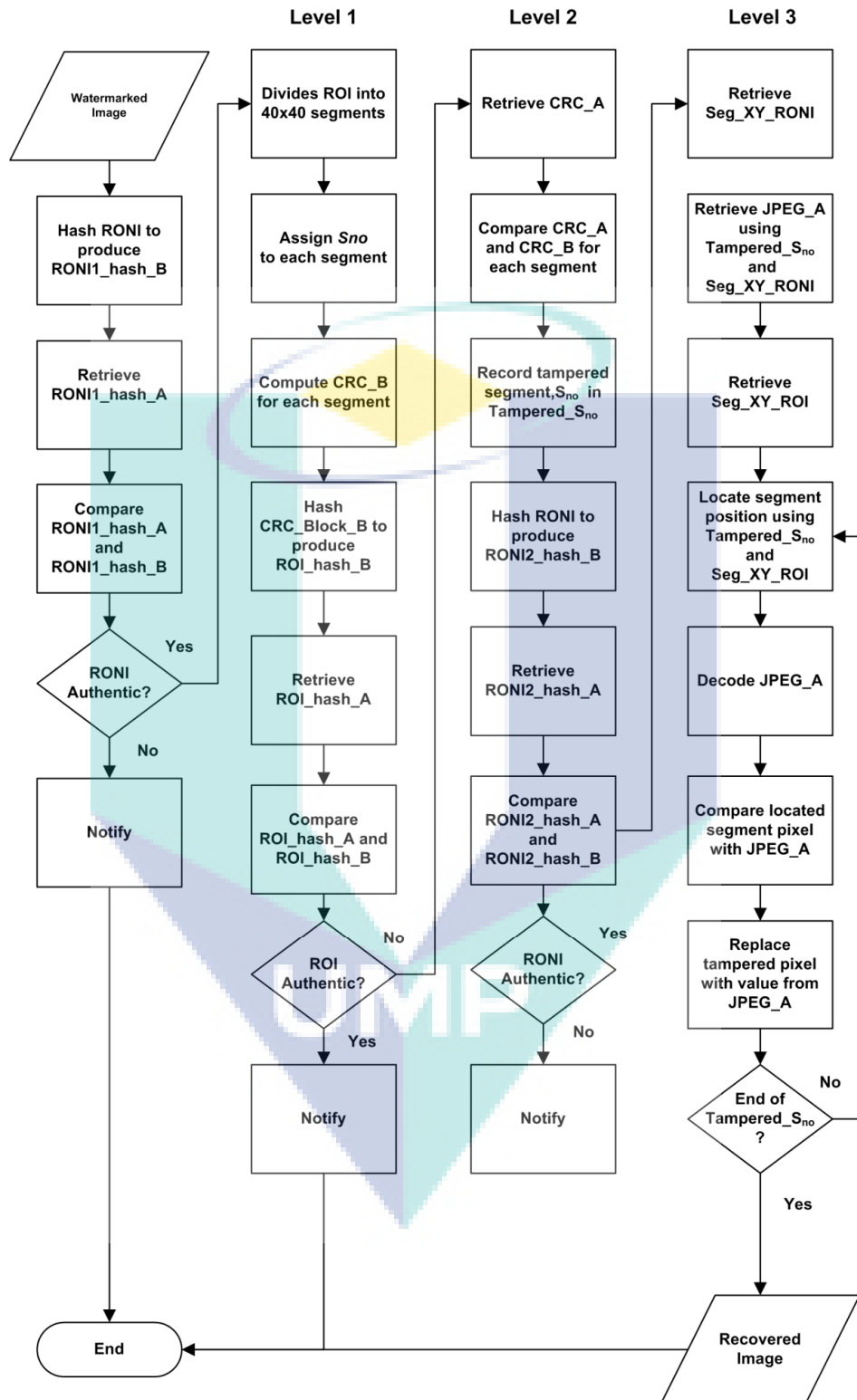


Figure 4.6 : The tamper localization and recovery process for all 3 levels

4.7 EXPERIMENTAL RESULTS

4.7.1 TALLOR

Eight different 8-bit monochrome grayscale ultrasound images measuring 640 x 480 pixels in size were watermarked. The ROI was losslessly compressed. The details of the experiment results are shown in Table 4.3. The average compression ratio and PSNR achieved is 0.61 and 48.3 dB respectively. The original and watermarked images for each sample are shown from Figure 4.7 to Figure 4.22.

Table 4.3: The experiment results for all samples using TALLOR

Total ROI Bits=307200				
Figure	Compression Output(bits)	Compression Ratio	PSNR(dB)	Total Watermark Payload(bits)
Sample 1	180704	0.59	48.1	180960
Sample 2	190680	0.62	48.0	190936
Sample 3	156248	0.51	48.9	156504
Sample 4	221976	0.72	47.9	222232
Sample 5	179616	0.58	48.8	179872
Sample 6	188288	0.61	48.6	188544
Sample 7	173920	0.57	48.6	174176
Sample 8	209264	0.68	47.5	209520
Average		0.61	48.3	

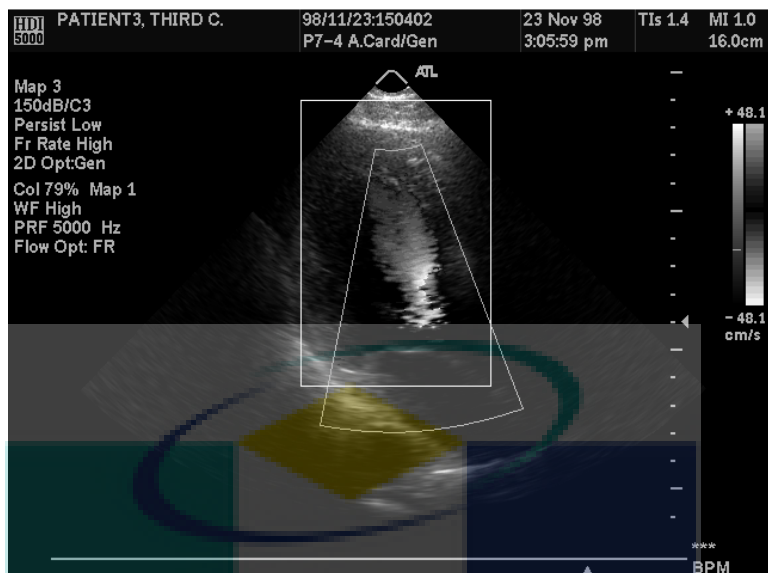


Figure 4.7: Original image of Sample 1 with ROI highlighted

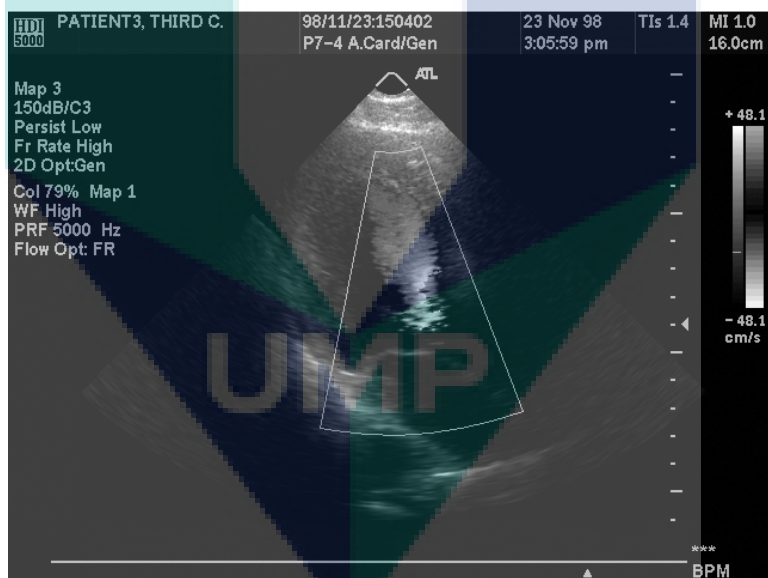


Figure 4.8: Watermarked image of Sample 1, PSNR= 48.1 dB

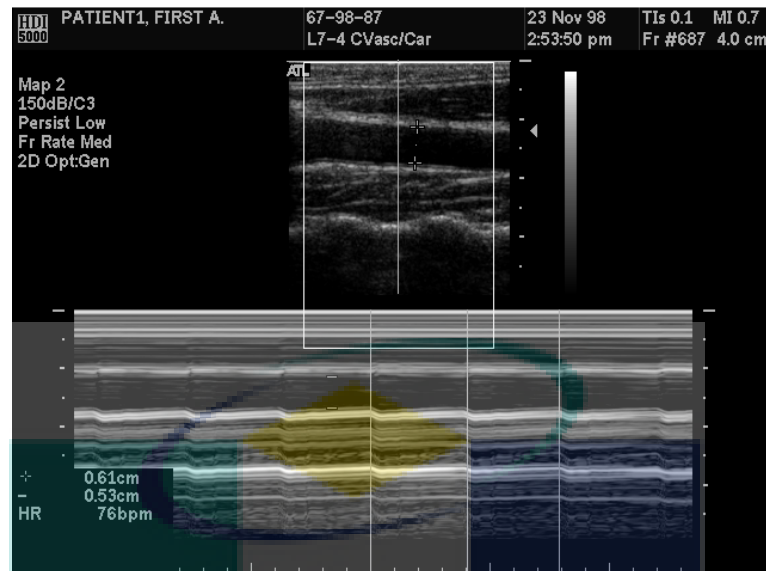


Figure 4.9: Original image of Sample 2 with ROI highlighted

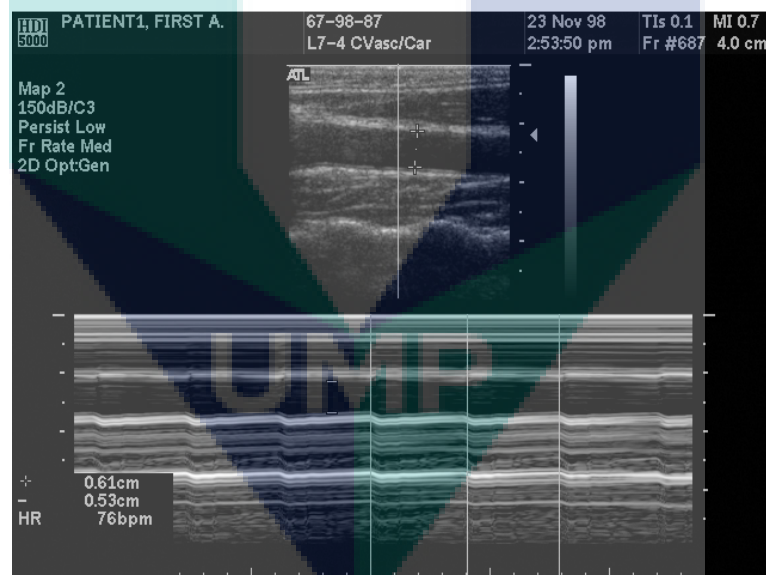


Figure 4.10: Watermarked image of Sample 2, PSNR= 48.0 dB

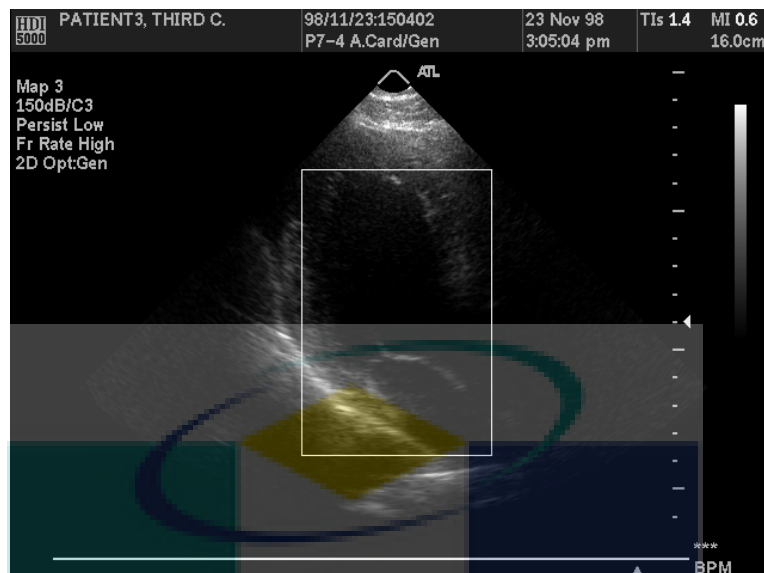


Figure 4.11: Original image of Sample 3 with ROI highlighted

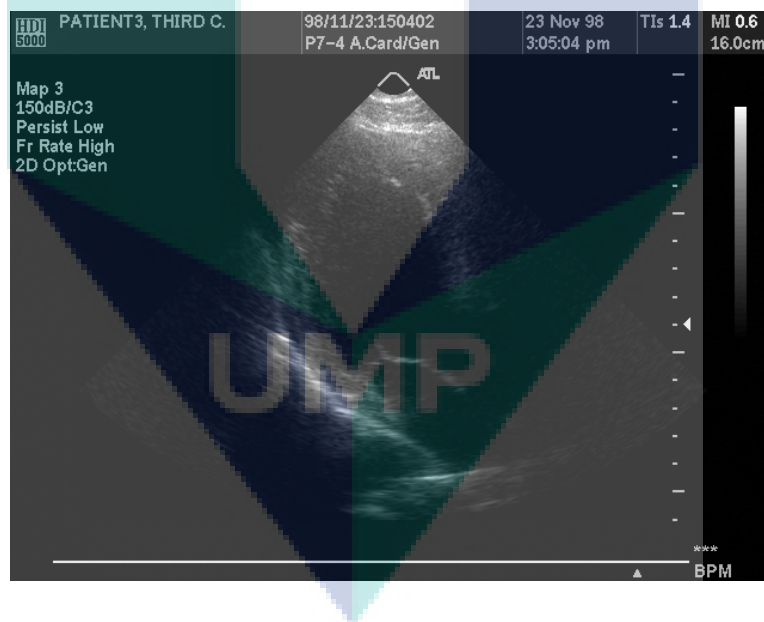


Figure 4.12: Watermarked image of Sample 3, PSNR= 48.9 dB

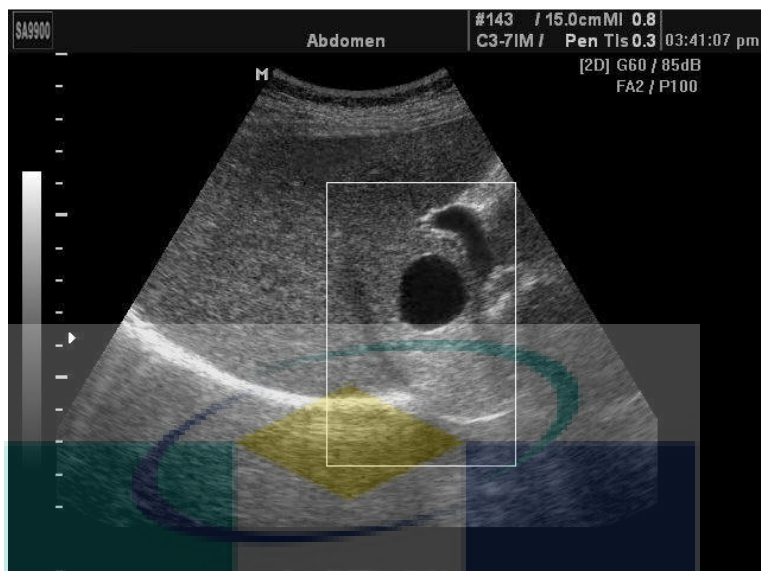


Figure 4.13: Original image of Sample 4 with ROI highlighted

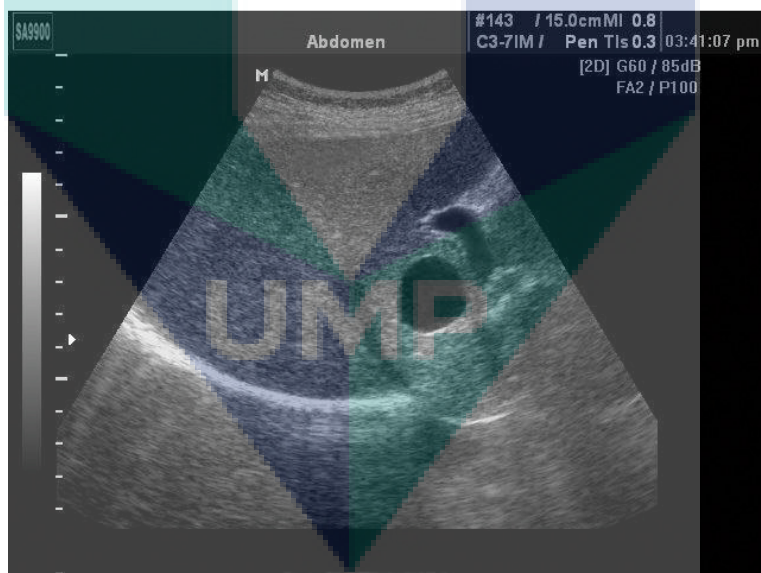


Figure 4.14: Watermarked image of Sample 4, PSNR= 47.9 dB

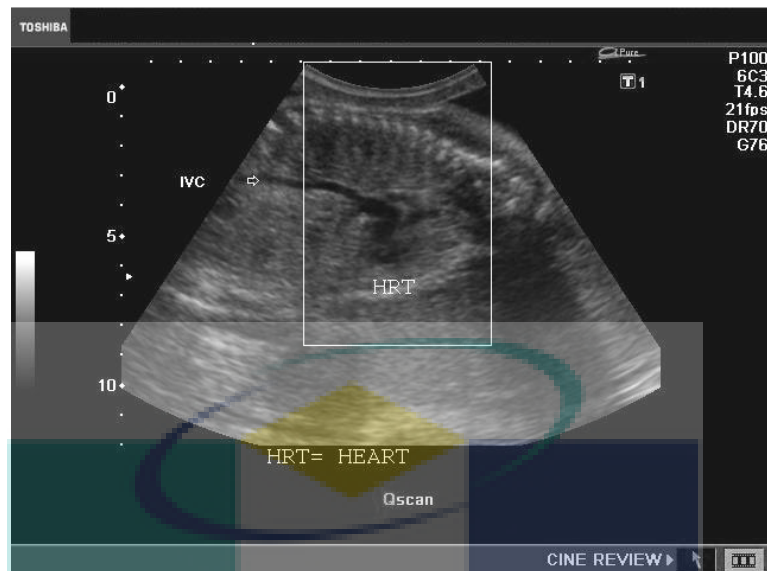


Figure 4.15: Original image of Sample 5 with ROI highlighted

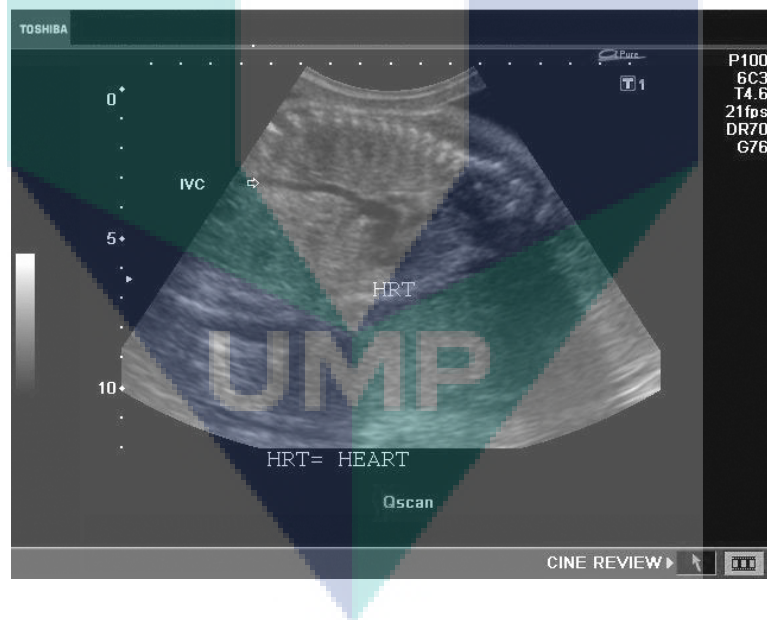


Figure 4.16: Watermarked image of Sample 5, PSNR= 48.8 dB

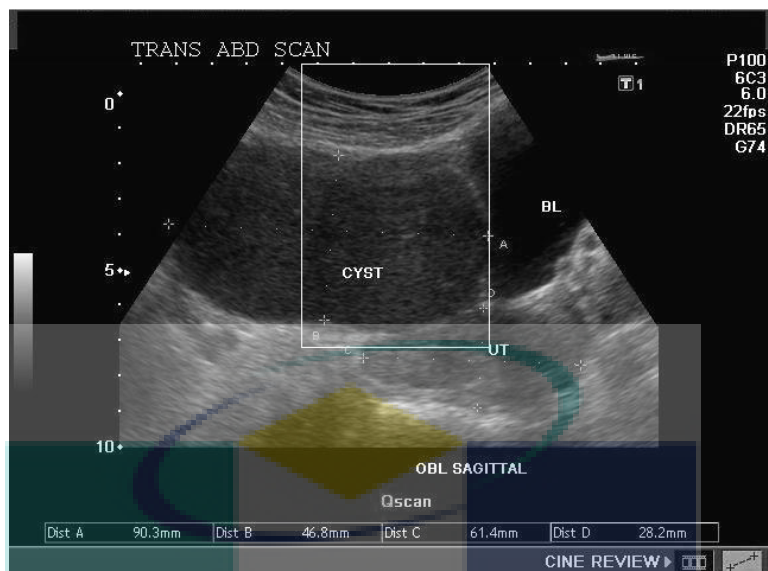


Figure 4.17: Original image of Sample 6 with ROI highlighted

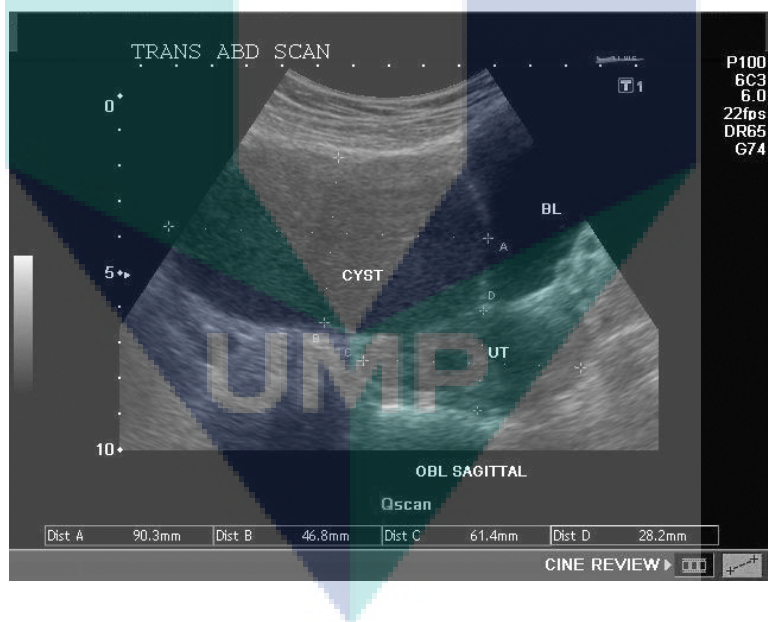


Figure 4.18: Watermarked image of Sample 6, PSNR= 48.6 dB

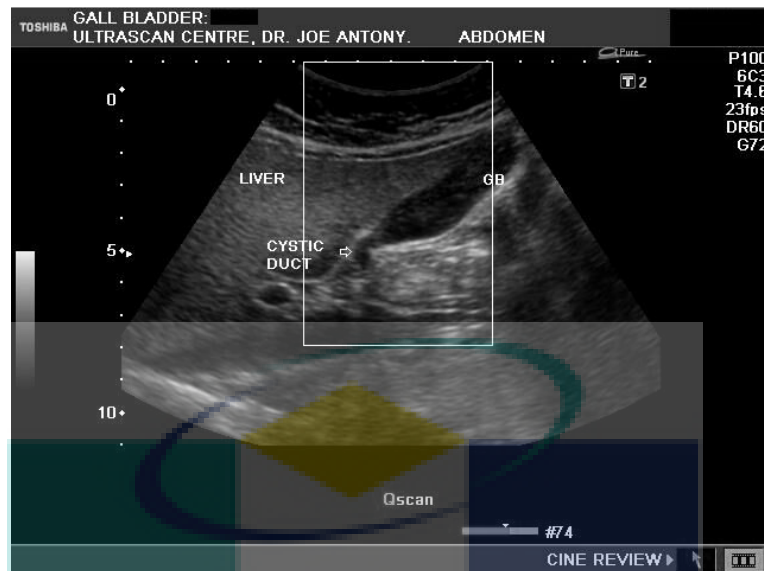


Figure 4.19: Original image of Sample 7 with ROI highlighted

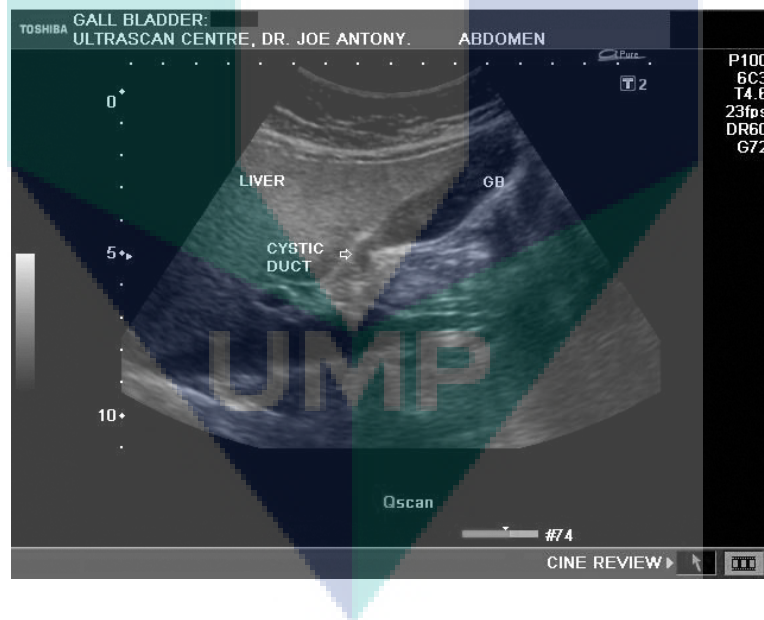


Figure 4.20: Watermarked image of Sample 7, PSNR= 48.6 dB

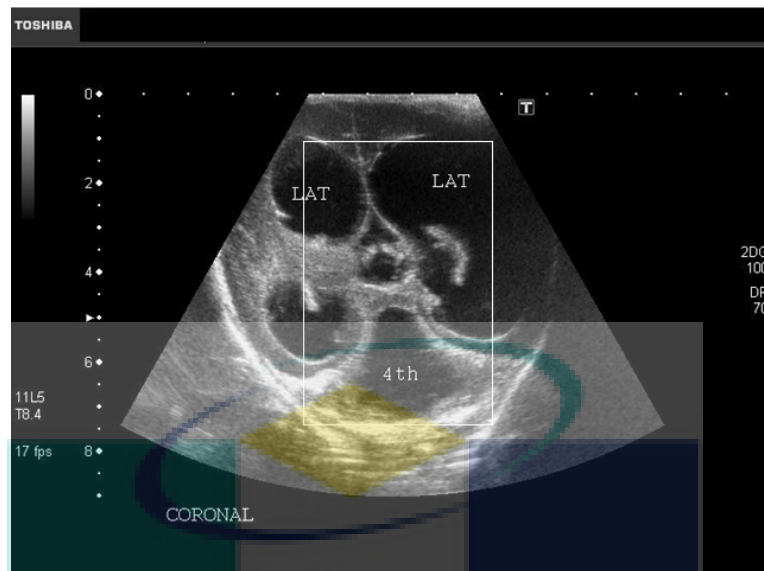


Figure 4.21: Original image of Sample 8 with ROI highlighted

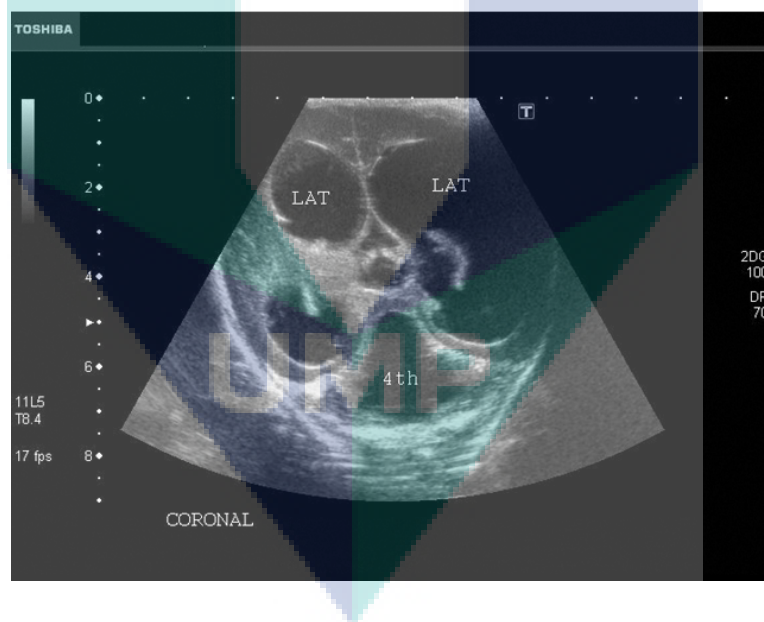


Figure 4.22: Watermarked image of Sample 8, PSNR= 47.5 dB

i. Tamper Localization and Recovery

The watermarked images were tampered by using ImageJ. Sample 1 and 5 as shown in Figure 4.23 and 4.24 were tampered by cloning an area measuring 60 x 90 pixels.

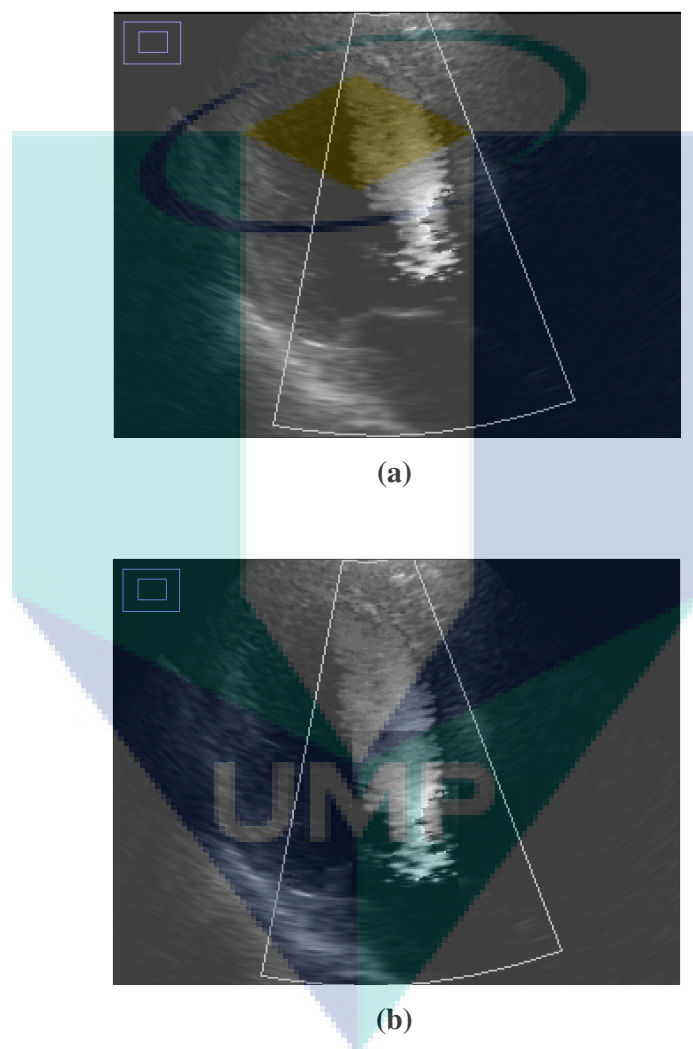


Figure 4.23: (a) Magnified original ROI of Sample 1 (b) Magnified ROI of Sample 1 that was cloned

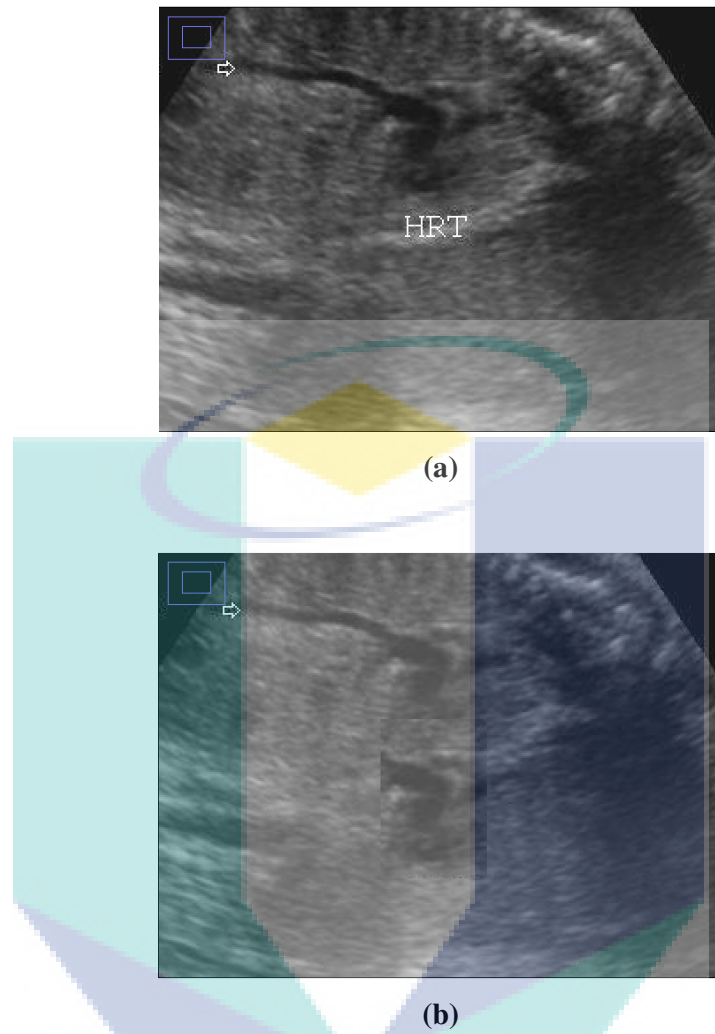


Figure 4.24: (a) Magnified original ROI of Sample 5 (b) Magnified ROI of Sample 5 that was cloned

The tampered image for Sample 1 was recovered as shown in Figure 4.25. The tampered ROI was fully recovered to its original state. The process of tamper localization and recovery took 28.0 second.

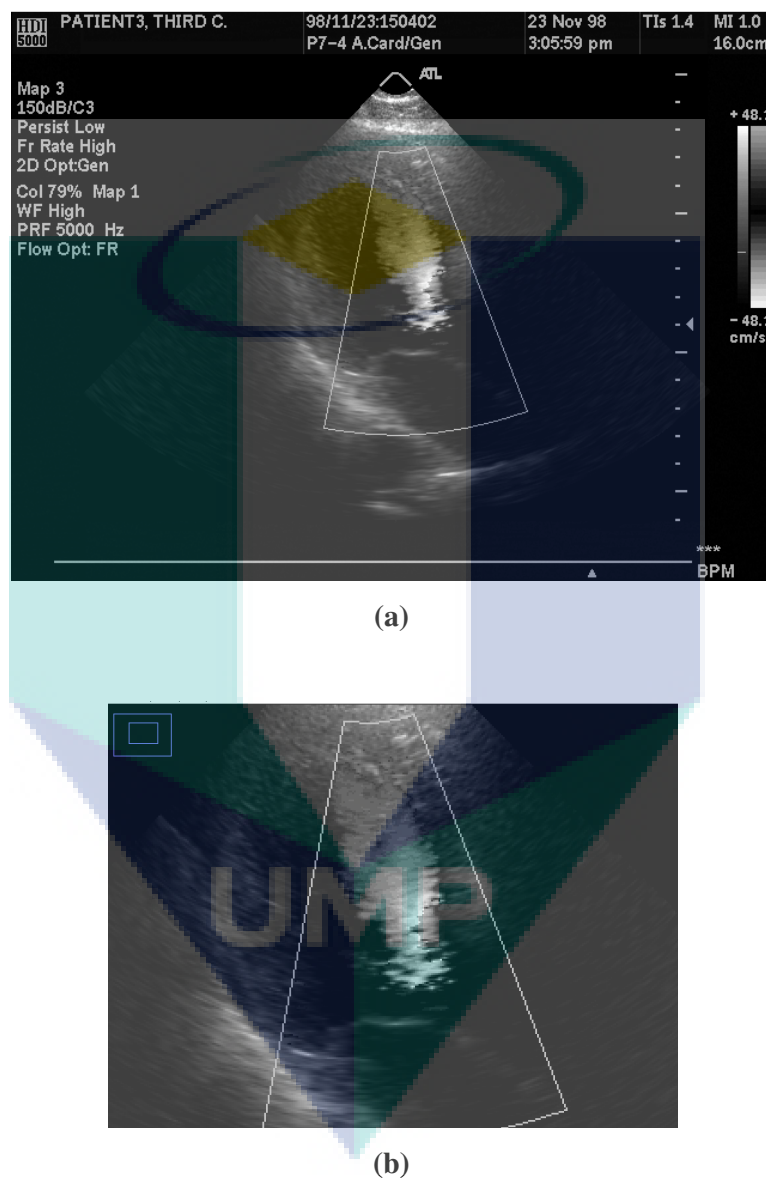


Figure 4.25:(a) Recovered image of Sample 1(b) Magnified recovered ROI of Sample 1

The tampered image for Sample 5 was recovered as shown in Figure 4.26. The tampered ROI was fully recovered to its original state. The process of tamper localization and recovery took 25.4 second.

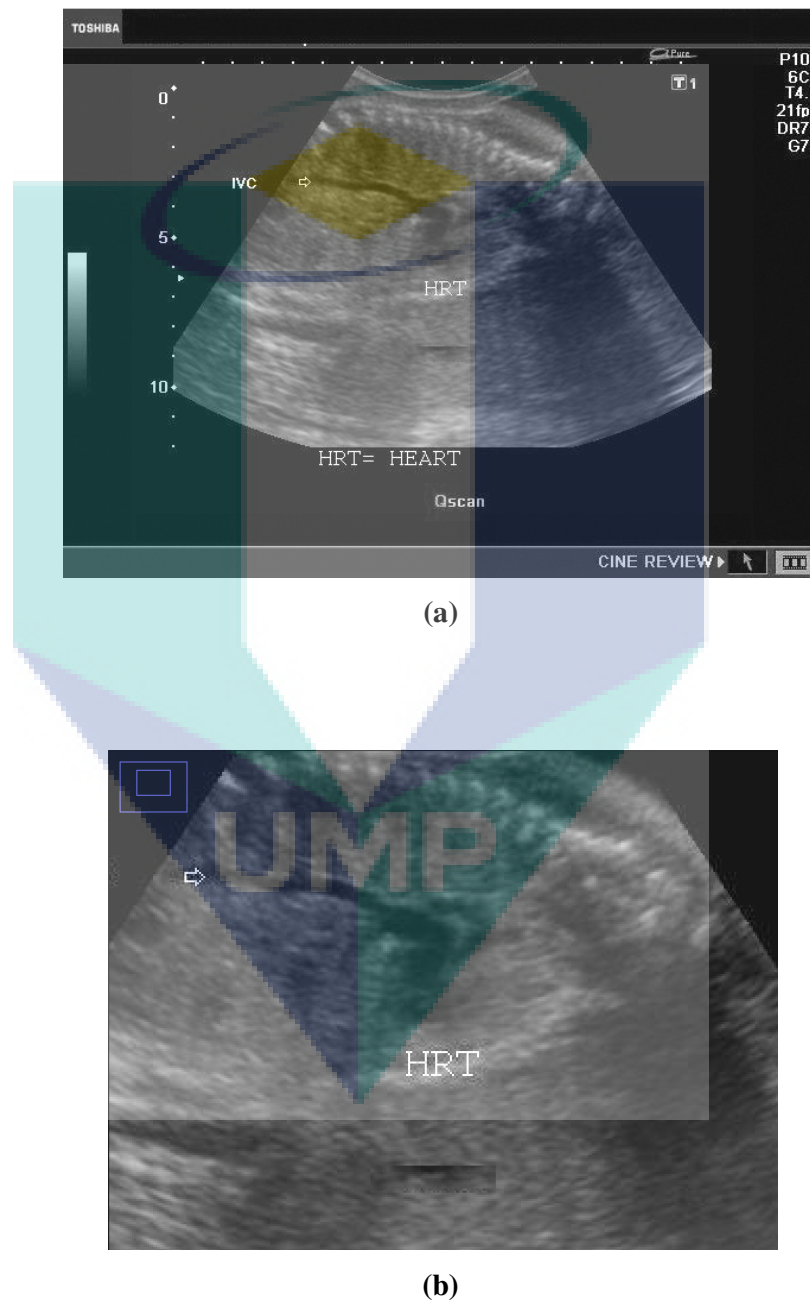


Figure 4.26:(a) Recovered image of Sample 5 (b) Magnified recovered ROI of Sample 5

Sample 2 and 6 were tampered by adding salt and pepper noise in the ROI as shown in Figure 4.27 and 4.28. The tampered area measuring 60 x 90 pixels.

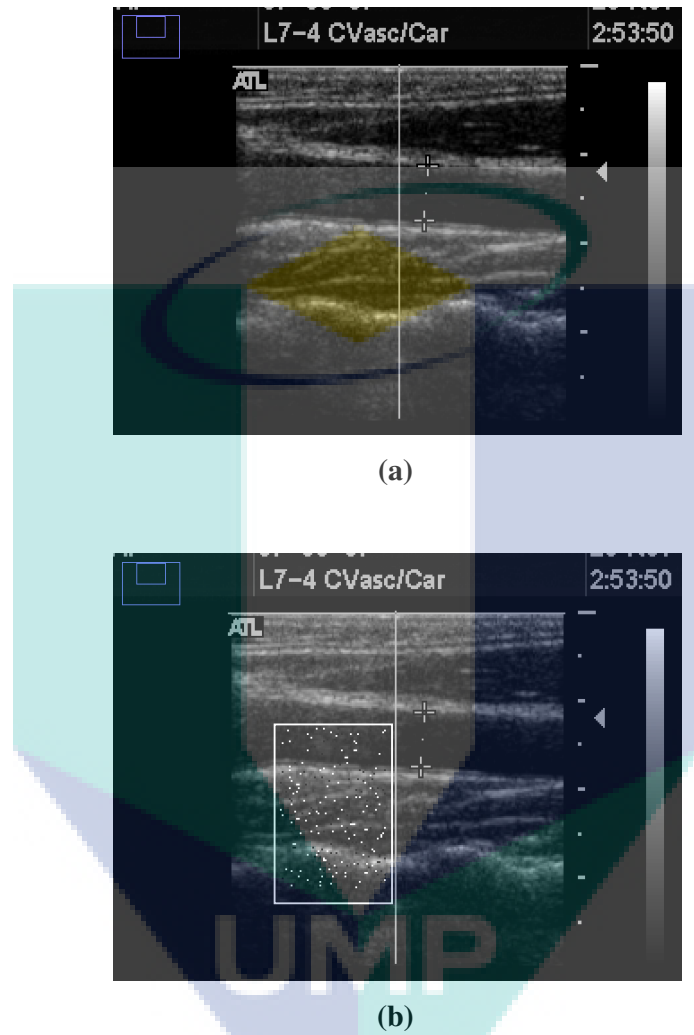


Figure 4.27: (a) Magnified original ROI of Sample 2 (b) Magnified ROI of Sample 2 tampered with salt and pepper noise as highlighted

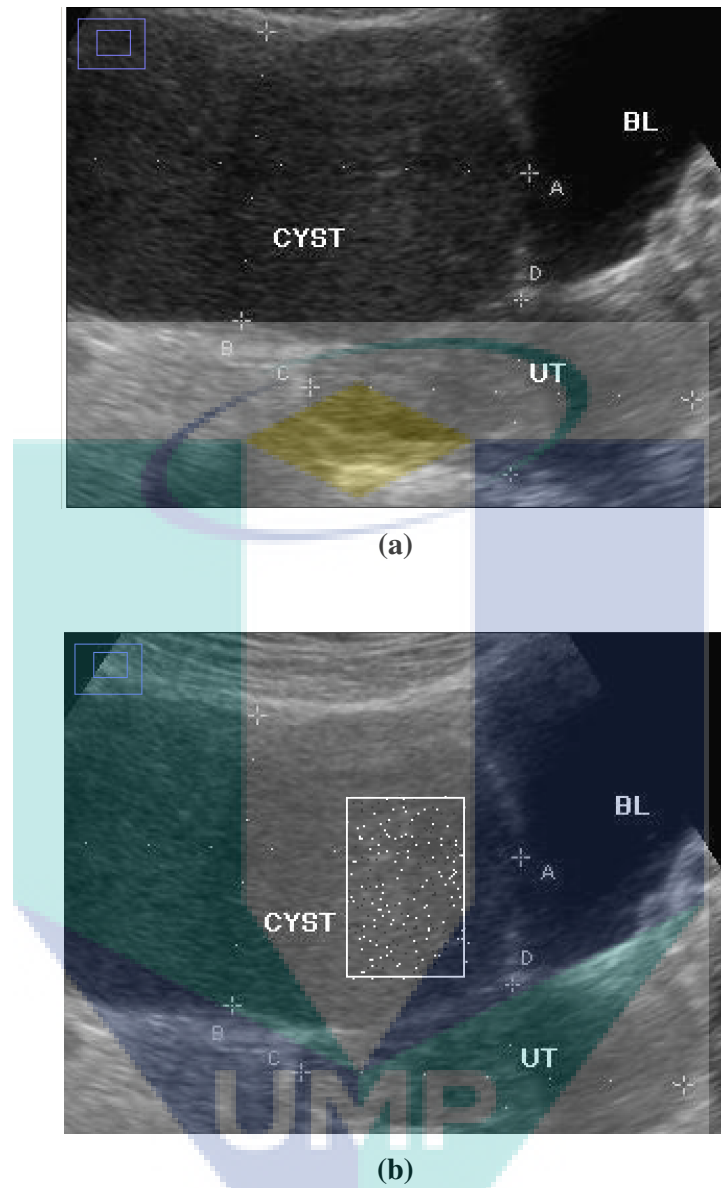


Figure 4.28: (a) Magnified original ROI of Sample 6 (b) Magnified ROI of Sample 6 tampered with salt and pepper noise as highlighted

Figure 4.29 shows the recovered image of Sample 2. The magnified ROI image shows that the tampered area had been recovered. The process of tamper localization and recovery took 27.8 seconds.

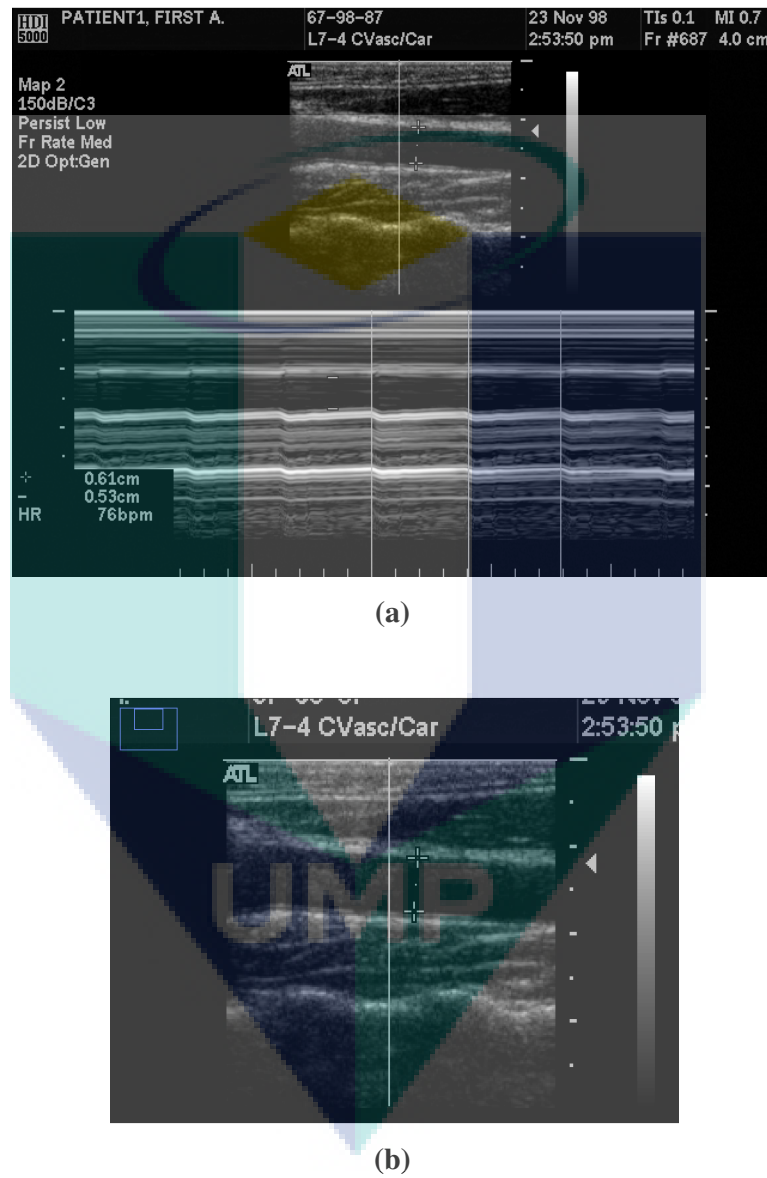


Figure 4.29: (a) Recovered image of Sample 2 (b) Magnified recovered ROI of Sample 2

Figure 4.30 shows the recovered image of Sample 6. The magnified ROI image shows that the tampered area had been recovered. The process of tamper localization and recovery took 29.0 seconds.

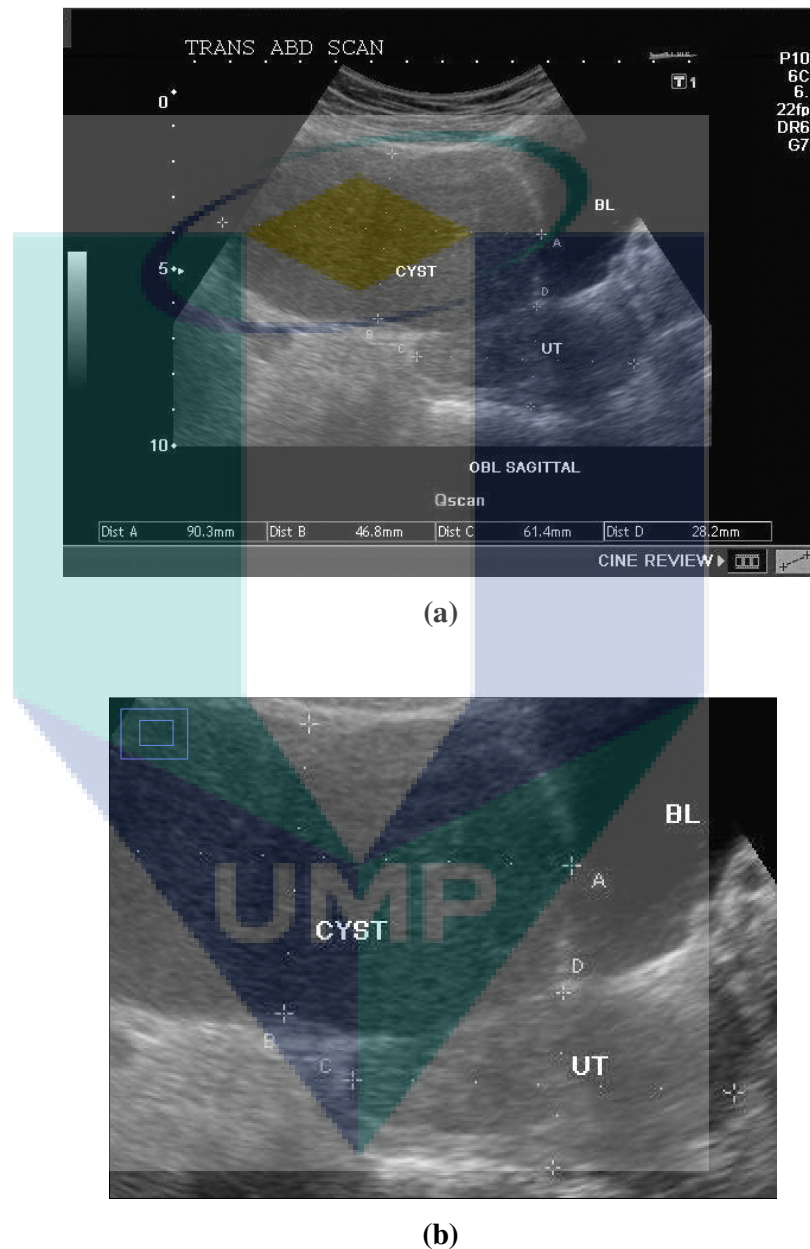


Figure 4.30: (a) Recovered image of Sample 6 (b) Magnified recovered ROI of Sample 6

The next tampering is done by rotating a portion of the ROI of Sample 3 and 7 by 180° as shown in Figure 4.31 and 4.32.

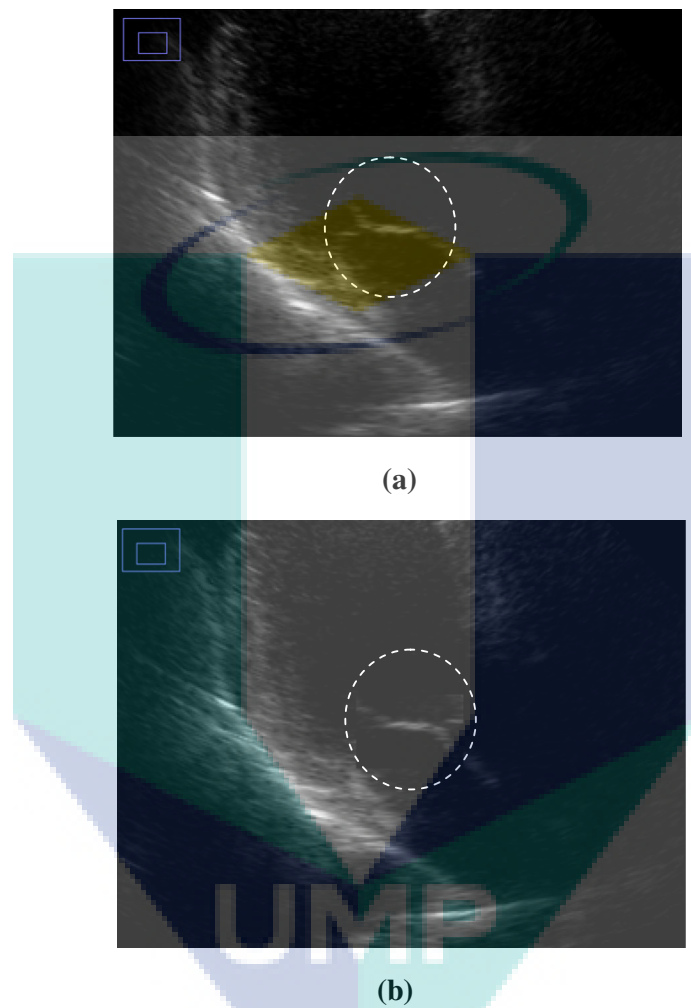


Figure 4.31: (a) Magnified original ROI of Sample 3 (b) Magnified ROI of Sample 3 tampered by rotating the highlighted area by 180°

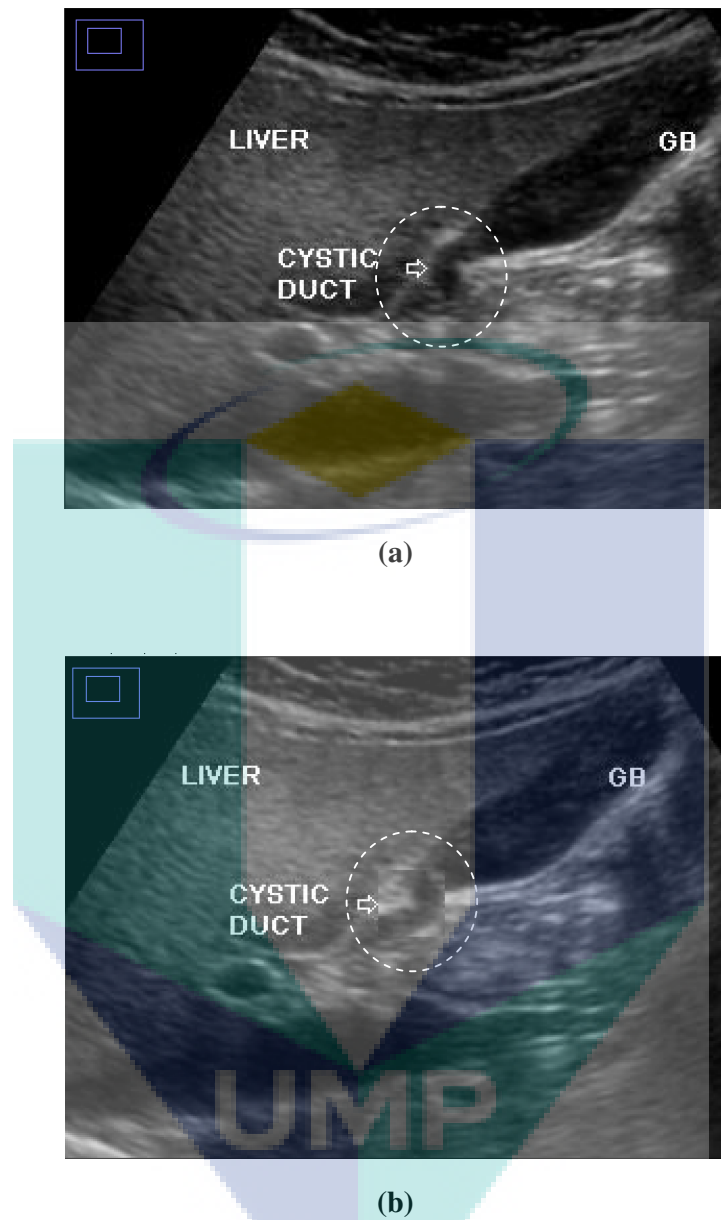


Figure 4.32: (a) Magnified original ROI of Sample 7 (b) Magnified ROI of Sample 7 tampered by rotating the highlighted area by 180°

Figure 4.33 shows the recovered image of Sample 3. The magnified ROI image shows that the tampered area as highlighted had been recovered. The process of tamper localization and recovery took 21.3 seconds.

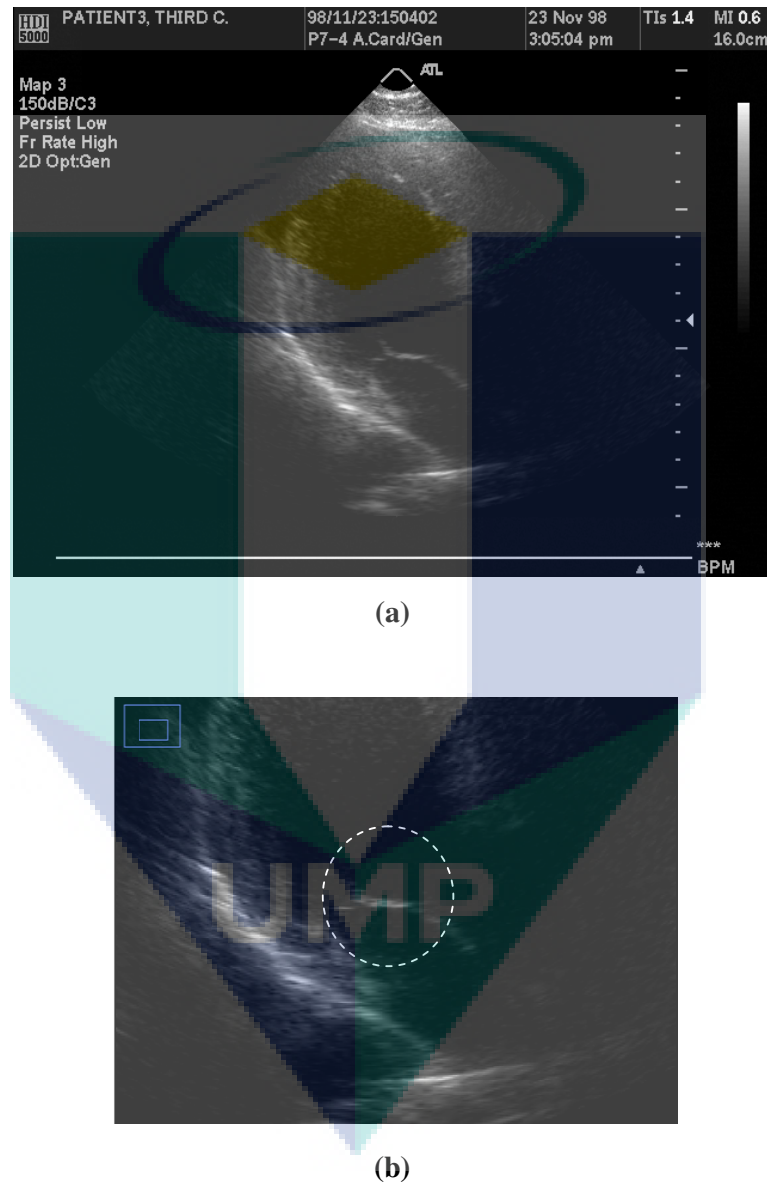
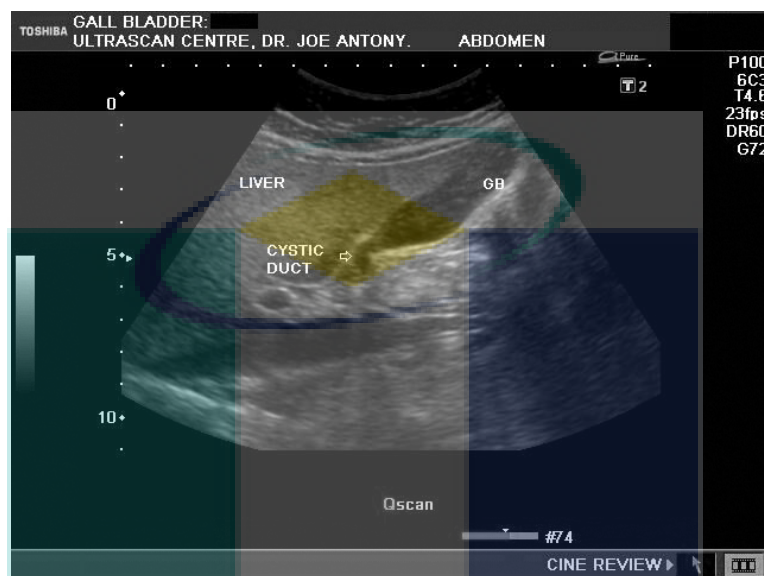
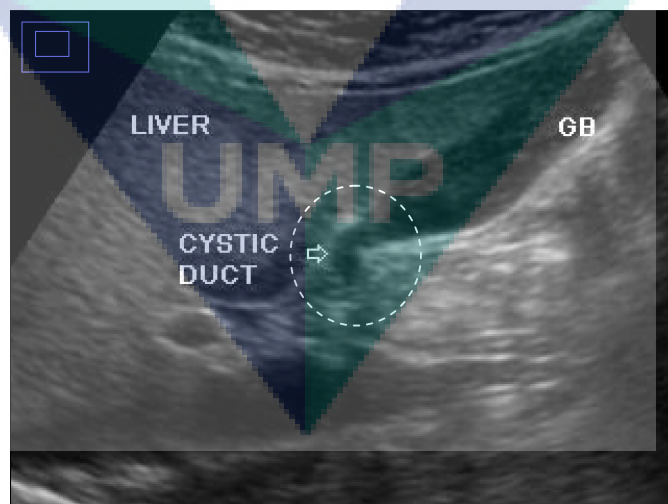


Figure 4.33: (a) Recovered image of Sample 3 (b) Magnified recovered ROI of Sample 3

Figure 4.34 shows the recovered image of Sample 7. The magnified ROI image shows that the tampered area as highlighted had been recovered. The process of tamper localization and recovery took 23.5 seconds.



(a)



(b)

Figure 4.34: (a) Recovered image of Sample 7 (b) Magnified recovered ROI of Sample 7

Sample 4 and 8 were tampered by smoothing the highlighted area as shown in Figure 4.35 and 4.36.

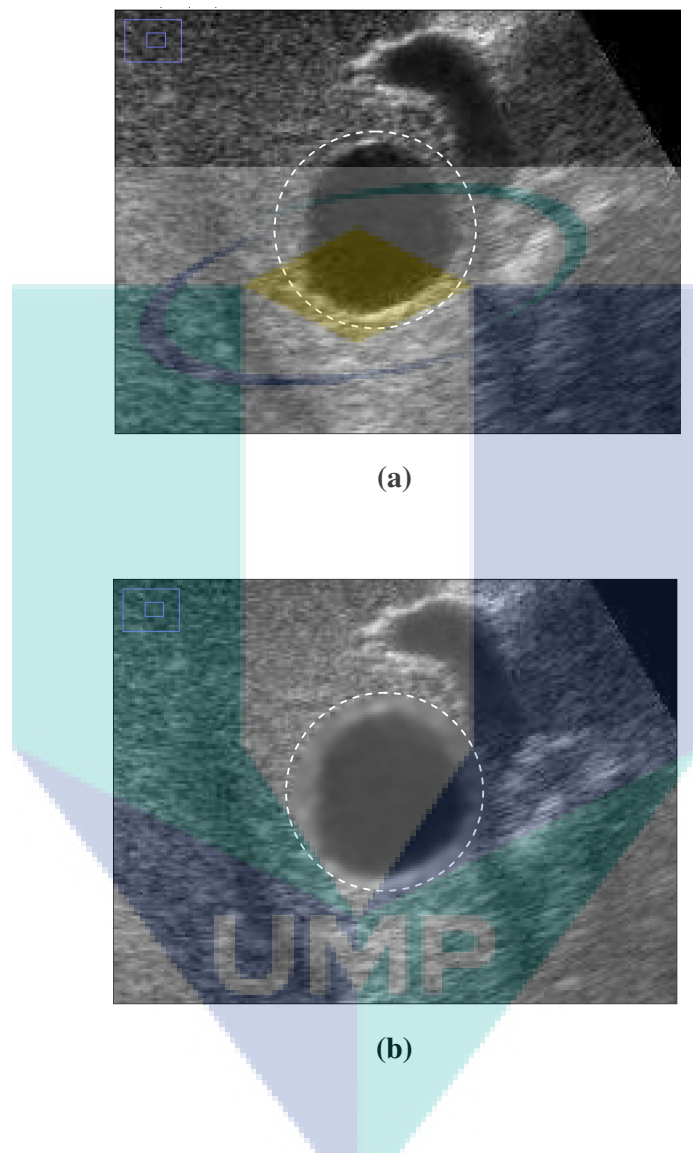


Figure 4.35: (a) Magnified original ROI of Sample 4 (b) Magnified ROI of Sample 4 tampered by smoothing the highlighted area

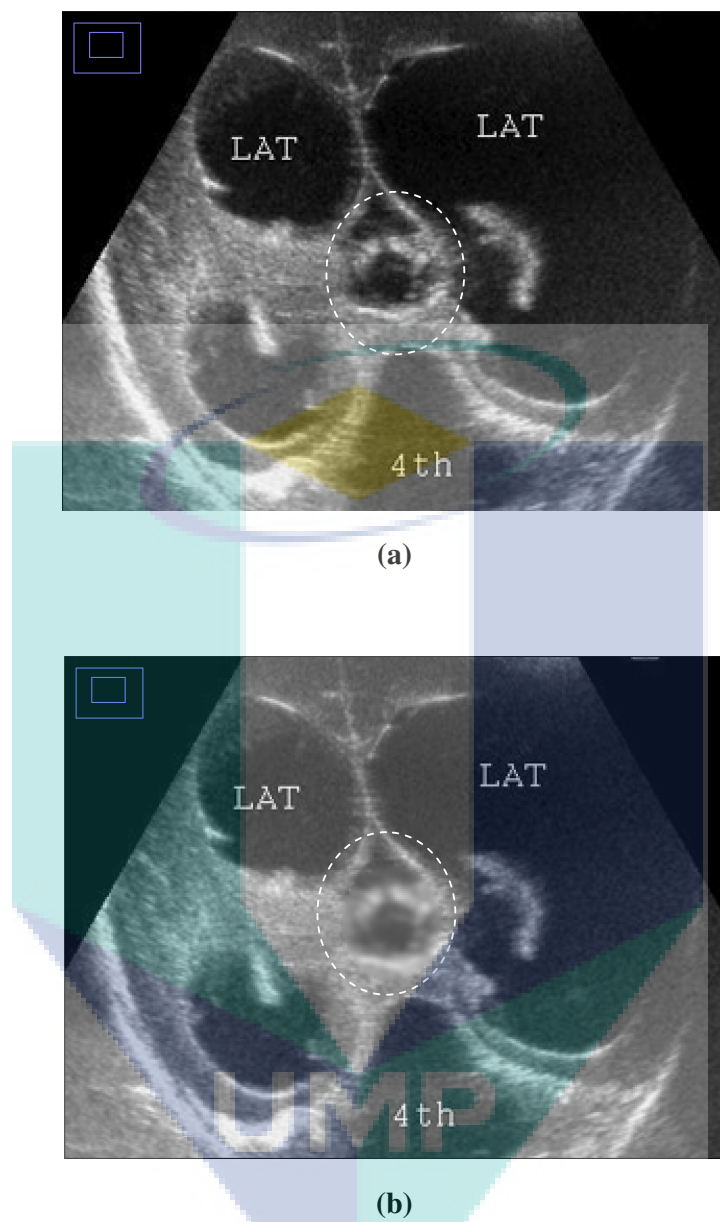
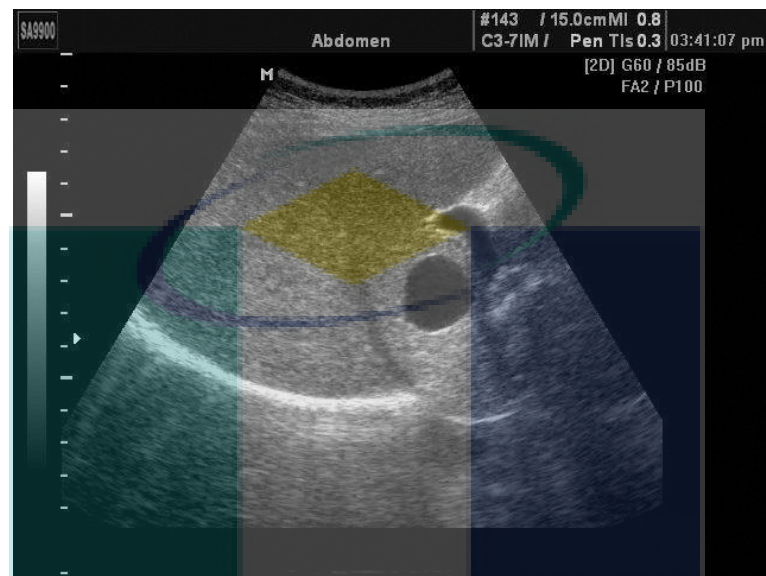
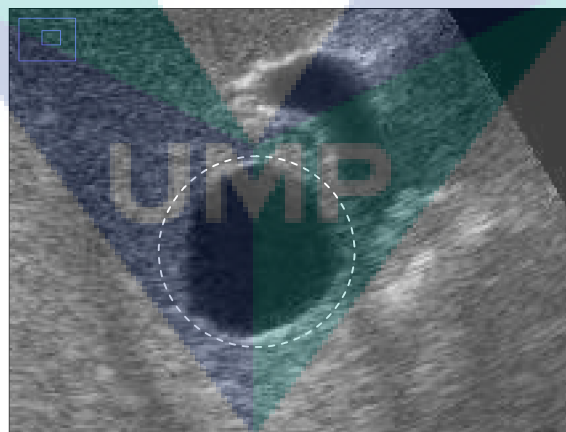


Figure 4.36: (a) Magnified original ROI of Sample 8 (b) Magnified ROI of Sample 8 tampered by smoothing the highlighted area

Figure 4.37 shows the recovered image of Sample 4. The magnified ROI image shows that the tampered area as highlighted had been recovered. The process of tamper localization and recovery took 36.7 seconds.



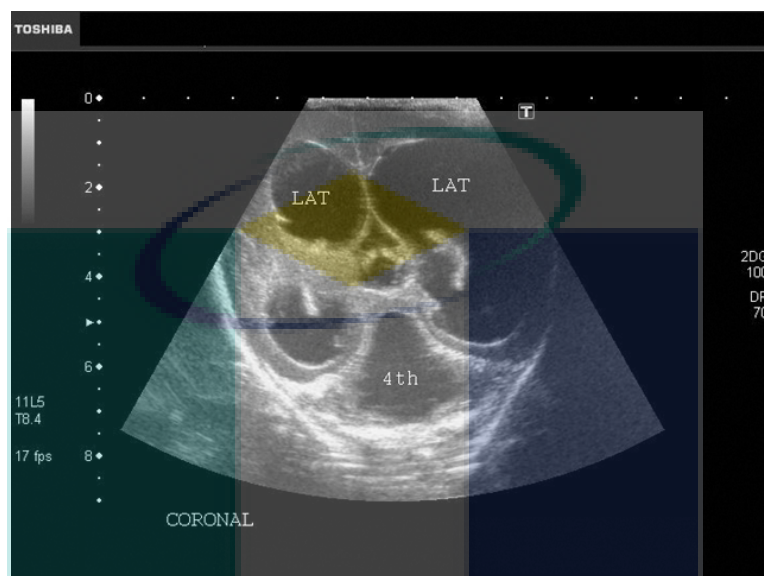
(a)



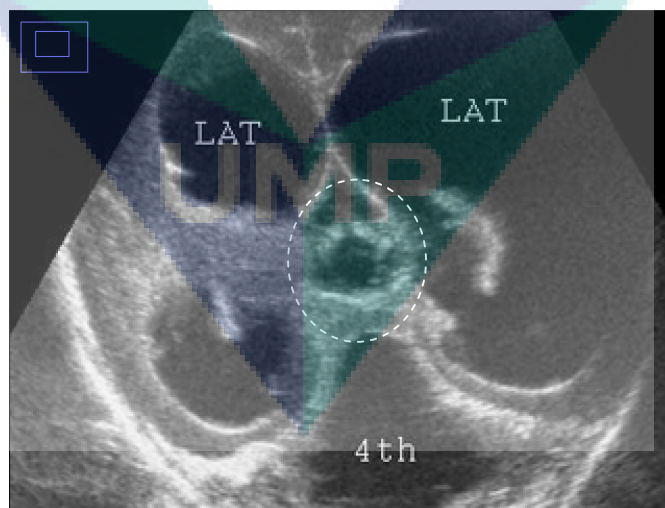
(b)

Figure 4.37: (a) Recovered image of Sample 4 (b) Magnified recovered ROI of Sample 4

Figure 4.38 shows the recovered image of Sample 8. The magnified ROI image shows that the tampered area as highlighted had been recovered. The process of tamper localization and recovery took 31.2 seconds.



(a)

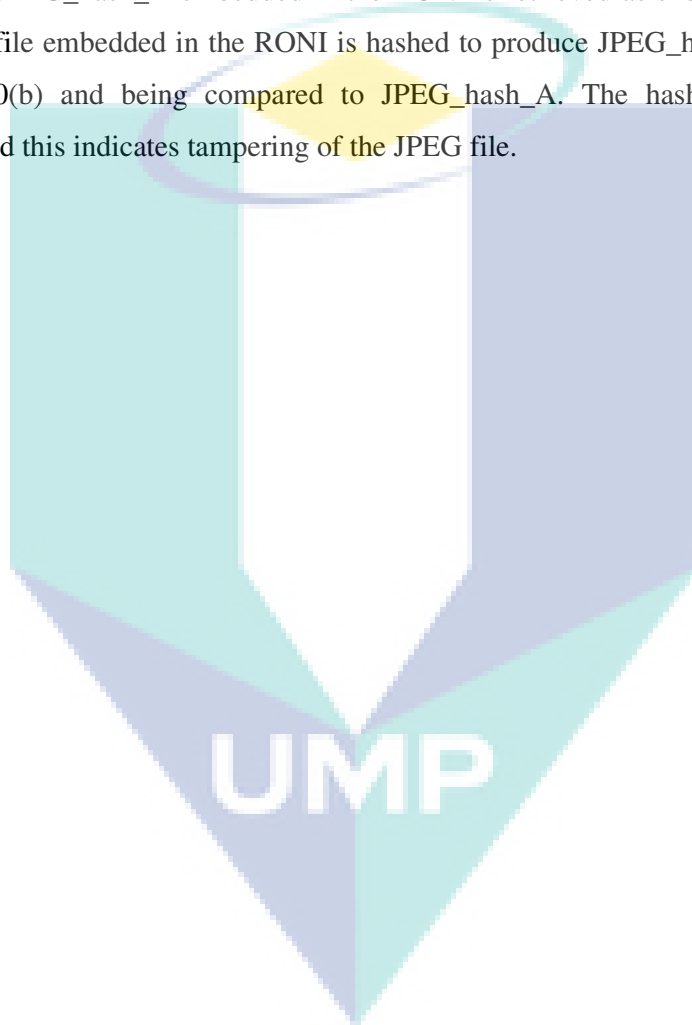


(b)

Figure 4.38: (a) Recovered image of Sample 8 (b) Magnified recovered ROI of Sample 8

ii. Hash Function Test

The authenticity of the embedded JPEG file in the RONI can be verified by comparing the hash values. The watermarked image of Sample 1 was tampered by modifying all RONI pixels to black as shown in Figure 4.39. This is to demonstrate one of the worst tampering scenarios that may occur in the RONI. The hash value for the JPEG file, JPEG_hash_A embedded in the RONI is retrieved as shown Figure 4.40(a). The JPEG file embedded in the RONI is hashed to produce JPEG_hash_B as shown in Figure 4.40(b) and being compared to JPEG_hash_A. The hash values were not identical and this indicates tampering of the JPEG file.



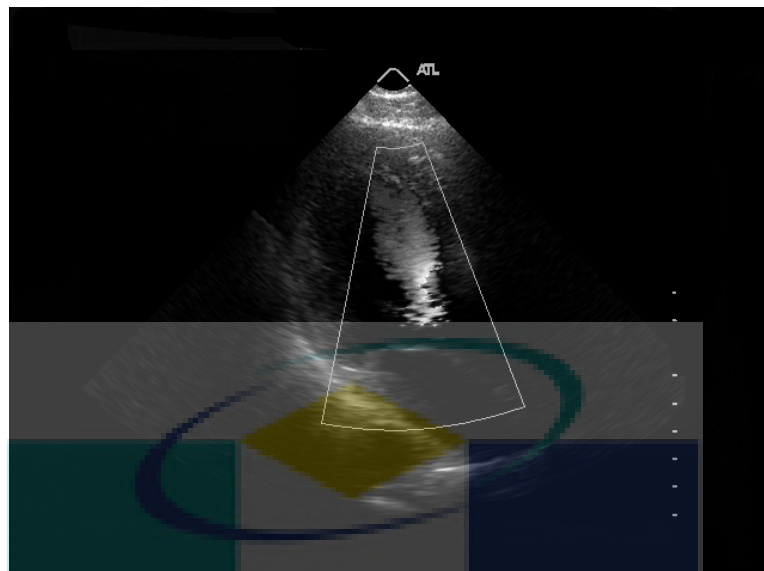


Figure 4.39: RONI of Sample 1 painted in black

e3219b10bb592a18393eb7ec0e0d57a2fbeeef17fc948c994ec9dbe7c8c2a116

(a)

dadedcd45c7e1f32618f8a641eef75ef6fc48c87b6de09cc6ccb2a1c93833c5dd

(b)

Figure 4.40: (a) JPEG_hash_A retrieved from the RONI (b) JPEG_hash_B computed from JPEG file retrieved from the RONI

iii. Lossy Compression

The ROI of Sample 1 was also compressed with lossy JPEG compression that has a quality scale between 0 to 100. The highest scale value applied will produce the highest image quality. The following Figure 4.41 shows the results of the ROI applied with different quality scales.

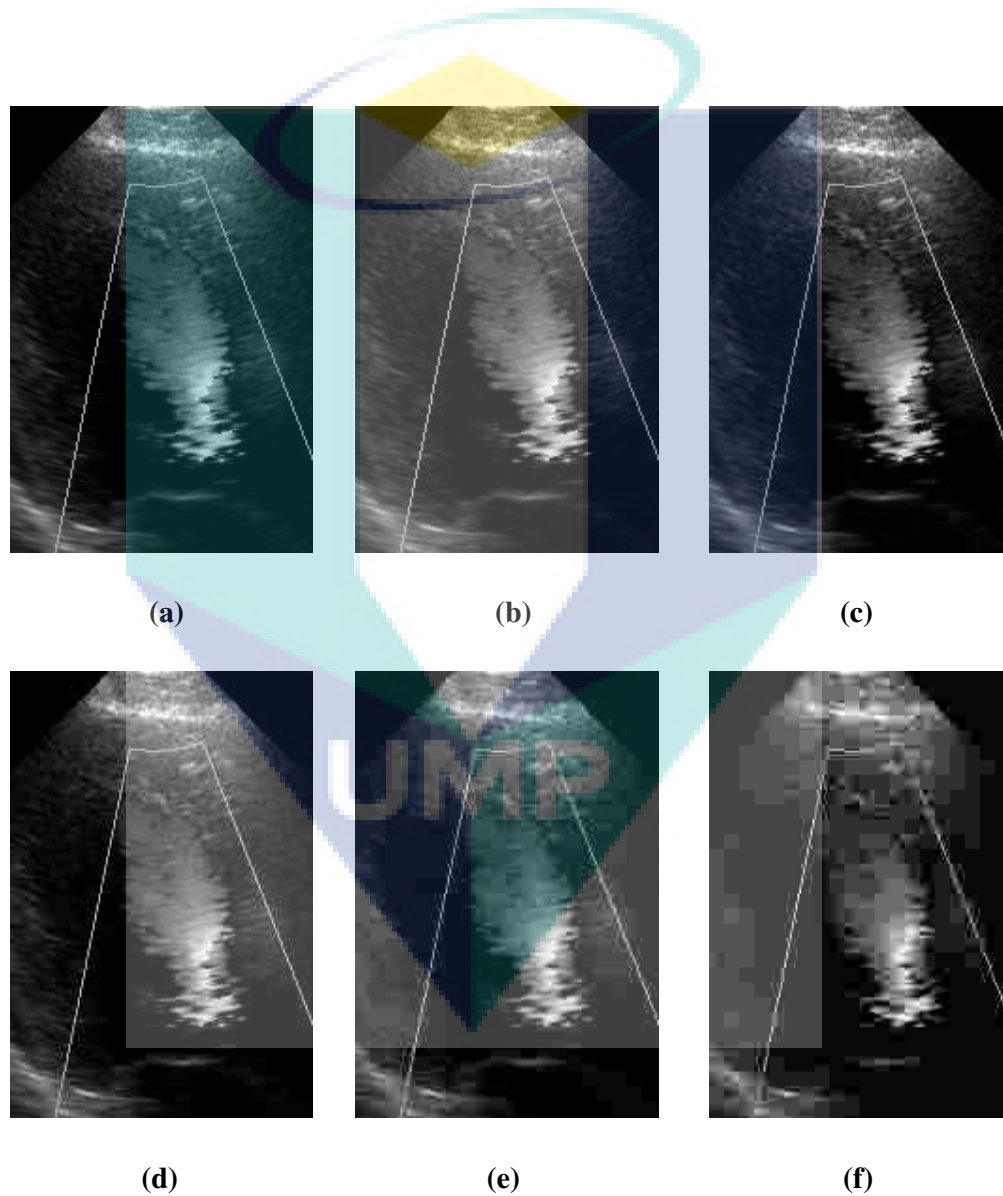


Figure 4.41: ROI of Sample 1 compressed with different scales (a) Scale=90 (b) Scale=75 (c) Scale=50 (d) Scale=25 (e) Scale=10 (f) Scale=5

4.7.2 TALLOR-RS

The same eight images used in TALLOR scheme were watermarked. The ROI was losslessly compressed in the same manner as in the TALLOR scheme. Figure 4.42 to 4.49 shows the watermarked images. The details of the experiment results are shown in Table 4.4. The average compression ratio and PSNR achieved is 0.63 and 48.2 dB respectively.

Table 4.4: The experiment results for all samples using TALLOR-RS

Total ROI Bits = 307200				
Figure	Compression Output(bits)	Compression Ratio	PSNR(dB)	Total Watermark Payload(bits)
Sample 1	176240	0.57	48.3	177008
Sample 2	189928	0.62	48.5	190696
Sample 3	157560	0.51	49.0	158328
Sample 4	231160	0.75	47.6	231928
Sample 5	188424	0.61	47.8	189192
Sample 6	195488	0.64	48.2	196256
Sample 7	179864	0.59	48.6	180632
Sample 8	218448	0.71	47.4	219216
Average		0.63	48.2	

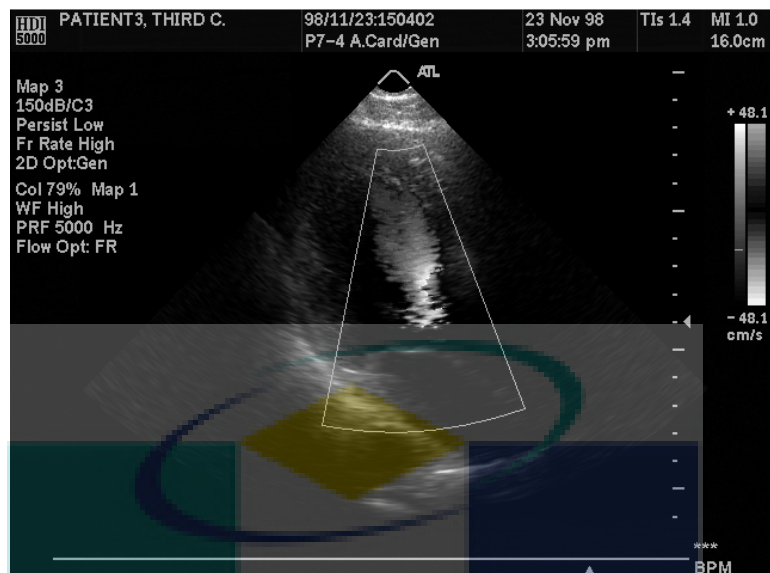


Figure 4.42: Watermarked image of Sample 1, PSNR= 48.3 dB

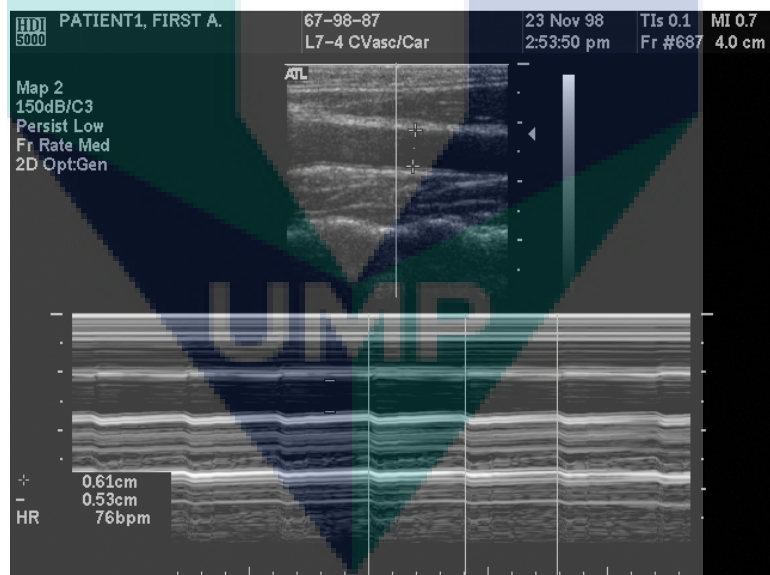


Figure 4.43: Watermarked image of Sample 2, PSNR= 48.5 dB

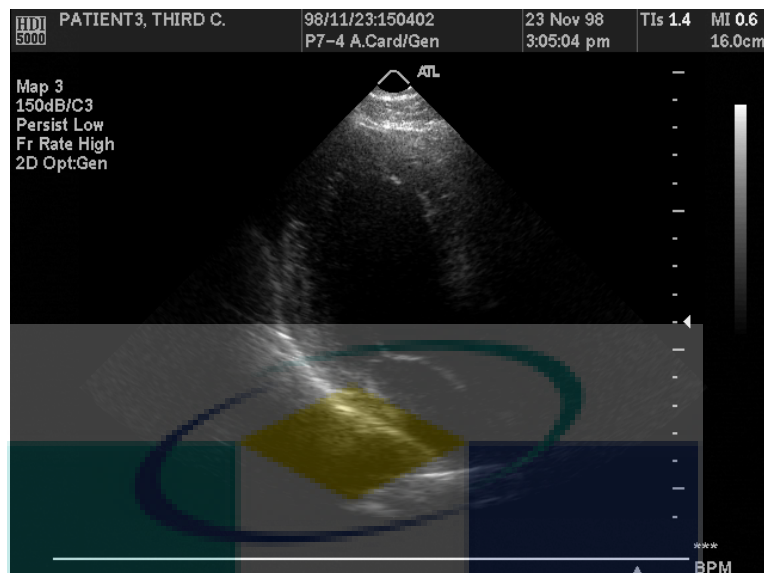


Figure 4.44: Watermarked image of Sample 3, PSNR= 49.0 dB

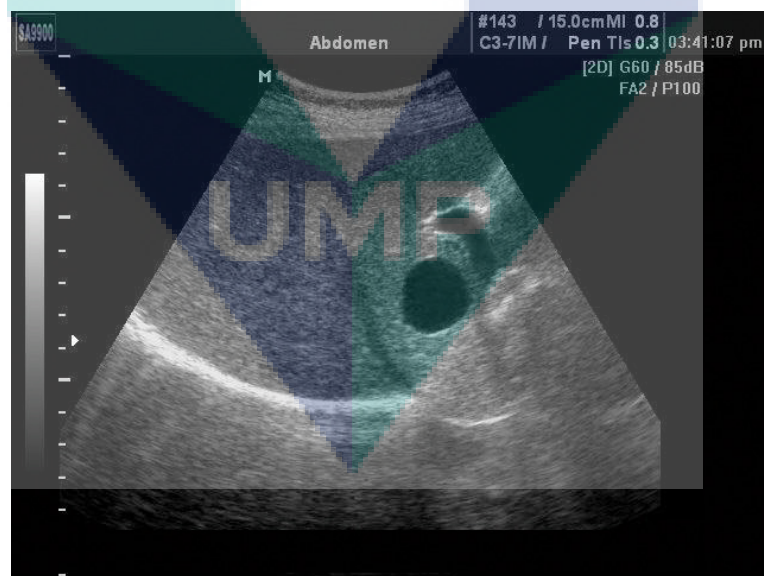


Figure 4.45: Watermarked image of Sample 4, PSNR= 47.6 dB

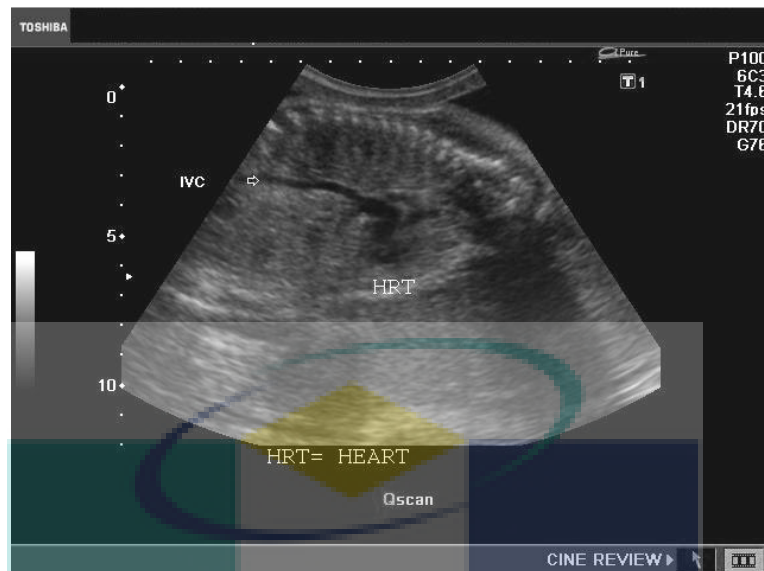


Figure 4.46: Watermarked image of Sample 5, PSNR= 47.8 dB

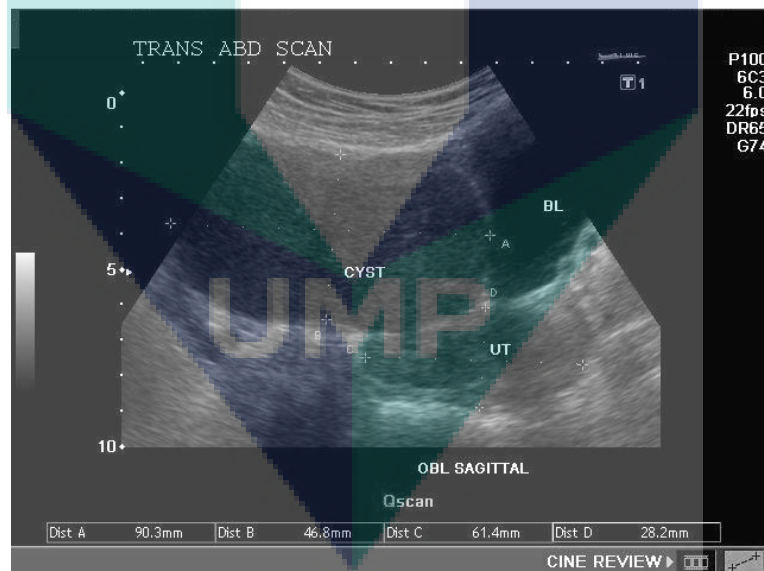


Figure 4.47: Watermarked image of Sample 6, PSNR= 48.2 dB

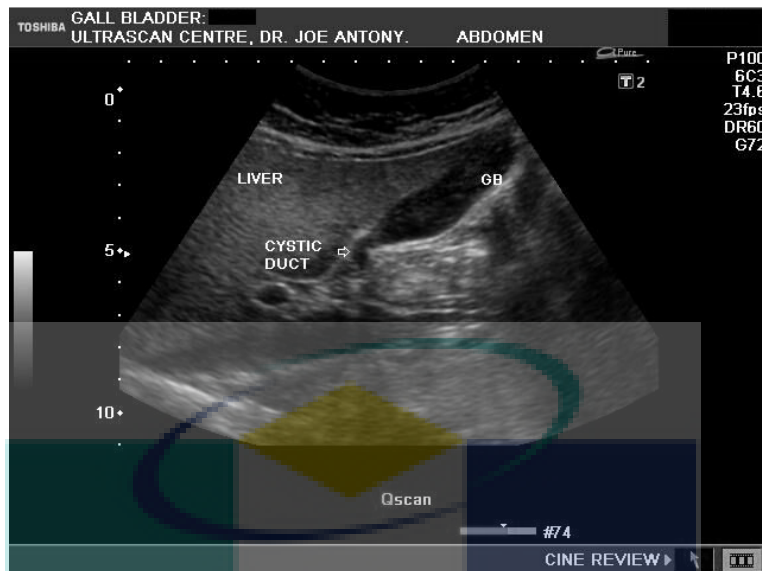


Figure 4.48: Watermarked image of Sample 7, PSNR= 48.6 dB

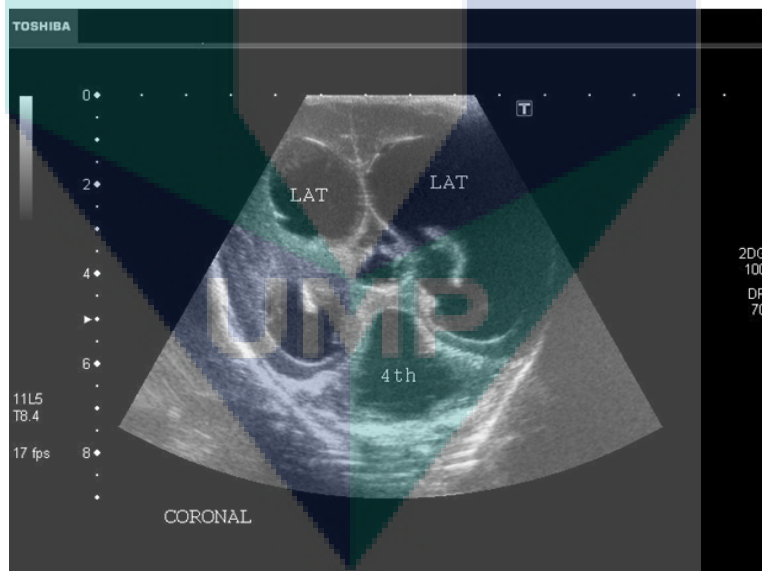


Figure 4.49: Watermarked image of Sample 8, PSNR= 47.4 dB

i. Tamper Localization and Recovery

For the purpose of comparison, the eight watermarked images were tampered similarly as in the TALLOR scheme. A portion of the ROI in Sample 1 and 5 was cloned as shown in Figure 4.50 and 4.51. Figure 4.52 and 4.53 shows the tampered ROI had been recovered. The tamper localization and recovery process for Sample 1 and 5 took 14.1 seconds and 12.4 seconds respectively.

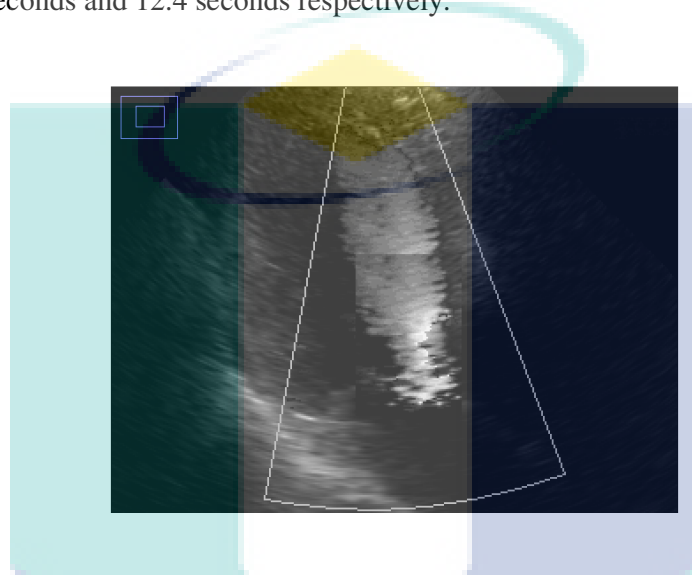


Figure 4.50: Magnified ROI of Sample 1 that was cloned

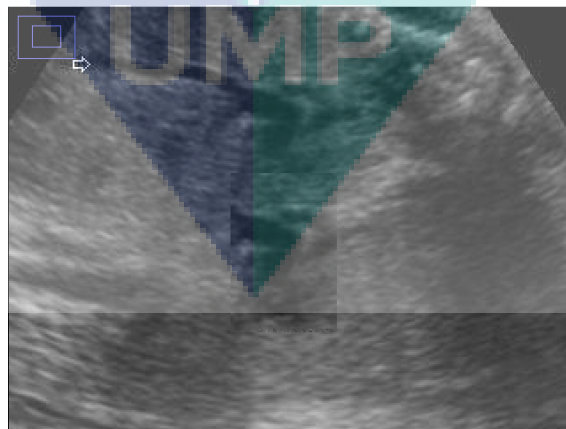


Figure 4.51: Magnified ROI of Sample 5 that was cloned

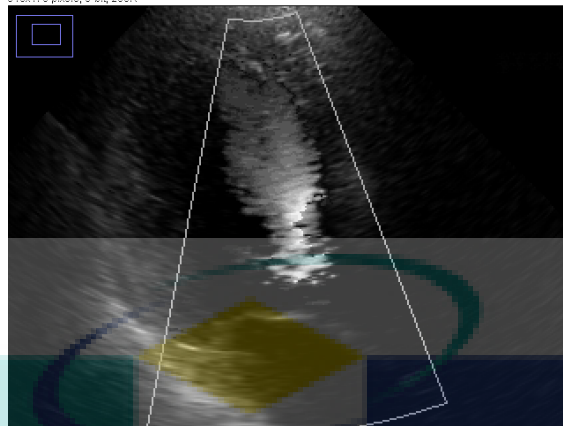


Figure 4.52: Magnified recovered ROI of Sample 1

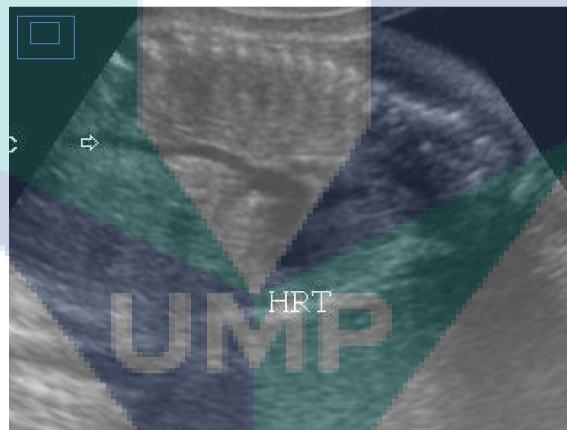


Figure 4.53: Magnified recovered ROI of Sample 5

Sample 2 and 6 were tampered by adding salt and pepper noise to the ROI as shown in Figure 4.54 and 4.55. The ROI was recovered as shown in Figure 4.56 and 4.57. The tamper localization and recovery process for Sample 2 and 6 took 13.9 seconds and 14.0 seconds respectively.

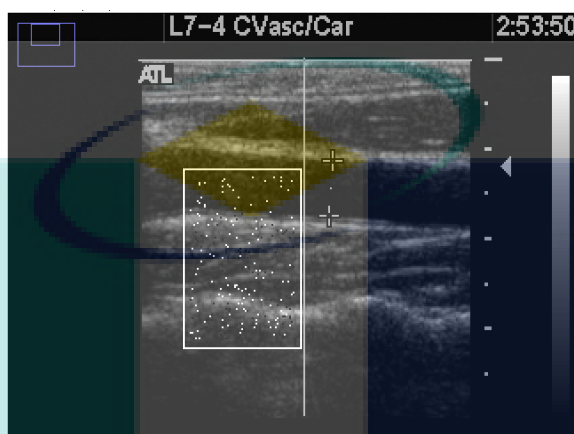


Figure 4.54: Magnified ROI of Sample 2 that was tampered by adding salt and pepper noise as highlighted

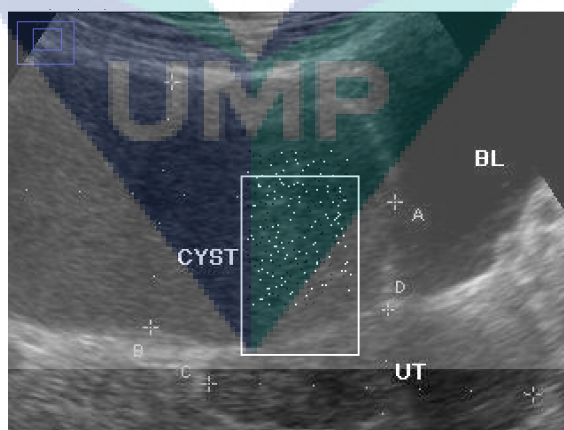


Figure 4.55: Magnified ROI of Sample 6 that was tampered by adding salt and pepper noise as highlighted

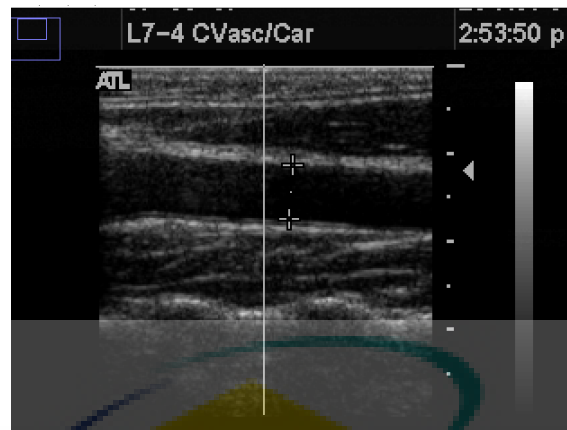


Figure 4.56: Magnified recovered ROI of Sample 2

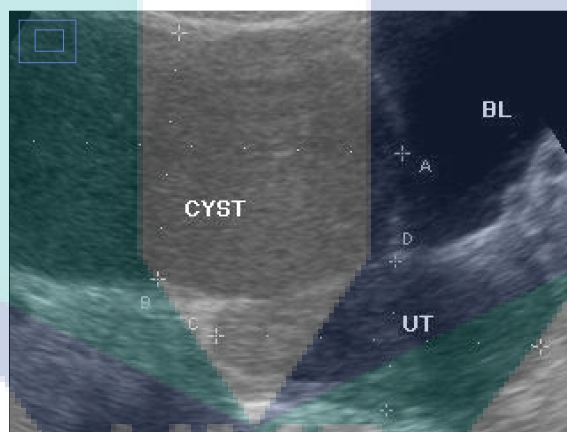


Figure 4.57: Magnified recovered ROI of Sample 6

The next tampering was done by rotating the highlighted area of Sample 3 and 7 as shown in Figure 4.58 and 4.59 by 180°. The tampered area was recovered as shown in Figure 4.60 and 4.61. The tamper localization and recovery process for Sample 3 and 7 took 9.6 seconds and 11.1 seconds respectively.

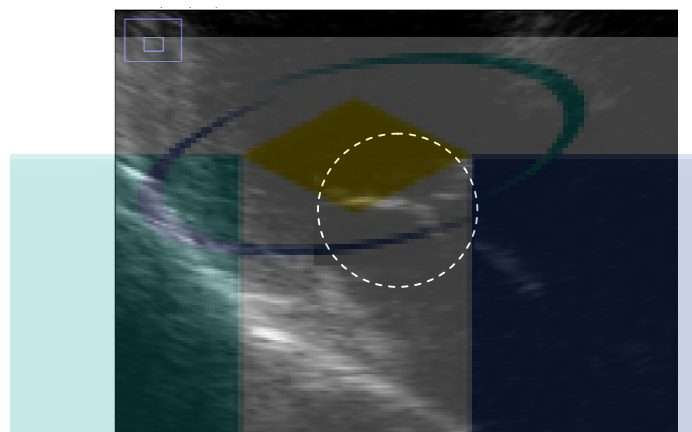


Figure 4.58: Magnified ROI of Sample 3 that was tampered by rotating the highlighted area by 180°

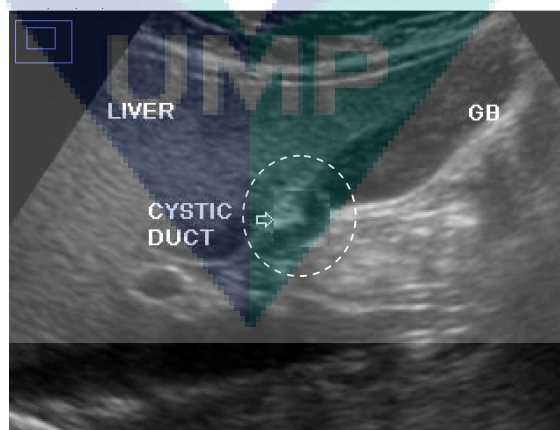


Figure 4.59: Magnified ROI of Sample 7 that was tampered by rotating the highlighted area by 180°

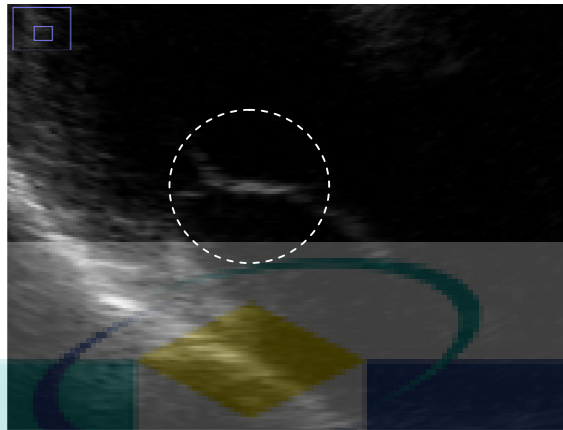


Figure 4.60: Magnified recovered ROI of Sample 3

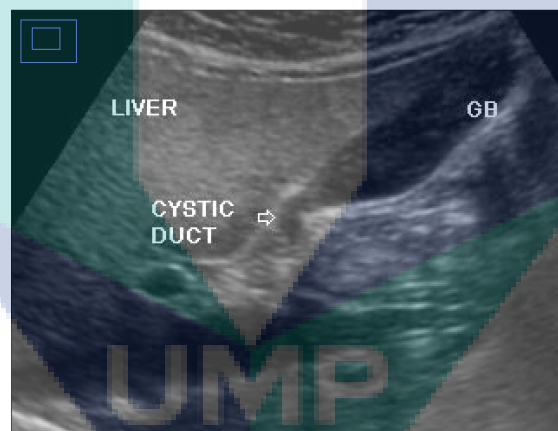


Figure 4.61: Magnified recovered ROI of Sample 7

The last tampering was done on Sample 4 and 8 by smoothing a portion of the ROI as shown in Figure 4.62 and 4.63. The tampered ROI was recovered as shown in Figure 4.64 and 4.65. The tamper localization and recovery process for Sample 4 and 8 took 12.8 seconds and 15.4 seconds respectively.

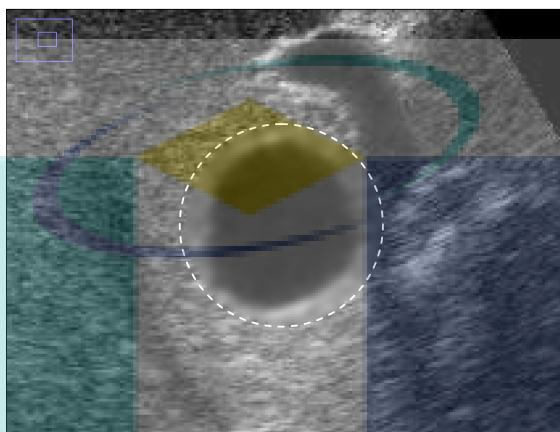


Figure 4.62: Magnified ROI of Sample 4 that was tampered by smoothing the highlighted area

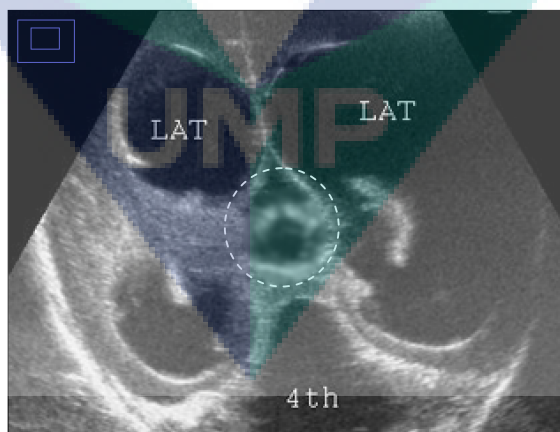


Figure 4.63: Magnified ROI of Sample 8 that was tampered by smoothing the highlighted area

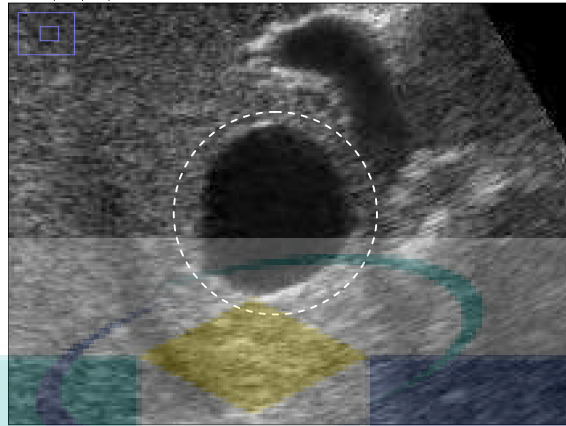


Figure 4.64: Magnified recovered ROI of Sample 4

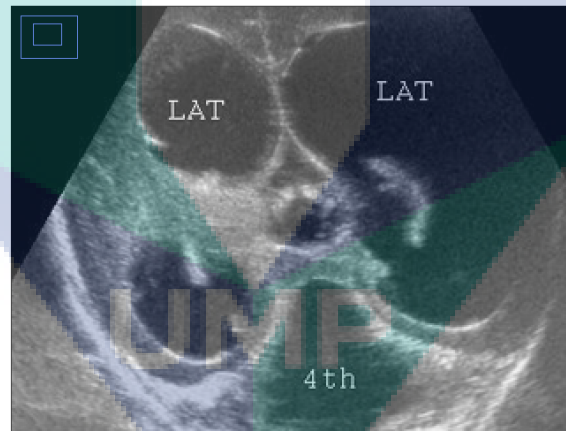


Figure 4.65: Magnified recovered ROI of Sample 8

ii. Hash Function Test

The authenticity of the embedded authentication and recovery information can be verified by comparing the embedded hash values, `RONI1_hash_A` and `RONI2_hash_A` with the current hash values at the time of authentication. The

watermarked image of Sample 3 was tampered by modifying the highlighted RONI pixels to black as shown in Figure 4.66. The RONI was then hashed to produce RONI1_hash_B and RONI2_hash_B as shown in Figure 4.67b and Figure 4.68b respectively to be compared with the retrieved hash values. The hash values were not identical

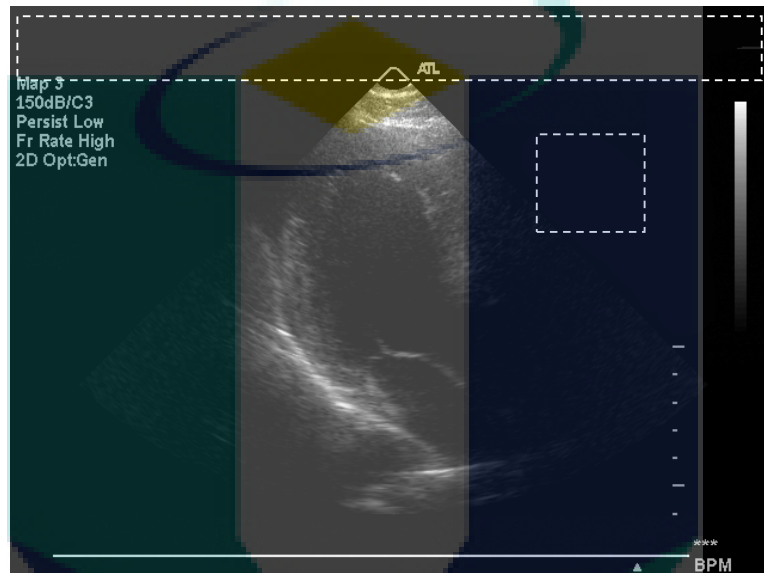


Figure 4.66: Highlighted RONI of Sample 3 painted in black

43ca8dca602ead9ffaecc5daa9a7b448f98467a3b9f14e32a023f15b7f2f07ac

(a)

6e0d785d541e60e99342e140c8d1aa7393bbc89846dafa54ff018b13006ea1bd

(b)

Figure 4.67: (a) RONI1_hash_A retrieved from the RONI (b) RONI1_hash_B computed at the time of authentication

1d0d9dfdc85adab17d3249104f2e17ed000cacd844ad6f33882a182a01704eab

(a)

34f036733eef4cfc47057d6db4ad18ea8648bf2b7cae9d7d638ab7ec8740011

(b)

Figure 4.68: (a) RONI2_hash _A retrieved from the RONI (b) RONI2_hash_B computed at the time of authentication

4.8 EVALUATION AND DISCUSSION

The analyses of the experiments performed for TALLOR and TALLOR-RS scheme are discussed as below:

4.8.1 Image Quality And Fidelity

The quality of the watermarked images is high with the average PSNR of 48.3 dB and 48.2 dB for TALLOR and TALLOR-RS, which are among the highest as compared to other watermarking schemes reviewed in the literature. A high PSNR indicates low distortion in the watermarked image. The watermark embedding only occurs in the RONI to maintain the originality of the ROI. The ROI of the watermarked images are identical with the ROI of the original images. Figure 4.69 shows the magnified RONI of the original image and watermarked image of Sample 1. Although the watermark was embedded in the LSB and second LSB of each pixel in the RONI, there was no noticeable distortion.

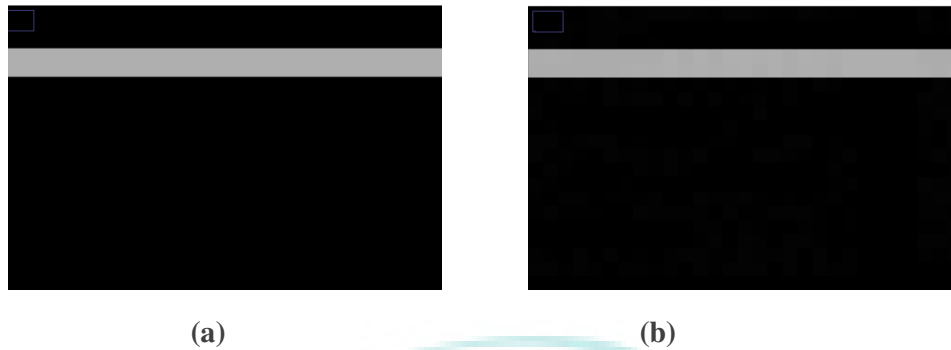


Figure 4.69: Magnified RONI of Sample 1 (a) Original image (b) Watermarked image

4.8.2 Tamper Localization and Recovery

The tampered ROI was localized and recovered with 100% success rate for all samples. Figure 4.70 shows the original and recovered image for Sample 1. The recovered image is identical with the original image. The quality of the recovered area was high where the pixels values were retrieved from the JPEG file which was losslessly compressed. The pixel values were the exact values originated from the non-tampered ROI. The recovered ROI may be used for diagnoses purposes due to its high quality.

As for the processing time as shown in Table 4.5, the average time for TALLOR and TALLOR-RS scheme are 27.9 seconds 13.0 seconds respectively. The method used in the TALLOR-RS scheme had been proven effective in reducing the tamper localization and recovery average processing time by approximately 53% when being compared with the TALLOR scheme.

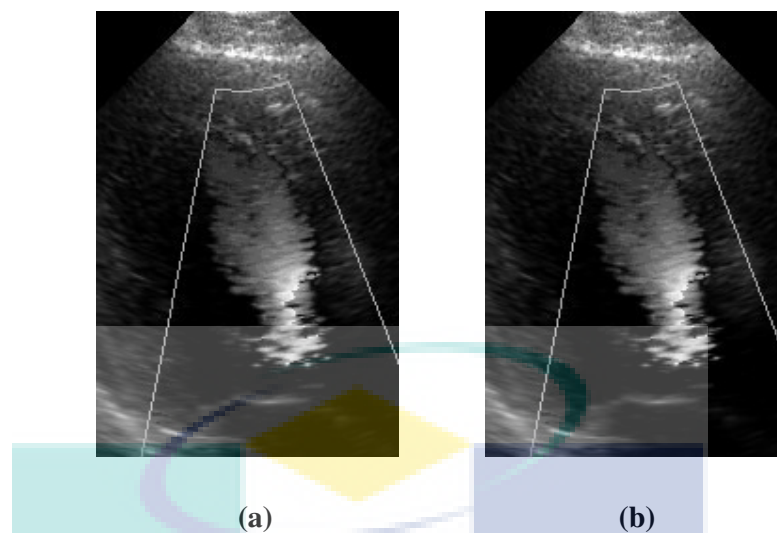


Figure 4.70: Image for Sample 1 (a) Original ROI (b) Recovered ROI

Table 4.5: Tamper localization and recovery processing time in seconds

Figure	Tampering	TALLOR	TALLOR-RS
Sample 1	Cloning	28.0	14.1
Sample 2	Salt and pepper	27.8	13.9
Sample 3	Rotation	21.3	9.6
Sample 4	Smoothing	36.7	12.8
Sample 5	Cloning	25.4	12.4
Sample 6	Salt and pepper	29.0	14.0
Sample 7	Rotation	23.5	11.5
Sample 8	Smoothing	31.2	15.4
	Average	27.9	13.0

4.8.3 Hash Function

The RONI was tampered as shown in Figure 4.39 for the TALLOR scheme and Figure 4.66 for the TALLOR-RS scheme. The comparison results between the retrieve hash values and the hash values produced at the time of authentication were negative. There are two possible scenarios in this situation. Firstly, the possibility of the retrieved hash values had been tampered and cannot be used for authentication. The second

scenario is that the RONI where the watermark is embedded had been tampered. In either scenario, it can be concluded that tampering in the RONI can be detected successfully in both TALLOR and TALLOR-RS scheme.

4.8.4 Compression

The ROI of the samples were losslessly compressed. Compression ratios between 0.51 and 0.75 were achieved. The compression ratios achieved for each sample in both schemes were not significantly different. The ROI of Sample 1 was also compressed using lossy JPEG compression with different compression scales. Based on the compression results, there was no noticeable difference between the image quality of the lossless compressed ROI and lossy compressed ROI at the scale of 90 as shown in Figure 4.71. The compression ratio for lossy compression at the scale 90 is at 0.30 as shown in Table 4.6 which is significantly lower to the ratio achieved using lossless compression.

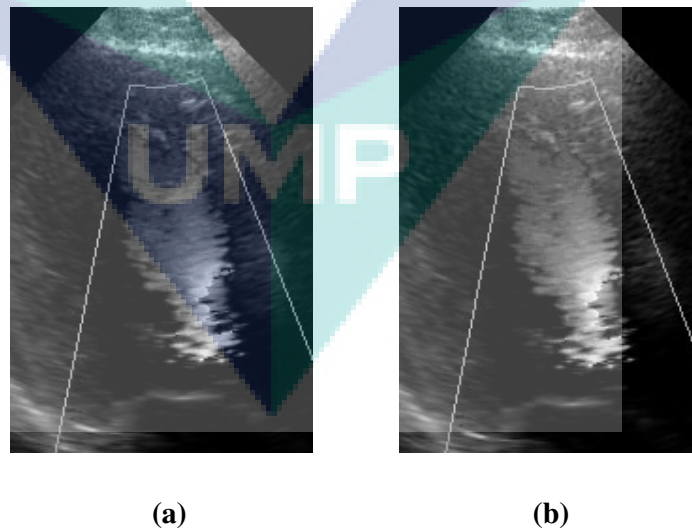


Figure 4.71: Sample 1 (a) Lossless compressed ROI (b) Lossy compressed ROI(scale=90)

In fact, the image quality degradation is only noticeable when the ROI is compressed at the quality scale of 25 as shown in Figure 4.41. This will allow a larger ROI to be defined if the recovered tampered ROI in a lossy compressed quality is acceptable. Based on the compression ratio achieved by using lossy compression, a larger ROI is defined for Sample 1 as shown in Figure 4.72. The image will only consist of four RONI instead of eight in the previous method. The four RONI has the total pixels of approximately 94,440 and this translates to storage capacity of approximately 188,880 bits if the LSB and second LSB of each pixel are used for embedding. The ROI has a size of 480 x 360 pixels or 1,382,400 bits. With the assumption that a lossy compression with the scale of 50 is used, the compressed output of the ROI will be approximately 179,712 bits. It is technically feasible to embed the lossy compressed ROI in the RONI without any difficulties.

Table 4.6: ROI of Sample 1 applied with different lossy compression quality scale

	Total input (ROI) bits = 307200					
Quality scale	90	75	50	25	10	5
Output size(bits)	93544	57696	39728	26464	15088	10656
Compression Ratio	0.30	0.19	0.13	0.09	0.05	0.03

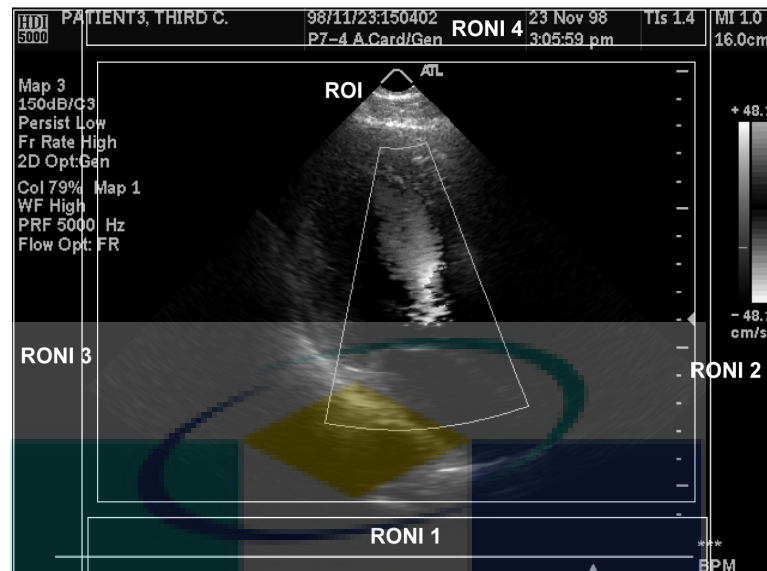


Figure 4.72: ROI of Sample 1 with an area of 480 x 360 pixels

4.8.5 Comparison

For the purpose of comparison, tamper localization and recovery scheme for medical images proposed by Osamah and Khoo (2011) which had been described earlier had been chosen due to data availability and the functions similarity of the watermark scheme. The comparison details are shown in Table 4.7. The data provided by Osamah and Khoo (2011) were based on experiment performed on an ultrasound image. The comparison shows that the proposed TALLOR and TALLOR-RS scheme are better in terms of embedding capacity and PSNR. The tamper localization accuracy of the proposed schemes are at one pixel as compare to 16 x 16 pixels by the scheme developed by Osamah and Khoo(2011). Both schemes also have the most accurate tamper localization when being compared to other schemes reviewed in the literature. The recovered ROI produced by the proposed schemes are also better in terms of quality due to exact recovery achieved where else only approximate recovery was achieved by Osamah and Khoo (2011). Proposed schemes maintain the originality of the ROI where watermark is embedded in the RONI. By contrast, scheme proposed by Osamah and Khoo (2011) embeds part of the watermark in the ROI which needs to be reversed later on. The schemes proposed by Osamah and Khoo (2011) and Chiang et al. (2008) have

possible problems in tamper detection as average intensities were used in authenticating the ROI. Some tampering may not be detected. This issue was discussed in details in section 3.7.2. The issue was not encountered by the proposed schemes where the exact pixel values and CRC were used to authenticate the ROI.

As for the comparison between TALLOR and TALLOR-RS scheme, both had performed equally well. The advantage of the TALLOR-RS scheme over the TALLOR scheme is the reduction in the tamper localization and recovery processing time by using a ROI segmentation and multilevel authentication. The usage of simple algorithm in the watermarking embedding and authentication process is the strength of the TALLOR scheme over the TALLOR-RS scheme.

Table 4.7: Comparison of the proposed TALLOR and TALLOR-RS scheme

	Osamah and Khoo (2011)*	TALLOR (Sample 1)	TALLOR-RS (Sample 1)
Image size	576 x 768,8 bit	640 x 480,8 bit	640 x 480,8 bit
Watermark size(bits)	136780	180960	177008
Embedding capacity (bits per pixel)**	0.31	0.59	0.58
PSNR(dB)	36.7	48.1	48.3
Localization accuracy(pixel)	16 x 16	1	1
ROI Recovery	Approximate	Exact	Exact

*Ultrasound image

**Embedding capacity = Watermark size/image size

4.9 CONCLUSION

In this chapter, a tamper localization and lossless recovery (TALLOR) scheme that uses compression technique was proposed. An enhanced version, that uses ROI segmentation, TALLOR-RS was also proposed. The ROI segmentation and multilevel authentication method used in TALLOR-RS managed to reduce the tamper localization and recovery average processing time by approximately 53%. This significantly reduces the waiting time for the user of an image to allow the image to be authenticated and recovered.

The average PSNR of the watermarked images for both schemes is at 48.3 dB and 48.2 dB for TALLOR and TALLOR-RS respectively. The proposed schemes have a 100% success rate for tamper localization and recovery. Exact recovery was achieved where the tampered area was recovered using the exact pixel values originated from the ROI. The RONI was successfully authenticated using hash function. The comparison results show that the proposed schemes performed better than the compared scheme. The proposed schemes have the option to allow lossy JPEG compression to be applied if necessary. The issues of the implementation of proposed schemes in PACS will be address in the next chapter.

CHAPTER 5

MEDICAL IMAGE WATERMARKING IN PACS

5.1 INTRODUCTION

This chapter consists of section 5.2 that presents the purpose of this chapter. The research methodology used in this chapter is in section 5.3. Section 5.4 presents an effectiveness test done on R-TLR and TALLOR /TALLOR-RS schemes in PACS. Section 5.5 proposes a design of a watermark embedder and image authenticator (WEIA). Section 5.6 presents the infrastructure modification and workflow needed to allow WEIA operate in a PACS. Section 5.7 evaluates and discusses the proposed items. Lastly, section 5.8 concludes the chapter.

5.2 OVERVIEW

In the previous two chapters, R-TLR and TALLOR/TALLOR-RS watermarking schemes that uses different techniques were proposed. In order for the watermarking schemes to be effectively implemented in real operation environment, the following questions needs to be answered:

- does R-TLR and TALLOR/TALLOR-RS schemes work effectively in PACS

- how can medical images be watermarked and authenticated efficiently
- where should the watermarking process take place in PACS
- what are the workflows involved

Currently there are no standards or guidelines on the implementation of watermarking process in medical images and in PACS. This chapter attempts to provide possible answers to the questions raised.

5.3 RESEARCH METHODOLOGY

In order to test the effectiveness of R-TLR and TALLOR/TALLOR-RS in PACS, Dcm4che2 toolkit will be used. It is an open source implementation of the DICOM standard. It provides implementation of the standard in creation, transmission, and storage of digital medical image and report data. It consists of 20 stand alone utilities developed using the Java programming language. The *Dcmsnd* utility acts as a Storage Service Class User (SCU) that sends DICOM objects to a Storage Service Class Provider (SCP). It loads composite DICOM objects from specified DICOM files or a directory structure and sends them to the specified remote AET (Application Entity). The *Dcmrcv* utility will run a DICOM server listening on the specified port for incoming association requests. Both *Dcmsnd* and *Dcmrcv* will form a simulated PACS environment. The samples that used in this testing are identical with the samples used in chapter 3 and 4. The effectiveness of the watermarking schemes is tested by comparing the tamper localization and recovery rate.

In order to design the application needed to facilitate the implementation of watermarking in PACS, requirements and specifications needs is identified. Infrastructures needed to allow image watermarking to operate in a PACS were identified along with necessary workflows.

5.4 PACS TEST

At the time of writing, there were no documented feasibility studies done on the effectiveness of watermarking in Picture Archiving and Communications System (PACS). Medical images need to be watermarked before they are permanently stored. Watermarked images need to be stored in a DICOM compliant format and may need to be transmitted across the network before reaching their storage location. The watermark embedded in the image needs to be proven effective when the image is stored in the DICOM format and after the image is being transmitted across the PACS. R-TLR and TALLOR/TALLOR-RS schemes are considered as fragile watermark. Any processing before the transmission such as compression may destroy the watermark or the watermarked image will be considered as tampered in the authentication process.

Two individual computers were used to form a simulated PACS. One of the computers, denoted as Comp_A executed the *Dcmsnd* application to act as a SCU. The other computer denoted as Comp_B executed the *Dcmrcv* application to act as a SCP where it listens to incoming request for association. The ultrasound images were watermarked in Comp_A and saved in DICOM format. The watermarked images were transmitted to Comp_B in a local area network using physical connection. The watermarked images were then tampered and recovered.

Both R-TLR and TALLOR/TALLOR-RS schemes were tested using the same images and tampering method used in chapter 3 and 4. The results of this test were consistent with the results produced in chapter 3 and 4. It is concluded that both schemes are proven effective in a simulated PACS.

5.5 WATERMARK EMBEDDER AND IMAGE AUTHENTICATOR(WEIA)

In this section, a design of a watermark embedder and image authenticator (WEIA) application is proposed. This application functions as the interface between the end users and the proposed watermarking schemes. R-TLR and TALLOR/TALLOR-RS watermarking schemes were developed using MATLAB. It is crucial that the

watermarking algorithms and codes remain hidden for the purpose of security. To achieve this, MATLAB Builder JA can be used where Java classes can be created by encrypting MATLAB functions and generating Java wrapper around them. An interface based on Java can be created to enable user to interact with the Java classes. Dcm4che2 toolkit will be used to allow the application to send and receive objects within a PACS. The next section describes the requirements and design of WEIA.

5.5.1 Requirements

The application must be able to operate in a DICOM compliant PACS where it is able to receive and send medical images from and to another AET within the PACS. The main function of this application is to embed watermark into selected images and authenticate images by using the embedded watermark. The authorized user will be able to choose which watermark scheme to be use. WEIA will check the type of watermark embedded before the authentication process begins. WEIA has the following requirements:

i. R-TLR

The R-TLR watermark can be embedded using WEIA. User will be notified whether an image had been tampered in the authentication process and tampered image will be recovered. WEIA allows the user to reverse the R-TLR watermark by request and the procedures are as shown in Figure 5.1. WEIA will notify the user if the RONI had been tampered and the possibility that the restored image would not be authentic. In this situation, the user has the option to proceed.

ii. TALLOR/TALLOR-RS

If this module is selected, in the embedding process, WEIA will allow the user to define a ROI or multiple ROIs. WEIA will calculate the space available in the RONI based on the output from the compression process. In the event where RONI space is not sufficient, the user will be asked to redefine a smaller ROI. The user may choose lossy compression to be applied if a large ROI is needed. The process is shown in Figure 5.2.

In the recovery process, the RONI will be authenticated and WEIA will notify user of any possible tampering in the RONI that may cause the failure in recovery of the tampered. The user has the option to proceed with the recovery process of the tampered image

iii. Image Transmission

WEIA allows the user to send and receive images from another AET within the PACS in this module. Images can be sent to another AET by providing the name, host name and port number. WEIA is always on standby mode to receive any incoming transmission. The user will be able to store incoming files at selected locations.

iv. Others

WEIA will have minimum security features such as login access to prevent unauthorized access. Other than operating in a Windows platform, WEIA can be modified to allow web based operation and modules can be accessed by multiple computers which will be explained in the workflow section.

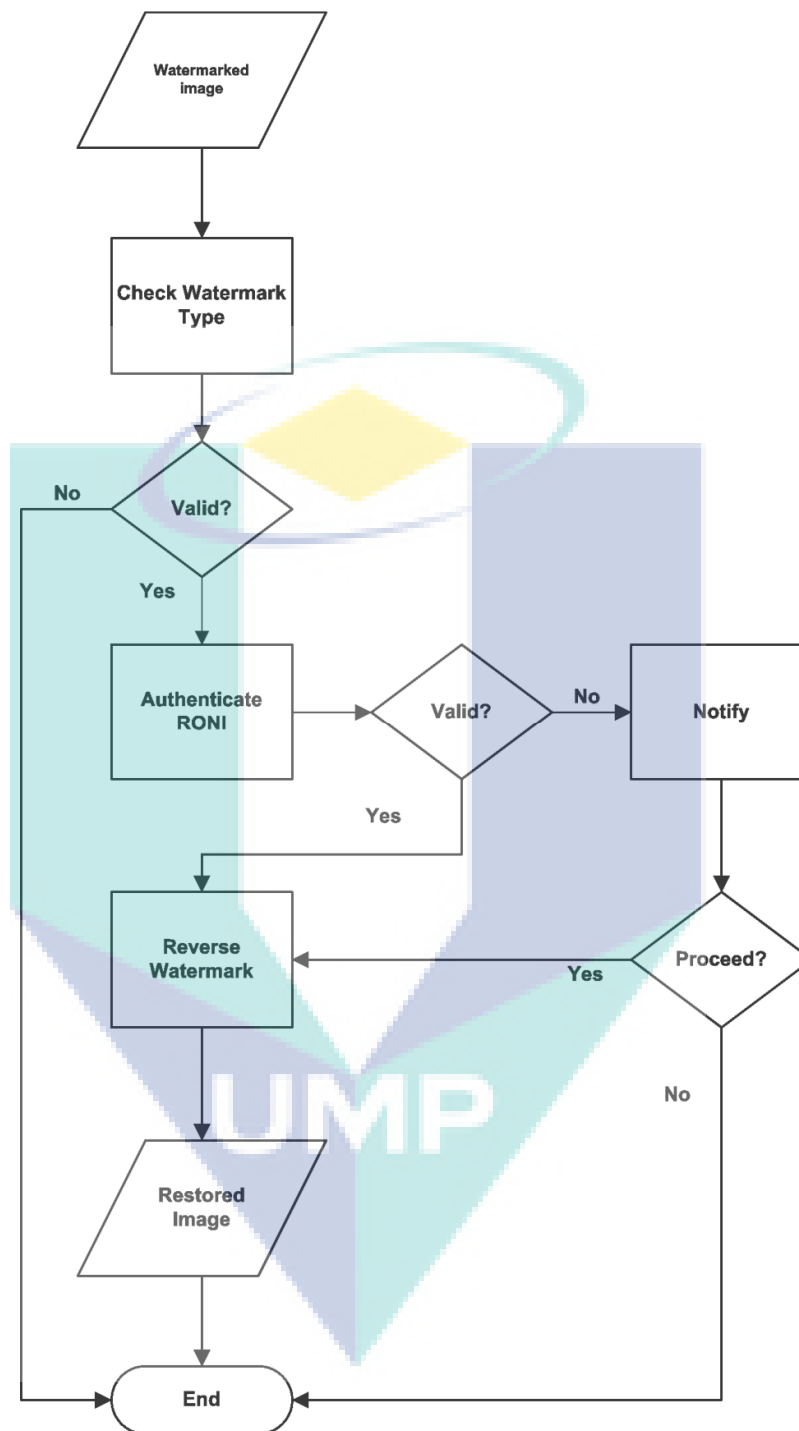


Figure 5.1: Reverse watermark process for R-TLR using WEIA

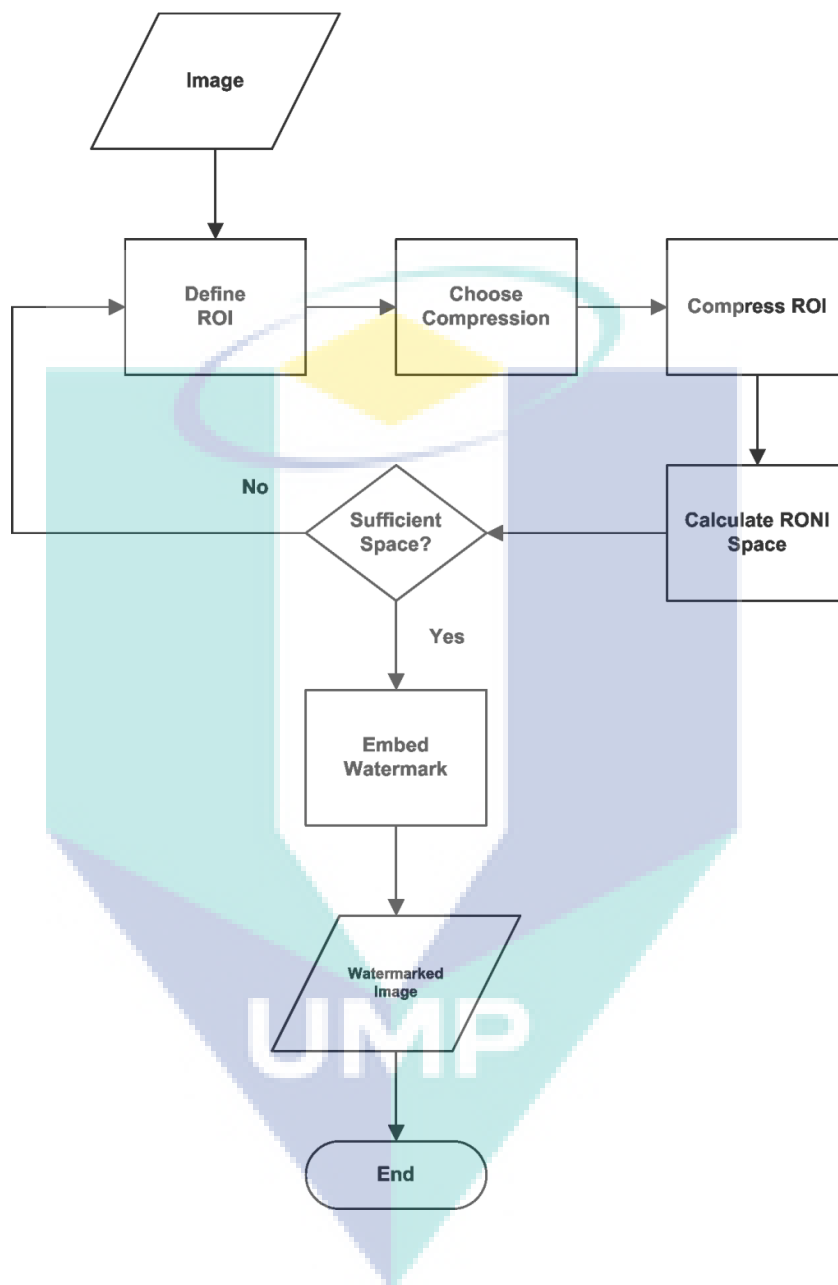


Figure 5.2: Embedding process of TALLOR/TALLOR-RS using WEIA

5.5.2 User Interface Design

In this section, the user interface design for WEIA will be shown and described. Figure 5.3 shows the first section of the WEIA. User can select different functions by selecting from the tab panels.

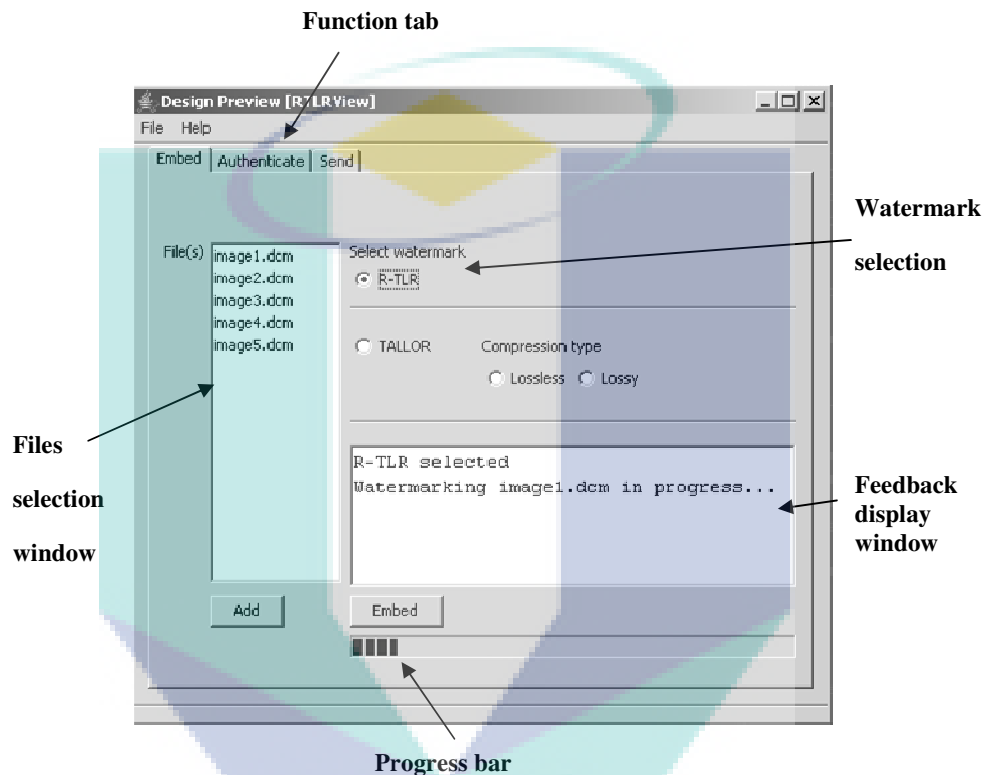


Figure 5.3: Embedding function for WEIA

i. Embed

In the embedding function panel, one or more files can be selected and selected files will be displayed in the files selection windows. It consists of options for watermark selection. The progress of the embedding process can be seen in the feedback window and progress bar. If TALLOR/TALLOR-RS watermark had been selected, further options are given to choose the type of compression to be applied. A pop up panel displaying the selected image to be compressed will appear as soon as the embed button is pressed as shown in Figure 5.4. The user will be able to define the ROI.

The ROI will be compressed and the feedback display window will notify the user the status of compression.

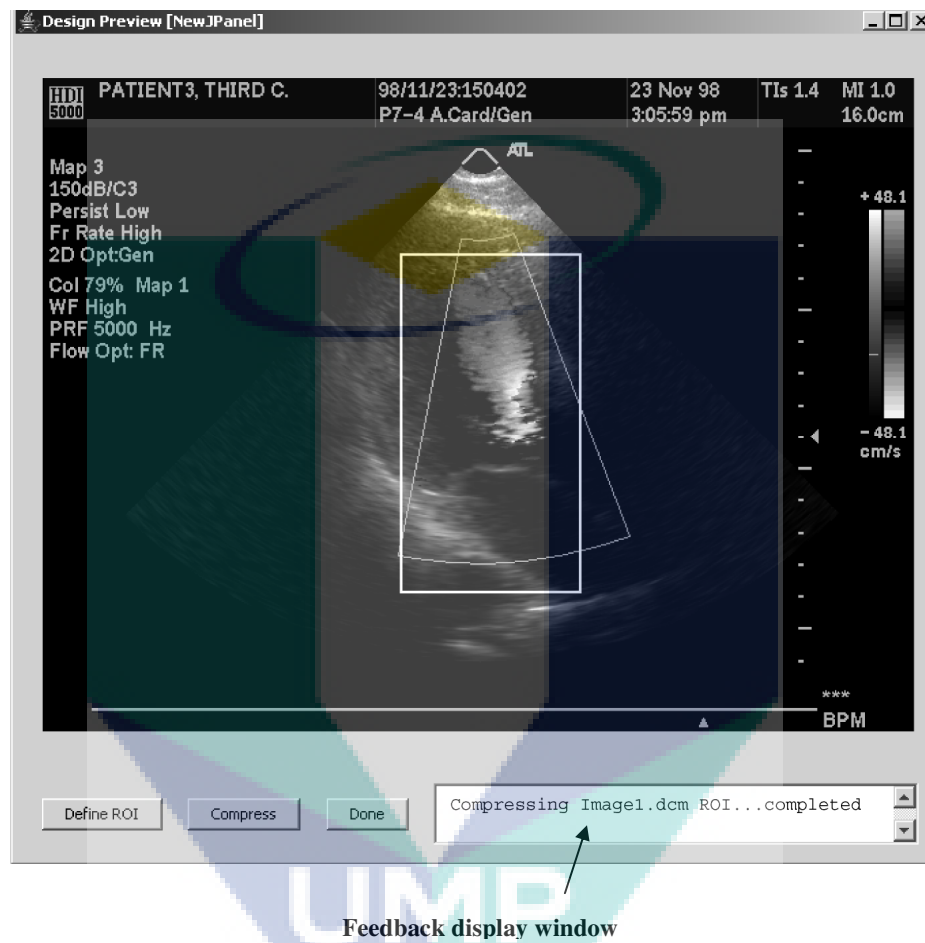


Figure 5.4: Panel to allow user to define ROI for compression

ii. Authenticate

For authentication purposes, one or more files may be selected for processing. The user may choose the reverse watermark option for R-TLR. Information on the processing status can be seen in the feedback display window as shown in Figure 5.5.

iii. Send

Figure 5.6 shows the panel for transmitting images to another AET within the PACS. It consists of files selections window and fields for destination information.

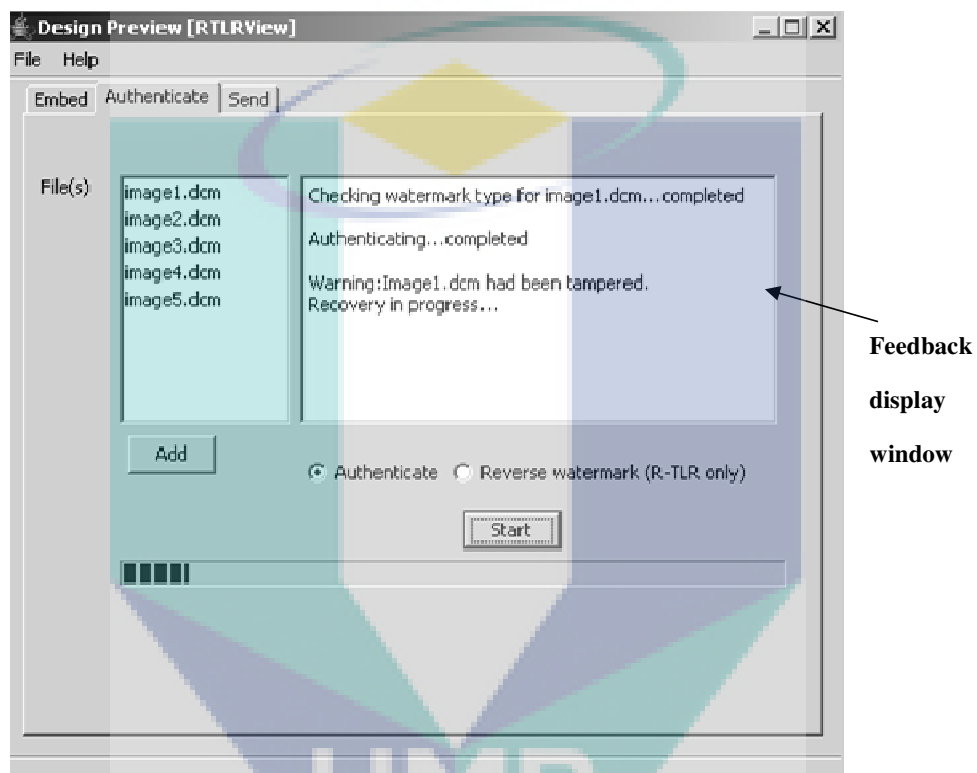


Figure 5.5: Authentication panel displaying processing in progress

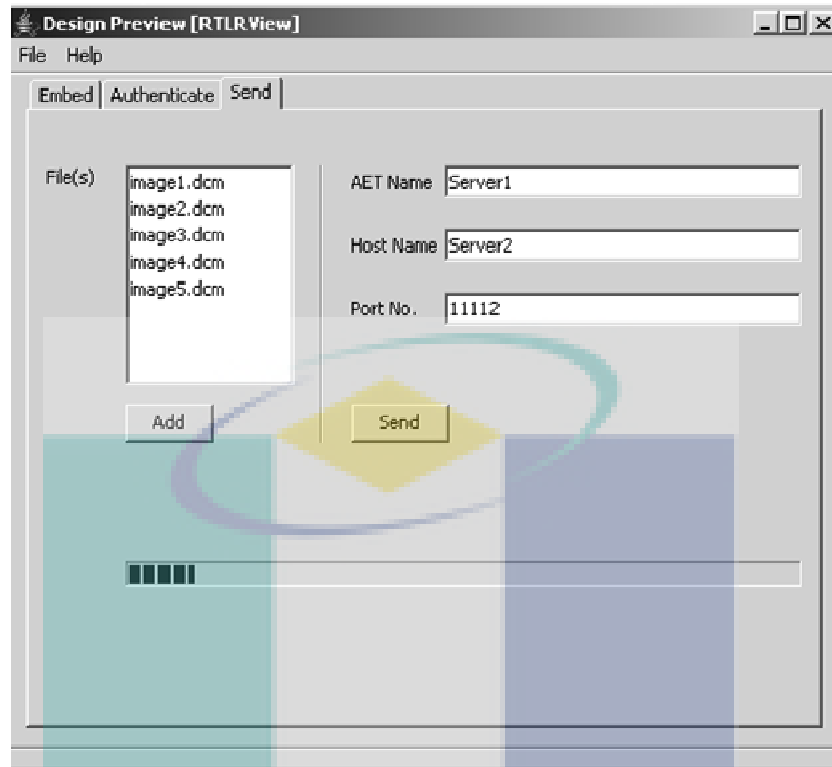


Figure 5.6: WEIA panel for image transmission

5.6 WEIA IN PACS

In order to allow WEIA to operate in a PACS, modification to the existing infrastructure is needed. In this section, additional components needed and their functions are proposed. The workflows for WEIA need to be defined.

5.6.1 Authentication Server

An authentication server is proposed to the existing PACS infrastructure as described by Huang (2004) in Figure 2.2. This server will be located in between the acquisition server and PACS server as shown in Figure 5.7. A dedicated server allows the watermarking process to be executed without affecting the operation of other servers. The authentication server can be bypassed when watermarking is not needed. Authentication server has the following functions:

- receive images from the acquisition server
- execute WEIA for image watermarking
- transmit watermarked images to PACS Server using WEIA
- process request for image authentication using WEIA

5.6.2 Watermark Embedding

The process of watermark embedding will be done using WEIA in the authentication server as shown in Figure 5.7. Medical images should be watermarked before being stored in the PACS server. Images from the acquisition will be received by the authentication server where the watermarking embedding will be done using WEIA. Watermarked images will be transmitted to PACS server for storage.

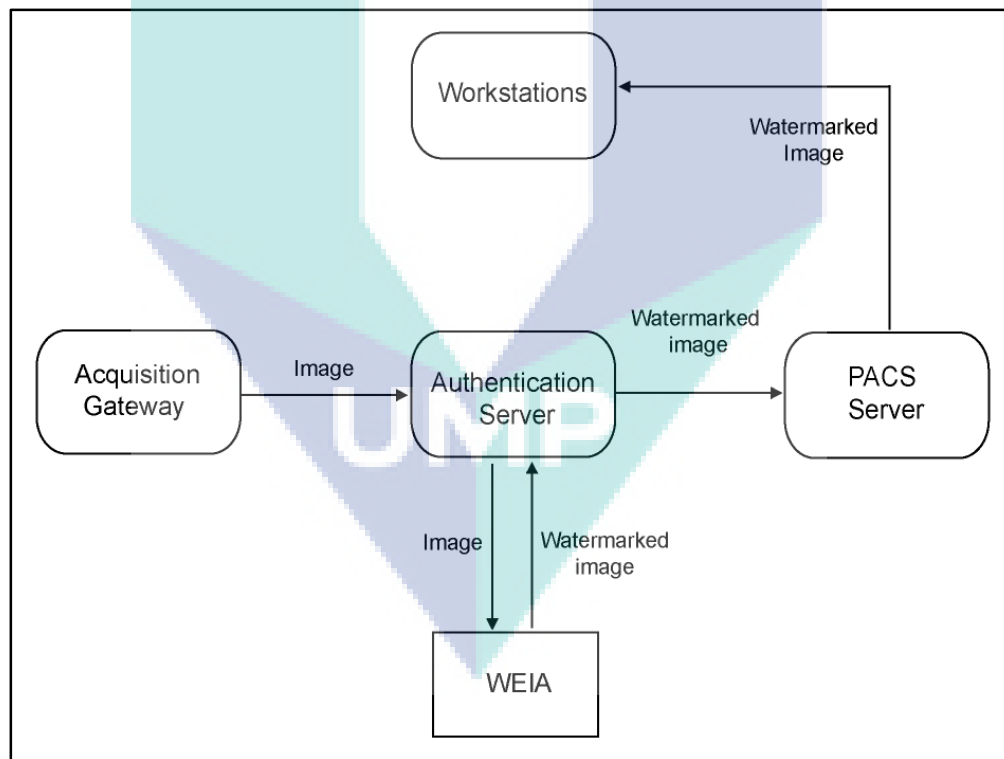


Figure 5.7: Authentication server and workflow for the watermark embedding process

5.6.3 Image Authentication

Image authentication procedure can be divided into two possible modes as follows.

i. Centralized

The process of authentication takes place in the authentication server as shown in Figure 5.8. A workstation can request for authentication for a particular image. Authentication server will retrieve targeted image from the PACS server. WEIA residing in the authentication server authenticates the requested image and the outcome of the authentication process will be delivered to the workstation in the form of notifications or recovered image. In the event where a particular image is found tampered, the recovered version of the image will be sent to PACS server for updating.

ii. Decentralized

The second mode is where the authentication process may be assigned to the workstations. This mode reduces the burden of the authentication server with the condition that the workstations have the computing resources needed to perform the job. Since WEIA can be operated in a web based environment, the authentication module can be accessed from the workstations by using a web browser. In the event where any image is found tampered, notification will sent to the PACS server for further action.

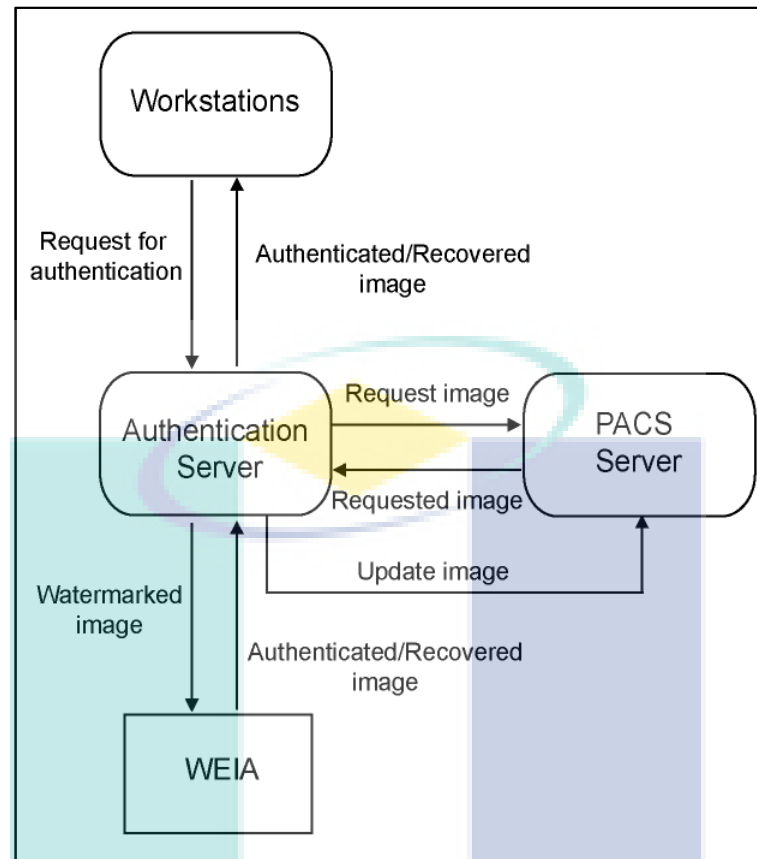


Figure 5.8: Centralized image authentication workflow

5.6.4 Reverse Watermark

The watermarking process can be reversed in two possible modes as following.

i. Centralized

Figure 5.9 shows the centralized process for image restoration by watermark removal. A workstation may make requests to remove the watermark from a particular image. WEIA in the authentication server will request the targeted image from the PACS server and restore the image to its original state. The restored image will be sent to the workstation. The original watermarked image in the PACS server will not be updated with the restored version but can be if necessary.

ii. Decentralized

The workstations can be granted access to remove watermark from a particular image similar to the authentication process. The workstations may remove the watermark from images for viewing purposes but updating in the PACS server will be forbidden.

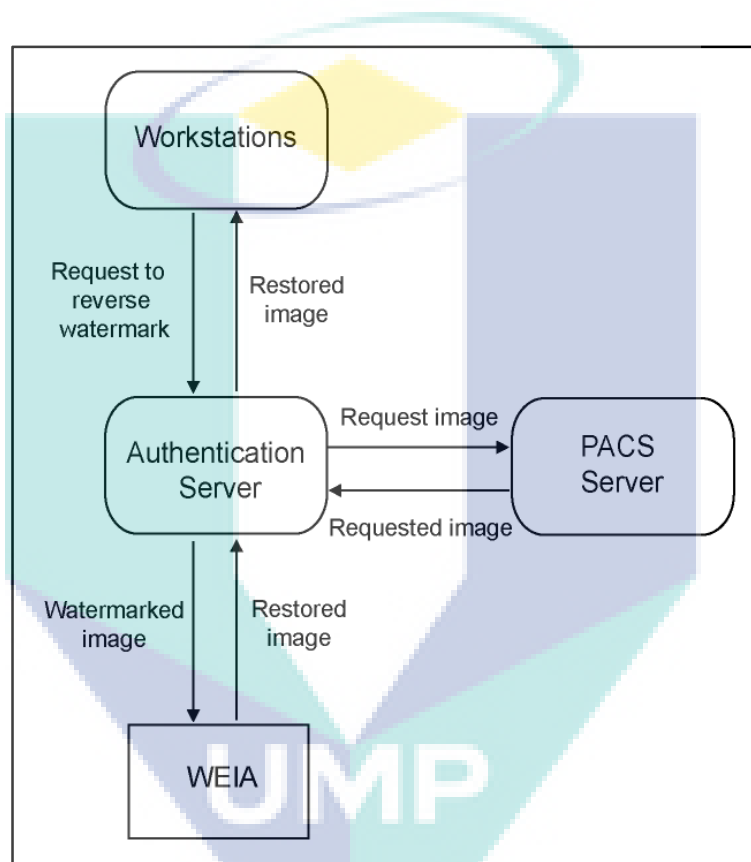


Figure 5.9: Centralized reverse watermark workflow

5.7 EVALUATION AND DISCUSSION

R-TLR and TALLOR/TALLOR-RS schemes were tested in a simulated PACS. The results proved that the watermarking schemes remain effective in a PACS environment. This test was done using transmission thru physical cable. In a real operation environment, there may be wireless connections being used. Further test is needed using this type of connection.

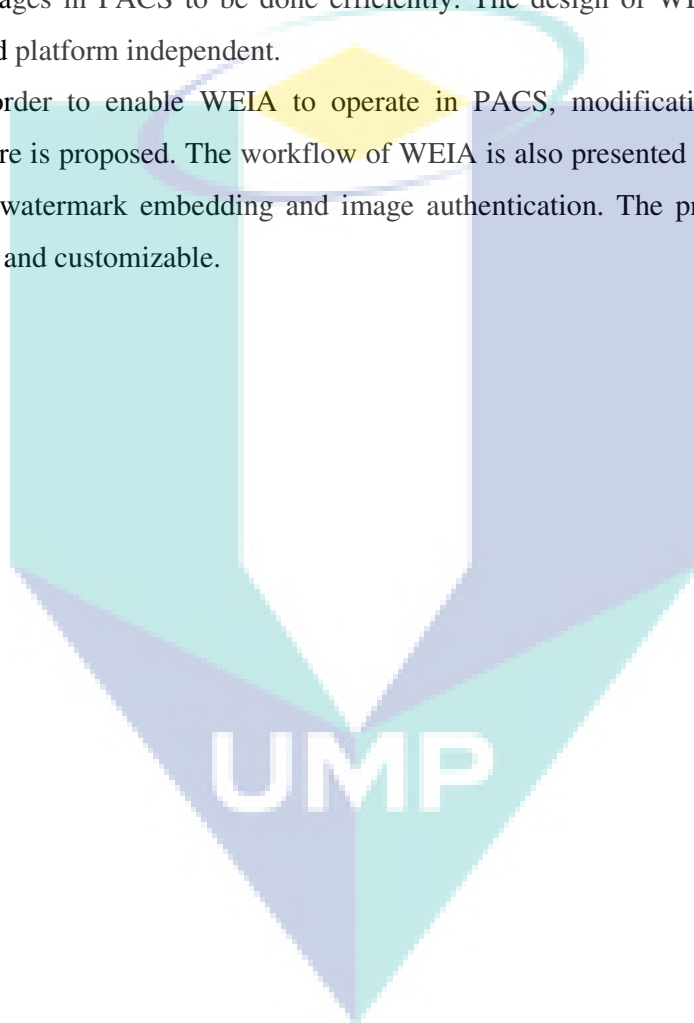
WEIA had been designed with the purpose to facilitate the watermarking and authentication of images in PACS. It functions as the interface between the user and the watermark algorithm. The watermarking codes remains secured and hidden as it had been encrypted before being converted to Java class files. The design has graphic user interface to allow easy usage. The design is also scalable and platform independent. Other hash functions to be applied by R-TLR and TALLOR/TALLOR-RS can be added as options to the interface. Future use of other types of watermarking schemes for other types of modalities can be added into WEIA. It can operate from any platform where a web browser is available such as Windows, Linux or even Android operating system. Remote access of WEIA is also possible with necessary security measures and policies in place. WEIA can be operated in a centralized and decentralized setting or even in a standalone computer. WEIA can be operated in the acquisition server if computer resource such as processing power is available. The proposed workflows can be customized to suits the needs of the health institutions. It is also simpler as there are no keys management involved compare to the workflows proposed by Huang (2004) and Tan et al. (2011).

The operation of WEIA is not fully automated and it needs human involvements in the watermarking embedding and authentication process. In a situation where thousands of images need to be processed, the process of watermarking and authentication can be tedious for the person in charge. WEIA can be modified to allow the process of embedding to be fully automated where a default watermark algorithm is set and the received images are automatically watermarked before being sent for storage.

5.8 CONCLUSION

In this chapter, R-TLR and TALLOR/TALLOR-RS were subjected to effectiveness test in a simulated PACS and both schemes had passed the test. The design of WEIA is also proposed. WEIA acts an interface between the user and the watermarking algorithm. It allows the process of watermarking and authentication of medical images in PACS to be done efficiently. The design of WEIA is easy to use, scalable and platform independent.

In order to enable WEIA to operate in PACS, modification to the existing infrastructure is proposed. The workflow of WEIA is also presented where it covers the process of watermark embedding and image authentication. The proposed workflows are flexible and customizable.



CHAPTER 6

CONCLUSIONS AND FUTURE WORK

6.1 INTRODUCTION

This chapter consists of section 6.2 that lists the contributions and limitations of the thesis. Section 6.3 describes the future work based on the outcome of this thesis. Lastly, section 6.4 summarizes the chapter.

6.2 CONTRIBUTIONS AND LIMITATIONS

The contributions of this thesis are as listed below:

- In chapter 3, a reversible tamper localization and recovery (R-TLR) watermarking scheme is proposed. This scheme uses the characteristic of the ultrasound images to allow the watermarking process to be reversed. The method used to allow reversibility is simple and requires very minimum processing. The original bits were embedded in the RONI. The watermarked images have a high average PSNR of 53.9 dB. The success rate of the tamper localization and recovery is close to 100%. The watermarked image has a low distortion level and can be reversed to its original state.
- A tamper localization and lossless recovery (TALLOR) scheme was proposed in chapter 4. An enhanced scheme, tamper localization and lossless recovery with ROI segmentation (TALLOR-RS) was also proposed. The ROI segmentation and multilevel authentication method used in TALLOR-RS managed to reduce the tamper localization and recovery average processing time by approximately

53%. Both schemes do not need to be reversed as the watermark is being embedded in the RONI. The average PSNR of the watermarked images for both schemes is at 48.3 dB and 48.2 dB for TALLOR and TALLOR-RS respectively. A high PSNR indicates low distortion in the watermarked image, which is an important factor to be considered in medical image watermarking. The proposed schemes have 100% success rate for tamper localization and recovery which is better than the R-TLR scheme. The tampered area can be exactly recovered using information stored with lossless compression. The recovered image may be used for clinical diagnoses due to its high quality. Both schemes also have the most accurate tamper localization of one pixel when being compared to other schemes reviewed in the literature. Lossy compression may also be applied to achieve higher compression ratio. The RONI can be authenticated using hash function. Both schemes are superior in terms of capacity, PSNR, localization accuracy, recovery quality and simplicity when being compared to the scheme produced by Osamah and Khoo (2011).

- In chapter 5, R-TLR and TALLOR/TALLOR-RS were subjected to effectiveness test in a PACS. It was concluded that the proposed schemes remains effective in a simulated PACS. The design of a watermark embedder and image authenticator (WEIA) is also proposed. WEIA acts as the interface between the user and the proposed watermarking schemes, namely R-TLR and TALLOR/TALLOR-RS. The advantages of WEIA are ease of use, scalable and platform independent.
- In the same chapter, a new infrastructure and its workflows are proposed. It allows WEIA to operate in a PACS. The proposed workflows are flexible and customizable due to the portability of WEIA.

The summary of the research contribution is shown in Table 6.1.

The limitations are as below:

- R-TLR and TALLOR/TALLOR-RS were developed specifically for ultrasound images.

- R-TLR and TALLOR/TALLOR-RS watermark may not survive geometry attack and some removal attack such as compression. Any compression of the watermarked image will be considered as tampering.
- The authentication and parity bit check used in R-TLR may be ineffective under certain conditions.
- TALLOR/TALLOR-RS were tested on standard computer. It might not reflect the real processing time.
- WEIA and its workflow is only a design and have not been tested.
- WEIA is not fully automated and human involvement is needed to operate it.

6.3 FUTURE WORK

Further improvements can be made based on the outcomes from this thesis. Below are some possible future works:

- Applying R-TLR and TALLOR/TALLOR-RS to images from other modalities such as magnetic resonance imaging.
- Medical images have acceptable compression format such as JPEG. Further research can be done to ensure R-TLR and TALLOR/TALLOR-RS scheme robust against image compression.
- Other types of lossless compression can be tested with TALLOR/TALLOR-RS such as arithmetic encoding, Huffman code and JPEG2000.
- Further study is needed to determine whether recovered tampered ROI in a lossy compressed image can be used for diagnoses purposes.
- WEIA can be further developed into a working application and be tested. The processing time needed by R-TLR and TALLOR/TALLOR-RS can be tested on real operation hardware with better computing capability.
- Further improvements can be made to allow WEIA to be operated with minimum human involvements.

6.4 SUMMARY

This chapter presented the research summary as well as the contributions and limitations of the research. The outcome from this research has opened up some possibilities for future work. Based on the results and evaluations, the objectives of this research outlined in chapter 1 had been achieved.

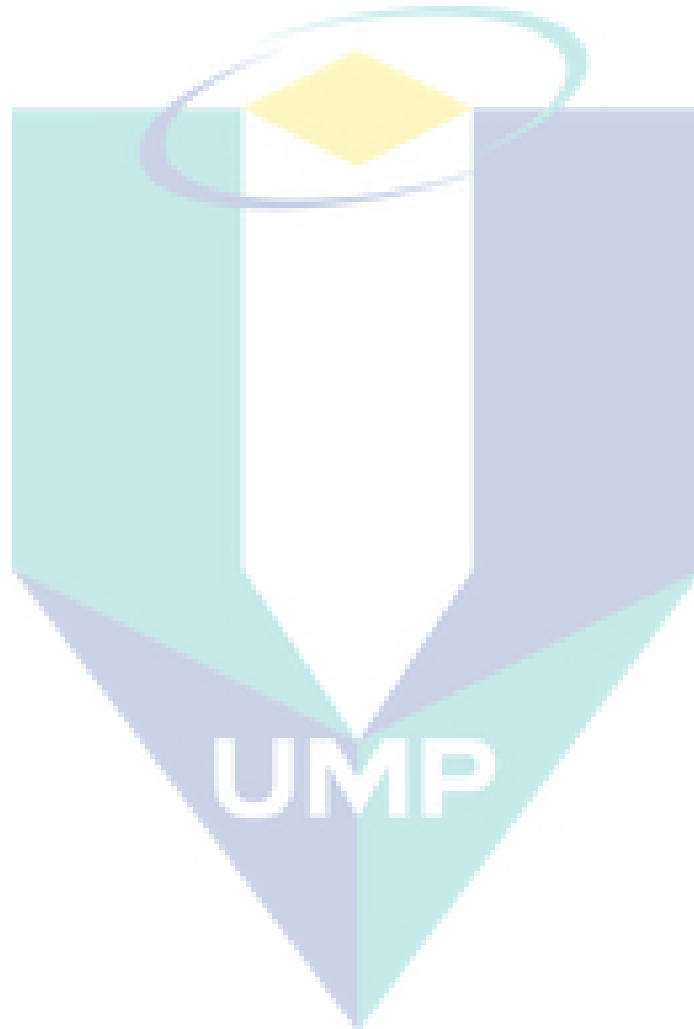


Table 6.1: Summary of research contributions

Research Process	Contribution
Theory	<ul style="list-style-type: none"> • The usage of ROI and RONI to allow watermark reversibility. • The application of compression to achieve exact or lossless recovery. • The usage of ROI segmentation and multilevel authentication to reduce processing time. • The usage of application to facilitate watermarking process in PACS.
Practice	<ul style="list-style-type: none"> • Development of a reversible tamper localization and recovery scheme. • Development of a tamper localization and lossless recovery scheme. • Designing an application with its needed infrastructure and workflows to facilitate watermarking process in PACS.
Outcome	<ul style="list-style-type: none"> • Reversible Tamper Localization and Recovery(R-TLR). • Tamper Localization and Lossless Recovery (TALLOR). • Tamper Localization and Lossless Recovery with ROI Segmentation (TALLOR-RS). • Watermark Embedder and Image Authenticator(WEIA) with its needed infrastructure and workflows.

REFERENCES

- Caldelli, R., Filippini, F. and Barni, M. 2006. Joint near-lossless compression and watermarking of still images for authentication and tamper localization. *Signal Processing: Image Communication*. **21**:890-903.
- Caldelli, R., Filippini, F. and Becaralli, R. 2010. Reversible watermarking techniques: An overview and a classification. *EURASIP Journal on Information Security*. **2010**:1-19.
- Cao, F., Huang, H.K and Zhou, X.Q. 2003. Medical image security in a HIPAA mandated PACS environment. *Computerized Medical Imaging and Graphics*. **27**:185-196.
- Chang, C.C., Lin, C.Y. and Wang, Y.Z. 2006. New image steganographic methods using run-length approach. *Information Sciences*. **176** (2006): 3393-3408.
- Chiang, K., Chang, K., Chang, R. and Yen, H. 2008. Tamper detection and restoring system for medical images using wavelet-based reversible data embedding. *Journal of Digital Imaging*. **21**(1):77-90
- Coatrieux, G., Lamard, M., Daccache, W., Puentes, W. and Roux, C. 2005. A low distortion and reversible watermark: application to angiographic images of the retina. *Proceedings of the 27th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp.2224-2227.
- Coatrieux, G. and Lecornu, L. 2006. A review of image watermarking applications in healthcare. *Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp.4691-4694.
- Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y. and Collorec, R. 2000. Relevance of watermarking in medical imaging. *Proceedings IEEE EMBS International Conference on the Information Technology Applications in Biomedicine*, pp.250-255.

Cobb, Michael 2006. Using steganography for securing data, not concealing it(online).<http://searchsecurity.techtarget.com/tip/Using-steganography-for-securing-data-not-concealing-it>(4 September 2010).

Cox, I.J., Miller, M.L. and Bloom, J.A. 2002. *Digital Watermarking*, San Francisco: Morgan Kaufmann.

Cox, I.J., Miller, M.L. and Linnartz, J.M.G 1999. A review of watermarking principles and practices. *IEEE Digital Signal Processing for Multimedia Systems*.**1**:461-482.

Department of Health and Human Services, USA 2007. Security Standards: Technical Safeguards. *HIPAA Security Series*. **2**(4):1-17.

Emad, E. A. Abdallah 2009. Robust digital watermarking technique for multimedia protection. P.h.D. Thesis. Concordia University.

Fawad, Ahmed, Siyal, M.Y. and Vali U.A. 2010. A secure and robust hash-based scheme for image authentication. *Signal Processing*. **90**(2010): 1456-1470.

Fontani, M., Rosa, A.D., Caldelli, R., Filippini, F., Piva, A., Consalvo, M. and Cappellini, V. 2010. Reversible watermarking for image integrity verification in hierarchical PACS. *Proceedings of the 12th ACM workshop on Multimedia and security*, pp. 161-168.

Friedman, G.L. 1993. The trustworthy digital camera: restoring credibility to the photographic image. *IEEE Transactions on Consumer Electronics*. **39**(4):905-910.

Fridrich, J., Goljan, M. and Rui Du 2002. Lossless data embedding—New paradigm in digital watermarking. *EURASIP Journal on Applied Signal Processing*. **2002**(2): 185-196.

Guo, X and Zhuang, T. 2009. Lossless watermarking for verifying the integrity of medical images with tamper localization. *Journal of Digital Imaging*. **22**(6): 620-628.

Huang, H.K. 2004. *PACS And Imaging Informatics-Basic Principles And Applications*, New Jersey: John Wiley & Sons, pp.409-430.

Jasni, Mohd. Zain and Abdul, R.M Fauzi 2006. Medical image watermarking with tamper detection and recovery. *Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp.3270-3273.

Jasni, Mohd. Zain, Abdul, R.M Fauzi and Azian, A. Aziz 2006. Clinical evaluation of watermarked medical images. *Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp.5459-5462.

Kundu, M.K and Das, S. 2010. Lossless ROI medical image watermarking technique with enhance security and high payload embedding. *Proceedings of the International Conference on Pattern Recognition*, pp.1457-1460.

Kutter, M. and Hartung, F. 1999. Introduction to watermarking techniques. *Information Techniques for Steganography and Digital Watermarking*.1:97-119.

Lappin, Y. 2006, Reuters admits altering Beirut photo, YnetNews. 8 January: 1.

Li, Mingyan, Poovendran, R. and Narayanan, S. 2005. Protecting patient privacy against unauthorized release of medical images in a group communication environment. *Computerized Medical Imaging and Graphics*.29:367-383.

Lin , Rey-Sern and Hu, Shang-Wen 2009. A Modified Run-length Image Data Hiding for High Embedding Capacity. *Proceedings of the 5th International Conference on Information Assurance and Security*, pp. 673-676.

Liu, Tong and Qiu, Zheng-ding 2002. The survey of digital watermarking-based image authentication techniques. *Proceedings of the 6th International Conference on Signal Processing*, pp. 1556- 1559.

Lou, D.C., Hu, M.C. and Liu, J.L. 2009. Multiple layer data hiding scheme for medical images. *Computer Standards and Interfaces*. 31(2009): 329-335.

Macq, B. and Dewey, F.1999.Trusted headers for medical images, *DFG VIII-DII Watermarking Workshop*.

Mcevoy, F.J. and Svalastoga, E. 2007. Security of patient and study data associated with DICOM images when transferred using compact disc media. *Journal of Digital Imaging*. **22**(1):65-70.

Meerwald, P. and Uhl, A. 2001. Watermark security via wavelet filter parameterization. *Proceedings of the International Conference on Image Processing*, pp.1027-1030.

Navas, K.A, Sasikumar, M., Sreevidya, S. 2007. A benchmark for medical image watermarking. *Proceedings of the 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services*, pp. 237-240.

Ni, Z., Y. Q. Shi, N. Ansari, W. Su, Q. Sun and X. Lin 2008. Robust lossless image data hiding designed for semi-fragile image authentication. *IEEE Transactions on Circuits and Systems for Video Technology*, **18**(4): 497–509.

Osamah, M. and Khoo, B. E. 2011. Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. *Journal of Digital Imaging*, **24**(1):114-125.

Piva, A. Bartolini, F. and Caldelli, R. 2005. Self-recovery authentication of images in the DWT domain, *International Journal of Image and Graphics*. **5** (1):149–165.

Pizzi, R. 2008. Medical records security at risk. *Healthcare IT News*. 3 June: 1.

Schutze, B., Kroll, M., Geisbe, T. and Filler, T.J. 2004. Patient data security in the DICOM standard. *European Journal of Radiology*. **51**(2004): 286-289.

Shih, F. Y. and Wu, Y-Ta 2005. Robust watermarking and compression for medical images based on genetic algorithms. *Journal of Information Sciences*. **175**(3):200-216.

Smitha, B. and Navas, K.A. 2007. Spatial domain-High capacity data hiding in ROI images. *Proceedings of the International Conference on Signal Processing, Communications and Networking*, pp.528-533.

Song, C., Sudirman, S., Merabti, M. and Llewellyn-Jones, D. 2010. Analysis of Digital Image Watermark Attacks. *Proceedings of the 7th IEEE Consumers Communications and Networking Conference*, pp. 1-5.

Tan, C.K., Ng, C., Xu, X., Poh C.L., Yong, L. G. and Sheah, K. 2011. Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability. *Journal of Digital Imaging*, **24**(3):528-540.

Tian, Jun 2003. Reversible data embedding using a difference expansion. *IEEE Transactions on Circuits and Systems for Video Technology*.**13** (8):890- 896.

Vleeschouwer, C. de, J. F. Delaigle, and B. Macq 2006. Circular interpretation of bijective transformations in lossless watermarking for media asset management. *IEEE Transactions on Circuits and Systems for Video Technology*.**16**(11):1423–1429.

Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J.J. and Su, J.K. 2001. Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. *IEEE Communications Magazine*.**39**(8):118-126.

Wakatani, A. 2002. Digital watermarking for ROI medical images by using compressed signature image, *Proceedings of the 35th Hawaii International Conference on System Sciences*, pp.2043-2048

Wang, X.Y, Feng, D.G., Lai X.J. and Yu, H.B. 2004. Collisions for hash functions MD4, MD5 HAVAL-128 and RIPEMD. Cryptology ePrint Archive Report.

Weng, S., Zhao, Y. P., Jeng-Shyang and Ni, R. 2007. A novel high-capacity reversible watermarking scheme. *Proceedings of the IEEE International Conference on Multimedia and Expo*, pp.631-634.

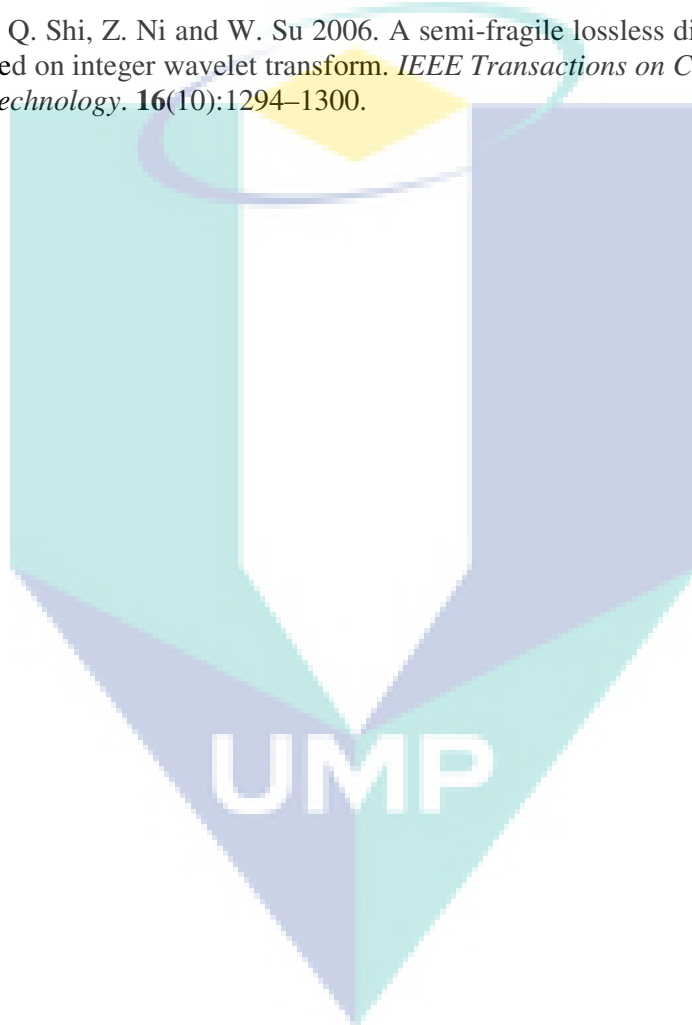
Wu, X. 2007. Reversible semi-fragile watermarking based on histogram shifting of integer wavelet coefficients. *Proceedings of Inaugural IEEE-IES Digital EcoSystems and Technologies Conference*, pp. 501–505,

Wu, J.H.K, Chang, Ruey-Feng, Chen,Chii-Jen, Wang,Ching-Lin, Kuo, Ta-Hsun, Moon, Woo Kyung and Che, Dar-Ren 2008. Tamper detection and recovery for medical images using near-lossless information hiding technique. *Journal of Digital Imaging*. **21**(1):59-76.

Yang, Bian, Schmucker, M., Xiamu Niu, Busch, C. and Shenghe Sun 2004. Reversible image watermarking by histogram modification for integer DCT coefficients. *Proceedings of the IEEE 6th Workshop on Multimedia Signal Processing*, pp. 143- 146.

Yang, Chun-Wei and Shen, Jau-Ji 2010. Recover the tampered image based on VQ indexing. *Signal Processing*, **90**(1):331-343.

Zou, D., Y. Q. Shi, Z. Ni and W. Su 2006. A semi-fragile lossless digital watermarking scheme based on integer wavelet transform. *IEEE Transactions on Circuits and Systems for Video Technology*. **16**(10):1294–1300.



APPENDIX A

PUBLICATIONS

The following publications had been made out of this thesis.

Journals

Siau-Chuin Liew and Jasni Mohamad Zain, “Reversible Tamper Localization and Recovery Watermarking Scheme with Secure Hash”, *European Journal of Scientific Research*, vol 49, issue 2, pp.249-264, 2011, EuroJournals, London, U.K.

Siau-Chuin Liew and Jasni Mohamad Zain, “Experiment of Tamper Detection and Recovery Watermarking in PACS”, *Journal of Computer Science*, vol 6, issue 7, pp.794-799, 2010, Science Publications, New York, USA.

Conferences

Siau-Chuin Liew and Jasni Mohamad Zain, “Tamper Localization and Lossless Recovery Watermarking Scheme With ROI Segmentation”, In submission for 4th International Congress for Image and Signal Processing (CISP’11), 15-17 Oct. 2011, Shanghai, China.

Siau-Chuin Liew and Jasni Mohamad Zain, “Tamper Localization and Lossless Recovery Watermarking Scheme”, Accepted for 2nd International Conference On Software Engineering and Computer Systems (ICSECS2011), 27-29 June. 2011, Kuantan, Pahang, Malaysia.

Siau-Chuin Liew, Siau-Way Liew and Jasni Mohamad Zain, “Reversible Medical Image Watermarking For Tamper Detection And Recovery With Run Length Encoding Compression”, *Proceedings of International Conference on Signal and Image Processing (ICSIP2010)*, 25-27 Aug 2010, Singapore.

Siau-Chuin Liew and Jasni Mohamad Zain, “Reversible Medical Image Watermarking For Tamper Detection and Recovery”, *Proceedings of 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT2010)*, 9-11 July 2010, Chengdu, China.

Siau-Chuin Liew and Jasni Mohamad Zain, “Experiment of Tamper Detection and Recovery Watermarking in PACS”, *Proceedings of the IACSIT 2nd International Conference On Computer Research And Development (ICCRD2010)*, 7-10 May 2010, Kuala Lumpur, Malaysia.

Siau-Chuin Liew and Jasni Mohamad Zain, “Watermark Embedder and Detector for Medical Images: The Requirements and Design”, Proceedings of the IACSIT 2nd International Conference on Computer Research and Development (ICCRD2010), 7-10 May 2010, Kuala Lumpur, Malaysia.

Siau-Chuin Liew and Jasni Mohamad Zain, “A Review of Medical Image Watermarking Schemes”, Proceedings of International Conference On Software Engineering and Computer Systems (ICSECS2009), 19-21 Oct. 2009, Kuantan, Pahang, Malaysia.

Siau-Chuin Liew and Jasni Mohamad Zain, “A Review of Medical Image Watermarking and Its Implementations”, Proceedings of Malaysian Technical Universities Conference on Engineering and Technology (MUCEET2009), 20-22 June 2009, Kuantan, Pahang, Malaysia.

