Multi-layered Semantic-based Watermarking for Medical Images

Jack Lau Sing Ik

Master of Engineering
2013

Supervisor:   A/Prof. Dennis Wong
Co-supervisor:   Sim Kwan Yong
Abstract

Digital watermarking has drawn great attention in data integrity control and authentication lately. From the medical media perspective, one of the main applications of digital watermarking includes the embedding of patient’s information into the medical media itself for the purpose of protecting the integrity of the medical media, as well as providing controls to the use of the media in the picture archiving and communication system (PACS). However, not all parts of a medical media carry the same level of importance for diagnosis and prognosis’ purposes, such as digital mammograms which we are focusing on in this thesis. Furthermore, with the finite embedding capacity of the media, it is a constant challenge for one to retain the visual quality of the important regions for ensuring accurate diagnosis purposes. Therefore, there is a need for these regions of higher importance to be “free” from visible watermarking distortion. Besides, it is also advantageous to implement some automated selection methods for these regions to eliminate the need of manual selection.

In this thesis, we have implemented a reversible watermarking scheme which is capable of large capacity of data hiding, automated medical importance regions definition, running authentication to assure the integrity of the important regions on the medical images, and original image restoration. As an empirical study, we have implemented five image segmentation methods to define the segments of the image; block average, pixel classification, improve moment-preserving thresholding (IMPT), saliency map, and IMPT on saliency map.

Furthermore, we conducted an analysis on both the watermarking techniques and the regions definition methods proposed in order to determine a robust combination of the above suitable for general scenarios. Besides, our scheme is capable of authentication on the protected image and verifying its integrity. The purpose for this feature is to prevent the unauthorized modification on the image which might leads to a medical misjudgment. Whenever a watermarked image is
defined authentic, the scheme is capable of reconstructing the original image from the watermarked image such that medical diagnosis and prognosis process can be carried out.

In addition to the above, a security analysis on the scheme is carried out to compare the proposed scheme with existing watermarking schemes with similar features and purposes. For real-time deployment, the embedding process of the proposed scheme is ported to the Compute Unified Device Architecture (CUDA) and an execution speed increase of up to 4× is observed from the empirical results.
Acknowledgement

This master research study is made possible through the support of Ministry of Science, Technology and Innovation (MOSTI) through an E-Science Grant (Grant No: 01-02-14-SF0005), and a research studentship from Swinburne University of Technology, Sarawak Campus.

First, I would like to take thank my principal coordinating supervisor, A/Prof. M. L. Dennis Wong. His advices and reminders helped me out in keeping my research focused and on track. If it were not for his patience and guidance, I would not have completed this thesis. My gratitude also goes to Mr. Sim Kwan Yong, my co-supervisor, who pointed me to related research directions at early stages of this research work.

For my time as a postgraduate student at Swinburne Sarawak, I would like to thank three persons. First, I would like to thank Professor Anatoli Vakhguelt, for all the supports I have received from, while he was the Head of School of Engineering, Computing, and Science. Secondly, I would like to thank Professor Clem Kuek (now with Curtin University Malaysia) for the helps he offered on my matter of postgraduate’s duty with the school, during his term of service at the research office. Thirdly, I would like to thank A/Prof. Wallace Wong, who kept my postgraduate’s candidature on track.

Besides, I would like to thank Dr. Goi Bok Min from Universiti Tunku Abdul Rahman and Ling Huo Chong from Multimedia University (Cyberjaya Campus) for collaborating with our team on this research project under the MOSTI grant mentioned above. Moreover, I would like to thank Chong Nguan Soon for his helps given for the programming work for Chapter 6.

On a more personal note, I would like to thank God for keeping me sane, balance, and motivated throughout the last two years. Next, I would like to thank
my friends who always show their support and encouragement. Last, but certainly not least, I would like to thank my family for always being there for me.
Declaration

I hereby declare that this thesis is my own work and effort and that it has not been submitted anywhere for any award.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone’s copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices.

Signature: __________________________  Date:  25 September 2013
Name:  Jack Lau Sing Ik
Table of Contents

Multi-layered Semantic-based Watermarking for Medical Images ...................... i
Abstract ......................................................................................................................... i
Acknowledgement ...................................................................................................... iii
Declaration .................................................................................................................. v
Table of Contents ........................................................................................................ vi

Chapter 1: Introduction and Motivation ................................................................. 1
  1.1 Background ...................................................................................................... 1
  1.2 Problem statement ...................................................................................... 2
  1.3 Preliminaries ............................................................................................... 3
    1.3.1 Digital watermarking ........................................................................... 4
    1.3.2 Review of applied watermarking techniques ...................................... 9
    1.3.3 Biomedical image segmentation (high-level semantic) .................... 9
    1.3.4 Visual quality assessment ................................................................. 12
    1.3.5 Existing issues ............................................................................... 13
    1.3.6 Significance of research ................................................................. 13
  1.4 Thesis contribution ...................................................................................... 14
  1.5 Thesis Organization ................................................................................... 15

Chapter 2: A Conceptual Framework of Digital Mammograms Watermarking ... 16
  2.1 Digital mammograms authentication scheme ............................................ 16
    2.1.1 Embedding procedure ...................................................................... 17
    2.1.2 Decoding procedure ...................................................................... 18
  2.2 Methodology ............................................................................................... 21
Chapter 2: Work evaluations

2.2.1 Watermarking techniques .................................................................21

2.3 Work evaluations ..................................................................................26

2.3.1 Watermarked mammograms .............................................................26

2.3.2 Capability of the scheme on mammograms of different class of abnormality .........................................................27

Chapter 3: Automated ROI Definition Methods ..................................................30

3.1 Block averaging ....................................................................................30

3.1.1 Choosing a suitable threshold ..........................................................31

3.2 Pixel classification ..................................................................................32

3.2.1 Fuzzy Inference System .................................................................33

3.2.2 Post-Processing .................................................................................35

3.3 Improved moment-preserving thresholding (IMPT) ................................35

3.4 Selective visual attention-driven model (saliency map) ........................35

3.5 IMPT on saliency map ...........................................................................36

3.6 Experimental results of the scheme with different ROI definition methods

3.6.1 ROI definition ....................................................................................37

3.6.2 Capability of different ROI definition methods on different class of mammograms .........................................................38

3.6.3 Overall performance of different ROI definition methods ..........43

3.6.4 Different embedding thresholds with different ROI definition methods 45

Chapter 4: Boundary Region Preserving .........................................................51

4.1 Defining boundary region .......................................................................51

4.1.1 Block-based scan .............................................................................52

4.2 Experimental results .............................................................................53
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.1 ROI defined using different ROI definition methods</td>
<td>54</td>
</tr>
<tr>
<td>4.2.2 Defining boundary region</td>
<td>57</td>
</tr>
<tr>
<td>4.2.3 Evaluation of the scheme with boundary region preserving</td>
<td>61</td>
</tr>
<tr>
<td>Chapter 5: Security Analysis</td>
<td>63</td>
</tr>
<tr>
<td>5.1 Security attacks</td>
<td>63</td>
</tr>
<tr>
<td>5.2 Attacks on the Yeung-Mintzer fragile watermarking technique</td>
<td>64</td>
</tr>
<tr>
<td>5.3 Security evaluation proposed by H. Kubota and K. Iwamura</td>
<td>67</td>
</tr>
<tr>
<td>5.4 Security evaluation of proposed scheme using the nine attacks</td>
<td>69</td>
</tr>
<tr>
<td>5.5 Evaluation results</td>
<td>73</td>
</tr>
<tr>
<td>Chapter 6: Real Time Implementation</td>
<td>74</td>
</tr>
<tr>
<td>6.1 Real world adaptive model</td>
<td>74</td>
</tr>
<tr>
<td>6.2 Scheme used in CUDA accelerated approach</td>
<td>74</td>
</tr>
<tr>
<td>6.3 CUDA acceleration</td>
<td>76</td>
</tr>
<tr>
<td>6.4 Experimental results</td>
<td>78</td>
</tr>
<tr>
<td>6.4.1 ROI Selection</td>
<td>78</td>
</tr>
<tr>
<td>6.4.2 Visual Quality</td>
<td>79</td>
</tr>
<tr>
<td>6.4.3 Speed Enhancement between CPU and GPU</td>
<td>80</td>
</tr>
<tr>
<td>6.5 Summary</td>
<td>81</td>
</tr>
<tr>
<td>Chapter 7: Conclusion</td>
<td>83</td>
</tr>
<tr>
<td>7.1 Summary</td>
<td>83</td>
</tr>
<tr>
<td>7.2 Further studies</td>
<td>84</td>
</tr>
<tr>
<td>References</td>
<td>86</td>
</tr>
<tr>
<td>List of Publications</td>
<td>95</td>
</tr>
</tbody>
</table>
List of Figures

Figure 1 Definition of mid-band coefficients. ............................................................. 8

Figure 2. Flowchart of the Embedding Process......................................................... 19

Figure 3 Flowchart of the Decoding Process ............................................................ 20

Figure 4 (a) Original mammogram, (b) Watermarked mammogram. PSNR = 47.01dB, SSIM = 0.9822. .......................................................................................... 26

Figure 5 (a) Original mammogram, (b) Watermarked mammogram. PSNR = 45.45dB, SSIM = 0.9802. .......................................................................................... 27

Figure 6 (a)-(g) Automatic ROI definition using block average method with different threshold, T_{BA}. ........................................................................................................... 32

Figure 7 (a) Original, (b) Mean, (c) Deviation, (d) Edginess.................................... 33

Figure 8 (a) The shapes of the linguistic variables \( v \), (b) The shapes of the linguistic variables \( e \). .................................................................................................................. 34

Figure 9 (a) ROI measured from FIS, (b) ROI after ASF ....................................... 35

Figure 10 Graph of average values of embedding capacity (bpp) of different ROI definition methods. ........................................................................................................... 43

Figure 11 Graph of average values of PSNR (dB) of different ROI definition methods......................................................................................................................... 44

Figure 12 Graph of average values of SSIM of different ROI definition methods... 44

Figure 13 Graph of dependency of average of embedding capacity (bpp) on average of PSNR (dB) using block average. ................................................................. 47

Figure 14 Graph of dependency of average of embedding capacity (bpp) on average of PSNR (dB) using pixels classification. ....................................................... 47

Figure 15 Graph of dependency of average of embedding capacity (bpp) on average of PSNR (dB) using IMPT................................................................. 48
Figure 16 Graph of dependency of average of embedding capacity (bpp) on average of PSNR (dB) using saliency map.

Figure 17 Defining surrounding pixels to boundary pixels.

Figure 18 Horizontal scan.

Figure 19 (a) Test image, (b) ROI map, (c) Boundary region.

Figure 20 Input mammograms.

Figure 21 ROI map defined using block average method.

Figure 22 ROI map defined using pixel classification method.

Figure 23 ROI map defined using IMPT method.

Figure 24 ROI map defined using saliency map method.

Figure 25 ROI map defined using IMPT on saliency map method.

Figure 26 Boundary region (block average) with SR = 10.

Figure 27 Boundary region (PixC) with SR = 7.

Figure 28 Boundary region (IMPT) with SR = 11.

Figure 29 Boundary region (SVAM) with SR = 10.

Figure 30 Boundary region (IMPT on saliency map) with SR = 8.

Figure 31 (a) Watermarked image. (b) Attacked image.

Figure 32 (a) Watermarked image. (b) Reduced size watermarked image.

Figure 33 (a) Original image. (b) Watermarked image.

Figure 34 (a) Watermarked image. (b) Attacked image.

Figure 35 (a) Watermarked image. (b) Atacked image.

Figure 36 Original input mammogram.
List of Tables

Table 1 - ROI defined using selective visual attention-driven model method. ........28
Table 2 - Evaluation on different ROI definition methods ........................................37
Table 3 (a)-(e) Embedding Results for 7 Mammograms of Different Class of Abnormality Present ..................................................................................................42
Table 4 Watermarking assessments for input mammograms A .........................61
Table 5 Watermarking assessments for input mammograms B .........................62
Table 6 Evaluation results of the security analysis between schemes .................73
Table 7 Embedding results for 7 mammograms of different class of abnormality present .................................................................................................................................79
Table 8 Processing time for the embedding process of the scheme .................81
Chapter 1: Introduction and Motivation

1.1 Background

Approximately 70,000 new cases of cancer were diagnosed among Malaysians in Peninsular Malaysia between 2003 and 2005, according to a report released in early 2008. Among which, breast cancer was the most frequently diagnosed form of cancer which accounted for approximately 31.1% of all newly diagnosed cancer cases during that period [1].

Despite from this, about 30% to 50% of cancer cases can be prevented by undergoing regular checks for early detection and seek the right treatment when necessary. With the increasing number of cases diagnosed over the year, the importance of early detection and treatment is becoming more apparent. Recently, computerized analysis of mammograms is playing a pivoted role of providing an emulated secondary opinion [2] to improve the consistency by providing a standardized approach to mammogram interpretation and hence increasing the detection sensitivity [3]. However, with the advancement of media editing software, one can now modify these digital mammograms at ease without causing noticeable perceptual difference. Unauthorized modification will lead to inaccurate diagnosis and the results will remain doubtful when the digital mammograms are to be submitted as evidence for insurance claims. Hence, there is a need for an image authentication process to ensure the content of the image [4].

In order to protect the authenticity of the digital mammograms, we propose a digital mammograms authentication scheme to prevent unauthorized alteration. The scheme uses reversible watermarking techniques to protect the integrity of the selected regions, i.e. the region of interest (ROI). Furthermore, the original content (the digital mammograms) can be reconstructed provided no attack has taken place. As the background of the mammogram does not provide much useful information for clinical activities, the scheme is focusing on protecting the integrity of the ROI
only. Furthermore, the scheme provides more embedding capacity by hiding the data into region of non-interest (RONI) as well.

We proposed an automated ROI selection algorithm to the scheme in order to highlight the medical important regions (semantic regions) from the digital mammograms. The automated ROI definition methods also mitigate the need of performing manual definition for the ROI and to minimize the chance of excluding portions of ROI by mistake. Also, the scheme preserves a region at the boundary of ROI and RONI from watermarking process in order for the decoder to define the exact ROI used in embedding the watermark. Moreover, the proposed scheme uses a multi-layered watermarking technique to allow the information collected from a region to be embedded or used in the other region. Firstly, a ROI map is created to serve as a reference to the following watermarking processes. Then, it follows by the second layer of watermarking process to collect the information needed from the digital mammograms from both the ROI and RONI. Finally, the watermarking processes to watermark the ROI and RONI take place.

1.2 Problem statement

The objective for this master thesis is to implement a reversible digital watermarking scheme capable of contents authentication of the digital mammograms, hiding patient’s data into the image, protecting the integrity of the digital mammograms, and medically readable watermarked image.

The thesis also includes the goal to define the medically important region automatically on the digital mammograms. Any random regions on the mammograms will not carry the same level of importance in terms of medical information. Therefore, there is a need to locate the medically important regions for its content protection. With the region of interest (ROI) defined, the scheme can avoid to create extra unnecessary data for authentication purpose hence providing larger data hiding capacity for patient’s data and also increasing the visual quality of the ROI.

The goals of this research work are to:
• Design and implement a content authentication scheme using reversible watermarking for digital mammograms mentioned above.

• Investigate means for automatic definition of ROI for digital mammograms.

• Analyze and compare the automatic ROI definition methods.

• Embed related medical information into the host images and eliminate the need to attach the metadata to the images.

1.3 Preliminaries

In the recent decades, many research works on the application of digital watermarking in the medical field have been reported. The advances of technology have brought lots of convenience to the modern healthcare today. Undeniably, the introduction of information technology into the medical field has elevated the healthcare system from conventional paper filing to the electronic patient record (EPR). Furthermore, the advent of multimedia has introduced a modern service in medical field, namely telemedicine. Hospital Information System (HIS), and its special cases of Radiology Information System (RIS), Picture Archiving and Communication System (PACS) forms the information infrastructure of modern healthcare [1], providing new means to store, access and distribute medical data.

There are concomitant risks together with the benefits for EPR and personal documents being accessible in an open network. Therefore, there is a need to measure the security level on the network and protocols must be made in the medical information systems. Hence, digital watermarking has been introduced as a way to protect the contents circulating in the open network.

In the development of medical media watermarking, one would normally segment a medical media into its ROI and RONI. The ROI refers to the critical and information bearing region and RONI referred to the otherwise. Al-Qershi et al. [10] proposed a scheme capable of hiding patient’s data, verifying authenticity of ROI, localize tampered areas, and recover the tampered areas within the ROI. The scheme uses original difference expansion (DE) technique proposed by Tian [9] to
watermark the image in RONI and modified DE technique developed by Guo et al.[11].

The scheme proposed two watermarks to be generated. The first watermark consists of compressed patient’s data which concatenated with compressed hash message for the ROI. The second watermark consists of the compressed version of the original ROI, average values of each block of 16 x 16 pixels of the ROI, the embedding map of ROI (EM1), the embedding map of RONI (EM2), the original LSB of changeable pairs in RONI (B), and the LSB of pixels of a predefined secret area in RONI used to embed side information necessary to initiate watermark extraction (Orgbits).

The ROI to be divided into quads and the first watermark is to be embedded into ROI using modified DE technique proposed by Guo et al. While the second watermark to be embedded into RONI using Tian’s DE technique [9]. The information defining the ROI is to be embedded into the secret area of RONI using Tian’s technique too.

1.3.1 Digital watermarking

Digital watermarking is originally devoted to digital rights management in multimedia [12]. Digital watermarking is the process of embedding a message about an image, audio clip, video clip, or other work of digital media within that work itself [13]. The idea of watermarking began in 1990 [14], and the field of digital watermarking only started to gain its popularity as a research topic in the latter half of the 1990s [15], [16]. Digital watermarking has drawn interest from healthcare domain for two of its elements, data hiding and information protection [17].

Generally, digital watermarking is divided into two types, namely visible watermarking and invisible watermarking. In visible watermarking, the information can be viewed on top of the picture or video. Typically, the visible watermarking applies in identifying the ownership of the media [18]-[22]. For example, television broadcaster adds its logo to the corner of the transmitted video. In invisible
watermarking, the message or the information is hidden into audio, video or image through embedding process. The message hidden cannot be seen perceptually. Invisible watermarking is important in many applications such as to copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. Digital watermarking is an application of steganography, where two parties or more communicate through a secret message embedded into the digital signal. A general watermarking framework (invisible watermarking) is defined as \( \Omega^* = (E, D, R, M, p_E, p_D, p_R) \);

\( E \) = the embedding function

\( D \) = detecting function

\( R \) = retrieval function

\( M \) = the message

Embedding parameters:

\( p_E \in P_E \) = the parameter set used for watermark embedding

\( p_D \in P_D \) = the detection parameters

\( p_R \in P_R \) = retrieval parameters

Each watermarking scheme may have different instances according to the values that the parameters may adopt. For example, a watermarking scheme \( \Omega \) will have an instance \( \Omega^* \) for a particular value of the parameter vectors. We only concern about the invisible watermarking in this research since the visible watermarking is not suitable to be applied in the scheme for content authentication. Hence, we only discuss the invisible watermarking process in the rest of the thesis.

There are two common groups of watermarking techniques, the spatial domain techniques and the frequency domain techniques [21], [23]-[25]. Some examples for the spatial domain techniques are direct watermarking [26] and [27], recording the difference between randomly selected pairs of points [28], Tian’s
difference expansion [9], Alattar’s difference expansion of triplets [33], and Alattar’s
difference expansion of quads [35]. Whereas, some examples for the frequency
domain include Kallel et al DCT fragile watermarking [34], I. J. Cox et al spread
spectrum watermarking [29], X. G. Xia et al multi-resolution wavelet transform
based watermarking [25], and more DCT-based watermarking [23]-[24], [30]-[32].

**Spatial Domain Techniques**

The watermarking techniques applied in the schemes studied can be grouped into
two classes, spatial domain methods and transform domain methods [36]. The
spatial domain techniques embed the watermark into a cover work by modifying the
pixel values directly. The transform domain techniques transform the cover work
into frequency domain for watermark embedding. The transform domain techniques
give better robustness in comparison to the spatial domain techniques.

The most straightforward method of watermark embedding would be to
embed the watermark into the least significant bits (LSB) of the cover object [37],
[26], [27]. Given the extraordinarily high channel capacity of using the entire cover
for transmission in this method, a smaller object may be embedded multiple times.
Even if most of these were lost due to attacks, a single surviving watermark would
be considered a success. LSB substitution however despite its simplicity brings a
host of drawbacks. Although it may survive transformations such as cropping, any
addition of noise or lossy compression is likely to defeat the watermark. An even
better attack would be to simply set the LSB bits of each pixel to one fully defeating
the watermark with negligible impact on the cover object. Furthermore, once the
algorithm is discovered, an intermediate party could easily modify the embedded
watermark. LSB modification proves to be a simple and fairly powerful tool,
however lacks the basic robustness that watermarking applications require. Another
technique for watermark embedding is to exploit the correlation properties of
additive pseudorandom noise patterns as applied to an image [38]. A pseudo-
random noise (PN) pattern \( W(x, y) \) is added to the cover image \( I(x, y) \), according to
the Eq. 1.
\[ I_{w}(x,y) = I(x,y) + k \cdot W(x,y) \]  

In equation (1), \( k \) denotes a gain factor, and \( I_{w} \) denotes the resulting watermarked image. Increasing \( k \) increases the robustness of the watermark at the expense of the quality of the watermarked image. Rather than determining the values of the watermark from “blocks” in the spatial domain, we can employ code division multiple access (CDMA) spread-spectrum techniques to scatter each of the bits randomly throughout the cover image, increasing capacity and improving resistance to cropping [38]. To detect the watermark, each seed is used to generate its PN sequence, which is then correlated with the entire image. If the correlation is high, that bit in the watermark is set to “1”, otherwise a “0”. The process is then repeated for all the values of the watermark. CDMA improves on the robustness of the watermark significantly, but requires several orders more of calculation.

**Frequency Domain Techniques**

The frequency domain watermarking involves transformation techniques such as fast Fourier transform or the classic and still most popular domain for image processing, discrete cosine transform (DCT) [63]. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they have to avoid the most visual important parts of the image (low frequencies) and without over-exposing themselves to removal through compression and noise attacks (high frequencies). One such technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. To begin, we define the middle-band frequencies (\( F_{M} \)) of an 8x8 DCT block as shown below in Figure 1.
Figure 1 Definition of mid-band coefficients.

\( F_L \) is used to denote the lowest frequency components of the block, while \( F_H \) is used to denote the higher frequency components. \( F_M \) is chosen as the embedding region as to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image.

**Reversible and irreversible watermarking**

Reversible watermarking is a technique used in digital watermarking where the original contents can be recovered exactly provided nothing changed in the watermarked media. There are numbers of reversible watermarking developed [7]-[9]. The watermarked media (Work) usually suffers from distortions to the original signal. Some of these distortions create problems in some fields such as medical, astronomical, and military images. Hence, the ability of the reversible watermarking to reconstruct the original image during judgment to take the right decision is highly concerned. The reversible watermarking is an emerging field for content authentication of images where the authentication information (Hash) is embedded inside the image.

Irreversible watermarking is a technique where the original contents cannot be recovered from the Work. In general, irreversible watermarking more likely related to robust watermarking. In this research, we only focused on reversible watermarking.
1.3.2 Review of applied watermarking techniques

Reversible watermarking

Tian [9] first proposed to embed watermarks using Difference Expansion (DE) through an integer transform of pixel pairs. The pixel pairs can either be any two horizontal or vertical adjacent pixels, or any two pixels selected in a pre-defined pattern. The pre-defined pattern may be initialized through the use of a security key and hence providing greater security to the scheme. As the scheme embeds a single bit for every pairs of pixels, the embedding capacity is then 0.5 bits per pixels (bpp). Tian published a journal on this work later [61].

In an attempt to increase the embedding capacity, Alattar proposed a reversible watermarking scheme of color image [33]. The proposed method used spatial and spectral triplets of pixels to hide two bits of information. Spatial triplet is any three pixel values chosen from the same spectral, or color component. On the other hand, the spectral triplet is any three pixels chosen from different spectral components.

Soon after the triplet difference expansion method was proposed, Alattar devised a new difference expansion of quads (a group of four pixels) for reversible watermarking of color images [35]. This improved scheme hides three bits in the difference expansion of quads (4 pixels). The quad is formed from 4 pixel values chosen from four difference locations within the same color component. The simplest way of choosing the quads is to consider every 2x2 adjacent pixel values as quad. The maximum embedding capacity of the new quad DE scheme is computed to be 0.75 bpp. However, in practice we can expect a lower capacity as some quads may not be embeddable.

1.3.3 Biomedical image segmentation (high-level semantic)

Content-based image retrieval is a great technology that helps to organize picture archives by number of features (visual contents) extracted from the images. In the recent years, the region-based features have attracted more research interests [68]-[70]. Hence, the construction of image segmentation has attracted more attention as
it is a key step to acquire a region-based feature. However, the image segmentation technique has its limitation when confronting many image types. The accuracy to define the image segments differs from one image type to another. For example, an image segmentation algorithm is accurate on image segmentation for animal image might fail to show an accurate segmentation on scenery image.

Due to the semantic gap, designing the image segmentation techniques with relevance feedback based on the user participation in the application is desirable [72]-[73], [81]. Long-term relevance feedback learning is demanded to achieve higher accuracy of the image segmentation [74]. Furthermore, the result of relevance feedback can be used for multipoint query [75] or manifold learning [76]-[77].

Since there is no general algorithm which is suitable to define all types of image, the image segmentation techniques are often combined in order to suit the definition desired by different types of image [71]. S. Sapna Varshney et al suggested classifying the image segmentation techniques into four classes [71]: clustering methods, thresholding methods, edge-detection methods, and region-based methods.

In the development of bio-medical watermarking, one would normally segment a medical media into its ROI and RONI. The ROI refers to the critical and information bearing region and RONI referred to the otherwise. Al-Qershi et al. proposed a scheme capable of hiding patient’s data, verifying authenticity of ROI, localize tampered areas, and recover the tampered areas within the ROI [10]. The scheme adopted Tian’s DE technique to watermark the RONI and a modified DE technique developed by Guo et al. [11] in the ROI.

Al-Qershi et. al.’s scheme proposed two watermarks to be generated. First, a watermark consists of compressed patient’s data which was concatenated with a compressed hash generated from the ROI. Then, a second watermark consists of a compressed version of the ROI, the average values of individual blocks (16 x 16) of the ROI, the embedding map of ROI \((EM1)\), the embedding map of RONI \((EM2)\), the original LSB of changeable pairs in RONI (B), and the LSB of pixels of a predefined
secret area in RONI used to embed additional information require to initiate the watermark extraction process (*Orgbits*).

After the formation of the respective watermarks, the ROI was divided into quads and the first watermark was embedded into the ROI using modified DE technique proposed by Guo et al. While the second watermark to be embedded into RONI using Tian’s DE technique [9]. The information defining the ROI is to be embedded into the secret area of RONI using Tian’s technique too.

**Mammograms segmentation**

There have been several previous works done in mammogram segmentation. Some of these methods proposed to use thresholding [39], [78], [79], gradients [41], and modeling background region by using a polynomial [42], fuzzy analysis algorithm [43], or active contours [44].

Generally, methods to approach to image segmentation can be grouped into three classes: pixel-based methods, regional (continuity-based) methods, and edge-based methods. Pixel-based methods are the least powerful and particularly susceptible to noise, but at the lowest level of difficulty in implementation. The other two groups of classes approach the segmentation task with opposing behaviors: continuity-based methods search for similarities while the edge-based methods search for differences.

**Selective visual attention-driven model**

S. Feng *et al.* [45] proposed a selective visual attention-driven model (SVAM). The proposed SVAM to be applied in localized content-based image retrieval (CBIR) where the user is only interested in a portion of the image.

In the improved saliency map construction algorithm, the multi-scale contrast features (saliency map) is defined as a linear combination of contrasts in the Gaussian image pyramid. L. Itti et al. proposed that 9 pyramid levels are to be constructed to compute the contrast between different levels [46]. On the other hand, S. Feng et al. proposed to compute the contrast between 3 different levels only and achieved satisfying results validated empirically.
**Improved moment-preserving thresholding**

Chen et al. [47] proposed an Improved Moment-Preserving Thresholding (IMPT) method for image segmentation through thresholding. The IMPT method is an improved version of Tsai’s moment-preserving thresholding method [48]. I-P. Chen et al. said that Tsai’s method does not work well when the peaks of a histogram have a great size variation. The improvement is done to overcome the drawback of Tsai’s method.

Tsai’s method defines the threshold as the middle of density of the histogram. Whereas I-P. Chen et al. suggested defining the threshold as the middle of the neighboring edges of two isosceles triangles. The isosceles triangles are used to simulate shapes of peaks in the histogram.

**Classifier (Fuzzy logic) based segmentation**

M. Wirth et al. [43] proposed an algorithm for breast region segmentation using fuzzy reasoning. The algorithm proposed consists of morphological pre-processing step to suppress artifacts and accentuate the breast region of the digital mammograms. Then, the segmentation is done through a classifier (fuzzy rule-based algorithm) to classify the breast tissue region.

**1.3.4 Visual quality assessment**

There are many techniques published up to date to assess the perceptual image quality between the distorted image and a reference image. Peak signal-to-noise ratio (PSNR) is the ratio between the reference signal and the distortion signal in an image, or in other words, ratio between the reference signal and the corrupting noise that affects the fidelity of its representation. The PSNR is given in decibels. In visual quality assessment, the higher value of PSNR meaning the quality of the distorted image is closer to the original image. Theoretically, high PSNR value usually indicates a higher quality image, but this is not always the case in practical. However, PSNR is easy to implement and fast to calculate while giving an acceptable result.
Structural similarity is an algorithm based on the human visual system which is highly adapted to process structural information [49]. The algorithm measures the change in this information between the reference and the distorted image.

### 1.3.5 Existing issues

The information infrastructure of modern healthcare has progressed rapidly in recent years. However, the integrity of the mammograms transferred over the communication channel still much questionable. Some of the existing issues with the information infrastructure of modern healthcare which we concerned in this research have been listed below:

1. Lack of efficient automated analysis of mammograms to assist the prognosis and diagnosis processes. Hence, more manpower is needed in the processes.

2. Lack of efficient authentication scheme to protect the integrity of the mammograms over the transmission channel.

3. In most of the cases, original image is expected than the watermarked image. Hence, irreversible watermarking scheme has minor application in the communication system of modern healthcare.

### 1.3.6 Significance of research

This research focused on building a scheme to detect the medical important regions on the mammograms and to provide protection from unofficial alteration to it. The proposed scheme is built to aid the picture archiving and communication system (PACS). With the scheme popularized in the PACS, we are expecting an impact to the society such as the chance of misjudgment in prognosis and diagnosis processes would be greatly reduced and lesser insurance fraud.

In additional, the efficiency of the scheme would help to save on the manpower of security measurement of the integrity of the mammograms. From economic point of view, the widespread of authentication scheme in the PACS will
greatly benefit the system, as reduction of the manpower would reduce the maintenance cost of the system.

Lastly, this research also provided a reference to the field of knowledge. We applied the images segmentation techniques [43],[45],[47],[48] to define the region of interest (ROI) of the mammograms automatically. Few methods were proposed to define the medical important regions of mammograms in the proposed scheme. Furthermore, we applied two different reversible watermarking techniques on ROI and RONI to obtain higher embedding capacity.

1.4 Thesis contribution

This thesis has contributed to the broad field of biomedical media authentication. More specifically, the methods of lossless watermarking and automatic region of interest (ROI) selection on the medical images were studied to allow for bandwidth savings during the authentication process. In practice, not all the segmented regions on the medical images carry the same level of importance for diagnostics. Usually, a ROI on the medical images refer to the regions that carry the important medical information. Therefore, it is necessary to locate the ROI on the medical images (high-level semantics) in order to emphasize on protecting its readability or visual quality while watermarking the medical images.

In this thesis, we focused on digital mammograms to other type of medical images as most of the mammograms show a similar type of ROI. This thesis has proposed a few methods of defining the ROI automatically which increase the efficiencies of the watermarking scheme. There are few methods suggested to meet the different scenarios in watermarking the digital mammograms. Further details on automated ROI selection methods are to be discussed in Chapter 4.

Furthermore, we have published two papers on this research work as listed below:


### 1.5 Thesis Organization

This thesis consists of seven chapters. First, Chapter 1 presents the general concept of digital watermarking and the fitting of digital watermarking in the medical field. Chapter 2 explains the development of the scheme together with the techniques used in the watermarking process. Chapter 3 describes the automated region of interest (ROI) definition methods used in the scheme in Chapter 2. Chapter 4 presents a study conducted on a solution to reduce the redundancy to be transmitted from the encoder to the decoder for authentication process. Chapter 5 presents an analysis study on the security level of the scheme. Chapter 6 documents the speed enhancement experiment of the scheme using Compute Unified Device Architecture (CUDA). Chapter 7 concludes the whole report.
Chapter 2: A Conceptual Framework of Digital Mammograms Watermarking

The scheme developed in this master research focuses on reversible watermarking on digital mammograms than other medical images. The digital mammograms are chosen for the scheme’s development for its relatively simple definition of region of interest (ROI). With less complexity of ROI introduced, the scheme is more capable of providing an accurate automated ROI definition.

The scheme runs a few times (layers) of watermarking process to embed in different regions on the image, a larger embedding capacity, and a complex steganography structure. Furthermore, the scheme is capable of providing image authentication. With the related secret information (hash code generated from the ROI) embedded into the image, the decoder is capable of running an authentication process (further explanation in Section 3.1.2). Besides, with the different watermarking techniques applied on the different layer of watermarking process, the ROI of the watermarked image remains a high readability.

2.1 Digital mammograms authentication scheme

With the automated region-of-interest (ROI) definition algorithm, the proposed scheme eliminates of the need of selecting the ROI explicitly by hand, providing a more convenient and accurate way to define the ROI comparing to Al-Qershi et al.’s scheme [10]. In additional, this has suggested a solution to issue No. 1 in section 1.3.5. Furthermore, the ROI selected by the algorithm conforms to shape of the breast and hence minimizes the redundant area in the defined ROI. Formally, there are numbers of methods to choose from in defining the ROI automatically for the digital mammograms input to the scheme. Moreover, the original mammogram is expected to be reconstructed exactly at the receiver side if the watermarked mammogram has not been tampered. This has proposed solutions to the issues No. 2
and No. 3 mentioned in section 1.3.5. The embedding and authentication procedures are presented below:

2.1.1 Embedding procedure

In the embedding procedure, the input digital mammogram is first determined for its format at step 1. In case where a Digital Imaging and Communications in Medicine (DICOM) format input is detected, the header of the DICOM file is to be checked for its medical information carried. At Step 2, the digital image information is to be extracted next for automatic ROI definition using the selected method. If a DICOM format input is detected in the first step, the medical information carried on the DICOM image are to be concatenated together with the user-added message to form a patient’s data.

Step 3, at the beginning of the watermarking process, the universal embedding threshold $T$ is set to 2 (smaller threshold values provide lesser embedding capacity). The universal embedding threshold serves as a reference to the embedding threshold used in deciding a pair of pixels to be expandable or changeable. In additional, setting the threshold to unity creates only a small amount of expandable difference for embedding. Then at step 4, the hash for ROI is to be calculated using SHA-256 algorithm forming $H_{roi}$ in the next step. Next, at step 5, the LSBs of the difference values of changeable pairs in ROI are collected as $B_{org1}$. After that, at step 6, patient’s data is compressed and concatenated with $H_{roi}$ to form the first bit stream to be embedded, $B_1$. If the length of $B_1$, $|B_1|$ is greater than the maximum embedding capacity of ROI, then the compressed version of patient’s data is partitioned into two parts, $PD_1$ and $PD_2$ where $|PD_1| = |B_1| - |H_{roi}|$. At step 7, $B_1$ is to be embedded in ROI using Alattar’s DE of quads method. The location map is formed using the improved location map method and forming first location map, $LM_1$. $B_1$ is to be embedded in both expandable and changeable quads in ROI. At step 8, the second location map, $LM_2$ for embedding in RONI is to be formed using Tian’s DE of pairs method in RONI. At step 9, the LSBs of the difference values of changeable pairs in RONI are collected as $B_{org2}$. Then, at step 10, $B_{org1}$ and $B_{org2}$ are concatenated to form $B_{org}$. At step 11, $LM_1$, $LM_2$, and $B_{org}$ are compressed and forming the compression headers, $LM_{1comp}$, $LM_{2comp}$, $B_{orgcomp}$ and then concatenated
with $PD_2$ (if exist) to form second bit stream, $B_2$. At step 12, $B_2$ is to be embedded into RONI using Tian’s DE of pairs method.

The embedding procedure fails if the length of $B_2$ is greater than the maximum embedding capacity of RONI. If the length of $B_2$ is greater than the maximum embedding capacity of RONI, the embedding process repeat from step 3 again with increased threshold value. The scheme decides to fail the watermarking if the length of $B_2$ is still greater than the maximum embedding capacity of RONI when the $T$ is larger than 15 (experimental results show that embedding capacity remain almost the same after 15, refer section 4.6.4 for more details). The embedding parameters inclusive of difference threshold applied for the embedding, the compression headers’ length, and also the ROI map are to be sent over to the decoder.

### 2.1.2 Decoding procedure

The proposed scheme is a non-blind scheme. Hence, some information is needed to start the decoding process. The embedding threshold, the information to reconstruct the ROI and the length of the compression headers are expected before the decoding process begins. At the step 1 on the decoder side, the ROI and RONI of the watermarked image are to be defined with the given information. Pixels in RONI are divided into pairs and processed using Tian’s DE of pairs method. Then at step 2, the difference value of the pairs to be partitioned into changeable set and not changeable set.

After that at step 3, the LSBs of the difference values from the changeable set are collected and decomposed into its original parts (with the help of the header lengths received): $LM_{1\text{comp}}$, $LM_{2\text{comp}}$, $B_{\text{orgcomp}}$, and $PD_2$. The parts are decompressed to obtain the original data: $LM_1$, $LM_2$, and $B_{\text{org}}$. At step 4, with $LM_2$ and $B_{\text{org}}$, the difference values which hold the watermark bit are restored and reconstruct the original RONI. At step 5, $B_1$ can be extracted from ROI using Alattar’s DE of quads method using $LM_1$. At step 6, $B_1$ is then decomposed into $PD_1$ and $H_{roi}$. At step 7, those quads which hold the watermark bit are reversed during extraction to reconstruct the original ROI.
Lastly at step 7, $PD_1$ and $PD_2$ are concatenated to and decompressed to obtain the patient’s data. A hash message is to be calculated from the recovered ROI and if it is equal to $H_{roi}$ then the reconstructed ROI is authentic.

Figure 2. Flowchart of the Embedding Process
Figure 3 Flowchart of the Decoding Process
2.2 Methodology

In this section, we describe the aims of the proposed scheme and the techniques applied. Main objective of the proposed digital mammograms authentication scheme is to protect the integrity of the digital mammograms. In a mammogram, not the whole image carries the equally important medical information. Hence, the scheme aimed to protect only the region of interest (ROI), which is the most medical information bearing region. The ROI is where the information that would affects prognosis and diagnosis processes outcomes [50].

The scheme used a combination of two reversible watermarking techniques: Tian’s difference expansion (DE) of pair [9] and Alattar’s difference expansion of quads [35] to embed the watermark. The digital mammograms (input images) are first to be auto-partitioned into ROI and region of non-interest (RONI) prior to the watermarking processes. More detail, we examined three methods of doing automatic image segmentation [47] and adopted pixel classification [39] to auto-determine the ROI and RONI of the input images.

2.2.1 Watermarking techniques

Tian’s difference expansion

J. Tian [9] proposed a high quality reversible watermarking method with high embedding capacity based on an integer transform, namely difference expansion (DE). In the method, watermark is to be embedded into the differences of pixels of the original image. The pixel pairs can be selected simply two horizontal or vertical adjacent pixels, or any two pixels selected in pre-defined pattern. The pattern can be used to serve as a security key.

The main things to be considered in DE are the difference of the pixel-pairs (difference numbers) $d$ and the average of the pixel-pairs $g$. For a pair of pixel $(x, y)$ in a grayscale image where $0 \leq x, y \leq 255$, the integer transforms for it in order to obtain the difference numbers $h$ and average $g$ is
\[ g = \left\lfloor \frac{x + y}{2} \right\rfloor, d = x - y \] (2)

where the symbol \( \lfloor \cdot \rfloor \) denotes the floor function which means “the least nearest integer”. The inverse transform of Eq. (2) is

\[ x = g + \left\lfloor \frac{d + 1}{2} \right\rfloor, y = g - \left\lfloor \frac{d}{2} \right\rfloor \] (3)

A grayscale value is bounded in \([0, 255]\). Hence, the inverse transformed pixel-pair values should be

\[ 0 \leq x \leq 255, 0 \leq y \leq 255 \]

\[ 0 \leq g + \left\lfloor \frac{d + 1}{2} \right\rfloor \leq 255, 0 \leq g - \left\lfloor \frac{d}{2} \right\rfloor \leq 255 \]

which is equivalent to

\[ |d| \leq \min(2(255 - g), 2g + 1) \] (4)

Overflow or underflow of the difference numbers out of this range would introduce information lost. To prevent these problems, the difference numbers \( d \) (after being embedded) must satisfy condition as shown in Eq. (4).

The least significant bit (LSB) of the difference number \( g \) is selected for embedding the watermark. If the difference number after its LSB has been embedded did not introduce overflow or underflow problem, the pixel pair is said to be changeable. Hence, only changeable difference numbers are chosen to be embedded to prevent overflow and underflow problems. As

\[ d = \left\lfloor \frac{d}{2} \right\rfloor \cdot 2 + \text{LSB}(d) \]

with \( \text{LSB}(d) = 0 \) or 1.
In the binary representation of integers, one can obtain an extra bit \( b \) after the LSB of the integers by left-shifting the bit stream representing the integers, with \( b = 0 \) or \( 1 \). This is equivalent to multiply the integers by 2. When a difference number has been multiply by 2 and it does not introduce overflow or underflow problems, the difference number is said to be expandable. Thus, for each expandable difference number, one could gain one extra bit by performing difference expansion \( d' = 2d + b \).

During the embedding process, the pixels is first to be paired up and the differences of the pixels of the pairs are calculated. Secondly, the changeable and expandable bits from the differences are determined. Next, the original changeable bits are to be compressed and concatenated with the compressed location of expandable differences (location map) and the hash of the original image to form a bit-stream (watermark). Then, the bit-stream is to be embedded into the embeddable differences (changeable and expandable differences) of the image. Finally, the inverse transform is applied to have the watermarked pixels from the resultant differences.

During watermark extraction, the differences of neighboring pixel values are calculated first. Next, the changeable bits are determined and the bit-stream embedded is to be extracted. Then, the compressed original changeable bits and location map, and the hash of original image are separated from the bit-stream extracted. Finally, the image is to be reconstructed with reference to decompressed location map and original changeable bits. The authenticity of the reconstructed image can be determined by comparing the hash of reconstructed image to the extracted hash.

Alattar’s difference expansion

In an attempt to increase the embedding capacity, Alattar [33] proposed a reversible watermarking scheme for color images in 2003. The method uses spatial and spectral triplets of pixels to hide pairs of bits. A spatial triplet is any three pixel values chosen from the same spectral, or color component. On the other hand, the spectral triplet is any three pixel values chosen from different spectral components.
(or different color components). The algorithm must have its own set of rules (or pattern) in keeping track of the triplet selected. For example, the three pixel values are chosen from different spectral components of the same pixel, or by using a mapping index.

A year later, Alattar further proposed a difference expansion of quads [35] for reversible watermarking of color images. This scheme hides three bits in the difference expansion of quads (a group of four pixels). The quad is formed from four pixel values chosen from four difference locations within the same color component. The simplest way of choosing the quads is to consider every 2x2 adjacent pixel values as quad. The maximal embedding capacity of the new quad DE scheme is computed to be 0.75 bpp. However, one expects to achieve a lower capacity as some quads may not be embeddable.

The integer transform for the quads \( q = (u_0, u_1, u_2, u_3) \) is defined as:

\[
v_0 = \left[ \frac{a_0 u_0 + a_1 u_1 + a_2 u_2 + a_3 u_3}{a_0 + a_1 + a_2 + a_3} \right]
\]

\[
v_1 = u_1 - u_0 \\
v_2 = u_2 - u_1 \\
v_3 = u_3 - u_2
\]

(5)

The inverse transform for the quads \( q^T = (v_0, v_1, v_2, v_3) \) is defined as:

\[
\overline{u}_0 = v_0 - \left[ \frac{(a_1 + a_2 + a_3)\overline{v}_1 + (a_2 + a_3)\overline{v}_2 + a_3\overline{v}_3}{a_0 + a_1 + a_2 + a_3} \right]
\]

\[
\overline{u}_1 = \overline{v}_1 + \overline{u}_0 \\
\overline{u}_2 = \overline{v}_2 + \overline{u}_1 \\
\overline{u}_3 = \overline{v}_3 + \overline{u}_2
\]

(6)

where \( q = (\overline{u}_0, \overline{u}_1, \overline{u}_2, \overline{u}_3) \) denotes the embedded quads.

The conditions to prevent underflow and overflow:
The quad is said to be expandable if the difference numbers below satisfy the conditions in Eq. (7):

\[
\begin{align*}
0 & \leq v_0 - \frac{v_1 + v_2 + v_3}{a_0 + a_1 + a_2 + a_3} \leq 255 \\
0 & \leq v_1 + u_0 \leq 255 \\
0 & \leq v_2 + u_1 \leq 255 \\
0 & \leq v_3 + u_2 \leq 255
\end{align*}
\]

(7)

The quad is said to be changeable if the difference numbers below satisfy the conditions in Eq. (8):

\[
\begin{align*}
\overline{v_1} &= 2 \times v_1 + b_1 \\
\overline{v_2} &= 2 \times v_2 + b_2 \\
\overline{v_3} &= 2 \times v_3 + b_3
\end{align*}
\]

(8)

with \( b_1, b_2 \) and \( b_3 = 0 \) or 1.

The quad is said to be changeable if the difference numbers below satisfy the conditions in Eq. (8):

\[
\begin{align*}
\overline{v_1} &= 2 \times \left\lfloor \frac{v_1}{2} \right\rfloor + b_1 \\
\overline{v_2} &= 2 \times \left\lfloor \frac{v_2}{2} \right\rfloor + b_2 \\
\overline{v_3} &= 2 \times \left\lfloor \frac{v_3}{2} \right\rfloor + b_3
\end{align*}
\]

(9)

with \( b_1, b_2 \) and \( b_3 = 0 \) or 1.

In an ideal scenario, where all the differences are expandable, the theoretical embedding capacity for Tian’s DE is 0.5 bits per pixel (bpp), whereas Alattar’s DE of quads is 0.75 bpp.

Automated ROI definition

There are five methods proposed in this thesis to define the ROI of the digital mammograms automatically. The ROI map defined through these methods will be in
binary form where the “high” level will represents the ROI and the “low” level will represents the RONI. Detailed of each ROI definitions methods will be discussed in Chapter 3.

2.3 Work evaluations

The main aim for the scheme is to retain the integrity of the digital mammograms when the watermarked works are transmitted from the owner to other peers. Meanwhile, the scheme aims to get rid of the complex steps needed to define the region of interest (ROI) manually while keeping a high visual quality work. Besides, this scheme allows the user to embed a part of patient’s data into the digital mammograms, which might be helpful in compensate of the absence of the DICOM header while watermarking a DICOM format mammogram.

The work here is referring to the watermarked output of the scheme. The evaluation process includes the visual quality of the work and also the capacity available for watermarking process.

2.3.1 Watermarked mammograms

Figure 4 (a) Original mammogram, (b) Watermarked mammogram. PSNR = 47.01dB, SSIM = 0.9822.
Figure 5 (a) Original mammogram, (b) Watermarked mammogram. PSNR = 45.45dB, SSIM = 0.9802.

Figure 4 and Figure 5 above are two of the examples mammograms before and after the watermarking process. The ROI of the mammogram shown in Figure 4 was defined using the pixel classification method. Whereas the ROI of the mammogram shown in Figure 5 was defined using the selective visual attention-driven model. Both Works remained in high visual quality. More experimental results on digital mammograms with different ROI definition methods will be shown in Chapter 3.

2.3.2 Capability of the scheme on mammograms of different class of abnormality

Seven mammograms of different class of abnormality were used to test the scheme, with threshold value of 5. The scheme used selective visual attention-driven model (SVAM) method to define the ROI. Table 1 shows the results of the embedding process of the scheme. G represents “fatty-glandular” and D represents “dense-glandular” in the character of background tissue column in the table. There are seven classes of abnormality present of the mammograms (in the third column): calcification denoted as CALC, circumscribed masses denoted as CIRC, Speculated masses denoted as SPIC, ill-defined masses denoted as MISC, architectural
distortion denoted as ARCH, asymmetry denoted as ASYM, and normal denoted as NORM.

<table>
<thead>
<tr>
<th>Image</th>
<th>Character of Background Tissue</th>
<th>Class of Abnormality</th>
<th>Image Size</th>
<th>Size of ROI (%)</th>
<th>Embedding Capacity (bpp)</th>
<th>PSNR</th>
<th>SSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>mdb001.pgm</td>
<td>G</td>
<td>CIRC</td>
<td>720x720</td>
<td>26.63</td>
<td>0.560758</td>
<td>46.460762</td>
<td>0.98225</td>
</tr>
<tr>
<td>mdb038.pgm</td>
<td>D</td>
<td>NORM</td>
<td>800x800</td>
<td>21.8</td>
<td>0.549547</td>
<td>47.11697</td>
<td>0.982479</td>
</tr>
<tr>
<td>mdb072.pgm</td>
<td>G</td>
<td>ASYM</td>
<td>800x800</td>
<td>21.63</td>
<td>0.548131</td>
<td>47.650039</td>
<td>0.982688</td>
</tr>
<tr>
<td>mdb124.pgm</td>
<td>G</td>
<td>ARCH</td>
<td>1024x1024</td>
<td>24.5</td>
<td>0.557096</td>
<td>46.835553</td>
<td>0.98298</td>
</tr>
<tr>
<td>mdb175.pgm</td>
<td>G</td>
<td>SPIC</td>
<td>1024x1024</td>
<td>30.39</td>
<td>0.568298</td>
<td>46.360396</td>
<td>0.979395</td>
</tr>
<tr>
<td>mdb211.pgm</td>
<td>G</td>
<td>CALC</td>
<td>1024x1024</td>
<td>34.16</td>
<td>0.577646</td>
<td>46.137654</td>
<td>0.979253</td>
</tr>
<tr>
<td>mdb264.pgm</td>
<td>G</td>
<td>MISC</td>
<td>1024x1024</td>
<td>37.47</td>
<td>0.58954</td>
<td>45.557789</td>
<td>0.979211</td>
</tr>
</tbody>
</table>

Table 1 - ROI defined using selective visual attention-driven model method.

The watermarked mammograms show good visual quality in terms of Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity (SSIM). The mammograms authentication scheme also shows high embedding capacity (with average of >0.56). The watermarked mammograms by the scheme were proven reversible by comparing the extracted mammograms with the original mammograms pixel by pixel. The authenticity of ROI can also be verified by comparing the embedded hash extracted with the recalculated hash of the reconstructed (reversed) ROI. From the simulations, the original mammograms can be reconstructed exactly in case of no tamper detected.
In this chapter, we presented the conceptual framework of the proposed scheme capable of hiding information, reconstruction of the original digital mammograms from watermarked Works using reversible watermarking, and providing authentication to ensure the integrity of the information and the digital mammograms at the decoder side.

Further results will be presented in Chapter 3 with different ROI definition methods. The results presented in this chapter focused on the practicality of the scheme on different types of mammograms. Whereas, the experiment results presented in Chapter 3 discussed more on the outcomes of the same type of mammograms with different ROI definition methods applied.
Chapter 3: Automated ROI Definition Methods

In this chapter, we will discuss the five types of automated ROI definition methods proposed to the scheme. We used five different types of image segmentation methods to meet different scenario. All the five methods have different level of accuracy and stability with different level of complexity in coding development. From the least development complexity and most straight forwarded method of block average to the highest level of complexity in development of pixels classification, each method has its pros and cons in different situations.

3.1 Block averaging

Block averaging method divides the digital mammogram into blocks of 2 x 2 pixels. The sum of the four pixel values in a block is used to determine the block belongs to "high” or “low” level in the ROI map. There will be a threshold set to determine the binary level of the sums. The threshold is determined empirically (refer below for more details). Then, a morphological close operation is to be applied to the ROI map to eliminate the unwanted small regions (noises) on the ROI map.
3.1.1 Choosing a suitable threshold

Original Mammogram

\[ T_{BA} = 10 \quad T_{BA} = 20 \quad T_{BA} = 30 \quad T_{BA} = 40 \quad T_{BA} = 50 \]
Figure 6 (a)-(g) Automatic ROI definition using block average method with different threshold, $T_{BA}$.

Figure 6 above shows a part of ROI maps defined using the block average method with different threshold values with mammograms from the mini-MIAS database. The smaller threshold, $T_{BA} = 10$ and $T_{BA} = 20$, left some small region of noise on the ROI map on average. Whereas the thresholds greater than that start to influence the shape of the boundary of the ROI. However, $T_{BA} = 30$ is found to eliminate most of the unwanted noise region and have only a small influence on the ROI boundary which is acceptable. Hence, we chose $T_{BA} = 30$ as the threshold to be used in the scheme for the block average method. A morphological close operation is to apply to the ROI map after applying the block average method to close the unwanted isolated regions on the ROI map.

3.2 Pixel classification

M. Wirth et al. proposed a rule-based fuzzy reasoning algorithm to do segmentation of the breast region in mammograms [43] in 2005. In the method proposed, the pixels classification measures is used to perform segmentation on digital mammograms.
First, the mean values of the blocks (size of 9x9) with center to pixel \((i, j)\) of the input mammograms are calculated. Then, the size of the deviations in the neighborhood surrounding \((i, j)\) and then the edginess in the neighborhood are measured. Examples of the mean, the deviation, and edginess images are shown in Figure 7.

3.2.1 Fuzzy Inference System

Fuzzy Inference System (FIS) from Fuzzy Toolbox in MATLAB was used to perform fuzzy decision making with two inputs: the deviations and the edginess, and one output: the classified measures. This process is to calculate the degree of membership to which the pixel belongs to in the four types. The deviations is
comprised of three fuzzy sets \{low, med, high\} and the edginess is comprised of two fuzzy sets \{low, high\} as shown in Figure 8.

![Graphs showing the shapes of linguistic variables v and e](image)

Figure 8 (a) The shapes of the linguistic variables v, (b) The shapes of the linguistic variables e

There is a series of four fuzzy rules which cover all the possible combinations used in calculating the output measures:

\[
\begin{align*}
\text{IF} & \ (v \text{ is low}) \quad \text{THEN} \ t = t_H \\
\text{IF} & \ (v \text{ is med}) \ \text{AND} \ (e \text{ is high}) \quad \text{OR} \quad (v \text{ is high}) \ \text{AND} \ (e \text{ is high}) \quad \text{THEN} \ t = t_E \\
\text{IF} & \ (v \text{ is med}) \ \text{AND} \ (e \text{ is low}) \quad \text{THEN} \ t = t_R \\
\text{IF} & \ (v \text{ is high}) \ \text{AND} \ (e \text{ is low}) \quad \text{THEN} \ t = t_A
\end{align*}
\]

where fuzzy OR is defined as max(a,b) and fuzzy AND is defined as min(a,b). \(v\) denotes the deviations and \(e\) denotes the edginess. The four types of pixels are homogeneous, edge, raster and aquarelle. When a pixel is homogeneous, a further check is taken to check whether the pixel had an intensity less than a threshold, \(T_1\) (chosen \(T_1 = 15\)). The homogeneous pixels which had intensity less than 15 are to be classified as background pixels.
3.2.2 Post-Processing

Post-processing is performed after the classification of the pixels has been derived from the FIS. A close-open alternating sequential filter (ASF) [51] with a disk-shaped structuring element (with diameter of 13) is used to smooth the breast contour and to eliminate the inconsistencies contents within the region of interest (ROI) and the region of non-interest (RONI). The ASF is capable of removing small false-positive and false-negative regions in the ROI and the RONI respectively, as shown in Figure 9.

![Figure 9](a) ROI measured from FIS, (b) ROI after ASF

3.3 Improved moment-preserving thresholding (IMPT)

Improved moment-preserving thresholding method [47] is a common global thresholding technique for image segmentation. The threshold is determined based on the location of the simulating isosceles triangles constructed. IMPT set pixels to high level if the value of the pixels is greater than the threshold. Then, the binarized image undergoes a morphological closing operation.

3.4 Selective visual attention-driven model (saliency map)

This method rescales the input image into 3 images with different dimensions as proposed by S. Feng et al.[45]. Then, all the 3 images are to be filtered with a
Gaussian low-pass filter. The filtered images are to be linearly combined again to form a saliency map. The ROI is defined through binarizing the saliency map together with the morphological close operation. The binarization is done with threshold value defined using Otsu’s method to convert an intensity image into binary image.

3.5 IMPT on saliency map

This is a method of binarizing the saliency map with the threshold defined using the IMPT method rather than Otsu’s method. The ROI map is defined through the threshold defined using IMPT method together with the morphological close operation.

3.6 Experimental results of the scheme with different ROI definition methods

To evaluate the effectiveness and practicality of the scheme provided, we have chosen to test the scheme with the mammograms from Mammographic Image Analysis Society (MIAS) Mini Mammographic Database (mini-MIAS database) [52]. Thirty digital mammograms from the mini-MIAS database were selected to run the simulations on automated ROI definitions. The universal embedding threshold (watermarking threshold for both techniques used in ROI and RONI) selected for the simulations is 5.
3.6.1 ROI definition

<table>
<thead>
<tr>
<th></th>
<th>Block average Pixels classification</th>
<th>IMPT</th>
<th>IMPT on saliency map</th>
<th>Selective Visual Attention-driven Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accurate boundary</td>
<td>Dependent on image quality</td>
<td>Highest</td>
<td>Lowest</td>
<td>Low</td>
</tr>
<tr>
<td>Accurate ROI</td>
<td>Dependent on image quality</td>
<td>Highest</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Image quality influence</td>
<td>Highest</td>
<td>Lowest</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Stability</td>
<td>Lowest</td>
<td>Highest</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Method complexity</td>
<td>Lowest</td>
<td>Highest</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

Table 2 - Evaluation on different ROI definition methods.

The ROIs defined using different definition methods for the 30 digital mammograms from mini-MIAS database is shown in Appendix A. Table 2 above shows the evaluation of the five ROI definition methods. Accurate boundary indicates the accuracy of the boundary of the ROI (used for boundary region preserving) defined by the methods. The accurate ROI indicates the accuracy of the methods to determine the ROI. Next, image quality influence indicates how much the input image quality will influence the methods to define the ROI. Stability indicates the ability of the methods to define different structural types of mammograms (different shapes). Finally, method complexity indicates the complexity to develop the methods. The results above were classified through the simulation results. As a
conclusion, the selective visual-attention driven model method and pixel classification method are preferred to the scheme. However, the pixel classification method is highly time-consuming.

### 3.6.2 Capability of different ROI definition methods on different class of mammograms

a) ROI defined using block average method.

<table>
<thead>
<tr>
<th>Image</th>
<th>Character of Background Tissue</th>
<th>Class of Abnormality Present</th>
<th>Image Size</th>
<th>Size of ROI (%)</th>
<th>Embedding Capacity (bpp)</th>
<th>PSNR</th>
<th>SSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>mdb001.pgm</td>
<td>G</td>
<td>CIRC</td>
<td>720x720</td>
<td>32.41</td>
<td>0.57593</td>
<td>46.301026</td>
<td>0.981556</td>
</tr>
<tr>
<td>mdb038.pgm</td>
<td>D</td>
<td>NORM</td>
<td>800x800</td>
<td>25.49</td>
<td>0.559939</td>
<td>46.976374</td>
<td>0.98201</td>
</tr>
<tr>
<td>mdb072.pgm</td>
<td>G</td>
<td>ASYM</td>
<td>800x800</td>
<td>25.32</td>
<td>0.560523</td>
<td>47.434595</td>
<td>0.982161</td>
</tr>
<tr>
<td>mdb124.pgm</td>
<td>G</td>
<td>ARCH</td>
<td>1024x1024</td>
<td>26.25</td>
<td>0.56429</td>
<td>46.689861</td>
<td>0.982561</td>
</tr>
<tr>
<td>mdb175.pgm</td>
<td>G</td>
<td>SPIC</td>
<td>1024x1024</td>
<td>34.29</td>
<td>0.579674</td>
<td>46.241781</td>
<td>0.978831</td>
</tr>
<tr>
<td>mdb211.pgm</td>
<td>G</td>
<td>CALC</td>
<td>1024x1024</td>
<td>38.83</td>
<td>0.59061</td>
<td>45.985246</td>
<td>0.978588</td>
</tr>
<tr>
<td>mdb264.pgm</td>
<td>G</td>
<td>MISC</td>
<td>1024x1024</td>
<td>43.97</td>
<td>0.608275</td>
<td>45.407293</td>
<td>0.978506</td>
</tr>
</tbody>
</table>
b) ROI defined using pixels classification method.

<table>
<thead>
<tr>
<th>Image</th>
<th>Character of Tissue</th>
<th>Class of Abnormality</th>
<th>Image Size</th>
<th>Size of ROI (%)</th>
<th>Embedding Capacity (bpp)</th>
<th>PSNR</th>
<th>SSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>mdb001.pgm</td>
<td>G</td>
<td>CIRC</td>
<td>720x720</td>
<td>30.73</td>
<td>0.570509</td>
<td>46.353717</td>
<td>0.981795</td>
</tr>
<tr>
<td>mdb038.pgm</td>
<td>D</td>
<td>NORM</td>
<td>800x800</td>
<td>24.46</td>
<td>0.556039</td>
<td>47.014641</td>
<td>0.982203</td>
</tr>
<tr>
<td>mdb072.pgm</td>
<td>G</td>
<td>ASYM</td>
<td>800x800</td>
<td>24.54</td>
<td>0.554845</td>
<td>47.483553</td>
<td>0.982353</td>
</tr>
<tr>
<td>mdb124.pgm</td>
<td>G</td>
<td>ARCH</td>
<td>1024x1024</td>
<td>26.71</td>
<td>0.561291</td>
<td>46.709489</td>
<td>0.982708</td>
</tr>
<tr>
<td>mdb175.pgm</td>
<td>G</td>
<td>SPIC</td>
<td>1024x1024</td>
<td>33.54</td>
<td>0.575484</td>
<td>46.243265</td>
<td>0.978938</td>
</tr>
<tr>
<td>mdb211.pgm</td>
<td>G</td>
<td>CALC</td>
<td>1024x1024</td>
<td>37.76</td>
<td>0.58588</td>
<td>46.02116</td>
<td>0.97874</td>
</tr>
<tr>
<td>mdb264.pgm</td>
<td>G</td>
<td>MISC</td>
<td>1024x1024</td>
<td>44.54</td>
<td>0.607308</td>
<td>45.451605</td>
<td>0.978537</td>
</tr>
</tbody>
</table>
c) ROI defined using improved moment-preserving thresholding (IMPT) method.

<table>
<thead>
<tr>
<th>Image</th>
<th>Character of Tissue</th>
<th>Class of Abnormality</th>
<th>Image Size</th>
<th>Size of ROI (%)</th>
<th>Embedding Capacity (bpp)</th>
<th>PSNR</th>
<th>SSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>mdb001.pgm</td>
<td>G</td>
<td>CIRC</td>
<td>720x720</td>
<td>19.12</td>
<td>0.543873</td>
<td>46.855743</td>
<td>0.983404</td>
</tr>
<tr>
<td>mdb038.pgm</td>
<td>D</td>
<td>NORM</td>
<td>800x800</td>
<td>17.89</td>
<td>0.542575</td>
<td>47.597428</td>
<td>0.983214</td>
</tr>
<tr>
<td>mdb072.pgm</td>
<td>G</td>
<td>ASYM</td>
<td>800x800</td>
<td>16.74</td>
<td>0.539123</td>
<td>48.042652</td>
<td>0.983422</td>
</tr>
<tr>
<td>mdb124.pgm</td>
<td>G</td>
<td>ARCH</td>
<td>1024x1024</td>
<td>21.31</td>
<td>0.552008</td>
<td>47.357718</td>
<td>0.983664</td>
</tr>
<tr>
<td>mdb175.pgm</td>
<td>G</td>
<td>SPIC</td>
<td>1024x1024</td>
<td>25.74</td>
<td>0.559402</td>
<td>46.629169</td>
<td>0.980206</td>
</tr>
<tr>
<td>mdb211.pgm</td>
<td>G</td>
<td>CALC</td>
<td>1024x1024</td>
<td>28.33</td>
<td>0.565418</td>
<td>46.429521</td>
<td>0.98029</td>
</tr>
<tr>
<td>mdb264.pgm</td>
<td>G</td>
<td>MISC</td>
<td>1024x1024</td>
<td>28.51</td>
<td>0.569684</td>
<td>45.890321</td>
<td>0.980245</td>
</tr>
</tbody>
</table>
d) ROI defined using improved moment-preserving thresholding (IMPT) on saliency map (SM) method.

<table>
<thead>
<tr>
<th>Image</th>
<th>Character of Background Tissue</th>
<th>Class of Abnormality Present</th>
<th>Image Size</th>
<th>Size of ROI (%)</th>
<th>Embedding Capacity (bpp)</th>
<th>PSNR</th>
<th>SSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>mdb001.pgm</td>
<td>G</td>
<td>CIRC</td>
<td>720x720</td>
<td>28.27</td>
<td>0.56392</td>
<td>46.450077</td>
<td>0.982126</td>
</tr>
<tr>
<td>mdb038.pgm</td>
<td>D</td>
<td>NORM</td>
<td>800x800</td>
<td>23.6</td>
<td>0.54852</td>
<td>47.102731</td>
<td>0.982585</td>
</tr>
<tr>
<td>mdb072.pgm</td>
<td>G</td>
<td>ASYM</td>
<td>800x800</td>
<td>22.98</td>
<td>0.548475</td>
<td>47.57704</td>
<td>0.98271</td>
</tr>
<tr>
<td>mdb124.pgm</td>
<td>G</td>
<td>ARCH</td>
<td>1024x1024</td>
<td>25.4</td>
<td>0.559267</td>
<td>46.794459</td>
<td>0.982896</td>
</tr>
<tr>
<td>mdb175.pgm</td>
<td>G</td>
<td>SPIC</td>
<td>1024x1024</td>
<td>32.52</td>
<td>0.568539</td>
<td>46.338478</td>
<td>0.979437</td>
</tr>
<tr>
<td>mdb211.pgm</td>
<td>G</td>
<td>CALC</td>
<td>1024x1024</td>
<td>35.88</td>
<td>0.580973</td>
<td>46.104731</td>
<td>0.979116</td>
</tr>
<tr>
<td>mdb264.pgm</td>
<td>G</td>
<td>MISC</td>
<td>1024x1024</td>
<td>39.21</td>
<td>0.593465</td>
<td>45.559251</td>
<td>0.979042</td>
</tr>
</tbody>
</table>
e) ROI defined using selective visual attention-driven model method.

<table>
<thead>
<tr>
<th>Image</th>
<th>Character of Background Tissue</th>
<th>Class of Abnormality Present</th>
<th>Image Size</th>
<th>Size of ROI (%)</th>
<th>Embedding Capacity (bpp)</th>
<th>PSNR</th>
<th>SSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>mdb001.pgm</td>
<td>G</td>
<td>CIRC</td>
<td>720x720</td>
<td>26.63</td>
<td>0.560758</td>
<td>46.460762</td>
<td>0.98225</td>
</tr>
<tr>
<td>mdb038.pgm</td>
<td>D</td>
<td>NORM</td>
<td>800x800</td>
<td>21.8</td>
<td>0.549547</td>
<td>47.11697</td>
<td>0.982479</td>
</tr>
<tr>
<td>mdb072.pgm</td>
<td>G</td>
<td>ASYM</td>
<td>800x800</td>
<td>21.63</td>
<td>0.548131</td>
<td>47.650039</td>
<td>0.982688</td>
</tr>
<tr>
<td>mdb124.pgm</td>
<td>G</td>
<td>ARCH</td>
<td>1024x1024</td>
<td>24.5</td>
<td>0.557096</td>
<td>46.835553</td>
<td>0.98298</td>
</tr>
<tr>
<td>mdb175.pgm</td>
<td>G</td>
<td>SPIC</td>
<td>1024x1024</td>
<td>30.39</td>
<td>0.568298</td>
<td>46.360396</td>
<td>0.979395</td>
</tr>
<tr>
<td>mdb211.pgm</td>
<td>G</td>
<td>CALC</td>
<td>1024x1024</td>
<td>34.16</td>
<td>0.577646</td>
<td>46.137654</td>
<td>0.979253</td>
</tr>
<tr>
<td>mdb264.pgm</td>
<td>G</td>
<td>MISC</td>
<td>1024x1024</td>
<td>37.47</td>
<td>0.58954</td>
<td>45.557789</td>
<td>0.979211</td>
</tr>
</tbody>
</table>

**Table 3 (a)-(e) Embedding Results for 7 Mammograms of Different Class of Abnormality Present**

Table 3 shows the embedding results for seven mammograms of different class of abnormality present. There are two types of background tissue in the digital mammograms used in the simulation. G represents “fatty-glandular” and D represents “dense-glandular” in the character of background tissue column in the table. There are seven classes of abnormality present of the mammograms (in the third column): calcification denoted as CALC, circumscribed masses denoted as CIRC, Spiculated masses denoted as SPIC, ill-defined masses denoted as MISC, architectural distortion denoted as ARCH, asymmetry denoted as ASYM, and normal denoted as NORM. Table 3 (e) has been shown in the previous chapter and Table 3 (a)-(d) are embedding results of different ROI definition methods. All the
Works from the proposed scheme scored high visual quality in both the visual quality assessments.

Some conclusions made from the embedding results shown Table 3:

- The larger the ROI, the lower the watermarked image quality.
- The larger the embedding capacity, the lower the watermarked image quality.
- The larger the ROI, the larger the embedding capacity.

### 3.6.3 Overall performance of different ROI definition methods

The average values in the graphs below are the average values calculated from the specific elements in the embedding results of different ROI definition methods. The average values are calculated based on the simulation results of the thirty digital mammograms from the mini-MIAS database. IMPT on saliency map method has been excluded from the simulations due to its inconsistence ROI defined at the edge of the image.

![Average of Embedding Capacity (bpp) of Different ROI Definition Methods](image)

**Figure 10** Graph of average values of embedding capacity (bpp) of different ROI definition methods.
Figure 11 Graph of average values of PSNR (dB) of different ROI definition methods.

Figure 12 Graph of average values of SSIM of different ROI definition methods.

Figure 10 shows the average values of embedding capacity (bpp) of the four different methods on ROI definition. Obviously, the block average method provides the highest embedding capacity to the scheme, which is close to 0.57bpp on average. Next, the fuzzy logic method is following up to it with average embedding capacity close to 0.56bpp. Then, the saliency map method ranked next with average embedding capacity slightly over 0.55bpp, and IMPT method ranked the last with average embedding capacity slightly over 0.54bpp.
Figure 11 depicts the average values of PSNR (dB) in visual quality assessments of the four different methods on ROI definition. From the graph above, the IMPT method provides the best visual quality in terms of PSNR, with average PSNR over 47dB, to the watermarked images on average. Next, it is follow up by the saliency map method, with average PSNR close to 47dB. Then, the fuzzy logic method ranked third, with average PSNR slightly over 46.5dB, and the block average method ranked last, with average PSNR close to 46dB.

Figure 12 shows the average values of SSIM in visual quality assessments of the four different methods on ROI definition. Similarly with the graph in Figure 11, the IMPT method provides the best visual quality in terms of SSIM, with average close to 0.983. Next, the saliency map method provides an average close to 0.982 in terms of SSIM measurement. Then, the fuzzy logic method provides an average reading slightly behind the saliency map method. Lastly, the block average method scores an average close to 0.98 only.

From the three figures above, a conclusion can be drawn on the relationship of the embedding capacity and the visual quality of the watermarked images: the embedding capacity is inversely related to the visual qualities (both PSNR and SSIM). In another words, when the embedding threshold increased, it results an increase in the embedding capacity, and the decreases in the visual qualities. The block average method allows the scheme to provide the largest embedding capacity with a much more distorted watermarked image. Due to the possibility of reconstructing the exact original mammograms from the authentic source, this method might be the most practical among the ROI definition methods proposed.

3.6.4 Different embedding thresholds with different ROI definition methods

The results in the previous section presented the strength of the different automated ROI definition methods. In this section, the stability of the relationship between the embedding capacity and the visual quality of the watermarked image is examined. Similarly, the average values in the graphs below are the average values calculated
from the related elements in the embedding results of different ROI definition methods. IMPT on saliency map method has also been excluded from the simulations due to the same reason.
Block averaging

Figure 13 Graph of dependency of average of embedding capacity (bpp) on average of PSNR (dB) using block average.

Pixels classification

Figure 14 Graph of dependency of average of embedding capacity (bpp) on average of PSNR (dB) using pixels classification.
Figure 15 Graph of dependency of average of embedding capacity (bpp) on average of PSNR (dB) using IMPT.

Saliency map
Figure 16 Graph of dependency of average of embedding capacity (bpp) on average of PSNR (dB) using saliency map.

Figure 13 depicts the dependence of the average embedding capacity (bpp) on average PSNR of the different embedding thresholds, from $T = 2$ to $T = 15$, using block average method of ROI definition. This graph shows the inverse relationship between the embedding capacity and the visual quality of the image, in terms of PSNR, on average.

Figure 14 shows the dependence of the average embedding capacity (bpp) on average PSNR of the different embedding thresholds, from $T = 2$ to $T = 15$, using pixels classification method of ROI definition. This graph shows the direct relationship between the embedding capacity and the visual quality of the image, in terms of PSNR, on average.

Figure 15 depicts the dependence of the average embedding capacity (bpp) on average PSNR of the different embedding thresholds, from $T = 2$ to $T = 15$, using IMPT method of ROI definition. This graph shows the inverse relationship between the embedding capacity and the visual quality of the image, in terms of PSNR, on average.

Figure 16 above depicts the dependence of the average embedding capacity (bpp) on average PSNR of the different embedding thresholds, from $T = 2$ to $T = 15$, using saliency map method of ROI definition. This graph shows the inverse relationship between the embedding capacity and the visual quality of the image, in terms of PSNR, on average.

From the four figures above, we observed a same relationship between the average embedding capacity with the average PSNR of the block average, IMPT, and saliency map methods. However, the fuzzy logic method shows a different kind of graph. This is due to the inconsistency in the results of the fuzzy logic method. For some test images at certain embedding thresholds, higher embedding capacity would gives higher visual quality. Additionally, we observed that, except for the fuzzy logic method, the embedding capacity turned stable when the universal embedding threshold is close to 15.
In this chapter, we presented methods used to define the ROI automatically and the experimental results from different ROI definition methods and their performance on different scenarios. The experimental results used in comparison between the ROI definition methods are the outcomes of the same type of mammograms with different methods applied.
Chapter 4: Boundary Region Preserving

A method is proposed to the scheme to get rid of the need to send the ROI map over to the decoder in order to reconstruct the exact ROI map. This method is named as ROI boundary region preserving method. However, this method only works on few mammograms out of the 30 selected mammograms from mini-MIAS database. Hence, this method only serves as additional feature to the scheme and it is documented for future reference.

4.1 Defining boundary region

The watermarking process will tends to modify the value of the pixels and hence leading to variations in the ROI in the redefinition of ROI. The methods used in defining the ROI depend most on the pixels’ intensity level. In digital mammograms, the pixels within the ROI usually have high intensity level. Hence, the border of the ROI and RONI become a critical region where the pixels having value around the selected threshold. Therefore, a new region (boundary region) at the border is defined intentionally to be excluded from watermarking process. Result from that, the decoder is expected to have no problem in redefining the ROI since the value of the pixels in the boundary region has not been changed.

The boundary region is to be excluded from embedding process. Hence, the decoder has to be informed of the width of the region in order to calculate the same ROI map again. With the boundary region excluded from watermarking process, the same ROI map used for embedding process can be regenerated at the decoding process automatically.

The boundary region is defined as the pixels surrounding the boundary of the ROI and RONI. The boundary region definition has been approached with block-based (window of 3x3) scan.
4.1.1 Block-based scan

The boundary region is defined as the region surrounding the boundary of ROI and RONI. The 8 pixels surrounding the pixel which detected to be the boundary were defined as the boundary region.

The algorithm to define the boundary region starts scanning the image pixel by pixel and performs checking on the pixel to check whether it is a boundary pixel or not at the same time. If the pixel is found to be a boundary pixel, the pixels surrounding it would be defined as boundary pixels too.

Sometime a boundary region defined like this is not enough for the decoder to calculate the same ROI map from the watermarked image. So, the repetition of the scan increased. Supposedly a boundary region defined with 3x3 block is defined for the first scanning. The figure below shows the process of defining the pixels surrounding the boundary pixels to boundary region (gray color pixel is the boundary pixel; darker gray color pixel is the current pixel) as shown in Figure 17.

![Figure 17 Defining surrounding pixels to boundary pixels](image)

When the depth of scan increased (scan repetitions increased), the algorithm scans through the firstly defined region and defines the pixels surrounding those pixels within the region to be boundary pixels too. So the width of the boundary region increased by 2 pixels (1 pixel left and 1 pixel right) for each time of scan, as shown in Figure 18.
4.2 Experimental results

An experiment on leaving the boundary region excluded from watermarking process has been carried out. Example of a ROI map defined from a test image and its boundary region is shown in Figure 19.

Two 8-bit digital mammograms ((A) with dimension of 600 x 466 and (B) with 1024 x 1024), as shown in Figure 20 below were used for the simulations of the scheme with boundary region preserving.
4.2.1 ROI defined using different ROI definition methods

Two of the mammograms used in experiment as shown in Figure 20 were selected to show the different outcomes of the different ROI definition methods.
Block average

This technique divided the pixels into blocks and determined the “high” or the “low” level with the sum of the blocks by the threshold value selected.

![ROI map of mammograms A](image1.png) ![ROI map of mammograms B](image2.png)

(a)ROI map of mammograms A (b)ROI map of mammograms B

**Figure 21 ROI map defined using block average method.**

Pixel classification

This technique defined types of the pixels belong to through a set of Fuzzy rules. The ROI map defined through this technique is shown in Figure 22.

![ROI map of mammograms A](image3.png) ![ROI map of mammograms B](image4.png)

(a)ROI map of mammograms A (b)ROI map of mammograms B

**Figure 22 ROI map defined using pixel classification method.**
IMPT

The ROI map constructed using IMPT technique for the input mammograms is shown in Figure 23. The ROI map successfully covered most of the medical information bearing region of the input mammograms.

(a)ROI map of mammograms A  (b)ROI map of mammograms B

Figure 23 ROI map defined using IMPT method.

Saliency map

This technique is used to detect the most visual attention drawing region on an image. The ROI map constructed using saliency map method is shown in Figure 24.

(a)ROI map of mammograms A  (b)ROI map of mammograms B

Figure 24 ROI map defined using saliency map method.
This method defined the ROI map with a binarization on the saliency map using the threshold generated with IMPT method. The ROI map constructed using saliency map method is shown in Figure 25.

![ROI map of mammograms A](image1.png) ![ROI map of mammograms B](image2.png)

(a)ROI map of mammograms A  (b)ROI map of mammograms B

Figure 25 ROI map defined using IMPT on saliency map method.

4.2.2 Defining boundary region

Block average

![Boundary region of mammograms A](image3.png) ![Boundary region of mammograms B](image4.png)

(a)Boundary region of mammograms A  (b)Boundary region of mammograms B
Figure 26 Boundary region (block average) with SR = 10.

Figure 26 shows the boundary region defined for the ROI map constructed through block average. The boundary region is defined with 10 scan repetitions (SR). This is the minimum region to be preserved for the decoder to redefine the same ROI map from the watermarked image.

Pixel classification

(a) Boundary region of mammograms A  (b) Boundary region of mammograms B

Figure 27 Boundary region (PixC) with SR = 7.

Figure 27 shows the boundary region defined for the ROI map constructed through pixel classification. The minimum SR for this ROI map is 7.
Figure 28 Boundary region (IMPT) with SR = 11.

Figure 28 shows the boundary region defined for the ROI map constructed through IMPT. The boundary region is defined with 11 scan repetitions (SR). This is the minimum region to be preserved for the decoder to redefine the same ROI map from the watermarked image.
Figure 29 Boundary region (SVAM) with SR = 10.

Figure 29 shows the boundary region defined for the ROI map constructed through saliency map method. The minimum SR for this ROI map is 11.

Figure 30 Boundary region (IMPT on saliency map) with SR = 8.
Figure 30 shows the boundary region defined for the ROI map constructed through IMPT on saliency map method. The minimum SR for this ROI map is 8.

### 4.2.3 Evaluation of the scheme with boundary region preserving

The image authentication scheme uses the hash code embedded in the watermarked image and the hash code calculated from the reconstructed image to justify the authenticity of the watermarked image. The watermarked image is said to be not authentic if the reconstruction of the input image from the watermarked image failed.

Apart from that, the visual quality of the watermarked image is another important issue to be concerned. Fortunately, the scheme is able to provide a very good visual quality of watermarked image. Assessments used in judging the visual quality of the watermarked image of the scheme includes the peak signal-to-noise ratio (PSNR) and the structural similarities (SSIM). Table 4 and Table 5 below show some of the watermarking assessments of the scheme with boundary region preserving.

<table>
<thead>
<tr>
<th>ROI Definition Methods</th>
<th>BRSR</th>
<th>PSNR (dB)</th>
<th>SSIM</th>
<th>Payload (bpp)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block average</td>
<td>10</td>
<td>44.563</td>
<td>0.981</td>
<td>0.525</td>
</tr>
<tr>
<td>Pixel Classification</td>
<td>7</td>
<td>43.455</td>
<td>0.977</td>
<td>0.568</td>
</tr>
<tr>
<td>IMPT</td>
<td>11</td>
<td>49.038</td>
<td>0.986</td>
<td>0.509</td>
</tr>
<tr>
<td>Saliency Map</td>
<td>10</td>
<td>44.789</td>
<td>0.982</td>
<td>0.52</td>
</tr>
<tr>
<td>IMPT on saliency map</td>
<td>8</td>
<td>43.836</td>
<td>0.979</td>
<td>0.552</td>
</tr>
</tbody>
</table>

*BRSR = Boundary region scan repetitions

Table 4 Watermarking assessments for input mammograms A
### Table 5 Watermarking assessments for input mammograms B

However, at the latter stage of the experiment we found that different digital mammograms have different suitable scan repetitions. Some of the mammograms required a much larger number of scan repetitions (>15), which is not feasible for the scheme to leave a big blank region excluded from the watermarking process. Hence, the scheme did not bring this method into application.
Chapter 5: Security Analysis

5.1 Security attacks

J. Fridrich et al. presented two attacks in the paper [53]. The first proposed attack infers the secret watermark insertion function and the binary logo from multiple images authenticated with the same key and containing the same logo. The attack shows a very good approximation to the logo and watermark insertion function to be constructed by just using two images. The second attack proposed is stated as “collage-attack” which is a variation of the Holliman-Memon counterfeiting attack [54]. The proposed variation differs from the original one proposed in [54] where the knowledge of the watermark logo is not required. The second proposed attack is to be ignored since it was proposed for color image which is not to be considered in our scheme.

M. Holliman and N. Memon proposed a counterfeiting attack for the watermarking techniques that embed information into a host image in a block-wise independent fashion [54]. To be specific, one can forge the watermark contained in a watermarked image into another image without knowing the secret key used for watermark insertion and in some cases even without explicitly knowing the watermark.

In Yeung-Mintzer technique [55], a watermark image $W$ (usually a binary logo image) is embedded into a source image $X$ to obtain a watermarked image $X'$. $W$ is of the same dimensions as the image $X$. In order to do the image verification, $W'$ extracted from $X'$ must be the same as the original watermark $W$.

H. Kubota and K. Iwamura proposed a new classification of attacks for security evaluation on fragile watermarking schemes and also a new fragile watermarking scheme [56]. In the classification, nine attacks on watermarked images were classified into three classes: watermarked image attacks, known original image attacks, and chosen original image attacks.
5.2 Attacks on the Yeung-Mintzer fragile watermarking technique

**Attack 1:** If the same logo lookup tables are used for multiple grayscale images, both the logo and the binary functions can be almost completely recovered from as few as two images. Given two grayscale \( M \times N \) images \( U \) and \( V \) watermarked with the same secret key \( K \) and a binary logo \( W \), one can write

\[
W(i,j) = f(U(i,j)) = f(V(i,j)) \text{ for every pixel (i,j)}
\]

This constitutes \( M \times N \) equations for 256 unknowns \( f(0), f(1), \ldots, f(255) \). Most of the equations are redundant and, depending on the image, there may not be a unique solution \( f \). We can start with the set \{0, 1, \ldots, 255\} divided into 256 subsets, each subset having exactly one gray scale level. Then, the first equation, \( f(U(1,1)) = f(V(1,1)) \), tells us that the values of \( f \) are the same for both \( U(1,1) \) and \( V(1,1) \). Thus, we can group together these two gray levels because the value of the binary function \( f \) is the same for both. Gradually, the 256 subsets will start to coalesce into a smaller number of larger subsets. At the end, there will be two large subsets, one corresponding to \( f(j) = 0 \), the other to \( f(j) = 1 \), and several other sets for which the value of \( f \) is undetermined.

**Counter-attack 1:** J. Fridrich *et al.* [53] proposed a counter attack to thwart the attack proposed by them. It is stated that making the binary function \( f \) depend on more than one pixel can thwart the attack.

**Counter-attack of scheme proposed (our scheme) 1:** The hashing function to calculate the hash code for authentication is depending on the whole ROI of the input digital mammograms. Hence, the scheme is capable of making different watermark for different host image. Without 2 same watermarks to be inserted into 2 different host images with the same key, it is not possible to “copy-paste” a watermark extracted from a watermarked image onto another host image to pass the authentication.

**Attack 2:** Given a key \( K \), we say that two image blocks \( X_i \) and \( X_j \) (of host image \( X \)) are \( K \)-equivalent if
\[ D_k(X_i) = D_k(X_j) = W \]

That is, blocks \( X_i \) and \( X_j \) are \( K \)-equivalent if the key \( K \) extracts the same watermark from both of them. One consequence of this property is that for a block-wise independent watermarking process, a given key \( K \) induces a partitioning of the set of all image blocks into equivalence classes, \( \{C_1, C_2, \ldots, C_m\} \), where \( m \) is the number of different possible watermark signals. The application of the watermark detection process to any block from a given equivalence class \( C_i \) results in the same watermark being recovered with key \( K \).

The counterfeiting process can be loosely represented by the following generic procedure:

**Input**: Image \( X' = X'_1, X'_2, \ldots, X'_{n} \) containing watermark \( W \)

Image \( Y = Y_1, Y_2, \ldots, Y_{n} \) in which we would like to forge \( W \)

**Output**: Image \( Y' = Y'_1, Y'_2, \ldots, Y'_{n} \) containing forged \( W \). \( Y' \approx Y \).

**Begin**

for \( I = 1 \) to number of blocks

Identify the equivalence class \( k \) to which the block \( X'_i \) belongs.

Construction an approximation \( Y'_i \) to \( Y_i \) such that \( Y'_i \in C_k \).

Replace \( Y_i \) by \( Y'_i \).

**End.**

Clearly, if the attacker knows the watermark, he/she also has at least partial knowledge of the equivalence class \( C_k \) corresponding to a given image block. Constructing an approximation \( Y'_i \) of \( Y_i \) such that \( Y'_i \) belongs to the required equivalence class \( C_k \) is achieved by applying vector quantization to the image, where the codebook used is the set of watermarked blocks in \( X' \) known to belong to \( C_k \). The blocks in \( X' \) that belong to \( C_k \) are available to the attacker and he/she could simply find the closest match among these as the required \( Y'_i \). In cases where the watermark
is not known, we show later in this thesis how an attacker may exploit partial knowledge of a watermark signal’s structure in order to forge a watermark. Although the specific approach used to achieve this would depend on the watermarking procedure, in general it is the block-wise independence that enables the attacker to construct a forged image by “pasting” together suitable blocks. In the next two sections we give specific examples of successful counterfeiting attacks against three different block-wise independent watermarking techniques.

**Counter-attack 2:** The “cut-and-paste” attacks proposed in this paper can therefore be defeated by making watermark insertion in a given block dependent upon other blocks in the watermarked image. In this case, an attacker cannot simply put together individual blocks that are K-equivalent to corresponding blocks in the original image in order to construct a counterfeit.

**Counter-attack of scheme proposed (our scheme) 2:** The watermark inserted into the image in our scheme is concatenated of a few bit-streams of different parameters. The watermark is beginning with headers, followed by location maps, original changeable bits, hash of original ROI, and patients’ information. We can say the every bit in the watermark is dependent on another bit (any change to a single bit will lead to authentication failure). The length of the headers serves as a public key to the decoder.

For the ideal case of attack, if the digital mammogram is successfully being attacked by collage attack, say forging $W$ into $Y$ constructing $Y'$, it will not pass the authentication process of the scheme due to the hash bit-stream embedded (calculate from $X$) is different from the hash calculated from the reconstructed image $Y$. 
5.3 Security evaluation proposed by H. Kubota and K. Iwamura

There are nine attacks included into three different classes in the evaluation. H. Kubota and K. Iwamura evaluated four fragile watermarking schemes together with their proposed scheme using the evaluation system proposed. The four schemes evaluated were Wong’s scheme [57], improved Wong’s scheme [58], Barreto’s scheme [59], and Fridrich’s scheme [60].

**Watermarked Image Attacks:** Image processing attack, collage attack, resize attack, open algorithm attack. These are performed using the watermarked images in the absence of the original images and watermark information.

1. Image processing attack: This attack is not a malicious type of attack and it involves modification by standard image processing such as affine transformation, noise addition, image compression, and image filtering.

2. Collage attack: This attack replaces at the same location blocks from the other watermarked images made by the same key, as described above.

3. Resize attack: This attack adds or deletes blocks. The attack is undetectable if the watermarking is performed independently for every block. It is undetectable even if the information of the size of the image is contained in the watermark. A forged image of different size is to be detected as modification of the whole image.

4. Open algorithm attack: This attack analyzes a watermarked image using the public algorithm and hence proposing a concrete attack depends on each watermarking algorithm.

**Known/Chosen Original Image Attacks:** Original image attack, watermarking information attack, overwriting attack, embedding machine construction attack. In these attacks, it is assumed that the attacker knows about the original images and the stamp image (the watermark) of other watermarked images apart from the target watermarked image (with same stamp image).
1. Original image attack: This attack compares the original and the watermarked image. Attacker aims to make a forged image using the information deduced.

2. Watermarking information attack: This attack embeds a special stamp image using the watermarking service.

3. Overwriting attack: This attack embeds different stamp images into the target watermarked image using the watermarking service. This attack does not specify a stamp image whereas “watermarking information attack” does. It follows the constitutive rule(s) for the stamp image (if any) in the watermarking service.

4. Embedding machine construction attack: The attacker constructs an embedding machine from the public algorithm. Similar to “overwriting attack” but this attack uses an embedding machine made by the attacker. The constitutive rule(s) for stamp image in the watermarking service can be ignored. The legality of the key for the machine is not guaranteed.

**Known/Chosen Watermarked Image Attacks**: Oracle attack. In this attack, attacker is assumed to have a watermark extracting machine that can obtain the stamp image from the watermarked image.

1. Oracle attack: The attacker orders the verification of a watermarked image by the watermarking service, and analyzes the watermarked image using the information returned.
5.4 Security evaluation of proposed scheme using the nine attacks

A) Image processing attack

Detectable as the attack influence the integrity of the watermark embedded (any change to a single bit of the watermark will causes error in decoding the watermark).

Figure 31 (a) Watermarked image. (b) Attacked image.

B) Collage attack

This attack is impractical on our scheme as the block size used in our scheme is only 1x2 (or 2x1) to 2x2. Replacement of other blocks with other pixels value but the same LSB (watermarked) will not guarantee the difference between pixels (our scheme embeds using difference expansion). Calculating the difference between the pixels in the new blocks to match the existing blocks is an open algorithm attack. Any change to the pixels in ROI will causes the authentication to fail as the hash calculated for authentication is based on the pixel values. Hence, this attack is detectable.

C) Resize attack

Deletion of blocks from ROI is detectable, but not all are detectable in RONI. If a block from the not embeddable set (difference expansion technique) been deleted or
added, it is not detectable. Information of the size of ROI and RONI should be added to prevent this attack.

![Watermarked image](image1.png) ![Reduced size watermarked image](image2.png)

**Figure 32(a) Watermarked image. (b) Reduced size watermarked image.**

D) **Open algorithm attack**

Arithmetic encoding is used in our scheme. The digital signature (the watermark) cannot be forged without knowing the secret key (parameters used in encoding and embedding process). Hence, this attack is detectable.

E) **Original image attack**

The information deduced from the difference of the watermarked image and the original do not provide any meaningful information before it is decoded. Embed the difference deduced blindly into another target image will fail the authentication (authentication process depends on the hash codes).
F) Watermarking information attack

The stamp image is built based on the input data to be embedded (patients’ information) and other embedding parameters (location maps, embedding strength, original LSB of changeable sets, headers, and etc.). Hence, this attack is detectable.

Figure 33(a) Original image. (b) Watermarked image. (c) Difference of (a) and (b) added.

Figure 34(a) Watermarked image. (b) Attacked image.
G) Overwriting attack

Once a block is replaced with a block from different embedding sets, the decoding process will fail (image cannot be reconstructed, hence leading to a different hash to be calculated). Replacing blocks with different pixel values will cause the difference in hash code calculated. Hence, this attack is detectable.

![Image](a) (b)

Figure 35(a) Watermarked image. (b) Atacked image.

H) Embedding machine construction attack

Embedding machine constructed by the attacker does not use the same secret keys. Hence, the watermark embedded cannot be decoded.

I) Oracle attack

There are many constitutive rules for constructing a watermark to be embedded. It is nearly impossible to construct a legal watermark which can be decoded with some other keys and carrying the hash of the target image at the same time. This attack is detectable.
5.5 Evaluation results

<table>
<thead>
<tr>
<th>Type of attacks</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Good</td>
<td>Bad</td>
<td>Poor</td>
<td>Poor</td>
<td>NR</td>
<td>Bad</td>
<td>Bad</td>
<td>Bad</td>
<td>Good</td>
</tr>
<tr>
<td>2</td>
<td>Good</td>
<td>Poor</td>
<td>Poor</td>
<td>Poor</td>
<td>NR</td>
<td>Bad</td>
<td>Bad</td>
<td>Bad</td>
<td>Good</td>
</tr>
<tr>
<td>3</td>
<td>Good</td>
<td>Poor</td>
<td>Poor</td>
<td>Poor</td>
<td>NR</td>
<td>Bad</td>
<td>Bad</td>
<td>Bad</td>
<td>Good</td>
</tr>
<tr>
<td>4</td>
<td>Good</td>
<td>Good</td>
<td>Poor</td>
<td>Poor</td>
<td>NR</td>
<td>Poor</td>
<td>Poor</td>
<td>Poor</td>
<td>Good</td>
</tr>
<tr>
<td>5</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>NR</td>
<td>NR</td>
<td>NR</td>
<td>Good</td>
<td>Good</td>
<td>NR</td>
</tr>
<tr>
<td>6</td>
<td>Good</td>
<td>Good</td>
<td>Poor</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
</tbody>
</table>

*NR = Not Relevant

*Schemes: (1) Wong’s scheme, (2) Improved Wong’s scheme, (3) Barreto’s scheme, (4) Fridrich’s scheme, (5) H. Kubota’s scheme, (6) Our proposed scheme

Table 6 Evaluation results of the security analysis between schemes.

Table 6 above shows the evaluation results of the schemes mentioned above for comparison with our scheme. “Good” indicates the attack can be detected by the scheme. Whereas, “Poor” means the attack has chance to succeed. Lastly, “Bad” means the attack cannot be detected by the scheme at all. The proposed scheme has advantages from the other schemes from the security attacks A to I except for attack C.
Chapter 6: Real Time Implementation

This chapter is a work done on an approach to speed up the processing time of the watermarking scheme. We have simulated this approach using an older version of the scheme as the simulations have been carried out at the earlier stage of the research. Hence, the proposed watermarking scheme mentioned in this chapter would be referring to the older version of the scheme. The scheme used in the simulations in this chapter would be discussed in section 6.2. The scheme developed in MATLAB has been tested to boost using Compute Unified Device Architecture (CUDA) in the simulations. In this chapter, we present the performance profile for three prototypes of the watermarking scheme, i.e. the MATLAB prototype, the CPU based prototype and the CPU/GPU based prototype. For the latter two, we implemented the prototypes using C programming language, and the GPU platform chosen was the NVIDIA “Computer Unified Device Architecture” (CUDA) framework.

6.1 Real world adaptive model

The watermarking process requires a real time or near real time performance in order to satisfy the users in real world applications. For ideal scenario, the watermarking process is expected to be done right at the moment the mammograms are acquired by the scheme. To attain a better user’s experience by speeding up the watermarking process, we proposed a general purpose graphic processing unit (GPU) based approach to accelerate the performance of the proposed watermarking scheme. Further in this chapter, works on the performance of the three prototypes of the watermarking scheme are to be discussed.

6.2 Scheme used in CUDA accelerated approach

In the proposed scheme, an automated ROI definition step has been implemented as a pre-processing step to the watermarking procedures. The automated ROI definition algorithm of the scheme eliminates of the need of selecting the ROI explicitly by
hand. Furthermore, the ROI selected by the algorithm conforms to shape of the breast and hence minimizes the redundant area in the defined ROI. The scheme uses IMPT on saliency map method to define the ROI automatically. The embedding and authentication procedures are presented below:

**Embedding process**

First, the mammogram was decomposed into a 3-level Gaussian Pyramid. Then we performed a linear combination of the individual levels to construct an intensity saliency map. A threshold value is then selected via the Chen et al.’s improved moment-preserving thresholding method. The ROI is then defined through binarisation of the saliency map at the given threshold value together.

Next, the hash message for ROI, $H_{roi}$, is calculated using SHA-256 algorithm. After which, the LSBs of the difference values of the changeable pairs in ROI are collected as $B_{org1}$. The patient’s data is then compressed and concatenated with $H_{roi}$ to form the first watermark bit stream to be embedded, $B_1$. If the length of $B_1$ is greater than the maximum embedding capacity of ROI, then the compressed version of patient’s data is partitioned into two parts, $PD_1$ and $PD_2$ where $|PD_1| = |B_1| - |H_{roi}|$.

$B_1$ is then embedded in ROI using Alattar’s DE of quads method. The first location map is constructed during the embedding process in ROI, denoted by $LM_1$. $B_1$ is to be embedded in both expandable and changeable quads in ROI.

The second location map, $LM_2$ is constructed based on Tian’s DE method in the RONI. The LSBs of the difference values of changeable pairs in RONI are collected as $B_{org2}$. Then, $B_{org1}$ and $B_{org2}$ are concatenated in series to form $B_{org}$.

$LM_1$, $LM_2$, and $B_{org}$ are then compressed and $LM_{1\text{comp}}$, $LM_{2\text{comp}}$, $Borg_{\text{comp}}$ and then concatenated with $PD_2$ (if exist) to form second bit stream, $B_2$, which is then embedded into RONI using Tian’s DE of pairs method.

Once the embedding procedures are completed as detailed above, the embedding parameters are then packaged and encrypted for delivery to the receiver along with the watermarked mammogram using a secure channel. The embedding parameters include the two embedding thresholds for the RONI and ROI.
respectively, as well as the ROI border information. For our scheme, we have set the embedding threshold $T$ is set to 5 and gradually increased by a step size of one, should the embedding process fails owing to insufficient embedding capacity. However, the scheme will terminate the embedding procedures eventually if the embedding capacity calculated, at $T = 30$, is insufficient for the given ROI. From the experimental results, it showed that embedding capacity remain almost constant for $T > 30$.

Authentication process

At the receiver’s end, the ROI and RONI are re-constructed with the given information of ROI’s border. Pixels in RONI are first divided into pairs and scanned using Tian’s DE of pairs method. The difference value of the pairs to be partitioned into changeable set and not changeable set.

The LSBs of the difference values from the changeable set are collected and decomposed into its original parts: $LM_{1\text{comp}}$, $LM_{2\text{comp}}$, $B_{org\text{comp}}$, and $PD_{2}$. $LM_{1}$, $LM_{2}$, and $B_{org}$ are then recovered through decompression. For $LM_{2}$ and $B_{org}$, the difference values which hold the watermark bit are then restored to reconstruct the original RONI. Using $LM_{1}$, $B_{1}$ can be extracted from ROI using Alattar’s quads method. $B_{1}$ is then decomposed into $PD_{1}$ and $H_{roi}$. The quad groups holding the watermark bit are restored during extraction to reconstruct the original ROI. $PD_{1}$ and $PD_{2}$ are then concatenated together and decompressed to obtain the patient’s data.

A hash message is then calculated from the recovered ROI and if it is equal to $H_{roi}$ then the mammogram is considered authentic. Otherwise, the mammogram is regarded as tampered.

6.3 CUDA acceleration

A MATLAB prototype was first implemented to assist in the division between CPU and GPU. We then run a performance profiling exercise on the prototype. From the profile we determined the sub-processes that are computational intensive and these sub-processes then analyzed for their suitability for GPU acceleration. Among these, the sub-processes that are parallel in nature are chosen to be implemented first.
Overall, in embedding operation, the Gaussian Pyramid decomposition, set classification and embedding sub-process were chosen to be ported onto CUDA [64]. Whereas for the authentication, adoption was applied to the set classification and region recovery sub-processes.

In the embedding process, the Gaussian Pyramid decomposition is the major focus of CUDA adoption. The construction of the Gaussian pyramid decomposition for the saliency map was done via naïve implementation by completing several runs of convolution of a 2D Gaussian filter on the input image with each run completing a level of the Gaussian Pyramid. Each CUDA thread in a CUDA block is responsible to load an equally size segment of image data from the global memory onto the shared memory of their respective block and then completes a convolution to a single pixel. The memory-loading phase was aided by the GPU’s hardware texture to avoid uncoalesced global memory read. As the saliency map is generated, ROI and RONI will be able to be sorted into respective vectors for speedier further processes.

The set classification sub-process refers to the classification of the RONI and ROI data into difference sets as proposed in Tien’s and Alattar’s DE scheme. This process followed after the regions had been sorted out from input image. The implementation of this sub-process is straightforward as the vectors were in one dimension. Each CUDA thread operates on one member in the vector thus labeling them into different sets as required for the embedding sub-process to take place. Then, the CPU side will need to prepare and package the necessary bit stream needed for embedding. After this, the actual embedding sub-process will be able to take place in GPU by adopting similar strategy where each threads handling one member in the vectors.

In the authentication process, the set classification sub-process is identical to the set classification sub-process in embedding process with minor difference in the classification condition. On the other hand, the region recovery sub-process in authentication operation, as its name suggest, removes the embedded bit stream from ROI and RONI vector, thus recovers the original image. It is in fact the reverse of the embedding sub-process in embedding operation. Therefore, similar strategy is adopted for them.
6.4 Experimental results

A few digital mammograms from the mini-MIAS database of mammograms has been used to evaluate the effectiveness and practicality of the scheme provided.

6.4.1 ROI Selection

![Original input mammogram](image)

**Figure 36 Original input mammogram.**

(a) ![Direct binarizing](image) (b) ![Saliency map binarizing](image) (c) ![IMPT on saliency map](image)

**Figure 37** (a) Direct binarizing (b) Saliency map binarizing (c) IMPT on saliency map

Figure 37 shows the ROI map (high level pixels represent ROI, while low level pixels represent RONI) of Figure 36. Figure 37(a) shows the ROI map constructed by direct binarizing the original input mammogram. While Figure 37(b) shows the ROI map constructed through binarizing the saliency map of the input mammogram. Lastly Figure 37(c) shows the ROI map constructed from thresholding the saliency map of the input mammograms using IMPT. We adopted the method of constructing Figure 37(c) in our scheme.
6.4.2 Visual Quality

![Original image](a) ![Watermarked image](b)

Figure 38 (a) Original image. (b) Watermarked image.

<table>
<thead>
<tr>
<th>Image</th>
<th>Character of Background</th>
<th>Class of Abnormality</th>
<th>Size of Image (ROI %)</th>
<th>Embedding Capacity (bpp)</th>
<th>PSNR</th>
<th>SSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>mdb001</td>
<td>G</td>
<td>CIRC</td>
<td>26.5</td>
<td>45.73</td>
<td>0.9798</td>
<td></td>
</tr>
<tr>
<td>mdb038</td>
<td>D</td>
<td>NORM</td>
<td>21.7</td>
<td>46.41</td>
<td>0.9809</td>
<td></td>
</tr>
<tr>
<td>mdb072</td>
<td>G</td>
<td>ASYM</td>
<td>21.5</td>
<td>46.91</td>
<td>0.9813</td>
<td></td>
</tr>
<tr>
<td>mdb124</td>
<td>G</td>
<td>ARCH</td>
<td>24.5</td>
<td>46.39</td>
<td>0.9822</td>
<td></td>
</tr>
<tr>
<td>mdb175</td>
<td>G</td>
<td>SPIC</td>
<td>30.4</td>
<td>45.28</td>
<td>0.977</td>
<td></td>
</tr>
<tr>
<td>mdb211</td>
<td>G</td>
<td>CALC</td>
<td>34.2</td>
<td>45.36</td>
<td>0.9776</td>
<td></td>
</tr>
<tr>
<td>mdb264</td>
<td>G</td>
<td>MISC</td>
<td>37.5</td>
<td>44.79</td>
<td>0.977</td>
<td></td>
</tr>
</tbody>
</table>

Table 7 Embedding results for 7 mammograms of different class of abnormality present.

Seven mammograms of different class of abnormality present with same image dimensions were used to test our scheme. All the mammograms used are of the
same size (1024x1024). Figure 38 shows one of the mammograms used to test the scheme in its original version and watermarked version. Table 7 shows the results of the embedding process of the scheme. The character of background tissue and the class of abnormality present is explained in Section 3.6.2.

The watermarked mammograms show good visual quality in terms of Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity (SSIM). The mammograms authentication scheme also shows high embedding capacity (with average of >0.53). The watermarked mammograms by the scheme were proven reversible by comparing the extracted mammograms with the original mammograms pixel by pixel. The authenticity of ROI can also be verified by comparing the embedded hash extracted with the recalculated hash of the reconstructed (reversed) ROI. From the results, the original mammograms can be reconstructed exactly in case of no tamper detected.

### 6.4.3 Speed Enhancement between CPU and GPU

A mammogram as shown in Figure 39 was used to demonstrate the speed enhancement achieved in CUDA porting. The sample was upsized linearly forming another 5 samples with increasing dimensions in both directions. The step size of the upsizing is 100% in both directions in dimension. The processing time for the embedding process of the samples of different size of the scheme in MATLAB, scheme ported to CPU through openCV, and scheme ported to GPU, were shown in Table 8.

In this attempt, the hardware employed was NVIDIA GeForce 9500 GS on a workstation equipped with Intel Core2 Quad Q9400 2.66GHz as CPU.
Table 8 Processing time for the embedding process of the scheme.

As indicated in Table 8, the speed improvement of CUDA is visible at larger input data size. At small data size, the overall embedding operation was overwhelmed by the time required for data transferring between GPU and CPU memory. However, as data size grows, this dominating factor become less significant where the processing of data took over most of the overall processing time.

6.5 Summary

In this chapter, we proposed to enhance the speed of watermarking process by porting it to CUDA. We proposed a ROI-based reversible fragile watermarking scheme for mammograms using two difference expansion methods: Tian’s DE and Alattar’s DE of quads. The scheme defined the ROI automatically by using the selective visual attention-driven model proposed by Feng et al. and then binarized the saliency map constructed by improved moment-preserving thresholding.
For speed enhancement, the CUDA platform was utilized. A MATLAB implementation of the scheme was first developed to profile and identify the sub-processes that are suitable for parallel processing. After which, we have selected the identified tasks to be developed in CUDA to accelerate the embedding process. From the experimental work, we conclude that the optimized result is achieved in the appropriate selection of suitable tasks for parallel processing.
Chapter 7: Conclusion

7.1 Summary

A content authentication scheme for medical media has been implemented with five automated ROI definition methods been proposed. In this case, digital mammograms were used for illustration purposes. Furthermore, an analysis has been carried out to compare the characteristics of the automatic ROI definition methods. In addition, the scheme proposed is capable of embedding related medical information into the host images and hence eliminated the need to attach the metadata to the images or to send the data separately.

The experiments have shown the practicality of the multi-layered watermarking approach on digital mammograms. It is however necessary to have segmentation works done on the medical images. The aims to define the ROI and RONI for different layer watermarking are to protect the integrity of the ROI, maximizing the embedding capacity while keeping the ROI at a high visual quality for more readability to human nude eyes. In addition, a good visual quality on the ROI is important for a diagnosis process.

The scheme developed has overall exhibited a good performance with a relatively higher embedding capacity and an improved visual quality than a single-layered watermarking process. The scheme is capable of embedding the metadata into the images, whereas it eliminates the redundancy data to be attached to the medical images (i.e. DICOM images). While providing a relatively large embedding capacity, the authentication feature on the scheme is used to protect the integrity of the medical images and to prevent unauthorized modification on the watermarked images. Meanwhile, the automated ROI defining feature eliminates the need to define the ROI explicitly by hand. This has eased the task of selecting the medical importance region on the medical images to retain its integrity.
Another key aspect when evaluating the scheme is to test them in realistic scenarios. The practicality of the scheme is tested with digital mammograms from mini-MIAS database while the processing speed of the scheme is enhanced by using CUDA to meet the real-time requirement. As for the practicality of the automated ROI defining methods, the block average method has the least complexity to develop, while it is capable to provide a large embedding capacity. The saliency map method has lesser embedding capacity comparing to the block average method, and the IMPT method has the least embedding capacity in comparison. However, the embedding capacity is related inversely to the visual quality for these three methods. Meanwhile, the fuzzy logic method has the highest complexity of development while keeping the automated ROI defining accuracy to the highest. However, this method does not show a stable relationship between the embedding capacity and the visual quality. This method is suggested if the processing time is not a concern in certain scenarios for its ROI definition accuracy since the Works with ROI defined using this method still remain a high visual quality (>40dB). Else, the other three methods are suggested.

From the empirical study in Chapter 6, has shown that it is possible to develop a real-time multi-layered semantic-based watermarking scheme up. The main problem that occurs in setting up a real-time device is all the clients using this watermarking scheme have to be CUDA-enabled (to have CUDA device installed on the clients).

### 7.2 Further studies

Digital watermarking in the medical field is gaining increasing research interest. Therefore, there are many research activities and a series of issues remained to be solved. Due to the limitation of time and resources, we have only focused on the fragile watermarking and image segmentation. However there are many issues that could be subjected to further studies.

First of all, some of the refinement could be made to the proposed scheme:

- More combinations of watermarking techniques to meet different scenarios.
• More image segmentation techniques to apply on different modal of biomedical data.

• More information security approaches to lift the security level of the protected images.

• Other features such as image recovery and robust watermarking to suit different kind of applications in medical domain.

• Solutions to reduce the redundancy to be transmitted from the encoder to the decoder (cf. Chapter 5).

Secondly, there are issues related to the simulator environment could be subjected to further studies:

• Other programming languages or devices or combinations of them that could speed up the watermarking process.

• Schemes to aid in diagnosis process.

• Development of a device for watermarking on the video in medical field.
References


List of Publications
