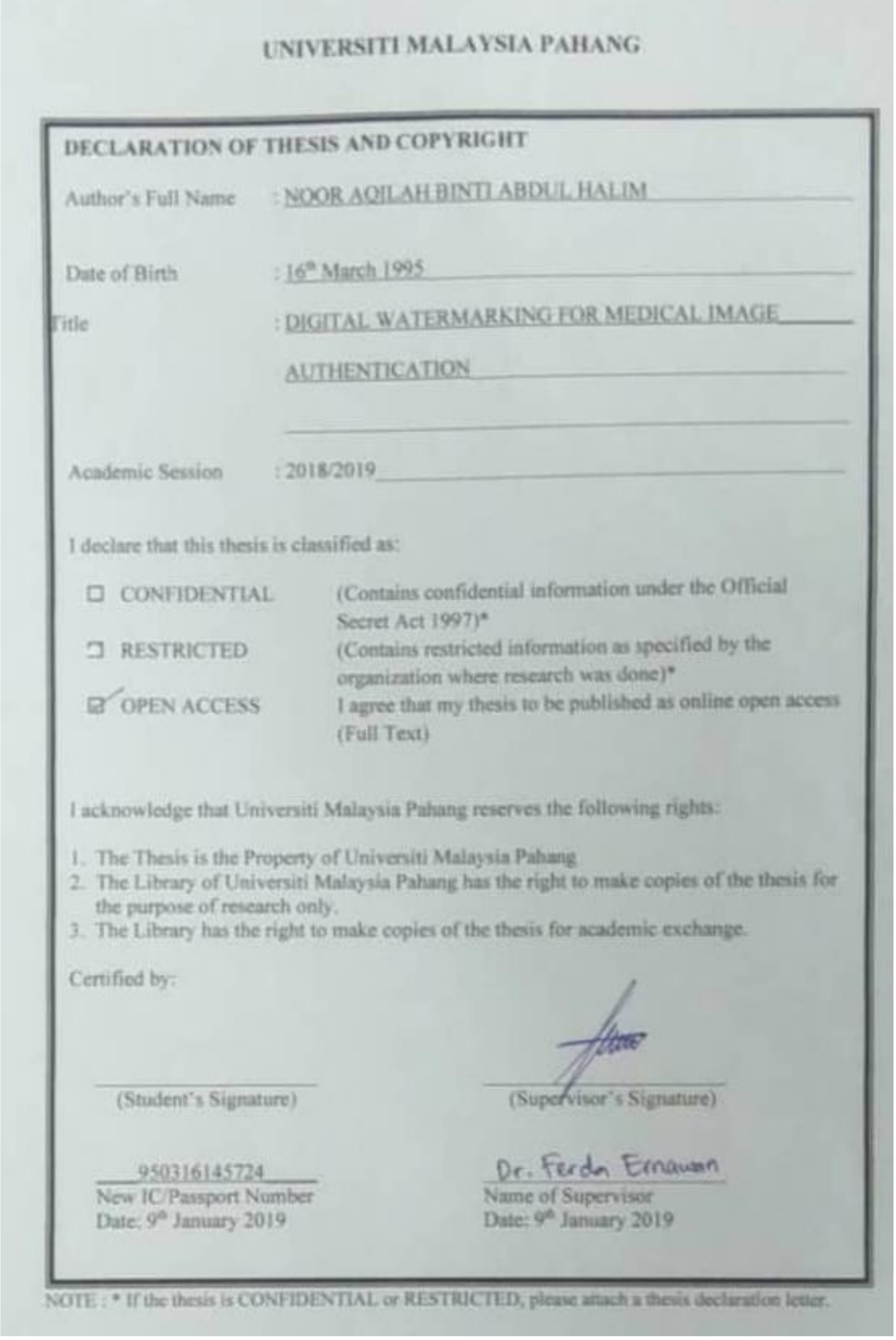
DIGITAL WATERMARKING FOR MEDICAL IMAGE AUTHENTICATION

NOOR AQILAH BINTI ABDUL HALIM

BACHELOR OF COMPUTER SCIENCE
UNIVERSITI MALAYSIA PAHANG



UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : NOOR AQILAH BINTI ABDUL HALIM

Date of Birth : 16th March 1995

Title : DIGITAL WATERMARKING FOR MEDICAL IMAGE AUTHENTICATION

Academic Session : 2018/2019

I declare that this thesis is classified as:

☐ CONFIDENTIAL (Contains confidential information under the Official Secret Act 1997)*

☐ RESTRICTED (Contains restricted information as specified by the organization where research was done)*

☑ OPEN ACCESS I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Universiti Malaysia Pahang reserves the following rights:

1. The Thesis is the Property of Universiti Malaysia Pahang
2. The Library of Universiti Malaysia Pahang has the right to make copies of the thesis for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

(Student's Signature)	(Supervisor's Signature)
950316145724	Dr. Ferda Ernawan
New IC/Passport Number	Name of Supervisor
Date: 9th January 2019	Date: 9th January 2019

NOTE : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach a thesis declaration letter.

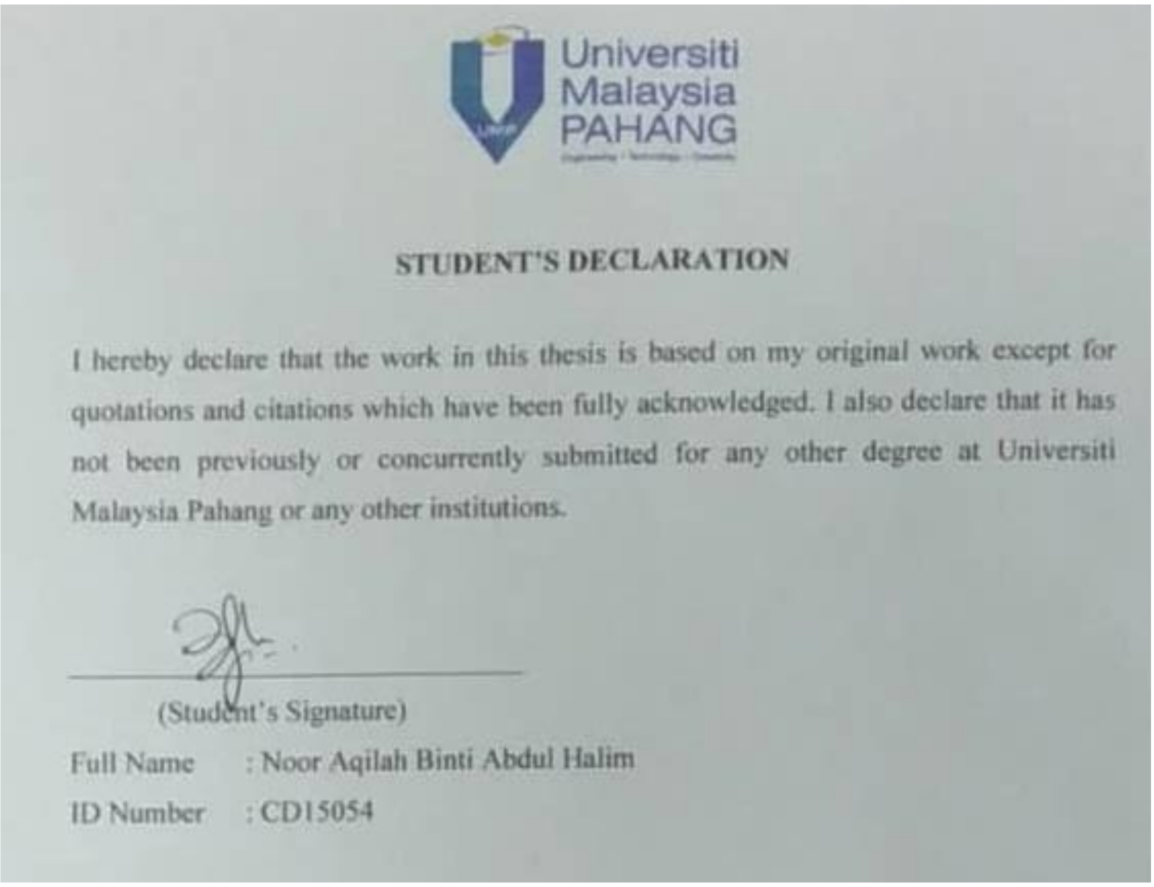
Universiti
Malaysia
PAHANG

SUPERVISOR'S DECLARATION

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

(Supervisor's Signature)

Full Name	: Dr. Ferda Ernawan
Position	: Senior Lecturer
Date	: 9th January 2019



Universiti
Malaysia
PAHANG

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been fully acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

(Student's Signature)

Full Name : Noor Aqilah Binti Abdul Halim

ID Number : CD15054

DIGITAL WATERMARKING FOR MEDICAL IMAGE AUTHENTICATION

NOOR AQILAH BINTI ABDUL HALIM

Thesis submitted in fulfillment of the requirements for the award of the degree of
Bachelor of Computer Science (Graphics & Multimedia Technology)

Faculty of Computer Systems & Software Engineering
UNIVERSITY MALAYSIA PAHANG

JANUARY 2019

ACKNOWLEDGEMENTS

Upon completing this thesis, I was in many contacts with many people, researchers and academicians. They have contributes so much towards improving my understanding in this field. In particular, I wish to express my greatest gratitude to my thesis supervisor, Dr. Ferda Ernawan. Without his continued advice, support and guidance, this thesis wouldn’t possibly be able to be completed as presented. Special thanks to Dr. Liew Siau Chuin who was so kind to share with me his previous research content that had helped me develop an improve method from his previous scheme.

I would like to thank my Final Year Project coordinator, Sir Mohd Arfian bin Ismail and Faculty of Computer Systems & Software Engineering of Universiti Malaysia Pahang for providing the needed resources, information, and knowledge required to complete my thesis.

I would like to thank my family and friends who have supported and motivated me whenever I needed it. Lastly, I would like to apologize to those I might have missed out to mention who had helped me throughout the process of completing this thesis.

ABSTRAK

Pengaruh imej digital dalam bidang perubatan telah membawa impak pada masa kini. Walau bagaimanapun, dengan peningkatan penggunaan imej perubatan dalam bentuk digital, turut meningkat potensi imej untuk terdedah kepada ancaman diubahsuai. Oleh itu, amatlah penting agar imej perubatan dilindungi daripada sebarang kerosakan. Watermarking digital sangat sesuai untuk diunakan dalam situasi ini. Tujuan penyelidikan ini adalah untuk mencadangkan kaedah penambahbaikan bagi pengesahan keaslian imej perubatan. Imej watermark akan dimasukkan ke dalam imej perubatan dengan menggunakan skema watermarking yang rapuh. Selepas itu, imej yang diagihkan akan diuji dengan pelbagai jenis ancaman seperti potongan dan pemampatan sebelum watermark tersebut diekstrak dari imej perubatan untuk memeriksa keasliannya. Watermarking yang boleh diterbalikkan memberikan mampu mengesahkan imej asal dan dapatkan kembali watermark yang telah ditanam. Untuk kajian ini, skema watermarking yang rapuh dijangka akan memastikan watermark yang tertanam akan musnah dengan mudah jika imej watermarked mengalami sedikit pengubahsuaian untuk membuktikan kesahihan imej perubatan. Ini akan membantu membuktikan kesahihan imej perubatan.

ABSTRACT

The influence of digital image in the fields of medical line had become a major impact nowadays. However, with the increasing use of medical image in digital form, so does the potential of the image to be exposed to threat of being modified. Therefore, it is crucial for the medical image to be protected from unauthorized usage. Digital watermarking serves well for this situation. The aim of this research is to propose an improve method for watermarking authentication of medical image. Watermark image will be embedded into the medical image by using fragile watermarking schemes. Afterwards, the watermarked medical image will be tested with various type of threat such as cropping and compression before the watermark is extracted back from the watermarked medical image to inspect its' authenticity. Reversible Watermarking provides the authentication that can retrieve the original image and the watermark. For this research, fragile watermarking is projected where the method of operation is to let the embedded watermark to be destroyed easily if the watermarked image undergoes even slight modification in order to prove the authenticity of the medical image. This will help in proving authenticity of medical images.

TABLE OF CONTENT

CONTENT **Page**

CHAPTER 1 INTRODUCTION

CHAPTER 2 LITERATURE REVIEW

CHAPTER 3 METHODOLOGY

CHAPTER 4 RESULT AND DISCUSSION

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

NROI	Non Region of Interest
ROI	Region of Interest
RLE	Run-length Encoding
LSB	Least Significant Bit
RONI	Region of Non Interest

CHAPTER 1

INTRODUCTION

1.0 INTRODUCTION

Nowadays, digital media have evolved the way still image are used, stored and transmitted, allowing growth to a wide range of new application that are expected to make an important impact on the multimedia industry. One of the advantages of digital multimedia is the ease of accessed, manipulation and duplication (Rippa & Secundo, 2018). However, this feature brought a major side effect since it causes unauthorized alteration of information such as data piracy. Hence, intellectual property rights protection of stored and transmitted images is a very important concern (Khanduja, 2017). Watermarking is a great way to help protecting the property rights of digital media. Digital watermarking is a process of embedding data into digital multimedia contents (Techopedia Inc, 2018). It can prove the originality of the content or to verify the identity of the digital content's owner.

Robust watermarking has a main goal which even when the watermarked image endures accidental or purpose attacks, the watermark embedded in the original image will be unaffected and can be extracted and identified (Pramila, Keskinarkaus, & Seppänen, 2018). Therefore, it is suitable for ownership verification. Meanwhile, fragile watermarking is used to verify the authenticity and integrity of digital images (Renza, L., & Lemus, 2018). Fragile watermarking can help prove the authenticity of medical image by proving the presence of tamper and mark it (Hisham, Muhammad, Badshah, Johari, & Zain, 2017).

1.1 EXISTING METHOD FOR IMAGE AUTHENTICATION

Previously, a few methods had been proposed for fragile watermarking to be used for medical image authentication. A dual watermarking method was proposed by Qiang and Hongbin for tamper detection and self-recovery by embedding the watermark data in two regions, which are in least significant bit (LSB) and the discrete wavelet transform (DWT) of the host image. The objective is to make sure that if any alteration occurs to at LSB, the data is still safely secured in DWT for the recovery process (Song & Zhang, 2010). The scheme proposed by (Bravo-Solorio & Nandi, 2011) has been suggested which integrating two methods to strengthen the tampering localization ability, which are a secure block-wise resilient to cropping mechanism and an iterative pixel-wise mechanism. It is said that this method manages to prevent cropping attack (Bravo-Solorio & Nandi, 2011). Block-based mechanism is a famous method for fragile watermarking. The researchers (Lin, Yang, & Xu, 2011)also used block-based mechanism for tampering detection, but the focus is on colour image. The algorithm has two main steps to locate any tampered region, which are a rough judgment and an accurate judgment step (Lin, Yang, & Xu, 2011). Another scheme for authentication proposed, involve the approach of RONI and ROI. The embedding locations for the watermarking bits are based on a chaotic key (Nasseem, Qureshi, Atta-ur-Rahman, & Muzaffar, 2013).

Image watermarking for medical image authentication focus more on determine whether the medical image authenticity is proven or not (Arsalan, Qureshi, Khan, & Rajarajan, 2017). Although the recovery feature is very helpful for the doctors to easily know whether the image is authentic or not but the most crucial process is to determine the validity of the image, whether any attack is performed or not and whether the manipulation could bring harms or misleading to the diagnosis. Therefore, the research will not cover on recovery of the altered medical image.

The numbering with spiral pattern method is not suitable for rectangular images. The scheme could only be embedded onto the square part of the centre and will leave the top and bottom uncovered from watermark thus making the result very promising when the tamper occurs only on the watermark region (Hisham, Muhammad, Badshah, Johari, & Zain, 2017). Hence it becomes a flaw to this method as it did could not perform well in non-square images while it is a norm since most medical images are produces or scanned in rectangle shape.

The objective of this research is to propose a more secure method to be used for medical image authentication. Thus, by comparing three methods from previous research, the advantages and drawback of implementing each method will be discuss.

1.2 RESEARCH QUESTION

Q1: What is the suitable watermark embedding technique for medical image authentication?

This research question asks about the suitable watermarking scheme to be used to test the medical image authenticity. The embedding scheme used must be convenient to help detecting if there is any alteration done on the medical image. The watermarking scheme use should be fragile against any attack to ensure that the medical image authenticity can be proven when there is no alteration detected due to the watermark not destroyed. The watermarking scheme should not cause the medical image to lose its' quality.

Q2: How can we locate modified part of the medical image to test its' authenticity?

This research question proposed that the process to locate the altered part is important to test the authenticity of medical image. The slightest change or alteration should be able to be recognized on the medical image.

Q3: How can we evaluate the performance of watermarking for medical image authentication method?

This research question asks about the best way to verify the performance of the each method for medical image authentication. There is a lot of existing method for image authentication which can be made as a reference on evaluation of the best authentication detection for medical image.

1.3 RESEARCH PROBLEM

Table 1.3 Research Problems

Problem	**Description**	**Effect**
The TALLOR embedded the watermark in a sequence order in selected Region of Non Interest (RONI). (Zain S.-C. L., 2011)	The embedded data coordinate is easily detected and replaced with new data.	Image is falsely detected as authentic.

From Table 1.3, it is shown that the Tamper Allocation and Lossless Recovery (TALLOR) have its flaw when it comes to embedding onto LSB of medical image in sequence. During embedding process the method proposed by (Siau-Chuin Liew, 2012) the scheme will embedded the watermark bits directly into the LSB of the RONI of original image in a one single line. When the watermarked image is tampered and the watermark bits in the RONI are changed, the image could be falsely detected as authentic. Therefore, an improvisation is needed to overcome this problem.

1.4 RESEARCH AIM AND OBJECTIVES

Based on the previous research questions, a research aim is formed.

The aim of this research is to propose an improved method for medical image authentication where the tampered area is easier to be detected and the watermark extracted is less perceptual. By doing this, it will help to prevent any unauthentic medical image be used for diagnosis which may caused to fault diagnosis by doctor.

Research objectives related to each research question is generated to accomplish the research aim. Three main objectives had been identified for this research and are listed as follow:

Aim and Objective:

i. To embed a watermark randomly into medical image by using Arnold Transform with secret key.

ii. To embed a watermark randomly into medical image by using Mersenne Twister with secret key.

iii. To test the performance of the proposed method of watermarking for image authentication with existing method.

1.5 RESEARCH SCOPE

The scope of this research is stated as below:

1. The type of digital media used will be image only.
2. The project will focus on medical image of ultrasound scan.
3. The image use is 480×640 pixel.

1.6 RESEARCH CONTRIBUTION

In this research, different method of watermarking scheme and detection will be investigated to test the medical image authenticity. The research will help contribute as follow:

1. Increase security of information transferred from one hospital to another.
2. Reduce the possibility of having the medical image altered irresponsibly.

1.7 THESIS ORGANIZATION

This thesis consists of five chapters. Chapter one discuss on the introduction to the project. Chapter 2 discusses about the study of the project in general through the existing proposed method. It describes the previous solutions to solve the issue.

CHAPTER 2

LITERATURE REVIEW

2.0 INTRODUCTION

In this chapter, we will discuss on the studies done by previous approach of digital watermarking for image authentication. By studying this research, methods used can be learn easily and modified to improve existing system.

2.1 CHAOS BASED INVERTIBLE AUTHENTICATION

A method which used Least Significant Bit (LSB) scheme as its method to embedded the watermark into the image (Nasseem, Qureshi, Atta-ur-Rahman, & Muzaffar, 2013). The scheme is performed by hiding data in the lower bit of the image pixels to prove the authenticity and integrity of the medical image (Zain, Baldwin, & Clarke, 2004). The study also provide extra feature for the ability to detect the tampering region besides recover the altered part of the medical image (ZHou, Huang, & Lou, 2001). This method focuses on the use of chaotic key to propose a secure and invertible authentication. First, the watermark information is scrambled with Arnold transform and then perform compression through RLE to enhance the capacity since the capacity must be high in reversible data hiding techniques (Nasseem, Qureshi, Atta-ur-Rahman, & Muzaffar, 2013). This scrambled and compressed watermark information (Nasseem, Qureshi, Atta-ur-Rahman, & Muzaffar, 2013) is embedded in the LSB's of NROI pixels of host image through a chaotic key. Considering that the watermark embedded is fragile, hence in case of any tampering, the receiver end will indicate that someone has meddled with the image. The advantage of using chaotic system is it is very relevant to represent real world system due to their sensitivity to initial conditions. Moreover, the behavior of this system is almost unpredictable by analytical methods when the secret key is unknown.

This method is separated into two stages of encoding and decoding with main steps as shown in Figure 2.1.1 and Figure 2.1.2 below:

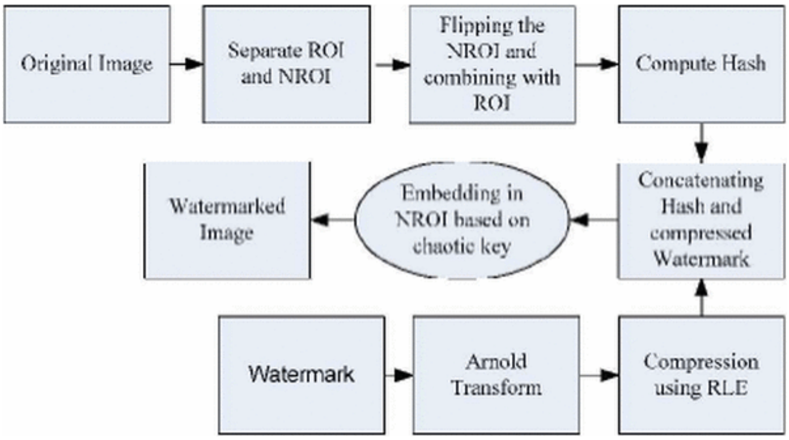

Original Image
Separate ROI and NROI
Flipping the NROI and combining with ROI
Compute Hash
Concatenating Hash and compressed Watermark
Embedding in NROI based on chaotic key
Watermarked Image
Watermark
Arnold Transform
Compression using RLE

Figure 2.1.1 Encoding Stage (Nasseem, Qureshi, Atta-ur-Rahman, & Muzaffar, 2013)

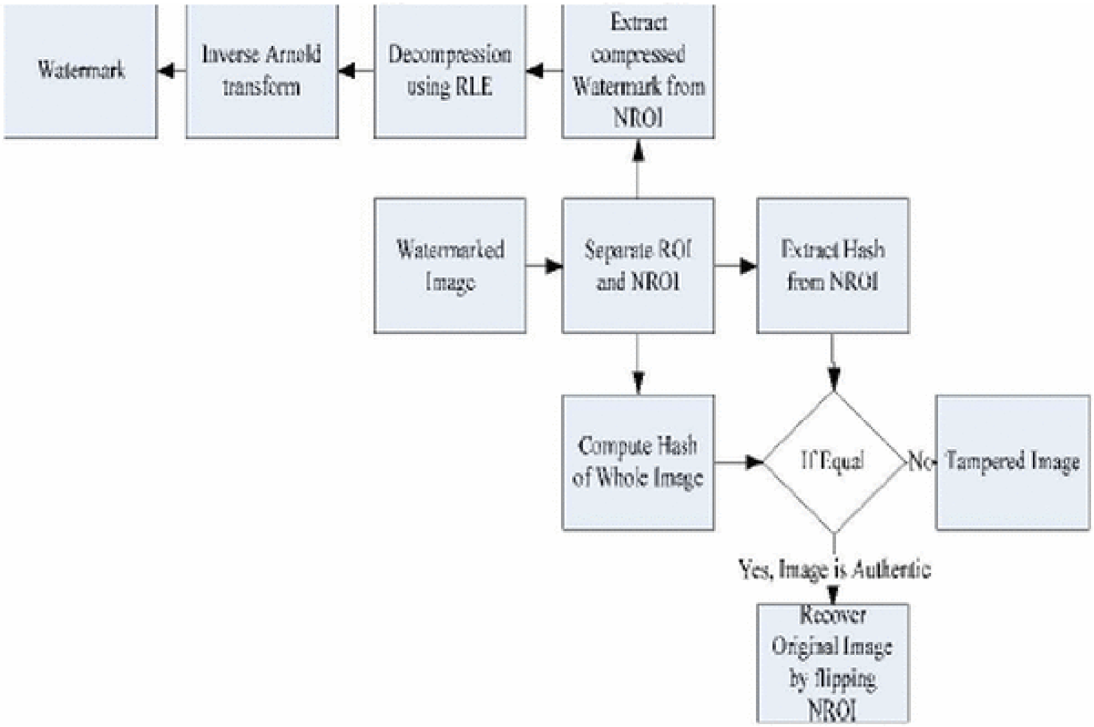


Figure 2.1.2. Decoding Stage (Nasseem, Qureshi, Atta-ur-Rahman, & Muzaffar, 2013)

In Figure 2.1.1 it shows that the encoding stage starts with separating the ROI and NROI portion of host image. Then, all pixel of NROI portion are arranged into same arbitrary vector. Afterwards, the chaotic sequence will be generated and map into integers. The chaotic sequence generated will then be used to make the LSB's of selected pixel in NROI to zero. The NROI pixel is then rearrange with ROI to form an image and then calculate the hash of whole image. The hash obtained is converted into bits and stored as hash 1 (Nasseem, Qureshi, Atta-ur-Rahman, & Muzaffar, 2013). The watermark logo that contains patient information is read and converted into bits and stored as hash 1. RLE encoding is performed on the concatenated watermark for compression Then the NROI pixels is arranged again in n arbitrary vector and the concatenated watermark is embedded on the basis of a chaotic sequence. The watermarked image is formed when NROI pixels is rearranged with ROI pixels.

Afterwards, as shown in Figure 2.1.2, the decoding stage starts with separating the ROI and NROI region in the watermarked image. All the NROI pixels are arranged in some arbitrary vector. Now, with the knowledge of the same chaotic key at embedding step, the watermark pixels are specified. This will provide location for extraction of the concatenated watermark from NROI. The concatenated watermark from the LSB's of NROI pixels is extracted using the chaotic sequence before putting a value 0 at the specified location. Hash1 and watermark is separated from the concatenated watermark. Then the NROI pixels are again rearranged with ROI pixels to form an image. The hash of the image is again computed and stored in Hash2 to restore the original image.

To test the authenticity of the image, Hash1 and Hash2 will be compared, if both hash are the same then the image is considered authentic, otherwise the image is mark as tempered (Nasseem, Qureshi, Atta-ur-Rahman, & Muzaffar, 2013).

An invertible and fragile watermarking for medical image is used for this method. During watermarking, the process of transmitting embedding location as a separate map with the image is unnecessary. With the knolwedge of a single chaotic key is known at the receiver end, watermark along with the host image can be extracted. The resulting image is proven fragile against any tampering.

2.2 TAMPER LOCALIZATION AND LOSSLES RECOVERY WATERMARKING SCHEME

The Tamper localization and lossless recovery watermarking scheme (TALLOR) proposed a simple tamper localization and recovery scheme that uses lossless compression. The lossy compression is applied in the scheme if necessary (Zain S.-C. L., 2011). This scheme is applied on medical image like ultrasound scan image.

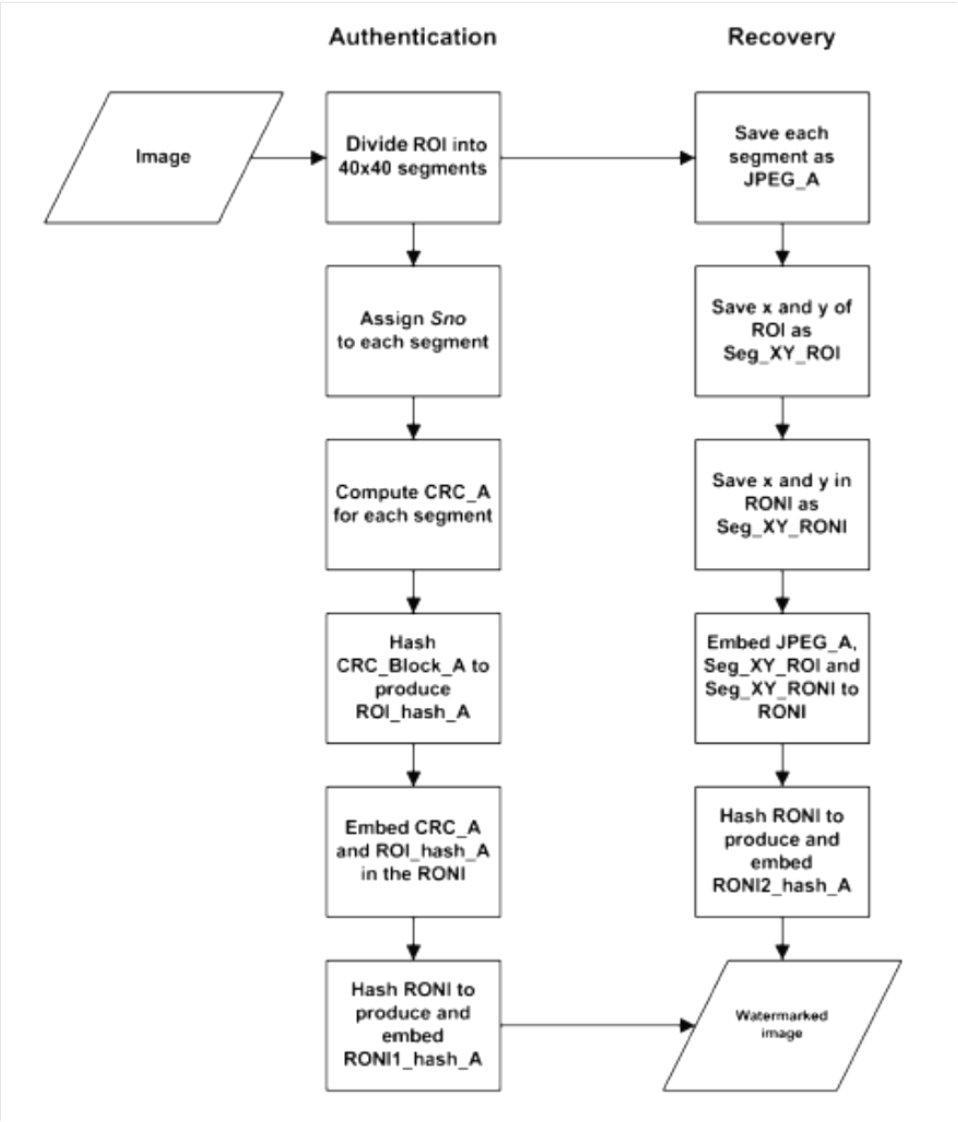

Authentication
Recovery
Image
Divide ROI into 40x40 segments
Assign *Sno* to each segment
Compute CRC_A for each segment
Hash CRC_Block_A to produce ROI_hash_A
Embed CRC_A and ROI_hash_A in the RONI
Hash RONI to produce and embed RONI1_hash_A
Save each segment as JPEG_A
Save x and y of ROI as Seg_XY_ROI
Save x and y in RONI as Seg_XY_RONI
Embed JPEG_A, Seg_XY_ROI and Seg_XY_RONI to RONI
Hash RONI to produce and embed RONI2_hash_A
Watermarked image

Figure 2.2a TALLOR Scheme Watermark Generation and Embedding and Recovery (Zain S.-C. L., 2011)

As shown in Figure 2.2a, the TALLOR schemes consist of two parts, the authentication part and image recovery part. The original medical image is first divided into region of interest which is the important most part of the medical image and several region of non interest (RONI). The medical image region of interest (ROI) is divided into 40×40 segments and each segment is numbered. Compute the Cyclic Redundancy Check for each segment. The CRC value is hashed to produce hash value of the region of interest. The CRC value and the hashed value of the ROI is embed into the RONI.

After embedding, the TALLOR schemes also propose a recovery method to help recover the ROI if there is any tamper occur. The recovery process starts by taking the medical image and divide it into 40×40 segments of ROI. Each segment of ROI is saved as JPEG. The scheme then save the x and y value of the ROI and store it in RONI. JPEG of RONI is embeds to RONI. The selected RONI is hash and embed into a different RONI.

2.3 NUMBERING WITH SPIRAL PATTERN

This method uses a unique numbering method which is spiral pattern that is proven to have a better distribution of embedded bits. Its' watermarking scheme capacity is small but sufficient (Hisham, Muhammad, Badshah, Johari, & Zain, 2017). The authentication data is embedded on the host image entirely regardless the region of interest (ROI) or region of noninterest (RONI). This ensures that all data is covered by authentication bits and recovery bits when part of the area is attacked or tempered. It allows localization to works on all data. This method used fragile watermarking scheme to alert the receiving end of the tempered region in the image. The scheme is effective as it scan the image twice with the inspection view encoding to a bigger block. Both tamper detection and recovery for tampered image can be performed through this scheme (Hisham, Muhammad, Badshah, Johari, & Zain, 2017).

This watermarking method is based on ideas reflected by the family of fractal based language (Scan) which is used mainly to encrypt 2D digital image. The numbering with spiral pattern method is also an improvement from the Authentication Watermarking with Tamper Detection and Recovery (AW-TDR) by Zain and Fauzi (Zain & ARM, 2006). The embedding process is as shown in Figure 2.1.1. The scheme is generated to ensure the recovery bit of each original block will be embedded as far as possible. This way can secure that although the image has been attacked with various attacks, the recovery bit can still be retrieved and the image is recoverable.

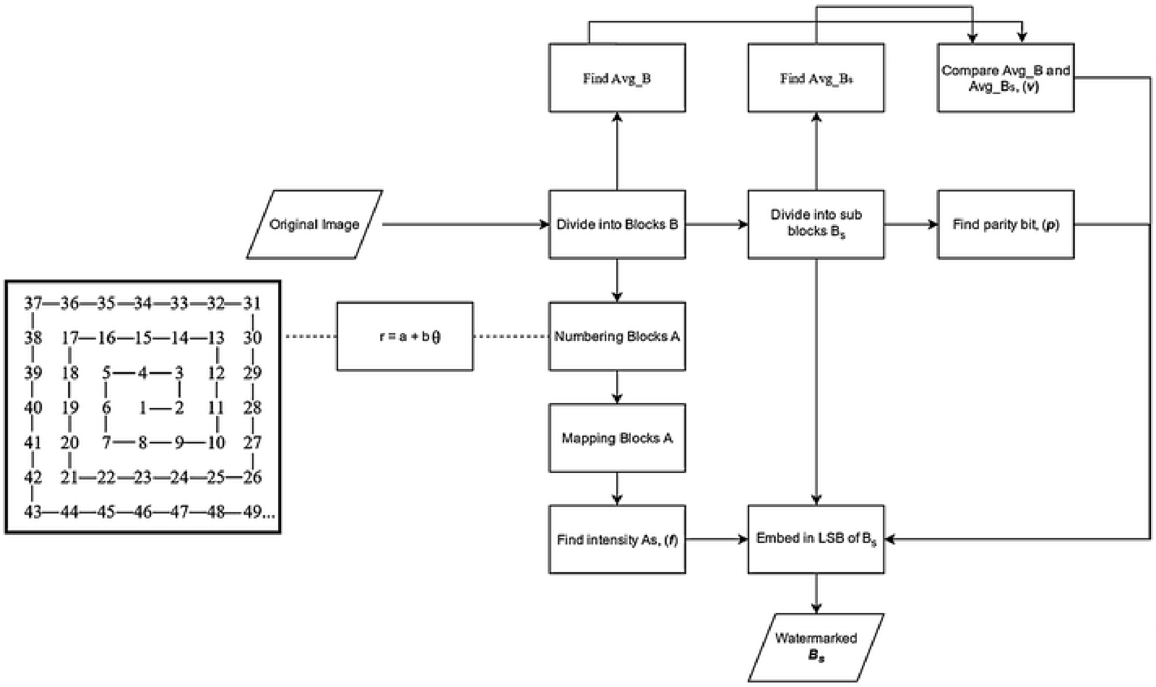


Figure 2.3a Functional Block Diagram for Watermark Numbering, Mapping, Generation and Embedding In the Proposed Scheme (Hisham, Muhammad, Badshah, Johari, & Zain, 2017)

This method starts with numbering the host image blocks in spiral pattern. Each block size is pre-determine where blocks per row and blocks per column are determine based on the width and the height of the image (height/block size, width/block size). Then, a key number is set using equation k = max (primes(numblock/2)). Afterwards, calculate the coordinate of each block to get the center of the block then the block is numbered in spiral manner. Ring level of the blocks is determined and all blocks are mapped. The method will then proceed to generating watermark and embedding using three-tuple watermark. The LSB of each pixel within the block is set to zero before the average intensity of the block and its sub-block is calculated. Authentication watermark and parity check bit is generated for each sub-block. Host image is then obtained from the mapping sequence and stored as recovery information. The average intensity of every small block is calculated again and retrieves the recovery intensity. Lastly, perform the three-tuple watermark in each one LSB of each pixel.

Numbering with spiral pattern used hierarchical tamper detection scheme. At level 1 detection LSB of each pixel is set to zero and average intensity of each sub-block is computed. The average comparisons and parity bits are compared to determine if the level is tempered. Meanwhile at Level 2 Detection, for each block of size 8 × 8 pixel the block number of block C is located. When the block is recognized as tempered, the block will be assumed as valid. Given that block C is valid, 7-bit intensity of each sub-block by taking the LSB from each pixel in the block within block C. Zero padding is added to the end to make an 8-bit value. Finally, compare the average sub-block and mark the block as tempered if they are different.

The use of block average intensity in tamper localization is proved as easy to perform without much calculation required. This scheme is able to find the altered region and mark it, and recover the tampered area to the valid image (Hisham, Muhammad, Badshah, Johari, & Zain, 2017).

2.4 COMPARISON TO THE EXISTING TECHNIQUES

Table 2.4a Comparisons of 3 Existing Techniques

Method	**Strength**	**Weakness**
1. Numbering With Spiral Pattern To Prove Authenticity And Integrity In Medical Images (Hisham, Muhammad, Badshah, Johari, & Zain, 2017)	➢ Watermark embedded is fragile with low imperceptibility. ➢ Embed all authentication data all over the image. ➢ Take fast processing time to embed. ➢ Tamper detection is accurate.	➢ Only works on grayscale images ➢ Works well on square images only.
2. Chaos Based Invertible Authentication of Medical Images (Nasseem, Qureshi, Atta-ur-Rahman, & Muzaffar, 2013)	➢ Watermark embedded is fragile with low imperceptibility. ➢ Chaotic behavior is unpredictable without secret key. ➢ Tamper detection is accurate.	➢ Can perform only on grayscale images
3. Tamper Localization And Lossles Recovery	➢ The most important region is protected. ➢ Can be applied on	➢ The hash of the ROI that is embeds is easily rewrite if the

Watermarking Scheme (Siau-Chuin Liew, 2012)	coloured medical image. ➢ Doesn’t need host image to test the authentication.	tamper image store its hash ROI into the same RONI. ➢ There is no secret key to protect the watermark information. ➢ Tamper is detected only if the ROI is tampered.

From the comparisons shown in TABLE 2.4, the strength and weakness of each method proposed by the previous research in image authentication will be discussed. Method 1 used spiral numbering pattern to number the block during watermark generation before embedding the watermark onto the of host image. The authenticity of each block is validated using parity check and intensity comparison to enhance accurateness of detecting the tampered region.

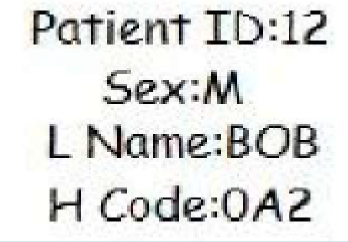
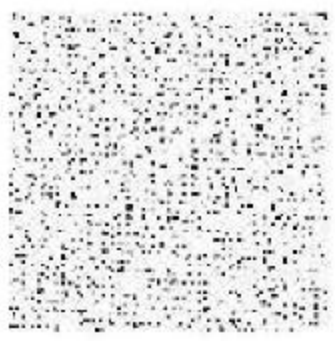
Table 2.4b Comparison with other watermarking methods that uses block-based mechanism

Method	Average PSNR value (dB)	Average processing time (s) to embed	Detection
Spiral manner numbering (Hisham, Muhammad, Badshah, Johari, & Zain, 2017)	67.26	0.9	Yes
2 LSBP embedding method (Bravo-Solorio & Nandi, 2011)	44	Not Stated	Yes
AW-TDR (Zain & ARM, 2006)	54.2	0.98	Yes
2D-DE (Hisham, Liew, & Zain1, A Quick Glance at DigitalWatermarking in Medical Images, 2013)	44.72	Not Stated	Yes

Table 2.4.2 displays the result comparing the spiral numbering method with other embedding method that uses block-based mechanism. At 0.9s average processing time taken to embed the watermark, it shows that the performance of this scheme is considered as fast since the time taken range between 0.2s to 2.5s. The average PSNR value of this scheme is 67.26 dB which is the closest to the highest value of 80 dB. The spiral numbering method is proven to be very good as the PSNR value is the highest among the other three studies from the Table 2.4.2.

In Method 2, the method focuses on using Arnold Transform to scramble and compressed the watermark information before embedded into the LSB's of NROI pixels of host image using chaotic key. This method is fragile against any tampering making it able to detect tampered region precisely. The watermark is securely embedded onto the host image while achieving high imperceptibility. The strength of this method relies on the chaotic behavior that is unpredictable without the knowledge of the secret key. However, this method performed best on grayscale image only. It hasn’t been tested on colour image.

Table 2.4c Security Analysis Result for Chaos Based Invertible Authentication

Condition	x(0)	r	Recovered Hash	Recovered Watermark
Exact initial condition	0.25	3.58	a16c4d371f512de40f836428ea2541	 Patient ID:12 Sex:M L Name:BOB H Code:0A2
Slight changed initial condition	0.25001	3.58	af51216c4d de40f836423718ea2541fe	

The security of this method is put to demonstration by using the same initial condition and slightly changes in initial condition at decoding stage afterwards. Table 2.4.3 shows that even the slightest change in the initial condition will destroy the recovered watermark and the recovered hash will be different as well. With the watermark failed to be recover when changes occur, it indicates that the image is tampered and proves that this method is highly secured.

Method 3 proposed a watermarking scheme for authentication that can be implemented on colored medical images. This method can test the authenticity of the image without using the original image. The scheme focuses on protecting the most important region on the medical image.

Table 2.4d Comparison of TALLOR scheme with Authentication and data hiding using a hybrid ROI-based

	Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images **(Al-Qershi OM, 2011)**	Tamper Localization And Lossles Recovery Watermarking Scheme **(Zain S.-C. L., 2011)**
Image Size	576×768.8 bit	480×640.8 bit
Watermark size (bits)	136,780	256
Embedding capacity	0.31	0.58
PSNR (dB)	36.7	48.3
Localization accuracy	16×16	1
ROI recovery	Approximate	Exact

As shown in Table 2.4b, method 3 which is TALLOR scheme is able to recover the image as exact to the original meanwhile the compared scheme recovery is just approximate. When compared in terms of PSNR value of the watermarked image with the original image, TALLOR appear to have higher PSNR value which shows that the scheme is able to generate watermarked image that very similar to the original image.

2.5 ARNOLD TRANSFORM

Arnold Transform is an encryption method that is used to scramble a data value (Ankita Vaish, 2017). Arnold transform is very popular to be used for scrambling pixel in many image encryption studies (Kumar, Singh, A.K.Yadav, & Kumar, 2018). The Arnold transform (AT) is also known as the Cat's mapping (PhoolSingh, A.K.Yadav, & KeharSingh, 2017) . Arnold transform of a pixel *(x,y)* pf an image *f(x,y)* of size $N \times N$ pixels is denoted by *(x',y')* and mathematically defined as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = AT\{(x,y),N\} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (mod\ N) \quad (1)$$

From equation of Arnold Transform above, "mod" denotes as the modulo operation. After Arnold transform, the total energy of the original image will remain the same (Vilardy, Torres, & Jimenez, 2013). Arnold Transform period is determine by:

$$Period = \min[p: \{AT(f(x,y),N)\}^p = f(x,y)] \tag{2}$$

Where "min" indicates the minimum value and p denotes the iteration number. For the scheme that will be proposed in this paper, *w* is used as a key which represents the number of iterations of Arnold Transform.

2.6 MERSENNE TWISTER

Mersenne Twister is a widely used random number generator (Harase, 2018). For a *w-bit* word length, the Mersenne Twister generates integers in the range $[0, 2^w - 1]$ (Saito & Matsumoto, 2006). The Mersenne twister algorithm is based on a matrix linear recurrence over a finite binary field. The sate required for a mMersenne Twister implementation is an array of n values of *w* bits each. To initialize the array, a *w*-bit seed value is used to supply x_0 through x_{n-1} by setting x_0 to the seed value and thereafter setting

$$x_i \ = f \times \left(x_{i-1} \oplus \left(x_{i-1} \gg (w-2)\right)\right) + \ i \tag{1}$$

For *I* from 1 to *n-1*, the first value the algorithm then generates is based on x_n, not on x_o. The constant *f* forms another parameter to the generator, though not part of the algorithm proper.

2.7 SUMMARY

In this chapter, the general process on watermarking for image authentication had been discussed along with 3 existing methods. The strength and weakness of each method is stated in Table 2.4a. This shows that each method have its own flaw where it can be improve with further research. Hence the algorithm of Arnold Transform and Mersenne Twister that will be used in the proposed method to improve the existing scheme is explained in this chapter as well.

CHAPTER 3

METHODOLOGY

3.0 INTRODUCTION

In this chapter, the proposed method for the research will be discussed. The prime aim of this research methodology is to define, analyze and describe the process involved. A flowchart diagram of digital watermarking for image authentication will be discussed in 3.1 to provide a better understanding of how it is implemented. In the following chapter, we will explain in details on the techniques used in digital watermarking for medical image authentication method. Afterwards, a few approach used to evaluate the performance of the method for this research will be defined.

3.1 DIGITAL WATERMARKING FOR MEDICAL IMAGE AUTHENTICATON USING ARNOLD HASH AND RANDOM COORDINATE EMBEDDING

Generally, digital authentication focuses on how to recognize the authenticity of the original content. This helps in preventing any alteration to be done on the digital media. For this research, the methodology proposed is based on the family of fractal based language (SCAN) that is usually used for 2D images encryption. This method is also an improvement from the Tamper Localization and Lossless Recovery Watermarking Scheme (Siau-Chuin Liew, 2012). This method combines 4 concepts which are region numbering, watermark data encryption using hash SHA256 and Arnold Transform with key, random embedding coordinate using Mersenne Twister with secret key.

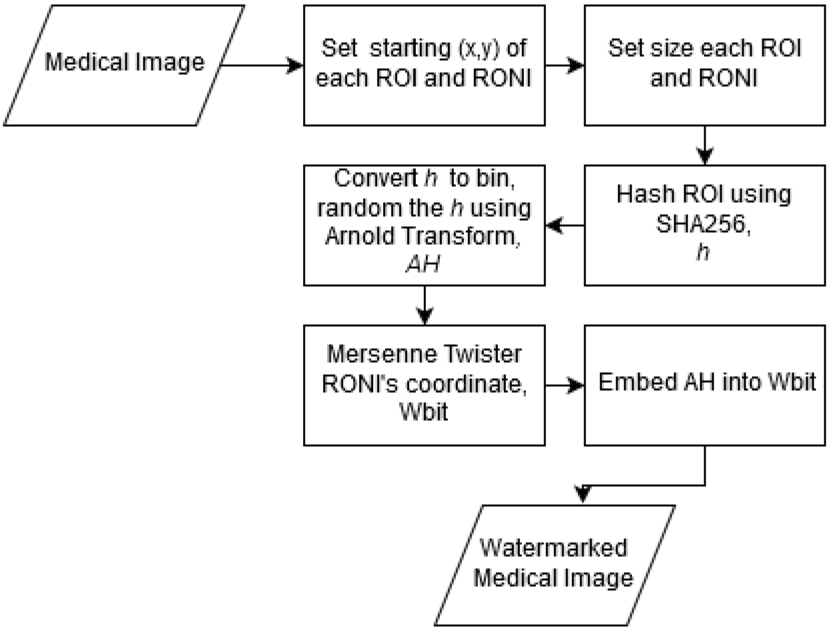

Medical Image
Set starting (x,y) of each ROI and RONI
Set size each ROI and RONI
Hash ROI using SHA256, *h*
Convert *h* to bin, random the *h* using Arnold Transform, *AH*
Mersenne Twister RONI's coordinate, Wbit
Embed AH into Wbit
Watermarked Medical Image

Figure 3.1a Embedding Process

Figure 3.1a shows the flowchart of the embedding process that the medical image undergoes using the proposed scheme. A watermarked medical image is produced by the end of the process. The steps of embedding will further be explained in detail in the next section.

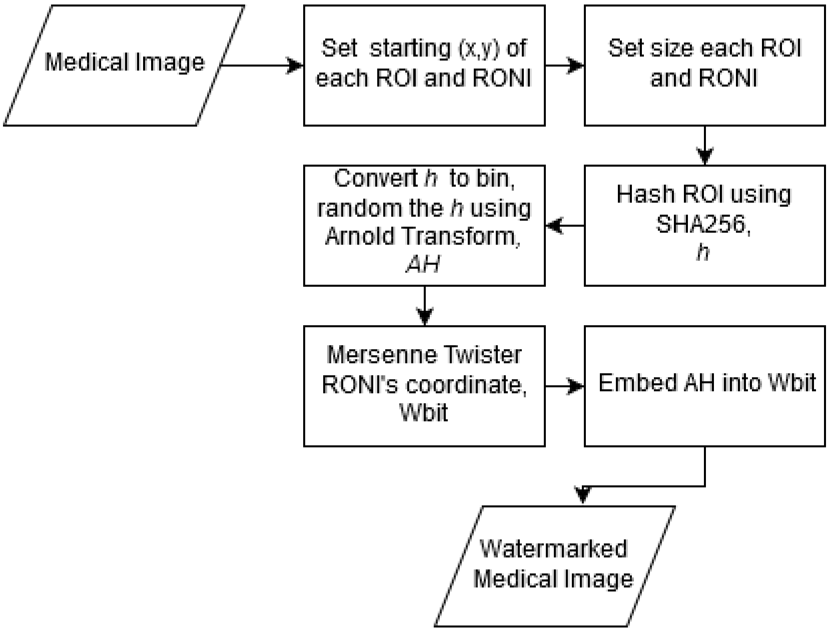

Medical Image
Set starting (x,y) of each ROI and RONI
Set size each ROI and RONI
Hash ROI using SHA256, *h*
Convert *h* to bin, random the *h* using Arnold Transform, *AH*
Mersenne Twister RONI's coordinate, Wbit
Embed AH into Wbit
Watermarked Medical Image

Figure 3.1b Authenticate Process

Figure 3.1b shows the process taken place to test the authenticity of a medical image. At the end of the process, the scheme will provide result of whether the medical image is authentic or not. The steps taken place in the process is explained in the next section.

3.2 IMAGE REGION PREPARATION

The medical image was divided into a non overlapping 1 Region of Interest (ROI) and 8 Region of Non Interest (RONI). The RONI is segmented into non overlapping 2×2 pixels.

The steps of how to determine the ROI and RONI is described as follow.

1. Set the size of the medical image.
2. Determine the starting coordinate (x,y) of each region.
3. Calculate the size of each region, the ROI is ensured to cover the important part of the medical image.

4. Each Region is named, ROI, RONI1, RONI2, RONI3, RONI4, RONI5, RONI6, RONI7, RONI8.
5. Segment the ROI into 1×1 pixel, calculate the total number of block.
6. Segment the RONI into 2×2 pixels, calculate the total number of block

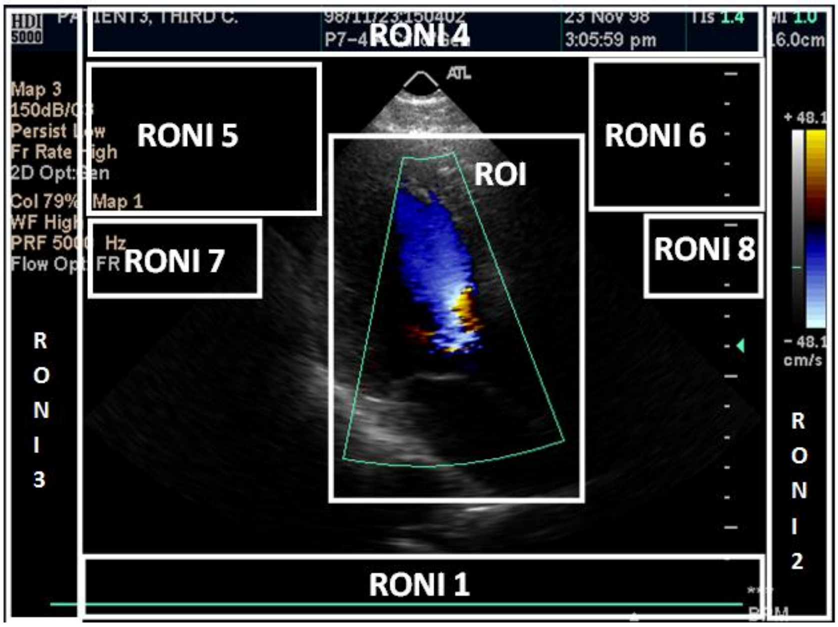


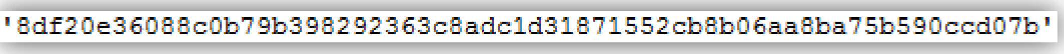
Figure 3.2a Position of ROI and RONI1 until RONI8 in Sample1

As shown in Figure 3.2a, the medical image is separated into ROI and 8 RONI. The ROI will be used for watermark information and the RONI will be used as the place to embed the watermark information.

3.3 GENERATING AND EMBEDDING WATERMARK

The watermark information from ROI will be used as authentication. The selected RONI will be used as the area for authentication information's embedding. The following will be the steps to generate watermark and embedding:

1. The ROI is taken and the value is hashed using SHA256and denoted as h as shown in Figure 3.2b.

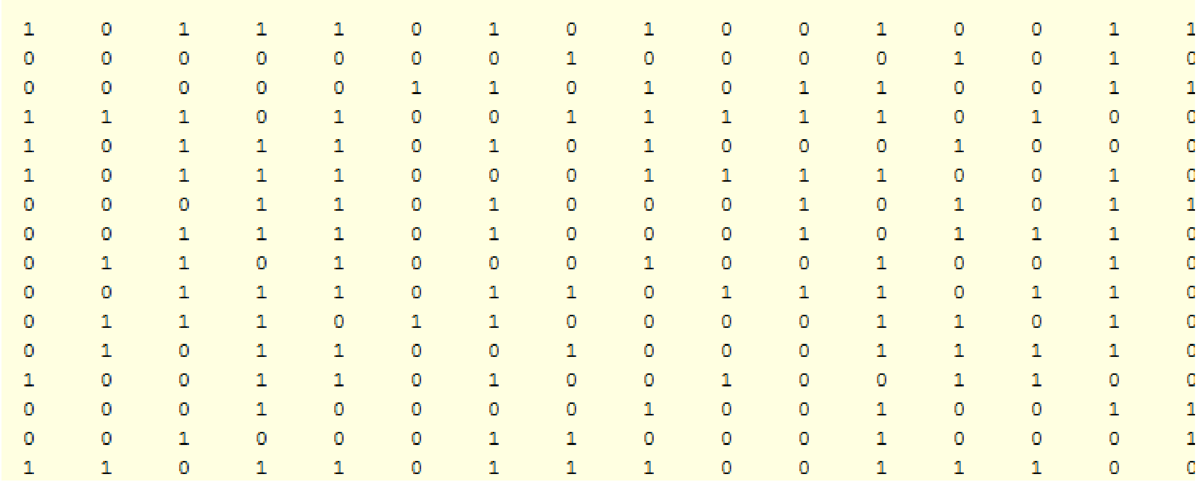


```
'8df20e36088c0b79b398292363c8adc1d31871552cb8b06aa8ba75b590ccd07b'
```

Figure 3.3a Hashed ROI Result

2. The hash value, h, is then converted to binary and denoted as hashbin.

3. The hashbin is then reshape into 16 by 16 matrices and Arnold Transform with key is perform to random the sequence of the hash that had been converted to binary and denoted as hashbinAH as displayed in Figure 3.2c.



```
1   0   1   1   1   0   1   0   1   0   0   1   0   0   1   1
0   0   0   0   0   0   0   1   0   0   0   0   1   0   1   0
0   0   0   0   0   1   1   0   1   0   1   1   0   0   1   1
1   1   1   0   1   0   0   1   1   1   1   1   0   1   0   0
1   0   1   1   1   0   1   0   1   0   0   0   1   0   0   0
1   0   1   1   1   0   0   0   1   1   1   1   0   0   1   0
0   0   0   1   1   0   1   0   0   0   1   0   1   0   1   1
0   0   1   1   1   0   1   0   0   0   1   0   1   1   1   0
0   1   1   0   1   0   0   0   1   0   0   1   0   0   1   0
0   0   1   1   1   0   1   1   0   1   1   1   0   1   1   0
0   1   1   1   0   1   1   0   0   0   0   1   1   0   1   0
0   1   0   1   1   0   0   1   0   0   0   1   1   1   1   0
1   0   0   1   1   0   1   0   0   1   0   0   1   1   0   0
0   0   0   1   0   0   0   0   1   0   0   1   0   0   1   1
0   0   1   0   0   0   1   1   0   0   0   1   0   0   0   1
1   1   0   1   1   0   1   1   1   0   0   1   1   1   0   0
```

Figure 3.3b 16×16 Matrices Arnold Hashbin.

4. The hashbinAH is reshape again into a single line and denote as AH.

5. Pick one RONI to be embedded with AH, take the assigned coordinate for the selected RONI.

6. Using Mersenne Twister with key assigned, the coordinate in the selected RONI to be embedded with watermark information is randomize, the random coordinate is denoted as Wbit..

7. The LSB of the selected coordinate is set to the value of AH until all AH value is embedded into the medical image.

8. The watermarked image is saved back as the same format as the original.

3.4 DETECTION OF TAMPERED REGION

For authentication, the watermarked medical image is taken and with the information of the secret key for both Arnold Transform and Mersenne Twister known, the selected RONI is also known, the same procedure in watermark generation will be repeated. The Mersenne Twister is inversed and the coordinate of the embedded watermark is gathered and the value of each LSB on the coordinate is collected. The value of hashed value of ROI in watermarked image will be compared with the bit retrieved from the embedded coordinate. Image is considered as tamper if there is one bit not same.

The following is the steps to authenticate the watermarked image:

1. The medical image is taken, divide the ROI and RONI as in 3.2
2. Hash the value of ROI in watermarked image using SHA256
3. The hash value, Auh, is then converted to binary and denoted as Ahashbin.
4. The Ahashbin is then reshape into 16 by 16 matrices and Arnold Transform with key is perform to random the sequence of the hash that had been converted to binary and denoted as AhashbinAH.
5. The AhashbinAH is reshaped again into a single line and denote as AuAH.
6. Take the same RONI that is used to store watermark information as the used in 3.3
7. Perform Mersenne Twister to find the coordinate the watermark is stores, retrieve the watermark information from the LSB of the coordinate and denote the value as AuWbit.
8. The AuWbit is then compared with AuAH until all AuAh is compared.
9. The medical image is considered as tampered if there is one bit not same when compared and marked as Invalid.
10. When all compared AuAh and Wbit is same, the image is consider as Valid hence marking the image as authentic.

3.5 GANTT CHART

Refer to Appendix A

3.6 SUMMARY

In this chapter, the methodology of the proposed scheme is explained in details. The use of Arnold Transform to further hash the hashed value of the ROI and the use of Mersenne Twister to generate a the random coordinate of RONI to be embed is hopefully able to improve the existing method proposed in TALLOR. Therefore the following method will be implemented and tested to see the performance of the proposed method on medical image.

CHAPTER 4

RESULT AND DISCUSSION

4.0 INTRODUCTION

In this chapter, the research design and the list of tools and files involved in the research will be presented. The results and analysis of the proposed digital watermarking for medical image authentication and to evaluate the proposed scheme based on comparison with other existing medical image authentication using watermarking scheme will be demonstrated as well. The outcomes of this research is expected to be helpful for further hits and guidelines in developing an improve watermarking for medical image authentication technique.

The imperceptibility of the watermark embedded and the tamper localization of each medical image will be tested. The proposed scheme will undergo evaluation based on its PSNR and MSE value after watermark is embedded and the processing time taken to embed and authenticate will be recorded. For comparison, dataset form existing scheme is chosen. The scheme used for comparison will further be discussed in section 4.1.

4.1 OVERVIEW ON WATERMARK FOR IMAGE AUTHENTICATION APPROACH

Watermarking is a method that is mainly used to determine the ownership of a digital content. Meanwhile, watermarking for authentication is used to determine the authenticity of an image. In this research, ultrasound medical image will be used as the media to implement the watermark for authentication because it is very important for doctor to make sure that the medical image they receive is authentic before undergoes further diagnosis of their patient. And because some tamper is very difficult to be detected through naked eye, hence it is important for the method to be able to detect any manipulation occur on the medical image.

Least Significant Bit (LSB) is one of the most common technique used to embed watermark information in determine the image authenticity due to its ability to easily destroyed at slightest alteration on the image. In this research, there will be dataset generated used to make as comparisons with my proposed scheme which is Tamper Localization and Lossless Recovery Watermarking Scheme.

4.1.1 EXISTING WATERMARK FOR IMAGE AUTHENTICATION

Watermark for Image Authentication Scheme 1:

Tamper Localization and Lossless Recovery Watermarking (TALLOR) Scheme

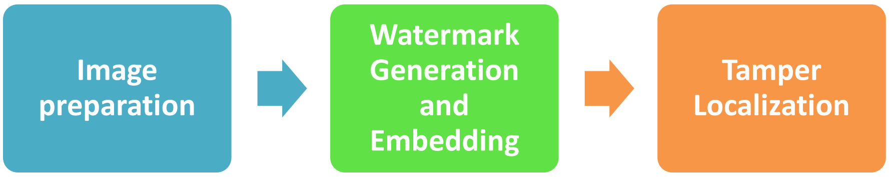
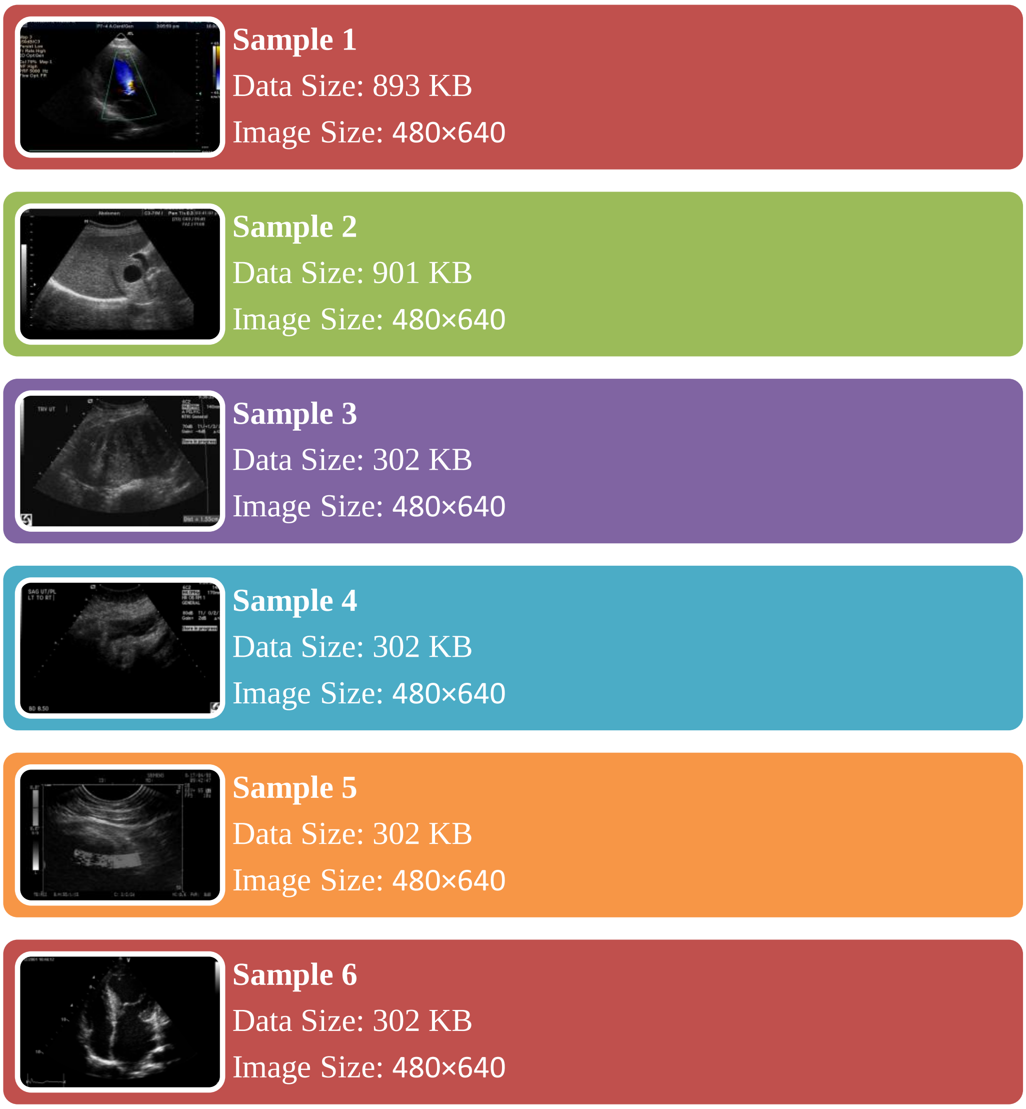


Figure 4.1.1a Simple Flow Diagram of Tamper Localization and Lossless Recovery Watermarking Scheme

Figure 4.1.1a shows the embedding and authentication process of TALLOR. This method starts by dividing the image into a single region of interest (ROI) and 8 part of Region of non-interest (RONI). The watermark consisted of authentication and recovery information. The RONI is then divided into one area to be embedded with the authentication information and another area to be embedded with recovery information. The authentication bit was computed by hashing the value of ROI with SHA-256 and the authentication information is embedded into the designated area in RONI. The ROI segment is saved as JPEG file. The ROI file size is then hashed with SHA-256 and the information is stored into designated RONI. The JPEG file of ROI was embedded to designated RONI. The watermarked medical image was saved as DCM file format image. The tamper localization phase begin with hashing the RONI where the authentication information was embedded using SHA-256.retrieved the hash value of RONI in watermark embedding phase and compare the value with previously computed hash of RONI. If the value id the same, the image is considered as authentic.

4.1.2 LIST OF TOOLS AND SOURCES

There is 6 different images (.bmp) format that will be used to test the scheme and generate the results. All the images are in 480×640 size. Different images are tested for each scheme to obtain the optimum result to prevent the result to depend only on a single image.



Sample 1
Data Size: 893 KB
Image Size: 480×640

Sample 2
Data Size: 901 KB
Image Size: 480×640

Sample 3
Data Size: 302 KB
Image Size: 480×640

Sample 4
Data Size: 302 KB
Image Size: 480×640

Sample 5
Data Size: 302 KB
Image Size: 480×640

Sample 6
Data Size: 302 KB
Image Size: 480×640

Figure 4.1.2.a Diagram of Sample Image for Testing

Figure 4.1.2a shows the sample images that will be used to test the performance of the existing method (TALLOR) and the proposed method. All the images are in .bmp format and the image data sizes range between 800KB to 300 KB and all the image size is 480×640.

4.2 EXPERIMENTAL RESULTS AND DISCUSSION

The images mentioned I Figure 4.1.2a were tested with 2 different image watermarking for medical images authentication schemes which are Tamper Allocation and Lossless Recovery (TALLOR) and the Proposed Schemes as mentioned in the previous

Chapter 3 respectively. This section will clearly display and discuss the experimental results between the two schemes based on its imperceptibility and performance in terms of embedding and authentication processing time.

4.2.1 PERFORMANCE ANALYSIS: IMPERCEPTIBILITY

The differences between an embedded medical image and the original should not be easily perceived trough Human Visual System (HVS). To measure the imperceptibility of an a watermarked medical image accurately, Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) is computed for measurement.

4.2.1.1 PEAK SIGNAL TO NOISE RATIO (PSNR)

The PSNR is the ratio between a signal's maximum power and the power of the signal noise. It can be used to measure the quality of the reconstructed images that has been embedded with watermark. If the PSNR value is high, the image is considered very similar to its original. Therefore, each image sample will undergoes the two schemes embedding process and the PSNR value of every samples produce for each method is obtained.

Testing on image samples *(Sample1.bmp, Sample2.bmp, Sample3.bmp, Sample4.bmp, Sample5.bmp, Sample6.bmp)*

The following table and figure will display the PSNR results obtained from testing with *Sample1.bmp, Sample2.bmp, Sample3.bmp, Sample4.bmp, Sample5.bmp,* and *Sample6.bmp* The proposed scheme was compared to the TALLOR schemes.

Table 4.2.1.1a Results of PSNR between TALLOR and Proposed Scheme on 6 different medical image samples after embedding the watermark.

	TALLOR	Proposed Scheme
Figure	PSNR	PSNR
Sample 1	52.925	86.6678
Sample 2	52.3162	86.842
Sample 3	49.4797	82.2132
Sample 4	49.5537	81.6062
Sample 5	48.3659	81.7665
Sample 6	47.9882	81.8991

Table 4.2.1a displays the results of PSNR obtained from both image watermarking for medical authentication schemes when tested on 6 different samples of medical image. The PSNR was calculated based on the ratio between the maximum possible value of a signal and the power of distorting noise that affects the quality of the watermarked medical image. The result shown in Table 4.2.1a is then plotted to visualize the differences.

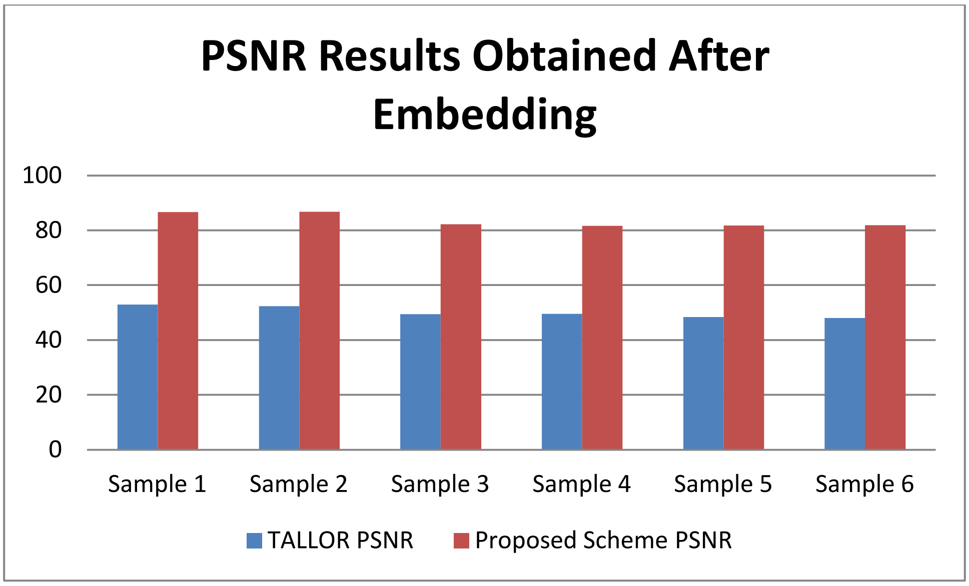


Figure 4.2.1.1a Comparisons of PSNR between TALLOR and Proposed Scheme on 6 medical image samples.

The outcome from Figure 4.2.1a has shown the average result of the PSNR value between TALLOR and Proposed Scheme. It is proven that PSNR value of the Proposed Scheme is higher than TALLOR scheme on average. This shows that embedding method used by the proposed scheme is more similar to the host medical image samples.

4.2.1.2 MEAN SQUARE ERROR (MSE)

The Mean Square Error (MSE) is the cumulative squared error between the embedded image and the original image. A lower value of MSE means lesser error is found in the watermarked image hence making it the most similar to the original image. Therefore, each image sample will undergoes the two schemes embedding process and the MSE value of every samples produce for each method is obtained.

Embedding test on image samples *(Sample1.bmp, Sample2.bmp, Sample3.bmp, Sample4.bmp, Sample5.bmp, and Sample6.bmp)*

The following table and figure will display the experiment results obtained from testing with *Sample1.bmp*, *Sample2.bmp*, *Sample3.bmp*, *Sample4.bmp*, *Sample5.bmp*, and

Sample6.bmp The proposed scheme was compared to the TALLOR schemes. The MSE value from the experiment is obtained.

Table 4.2.1.2a Results of MSE between TALLOR And Proposed Method on 6 Medical Image Sample

Figure	TALLOR	Proposed Scheme
	MSE	MSE
Sample 1	0.3316	1.40E-04
Sample 2	0.3815	1.35E-04
Sample 3	0.733	3.91E-04
Sample 4	0.7206	4.49E-04
Sample 5	0.9473	4.33E-04
Sample 6	1.0334	4.20E-04

Table 4.2.2a shows the result of the MSE obtained from the embedding stage of TALLOR scheme and Proposed Scheme that is implemented on six medical image samples. The MSE is calculated by taking the square of the differences between every pixel in the original sample image and the corresponding pixels I watermarked medical image, sum it up and divide it by the number of pixels. The result shown in Table 4.2.2a is then plotted to visualize the differences.

The outcome shown in Table 4.2.2a displays that MSE obtained from both scheme achieve positive result with low MSE value which shows that both methods create a watermarked image very similar to their respective host medical image sample. However, the line of the Proposed Scheme is much lower compared to TALLOR scheme. This shows that compared to TALLOR scheme, the Proposed Method is able to generate watermarked medical images with higher similarity to the original medical image.

4.2.2 PERFORMANCE ANALYSIS: PROCESSING TIME

An effective watermarking for authentication scheme should be able to implement their scheme in low processing time. If the time taken to implement the method took too long to process, it will limit the method to be more suitable for small sized medical images. It is well known that most medical image comes in a very large file size. The larger the medical image, the longer time it will take to embed and authenticate the image. Therefore, in this section, the analysis will be divided into two parts of processing time which is embedding processing time and authentication process time. All 6 medical image samples is tested with TALLOR scheme and Proposed scheme. Then the time taken for each method to embed and authenticate is recorded.

4.2.2.1 EMBEDDING PROCESS TIME

The embedding process is the process of embedding watermark onto the original sample medical image. As explained in 4.1.1, TALLOR method used multilevel embedding process where it embeds the watermark in several different locations. Meanwhile, the Proposed Scheme picks only one region for embedding but perform the Mersenne Twister first to randomize the coordinate to embed.

Testing on 3 Sample Images *(Sample1.bmp, Sample2.bmp, Sample3.bmp)*

The following table represents the Processing Time to embed the watermark into each sample images. The sample images used are varies in sizes where the largest image file size is Sample 2 with 901KB and the smallest image file size is Sample 3 with 302 KB.

Table 4.2.2.1a Embedding Process Time for TALLOR and Proposed Method

Figure	File Size (KB)	TALLOR	Proposed Method
		Elapsed Time (s)	Elapsed Time (s)
Sample 1	893	95.5	1.5
Sample 2	901	141.7656	1.7031
Sample 3	302	40.8281	1.125

The results in Table 4.2.2.1a show all the total time taken from the scheme to embed the watermark into the sample image. With the various sample image size, the time taken to embed varies as well. Optimum embedding time is the method that is able to perform embedding in short amount of time.

In Table 4.2.2, the time taken to embed the watermark into the sample image of different file sizes is displayed. The data shows that the larger the file size, the longer time is taken to embed the watermark into the sample images. From the table, it shows that TALLOR scheme took longer time to embed the watermark compared to the Proposed Scheme. When a bigger file sizes is used, the time taken to embed also increase. However, when compared with TALOR scheme, the Proposed Schemes seems to be performing much better with faster embedding time. Although the time taken did increase when the file size increase for the proposed method, but it does not took as long as TALLOR. This proves that in terms of the processing time, the proposed method performs faster.

4.2.2.2 AUTHENTICATION PROCESSING TIME

The authentication process is the process to determine the authenticity of a medical image. As explained in 4.1.1, TALLOR method used two level authentication proces where it will compare the extracted watermark from the previously selected region and the hashed value of the watermarked image. Meanwhile, the Proposed Scheme will first inverse the Mersenne Twister to get the coordinate of the embedded watermark and compare it with the hash value of the watermarked medical image.

Testing on 3 Sample Watermarked Images *(Sample1_watermarked.bmp, Sample2_watermarked.bmp, Sample3_watermarked.bmp)*

The following table represents the Processing Time to authenticate the watermark into each sample images. The sample images used are varies in sizes where the largest image file size is Sample 2 with 901KB and the smallest image file size is Sample 3 with 302 KB. Consider that there are no tamper performed on the watermarked sample images, the result of the process time to test the authenticity of the image is displayed below.

Table 4.2.2.1a Authentication Process Time for TALLOR and Proposed Method

Figure	File Size (KB)	TALLOR	Proposed Method
		Elapsed Time (s)	Elapsed Time (s)
Sample 3	302	1.375	1.3906
Sample 1	893	1.3125	1.4844
Sample 2	901	1.125	1.5469

Table 4.2.2.1a displays the results when watermarked image of different file size undergoes authentication process to determine the authenticity of the image. The authentication process is performs by repeating the same step as the watermark generation and retrieve the watermark information from the selected region and compare the value of those two. If the two values are the same, the image is considered authentic. Since 3 watermarked sample images of different sizes are used for this test, the time taken to

authenticate each image using TALLOR scheme and Proposed Scheme is visualize as follows.

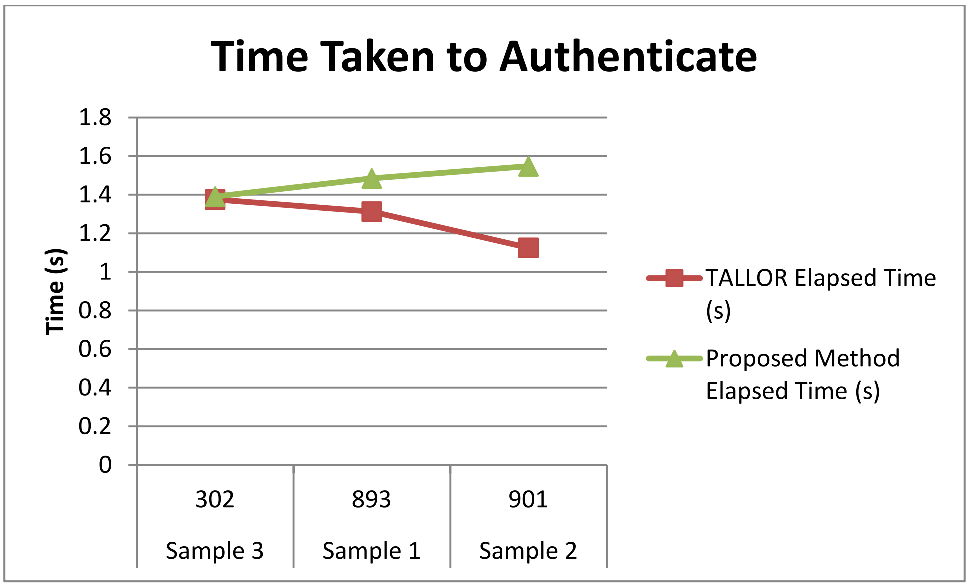


Figure 4.2.2.1a Comparison between the TALLOR and Proposed Scheme in Time Taken To Authenticate

As visualizes in Figure 4.2.2.1a, the time taken to determine the authenticity of each watermarked images of different file sizes are obtained. Both TALLOR scheme and Proposed Scheme is able to detect the authenticity and of an image successfully. The TALLOR is shown to perform faster in terms of determine the authenticity of the watermarked images in Figure 4.2.2.1a. The Proposed Method took longer time to authenticate and the time increases as the file size increase. This is due to the inverse Mersenne Twister with key must first be performed to find the coordinate where the watermark information is stored before extracting it thus making the time taken is longer than TALLOR. However this step is crucial to improves the security of the embedded data where instead of embedding in one line in a region, the Proposed Method randomize the embedding coordinate in a specific region to prevent the embedding data from being stolen.

4.3 SUMMARY

In this chapter, the result from the implementation of the proposed method onto the medical image is displayed and discussed. The proposed method has successfully able to detect whether the medical image is tampered or not. When compared with the existing method, TALLOR, the proposed method shows a positive performance where it able to embed faster and the watermarked medical image is very similar to the original medical image.

CHAPTER 5

CONCLUSION

5.0 INTRODUCTION

In this thesis, we have introduced a digital watermarking for medical image authentication scheme using embedding on LSB with SHA256, Arnold Transform and Mersenne Twister in watermark generating and authenticate. The main objective for proposing this method is to figure out the ideal embedding scheme to determine the authentication for medical image. The effectiveness is tested in terms of its ability to detect any tamper occur on the watermarked image and authenticate the image, the imperceptibility of embedded images and the time taken for the scheme to generate watermark, embed and authenticate. Through the proposed scheme, a method that is able to authenticate watermarked images with fast processing time and able to retain the quality of the image after embedding is found.

5.1 RESEARCH CONSTRAINTS

Upon completing the research, a few constraints were established. The main constraints would be the limited amount of time provided to do the research. Since watermarking for image authentication has been introduced for quite a long time, many research have been done to contribute on the field hence making the knowledge expands wider than before. A lot of method and scheme has been develop thus making it a lot harder to cover all the knowledge for the research. Therefore, time gets restricted to go through one article after another to gather information for the research.

Lacks of knowledge on the required field of watermarking for authentication become one of the constraints. Watermarking for Image authentication has a broad range technique to be implemented and investigated. It is important to really master the technique to fully understand the theories that work behind the method. This can be overcome by spending more time to master the fields but that would lead back to the main constraint which is insufficient research time.

5.2 RESEARCH CONCLUSION

An improved watermarking for medical image authentication scheme using data encryption and random embedding places has been proposed. The aim of this proposed scheme is to find out the ideal method to generate watermark and embed faster than existing scheme, TALLOR with high security level watermark data embedding that is better if not the same as TALLOR.. As a result, proposed method performs faster than TALLOR in watermark generation and embedding processing time. Regarding the imperceptibility, the proposed scheme has been successful at maintaining the quality of the original medical image. This clearly shows that the proposed method had improved the TALLOR scheme. However, the scheme have a flaw where it the only use ROI of the image as watermark. With that, the medical image can now be securely identified as authentic of tampered by implementing the scheme.

5.3 FUTURE WORK

The algorithm used in region based embedding is very useful as it enhance the art of watermark embedding by emphasizing the use of data encryption such as SHA256 and Arnold Transforms. A significant improvement on the imperceptibility can be made when using LSB to embed the watermark. Moreover, there are many methods to perform authentication detection other than using watermarking for authentication that may provide a faster and more accurate result. This is worth to be explored in the future research. In the mean time, this proposed scheme opens up a new idea for future researchers to protect the authenticity of medical images by making a scheme that is able to detect a slight tamper perform on the image. This will contribute in helping medical practitioner to safely distribute their patients medical image to other doctors without worries if any tamper is made on the transferred medical images. Further research can be made on this field without focusing only on ultrasound medical image but also on other type of medical images such as CT scan and MRI.

REFERENCES

Al-Qershi OM, K. B. (2011). *Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images.*

Ankita Vaish, M. K. (2017). Color image encryption using MSVD, DWT and Arnold transform in fractional Fourier domain. *Optik Volume 145*, 273-283.

Arsalan, M., Qureshi, A. S., Khan, A., & Rajarajan, M. (2017). Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique. *Applied Soft Computing*, 168-179.

Bravo-Solorio, S., & Nandi, A. K. (2011). Secure fragile watermarking method for image authentication with improved tampering localisation and self-recovery capabilities. In S. Bravo-Solorio, & A. K. Nandi, *Signal Processing*, 728-739.

Harase, S. (2018). Conversion of Mersenne Twister to double-precision floating-point numbers. *Mathematics and Computers in Simulation*.

Hisham, S. I., Liew, S.-C., & Zain1, J. M. (2013). A Quick Glance at DigitalWatermarking in Medical Images. *Biomedical Engineering Research*, 79–87.

Hisham, S. I., Muhammad, A. N., Badshah, G., Johari, N. H., & Zain, J. M. (2017). *Numbering with spiral pattern to prove authenticity and integrity.*

Khanduja, V. (2017). Database watermarking, a technological protective measure: Perspective, security analysis and future directions. *Journal of Information Security and Applications*, 38-49.

Kumar, J., Singh, P., A.K.Yadav, & Kumar, A. (2018). Asymmetric Cryptosystem for Phase Images in Fractional Fourier Domain Using LU-Decomposition and Arnold Transform. *Procedia Computer Science*, 1570-1577.

Lin, H., Yang, S., & Xu, L. (2011). Watermark algorithm for color image authentication and restoration. *Proceedings of 2011 International Conference on Electronic & Mechanical Engineering and Information Technology*, 2773–2776.

Nasseem, M. T., Qureshi, I. M., Atta-ur-Rahman, & Muzaffar, M. Z. (2013). Chaos based invertible authentication of medical images. *2013 IEEE 9th International Conference on Emerging Technologies (ICET)*, 1-5.

PhoolSingh, A.K.Yadav, & KeharSingh. (2017). Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition. *Optics and Lasers in Engineering*, 187-195.

Pramila, A., Keskinarkaus, A., & Seppänen, T. (2018). Increasing the capturing angle in print-cam robust watermarking. *Journal of Systems and Software*, 205-215.

Renza, D., L., D. M., & Lemus, C. (2018). Authenticity verification of audio signals based on fragile watermarking for audio forensics. *Expert Systems with Application*, 211-222.

Rippa, P., & Secundo, G. (2018). Digital academic entrepreneurship: The potential of digital technologies on academic entrepreneurship. *Technological Forecasting and Social Change*.

Saito, M., & Matsumoto, M. (2006). SIMD-Oriented Fast Mersenne Twister: a 128-bit Pseudorandom Number Generator. *Monte Carlo and Quasi-Monte Carlo Methods*, 607-622.

Siau-Chuin Liew, J. M. (2012). Tamper Localization and Lossless Recovery Watermarking Scheme with ROI. *Journal of Digital Imaging*, 316-325.

Song, Q., & Zhang, H. (2010). Image Tamper Detection and Recovery Using Dual Watermark. *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM).* Chengdu, China: IEEE.

Techopedia Inc. (2018). *What Is Digital Watermarking? - Definition from Techopedia*. Retrieved March 21, 2018, from Techopedia.com: https://www.techopedia.com/definition/24927/digital-watermarking

Vilardy, J. M., Torres, C. O., & Jimenez, C. J. (2013). *Double image encryption method using the Arnold transform in the fractional Hartley domain.*

Zain, J. M., & ARM, F. (2006). Medical image watermarking with tamper detection and recovery. *The 28th annual international conference of the IEEE Engineering in Medicine and Biology Society.* New York, USA: IEEE.

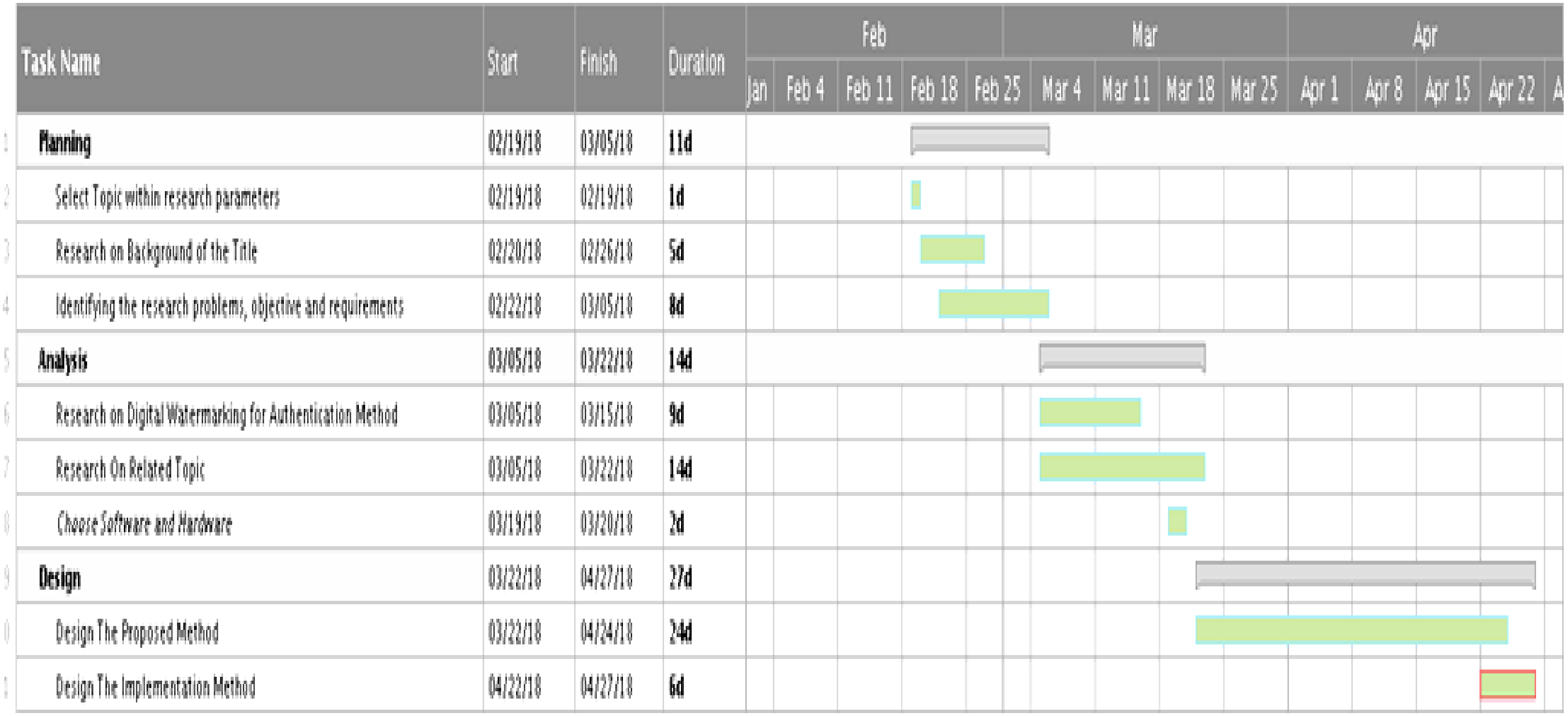
Zain, J., Baldwin, L., & Clarke, M. (2004). Reversible watermarking for authentication of DICOM images. *Proceedings of 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 3237-3240.

Zain, S.-C. L. (2011). Tamper Localization and Lossless Recovery Watermarking Scheme. *Communications in Computer and Information Science book series*, 555-566.

Zheng, L., Zhang, Y., & Thing, V. L. (2018). A Survey on Image Tampering and Its Detection in Real-world Photos. *Journal of Visual Communication and Image Representation*.

ZHou, X., Huang, H., & Lou, S. (2001). Authenticity and integrity of digital mammography images. *IEEE Transactions on Medical Imaging*, 748-791.

APPENDIX A



	Task Name	Start	Finish	Duration
1	**Planning**	02/19/18	03/05/18	**11d**
2	Select Topic within research parameters	02/19/18	02/19/18	**1d**
3	Research on Background of the Title	02/20/18	02/26/18	**5d**
4	Identifying the research problems, objective and requirements	02/22/18	03/05/18	**8d**
5	**Analysis**	03/05/18	03/22/18	**14d**
6	Research on Digital Watermarking for Authentication Method	03/05/18	03/15/18	**9d**
7	Research On Related Topic	03/05/18	03/22/18	**14d**
8	*Choose Software and Hardware*	03/19/18	03/20/18	**2d**
9	**Design**	03/22/18	04/27/18	**27d**
0	Design The Proposed Method	03/22/18	04/24/18	**24d**
1	Design The Implementation Method	04/22/18	04/27/18	**6d**