# AN IMPROVED MAPPING PATTERN FOR DIGITAL WATERMARKING

MOHAMAD NAZMI BIN NASIR

Bachelor of Computer Science (Computer Systems & Networking)

UNIVERSITI MALAYSIA PAHANG

## UNIVERSITI MALAYSIA PAHANG

**DECLARATION OF THESIS AND COPYRIGHT**

| | |
|---|---|
| Author's Full Name | : MOHAMAD NAZMI BIN NASIR |
| Date of Birth | : 14 NOVEMBER 1995 |
| Title | : AN IMPROVEMENT IN NEW MAPPING PATTERN IN DIGITAL WATERMARKING |
| Academic Session | : 2019/2020 |

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)

_______________________

_______________________
Name of Supervisor
Date:

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

Universiti
Malaysia
PAHANG
Engineering • Technology • Creativity

# 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 Bachelor of Computer Science (Computer Systems & Networking)

_______________________________

(Supervisor’s Signature)

Full Name : DR. SYIFAK BINTI IZHAR HISHAM

Position :

Date : 24 MAY 2019

UMP Universiti Malaysia PAHANG

Engineering • Technology • Creativity

# 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 duly 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 : MOHAMAD NAZMI BIN NASIR

ID Number : CA15042

Date : 24 MAY 2019

# AN IMPROVED MAPPING PATTERN FOR DIGITAL WATERMARKING

MOHAMAD NAZMI BIN NASIR

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Bachelor of Computer Systems

Faculty of Computer Systems & Software Engineering

UNIVERSITI MALAYSIA PAHANG

MAY 2019

# ACKNOWLEDGEMENTS

During the process of completing this research, it was fully supported by the Faculty of Computer Systems & Software Engineering Universiti Malaysia Pahang. I would like to express my gratitude to my supervisor Dr Syifak Izhar who provided assistance for me to complete this research and also for teaching me about digital watermarking, and last but not least the evaluator who moderated this paper and in the same time help improved the manuscript significantly.

I have to express my appreciation to my supervisor for sharing all her knowledge in the process of completing this research. I would like to also thanks my family for their love, emotional and financial support throughout my life. And last but not least a big thanks to my friends, John Arthur and Syahirah who always supported me in hard times during the semester.

All of the encouragement and support are deeply appreciated and it is a part of my journey for me to complete my research. Thank you.

# ABSTRAK

Pada zaman kini, watermark memainkan peranan yang penting terutamanya dalam penghasilan produk yang mempunyai hak cipta terpelihara oleh mana-mana pihak tidak kiralah dalam bentuk fizikal mahupun digital. Kepentingan watermark ini meningkat disebabkan oleh peningkatan penggunaan teknologi internet dalam menghantar data ke pihak yang tertentu. Oleh yang demikian, terma digital watermark menjadi bertambah terkenal apabila kita semakin menggunakan banyak informasi yang melibatkan teknologi digital. Digital watermark boleh digunakan ke atas gambar RGB untuk melindungi hak cipta gambar tersebut. Setiap gambar mempunyai piksel yang banyak dan digital watermark ini menggunakan Least Significant Bit(LSB) untuk meletakkan digital watermark tersebut. Hal ini adalah kerana untuk mengurangkan kekacauan ke atas gambar asal sebanyak mungkin kerana ianya berkemungkinan akan mengubah warna gambar asal tersebut. Digital watermark ini terletak di LSB kerana daya penglihatan mata manusia yang terhad untuk melihat pemindaan yang amat sikit sekali di dalam gambar asal. Semakin sedikit pemindaan yang nampak di dalam gambar asal, semakin baik digital watermark itu kerana objektif utama menggunakan digital watermark ini adalah untuk meletakkan ciri keselamatan yang paling tinggi ke dalam gambar dan dalam masa yang sama meletakkan kekacauan yang paling sedikit ke atas gambar tersebut. Kajian ini mencadangkan untuk mengaplikasikan Hilbert-Peano pattern untuk digunakan untuk memenuhi syarat ini untuk menjamin keselamatan gambar digital tersebut setinggi yang mungkin. Keputusan dari eksperimen yang akan dijalankan menggunakan Hilbert-Peano pattern ini akan dibandingkan dengan hasil keputusan dari pattern yang sedia ada untuk membandingkan keputusan dari segi aspek keselamatan. Kajian ini menjangkakan keputusan yang lebih baik dari aspek keselamatan berbanding pattern yang sedia ada.

# ABSTRACT

In the present, watermark plays an important part in all copyrighted content whether it is physical or digital. The importance of watermark in digital data increases as the usage of internet in transferring data increases day by the as the improvement in technologies improves. Therefore, the term digital watermark become more and more famous as we become more dependent on digital information. Digital watermarking can be used on RGB images to protect the ownership of the images. An image consists of many pixels and the digital watermark uses the Least Significant Bit (LSB) to apply the watermark. This is to reduce the disturbance to the original image as much as possible as it might alter the colour of the original image. The digital watermark is located in the LSB because the human eye has a limit on seeing the fewest disturbance that has been made on the original image. The fewer the disturbance on the original image, the better the digital watermark as the main objective of using digital watermark is to apply the highest security as possible to the digital image and in the same time to reduce as most disturbance as possible that can be visible to the human eye. This research proposed a hybrid mapping pattern which is Hilbert Peano Curve to try to achieve the highest security as possible from alteration. The result of the experiments will be compared with the existing watermark to prove the security of the proposed pattern. The results of this research are expected to be better in terms of security if compared to other digital watermarking schemes.

# TABLE OF CONTENT

# LIST OF TABLES

# LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | |
|---|---|
| RGB | Red Green Blue |
| LSB | Least Significance Bit |
| JPEG | Joint Photographic Experts Group |
| DCT | Discrete Cosine Transform |
| SVD | Singular Value Decomposition |
| DFT | Discrete Fourier Transform |
| DWT | Discrete Wavelet Transform |
| ACF | Auto Covariance Function |
| CT SCAN | Computed Tomography Scan |
| MRI | Magnetic Resonance Imaging |
| PET | Positron Emission Tomography |
| DTI | Diffusion Tensor Imaging |
| PSNR | Peak Signal to Noise Ratio |
| DB | Desibels |
| NCC | Normalized Cross Correlation Coefficient |
| SSIM | Structutal Similarity Index Measure |
| MSE | Mean Square Error |

# CHAPTER 1

# INTRODUCTION

In this modern era where most communication that happens in this world requires the internet, almost everyone transmits most of their data online. The rise in the usage of social media replacing real life meeting or communications has made people share most of their information over the internet through digital media. Most people now prefer to share what they are doing by posting pictures of them through social media such as Facebook and Instagram and all these applications requires the internet connection. In the aspect of work, people nowadays prefer to use emails to send their documents instead of printing and posting them because by using the email, it requires less effort and less money if you want to deliver the documents to other people. All of these examples prove that people nowadays are using more and more digital media as their method of choice rather than using the traditional method such as sharing an album of photo of themselves or even use the mail to deliver documents to the other company.

In the process of sharing information on the internet, security play a big role in ensuring the data transferred from the sender arrives to the receiver without any disturbance from an unknown entity that might be stealing any information from the transferred data. All of the data on the internet should be kept secret from the others except the sender and servers since that the data may be security-sensitive (Singh, 2018). The data also requires authentication to provide confirmation on the authenticity of the data. The data also must be confirmed that it does not been tampered by any outside entity.

The most important aspects about transmitting the data on the internet is the data security. Data security is making sure that our data is safe from accidental or malicious damage (Morrissey, 1996). Security is an important aspect in every process in the internet because we are not sure who or what we are dealing with when we are sharing our information on the internet.

The most known data security techniques can be classified into two categories: Digital watermarking is one of the techniques that can be used to solve this problem. Digital watermarking is a capability for inserting information known as watermark, into an image which later can be extracted or observed for various purposes such as identification and authentication. Besides providing security, this technique can also be utilized to gain information about the source, owner, distributor or creator of an image or a document. The second category is steganography which focuses more on bandwidth of the hidden messages while hiding a message, file or an image within another message, file or image but in the aspect of watermarking, the watermark robustness is the key performance parameter.

This paper will discuss about the current available digital watermarking pattern and effectiveness in protecting the digital data and will also figure out if there is any possible improvement in new mapping pattern for digital watermarking.

## 1.1 Problem Statement

Two fragile watermarking schemes CLSB-SPIRAL and LSB-HILBERT for authentication have been developed with the special feature of embedding. They applied unique pattern of numbering to decide the watermark bits location. These schemes have extended the current technology of fragile watermarking. The watermarked images age proven theoretically and experimentally as good and qualified to use in clinical diagnosis. The accepted noise for human sight is 32dB, and they managed to get below this value. However, the current watermarking pattern took some time to embed the chosen watermark into the images. Thus, research is to test whether the proposed watermarking pattern is faster than the current watermarking pattern available.

## 1.2 Objective

The objectives of this thesis are:

i. To study about fragile watermarking schemes for authentication and mapping techniques

ii. To apply new mapping pattern in fragile watermarking

iii. To evaluate the quality of new pattern

## 1.3 Scope

The research will be focusing on watermarking in medical images.

## 1.4 Significance

After completion of this thesis, it will:

i. Improve on current digital watermarking methods

ii. Conclude that whether the new proposed pattern is better than the current

iii. Helps as a reference to future research

## 1.5 Thesis Organization

This thesis consists of five chapters which are introduction, literature review, methodology, implementation, testing and result discussion and conclusion.

Chapter 1 will discuss on the introduction of the proposed watermarking scheme. It also contains the problem statement, objectives, scope, the research significance and the thesis organization.

Chapter 2 will discuss the literature review which is based on the current available watermarking technique that is available. There will explanations about the techniques of watermarking, requirement of watermarking, types of attack on watermarks and the comparison between some of the available watermarking methods.

Chapter 3 will discuss about the research methodology and the workflow to achieve the objective of this research.

Chapter 4 will discuss on the experimental results that has been done. This chapter will explain about the results and if it manages to achieve the objective of the research.

Chapter 5 will give the conclusion that can be made from this research. Research constraint will also be discussed alongside future work.

# CHAPTER 2

# LITERATURE REVIEW

## 2.1 Introduction

In this chapter, the types of security of images which consists of cryptography, steganography and the type that we will be focus on which is watermarking will be discussed. This chapter will also discuss about the techniques of watermarking which are spatial domain, transform domain and frequency domain which are mostly used in digital watermarking.

## 2.2 Types of Security for Images

### 2.2.1 Cryptography

Cryptography is a technique that has been practised for years to hide the data by the process of encryption and decryption (Sharma, 2017). Cryptography (Mishra & Bhanodiya, 2015) is defined as "art and science" of gaining security through the encrypted messages to make them informative. The rise of growth in the networks is leading a common culture for exchanging of the data at a very fast pace. The word Cryptography is taken from a combination of two Greek words. The first word is "Krypto" meaning hidden and "graphene" meaning writing. Hence, it is defined as hiding the written message from the sender to the recipient (Sharma, 2017). Cryptography also has been pooled with the systems which has been known as "cryptosystems" which has been utilized for coding and decoding of the messages.

### 2.2.2 Steganography

Steganography originated from a Greek word "steganos" and "graphie" which can be defined as "enclosed writing" In 1499, the steganos term was used by Johannes Trithemius in his Stegano-graphia. He has a thesis about cryptography and Steganography disguised as a book on magic. Thus, the message which is hidden under the object is considered as cover which can be of anything such as images, articles, news, or any other cover text.

Steganography is the process of hiding the data in a media file which appears to be unimportant and the media can be transmitted easily by the user containing the hidden information (Pendyala & Gokhale, 2016). It is a process of embedding the unique or authentication information which a user chooses to hide called as Watermark. The means of media elements like audio, image, or even video by which a user succeeds in hiding the information and can protect the content or information from alteration will serve as a Host to the Watermark (Pendyala & Gokhale, 2016).

### 2.2.3 Watermarking

The security of our data basically means to be able to protect our data from any unauthorized access from another person or any other parties and in the same time providing the highest level of security possible to avoid data alteration. The usage of watermark is permanently projected into the digital data so that the authorized user can easily inspect it for clarification purposes (Mathur, 2017). Digital watermarking is a technique that allows users to improve the security and ownership of the data that their own such as digital image, audio, video or even online documents (Mathur, 2017).

The existing methods of watermarking can be divided into the criteria: the mode of insertion and the domain of insertion of the signature (Larijani & Rad, 2008). According to the first criteria, there are two modes of insertion: the "additive mode" where the signature is inserted to the components of the image, and "substitutive mode" where signature takes the place of some components of the image (Larijani & Rad, 2008). These two modes are used alternatively in some projects and both mode present its advantages and disadvantages. For the second criteria: in digital watermarking, a host signal is transformed into a watermark domain in which modifications are imposed on the domain coefficients to embed the watermark (Larijani & Rad, 2008). We can distinguish three main spaces of insertion. The spatial space where insertion is based on manipulation of image's pixel, the frequency space where insertion is based on manipulation of image's pixel, the frequency space where we insert the signature into the DFT or DCT constituents of the image and multiresolution space where insertion is made after wavelet transformation of the image.

Based on (Chandran & Bhattacharyya, 2015), Digital watermarking is the process of adding protected information by making some changes to the pixel values in the image with the least amount of perceptual interruption. Some preferable features of valuable watermarking methods include robustness, imperceptibility and security. The strength of the watermark against manipulations is that it is robust to linear and nonlinear filtering, lossy compression, cropping and scaling (Chandran & Bhattacharyya, 2015).. The watermark can be made imperceptible under untailored observation by embedding the watermark in a discreet, self-effacing manner. The attacks are not limited to elimination of the watermark content, but they also comprise the watermark falsification or estimation, collusion and uncertainty attacks (Chandran & Bhattacharyya, 2015).

## 2.3 Techniques of Watermarking

### 2.3.1 Spatial Domain

A watermark method that is based in the spatial domain is embedded with the scattered information to make the information more secure so that it will be very complicated to identify (Nandini, 2017). It uses some of the minor changes in the value of the pixels. It also has an advantage which is it is very powerful for cropping and translation. Spatial domain watermarking embed the watermark in the pixels of host images by interchanging the lower order bits of the pixels with the watermark or adding some fixed intensity value representing a visual watermark to the pixel values of the picture(Larijani & Rad, 2008).

The main advantage of the spatial domain techniques is the relatively low complexity of calculation as compared to any other techniques that requires domain transforms (Larijani & Rad, 2008). This type of watermarking doesn’t cause any changes in the quality of the image, it assures a high visibility, however it does shows low robustness against several attacks. The simplest form of spatial domain method is the “Least Significant Bits” or LSB.

For every image, each pixel of the color in the image has three components; red, green and blue (RGB). Let us assume that we allocate each pixel with three bytes. Then each colour has one byte, or eight bits, in which the intensity of that colour is specified on a scale from 0 to 255 bits. So, a pixel which is bright purple in colour has the full intensities of the colour red and blue, but no green, the pixel can be represented as x0 = {R=255 bits, G=0 bits, B=255 bits}

Another pixel:

x1 = {R=255 bits, G=0 bits, B=254 bits}

All the values of B are changed here, For the eye, detecting a difference of 1 on a color scale of 256 is almost impossible.

Now each color is stored in a separate byte, the last bit in each byte stores this difference of one. That is, the difference between the bit values of 255 and 254 or 122 and 123 is stored in the last bit which is called the Least Significant Bit.

Since this difference does not matter much, when we replace the information of the color intensity in the Lease Significant Bit with watermarking information, the image will still be able to view like the same through the naked eye.

Therefore, for every pixel of three bytes (24 bits), we can hide 2 bits of watermarking information, in the LSB.

### 2.3.2 Transform Domain

In transform domain techniques, at first the cover image will be transformed and then the watermark will be embedded to the coefficients of the transformed image (Araghi, Manaf, Zamani, & Araghi, 2016). In order to retrieve the original image, an inverse transform of the modified coefficients needs to be taken. Embedding the watermark in transformed domain proves to be more robust against attacks like JPEG compression (Araghi et al., 2016). Transform domain-based algorithm are usually used in robust watermarking to ensure the flexibility of the watermark to common signal processing attacks. The most important reason for using transform domain-based embedding is the possibility of choosing only samples of the transform domain watermarked having desired specifications in terms of fidelity and robustness (Araghi et al., 2016).

There are variety of transform domain watermarking techniques such as discrete cosine transforms (DCT), singular value decomposition (SVD), discrete Fourier transforms (DFT), and discrete wavelet transforms (DWT). The variety of these methods is to provide better imperceptibility and higher robustness to image manipulations and common signal processing attacks, but the cost of computation is higher than spatial domain watermarking methods. The above mentioned techniques, have their own advantages such as computing speed for watermarking, but they cannot make a balance between imperceptibility and robustness automatically in watermarking (Araghi et al., 2016).

## 2.4 Requirement for Image Watermarking Methods

### 2.4.1 Imperceptibility

Imperceptibility here means that the watermarked image does not visible to the human eye on the original image. It also means that there are no defect that is involved in the digital watermarking process is visible to the human eye. In the same time, the quality of the original image should not be degraded of the watermark (Araghi et al., 2016).

### 2.4.2 Robustness

A digital watermark is called robust if it can withstand the transformation that is applied to it (Pardhu & Perli, 2016). Even if the watermarked image is made public, any attempt of removing the watermark should be impossible unless by the authorized persons(Araghi et al., 2016).

### 2.4.3 Security

The watermarked image must be capable of resisting any attacks that tries to remove the watermark or the embedded information on the image (Araghi et al., 2016). For the attacker to remove the watermark, it should be impossible unless they have the knowledge of the watermark algorithm (Araghi et al., 2016).

## 2.5 Attacks on Watermarked Images

### 2.5.1 Removal attacks

Removal attack aims at the complete removal of the watermark information from the watermarked image without cracking the security of the watermark algorithm. This means that there are no processing, even prohibitively complex, can ever recover the watermark information from the attacked data. This includes quantization, denoising, collusion attacks and remodulation. Not all of these methods managed to completely remove the watermark, but they may nevertheless damage the watermark information significantly Sophisticated removal attacks try to optimize operations like nosing or quantization to impair the embedded watermark as much as possible while keeping the quality of the attacked document high enough. Usually, the statistical models for the watermark and the original data are exploited within the optimization process (Voloshynovskiy, Pereira, & Pun, 2001).

### 2.5.2 Geometric Attacks

In geometric attacks, it does not actually remove the embedded watermark itself but intend to damage the watermark detector synchronization with the embedded information. The detector could recover the embedded watermark information when perfect synchronization is regained. However, recent watermarking methods survive these attacks due to the use of special synchronization techniques. Robustness to global geometric distortions often relies on the use of either a transform-invariant domain (Fourier-Melinne) or an additional template, or specially designed periodic watermarks whose auto-covariance function (ACF) allows estimation of the geometric distortions (Patel, Swati, & Chauhan, 2014). However, the attacker can design dedicated attacks exploiting knowledge of the synchronization scheme. Robustness to global affine transformations is more or less a solved issue. Therefore, pixels are locally shifted, scaled and rotated without significant visual distortion.

### 2.5.3 Cryptographic Attacks

Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information of to embed misleading watermarks (Patel et al., 2014). This technique is brute-force search for the embedded secret information. Another attack in this category is the so-called Oracle attack, which can be used to create a non-watermarked signal when a watermark detector device is available. Practically, application of these attacks is restricted due to their high computational complexity.

## 2.6 Digital Watermarking Mapping Pattern

### 2.6.1 HILBERT-LSB-C

(Hisham, Zain, Arshad, & Liew, 2015) suggested the HILBERT LSB C as the Authentication System for Color Medical Images. This is because of the variety of sizes and modalities of medical images such as CT-SCAN, MRI and X-ray. The watermarking scheme used for medical images should invisibly embedded in the image without altering the image size or format. This paper used samples from various modalities such as CT, MRI, PET, ultrasound, mammogram, DTI and X-Ray images. All of these samples have different size, qualities, width and height. Some of it are 8 bits and some are 16 bits. The paper proposed a scheme that can perform both tamper detection and recovery. This paper proposed an embedding technique started with numbering by the Hilbert manner. The first step in suggested in this paper is numbering the pattern. All of the blocks in the image should be numbered and mapped to decide the location of the blocks as the watermark data. A unique method of numbering and mapping the pixels can guarantee the top performance of authentication system by spreading the numbered data as far as possible from the original location. It starts at a random pixel and directly follows the generated iteration, which is +L, -L and -R. For a M x N sized RGB cover image, each color plane is divided into non-imbricating blocks of size m_height x m_width. In this paper, the blocks are set to 8 x 8 blocks when designing the HILBERT-LSB-C scheme. Then the numbering process takes place by applying the Hilbert path to get the non-sequential, unique order of image blocs of pixel before mapping. Then the mapping is done pseudo-randomly for all of the blocks generated by a one-dimensional transformation.

Embedding is then done after the block numbering is done. The embedded watermark in each sub-block is a 3-tuple(v, p, r) where both v and p are 1-bit authentication watermark, and r is a 7-bit recovery watermark for the recovering sub-block within the original block (block A) mapped to the watermarked block(blok C) In this scheme, the watermark on the cover image is formed by authentication information of 2 bits and recovery information of 7 bits for each sub-block that contains 16 pixels of 4 x 4, which make the total of 21 bits from three planes for each 16 pixels. By using the block mapping sequence, the authentication and recovery information of the original or cover plane are generated and embedded into its mapping block of host plane of the image.

The metric used in this research is Peak-signal-noise-ratio (PSNR), one of the metrics to determine the degradation in the embedded image with respect to the host image. A general rule of PSNT is that the values of 36 dB In PSNR are acceptable in terms of degradation, which means there are no significant degradation is observed by human eyes. The average PSNR value for watermark embedded images is satisfactory, 57.98 dB. As the PSNR value is high, there is no visual difference between the original image and the watermarked image.

### 2.6.2 Save Algorithm

Save algorithm is a Spatial domain Watermarking technique that was proposed by H.H Larijari, G.R.RAD (Pendyala & Gokhale, 2016). This technique includes a fixed threshold instead of an optional threshold to improve the computational time. The fixed threshold is included instead of the optional value based on the capability of human sight can only distinguish 32 grey intensity levels out of the 256 intensity levels. This means that the human eye can only distinguish between the intensity values of 34 and 43 but no able to distinguish between the intensity values of 34 and 36 as it will show a little bit of grey shade.

This Watermarking algorithm saves part of the pixels of the host image depending on the similarity if the pixel values in the Host and Watermark image as a secret key in the embedding process and then it uses the secret key to retrieve the watermarked image during the extraction process. The secret key is needed for the authentication purpose of the watermarked image.

The algorithm used in this watermarking scheme makes a comparison of the pixel values between the Host and Watermark Image. The Host image will act as a carrier to the Watermarked image pixel values. The size of the Watermarked image is stored in the contents of the Secret key vector. Then it is followed by the comparison of pixel values that it is carrying starting with the first Watermarked pixel. If there is a match between the Watermarked image and the Host image, then the information is located inside that pixel.

To test the robustness of the algorithm, multiple watermarking attacks was performed. The effectiveness of the algorithm is measured in Peak Signal to Noise Ratio (PSNR), Normalized Cross Correlation Coefficient (NCC) and Structural Similarity Index Measure (SSIM) to calculate how similar the watermarked image after the attack if compared to the original watermarked image. The analysis of testing the Host Image with noise and transformation attacks shows that the algorithm is robust to the attacks and the PSNR value is above 18dB, NCC is above 0.84 and SSIM is above 0.71.

### 2.6.3 Combination of LSB and DCT

In this paper by (Mathur, 2017), the author suggested to apply a hybrid technique which is a combination of Least Significance Bit (LSB) and Discrete Cosine Transformation (DCT). The LSB is the most known technique to embed a watermark. The LSB technique changes the images into pixels to bits. The LSB methods uses a pseudorandom number generator to confirm the pixels that are to be used to embed the watermark. The DCT method relies on the orthogonal transform which is the most normally used linear transform in digital signal process.

The flow of this method is that the author suggested to try a combination of LSB-DCT watermarking method. In this approach, the author applies the watermark on the edge of the original image as a watermarked image that is calculated using edge detection technique. The watermark is embedded on the original image using LSB approach. Once the first watermarking method is completed, the next watermark will be embedded in the first image with the application of DCT watermarking.

The result of these combination are calculated on the Experiment is done on multiple images. The quality of the image is slightly damaged after applying LSB watermark. This Dual watermarking is not a highly recommended method as after applying the LSB on the image, it disturbs the quality of the image and also very easy to modify the watermark.

## 2.7 Comparison of The Methods

Table 2.7 Comparison of the Watermarking Methods

| Techniques | Advantages | Disadvantages |
|---|---|---|
| DCT AND LSB | 1. Difficult to erase the security information<br>2. DCT over LSB does not affect the originality of the image<br>3. Dual watermarking hides the owner information in an efficient manner meaning that DCT does not alter the information embedded using LSB | 1. This method required more time to embed the watermark |
| Save Algorithm | 1. Time for watermark embedding is faster<br>2. Gives flexibility of utilizing multiple watermarking technique with different watermark images | 1. The embedding requires a lot of RAM to perform |
| HILBERT-LSB-C | 1. The Hilbert numbering for color method can cover all the criteria needed for medical image watermarking<br>2. The Hilbert numbering method also proved to be compatible for any type of images | 1. The limitation of watermarking only on square images |

## 2.8 Conclusion

Based on the research, there are some protective measures to protect our images on the internet namely steganography, cryptography and the one that we are discussing in this research is digital watermarking. And in digital watermarking there are two techniques which are spatial domain and transform domain. Both of these techniques have their own advantages and disadvantages in terms of the characteristics of the watermarked image such as robustness, perceptibility and security. The digital watermarking mapping pattern have their own advantages in terms of time taken and the security and these are the two characteristics that we are going to test by using our own data which are medical images.

# CHAPTER 3

# METHODOLOGY

## 3.1 Introduction

In this chapter, it will be focused on the proposed mapping pattern which is the Hilbert-Peano curve. The purpose of this chapter is to elaborate in detail on the processes and methods that are used in the selected algorithms.

## 3.2 Methodology

The research methodology of this study contains four fundamental contents. It contains the workflow diagram, the algorithm of the mapping pattern, the list of hardware and software required to execute the pattern, and the Gantt Chart for the research.

### 3.2.1 Workflow

Based on Figure 3.1 below, during the process of completing this research, there are specific processes or steps need to be done. The first process is to figure out the problem statement and the solution. The problem statement for this research is to discover whether there is a better mapping pattern other than Hilbert-SB-C (Hisham et. al, 2014) as reviewed in Chapter 2 and figure out if the discovered pattern is better in terms of time consumption, effectiveness and higher security.

Then we decide the objectives and the expected results which is if the new proposed pattern is faster and offers more security than the existing pattern. The Hilbert-LSB-C will be the reference in this research.

The third process is to gain some knowledge based on other research papers and existing methodologies which are published from year 2015 until recent. The main reason in reviewing these papers is to discover the recent update in the existing methodologies and what have the recent papers implemented to improve the mapping pattern of fragile watermarking.

After reviewing all the papers and all the other methodologies, a decision is made to propose an improvement to the current mapping pattern. Nevertheless, the proposal to improve the current mapping pattern does not guarantee a full success. It might be better in some aspect but not in all of the aspects that is required to be a successful mapping pattern. In choosing the proposed pattern, there are some aspects that need to consider such as below;

i) Time taken
ii) Robustness
iii) Level of security

The next step is to perform testing with the proposed pattern. The proposed pattern in this research is Hilbert-Peano pattern and then we will get the results to show whether Hilbert-Peano pattern is better than CLSB-SPIRAL and LSB-HILBERT in some chosen aspect.

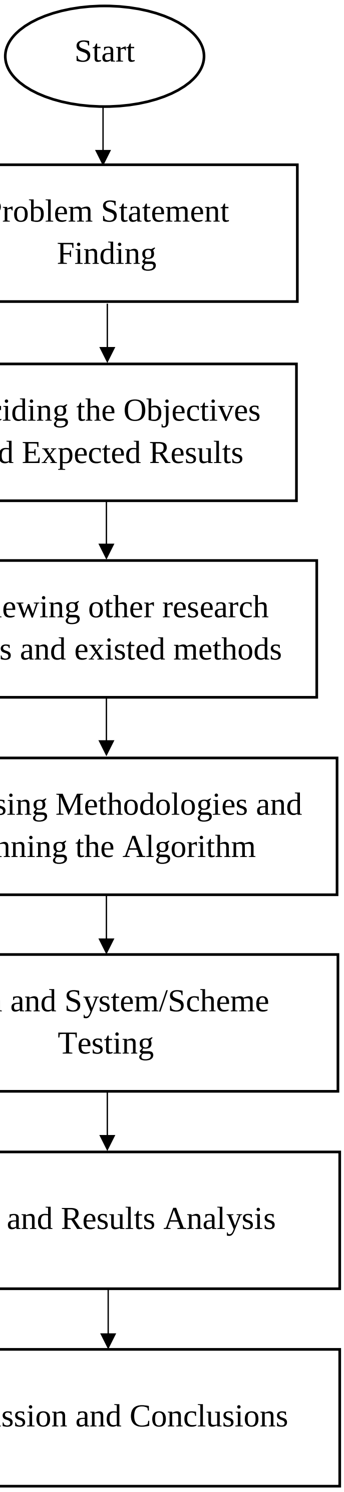

Start
Problem Statement Finding
Deciding the Objectives and Expected Results
Reviewing other research papers and existed methods
Discussing Methodologies and Planning the Algorithm
Data and System/Scheme Testing
Data and Results Analysis
Discussion and Conclusions

Figure 3.1 The workflow of the Research

### 3.2.2 Algorithm

This subchapter will focus on the algorithm that is involved in the process of developing the Hilbert-Peano pattern. The scope of this research is to use the proposed pattern on RGB images. The algorithm of the mapping pattern starts with numbering, block division and mapping and ends by watermark embedding. The embedded images will be verified on detection phase. Figure 3.2 shows the plan that will be implemented in this research as to create the numbering pattern. Figure 3.3 will show the flow of the embedding phase and Figure 3.4 will show the flow of the detection phase.

#### 3.2.2.1 Block Numbering

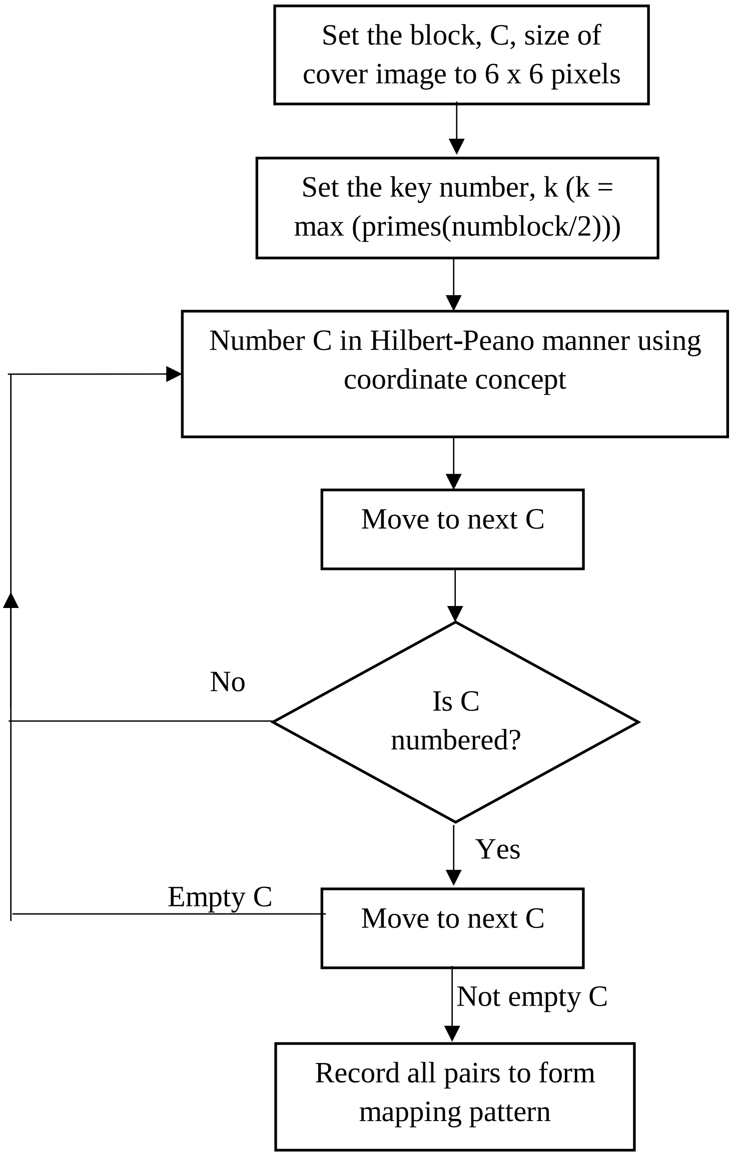

Set the block, C, size of cover image to 6 x 6 pixels
Set the key number, k (k = max (primes(numblock/2)))
Number C in Hilbert-Peano manner using coordinate concept
Move to next C
No
Is C numbered?
Yes
Empty C
Move to next C
Not empty C
Record all pairs to form mapping pattern

Figure 3.2 The Flow Diagram for Proposed Numbering Technique (Syifak, 2016)

Before the embedding process, all the blocks in the image are numbered and mapped with the mapping pattern to determine the location and mark the blocks as the watermarked data to avoid redundancy in the embedding process. By using a specific style of numbering and mapping of each block, it could assure the top performance of the authentication system by spreading the numbered data as far as possible from the original location. The numbering of the block is determined on the user whether they want to divide the block into 6 by 6 smaller blocks or 8x8 even smaller blocks.

The blocks of the original images are labelled as C and the blocks of watermarked image as H. The proposed mapping pattern starts with numbering C using the Hilbert-Peano method and map it using the pseudorandom way. The numbering then will start at a random pixel and then followed by moving to the next block. All of the block then will be embedded and numbered.

In the process of generating the Hilbert-Peano pattern, it follows a recursive algorithm as follows:

Step 1: Set the block size as *C*,

Step 2: Set *k* as the key number,

Step 3: Calculate the number of blocks to get the total number of columns and rows,

Step 4: Choose the starting point then start the block numbering,

Step 5: After the block numbering is completed, each block then will be mapped using the proposed mapping pattern.

### 3.2.2.2 Process to Generate the Hilbert-Peano pattern.

A. Divide the Hilbert-Peano pattern

Based on the Hilbert-Peano pattern, the pattern are generated by using two basic elements, corresponding to the connected curve. Below, the figure shows the two basic elements of the pattern.

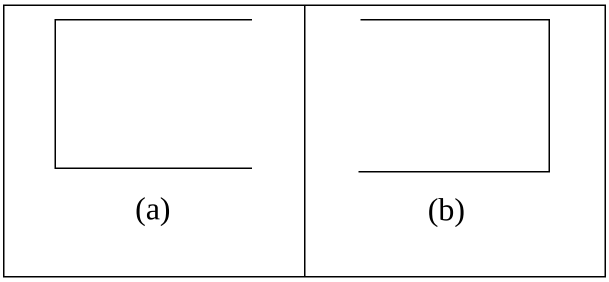


Figure 3.3 Basic generated elements

B. Iterative Matrix

The Hilbert-Peano pattern generating element is simple but according to its characteristics, as the number of iterations increases, the number of the iteration of the infinity curve will traverse the area within the scope of all of the points. Based on the curve of each iteration characteristics, the amplification of iterative matrix is applied to describe the curve generation process, as demonstrated in Figure 3.5.

The generation of the curve for the first iteration will be as below;

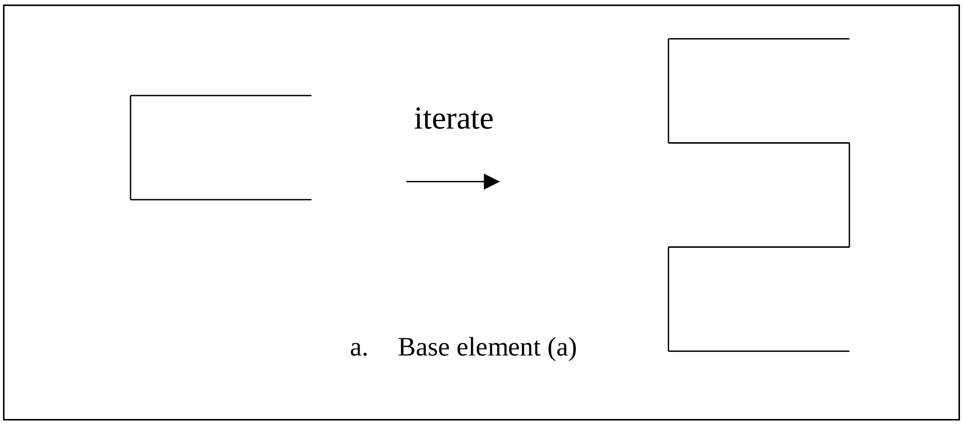


Figure 3.4 Generation of the pattern

C. The connection between the generated curve.

According to the characteristics of the Hilbert-Peano pattern, the curve has one entrance and one exit meaning that the repeated traversal area must demand the curve to be continuous at all squares. By the n number of iterations of the Hilbert-Peano pattern after it has been translated to a $6^n \times 6^n$ iterative matrix according to the rules.

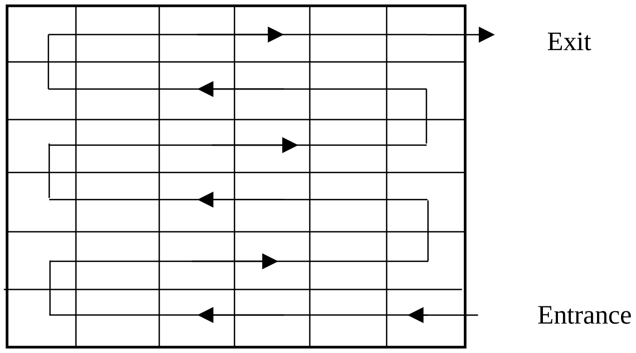


Figure 3.5 Path of the Hilbert-Peano pattern

### 3.2.2.3 Process of Tamper Detection.

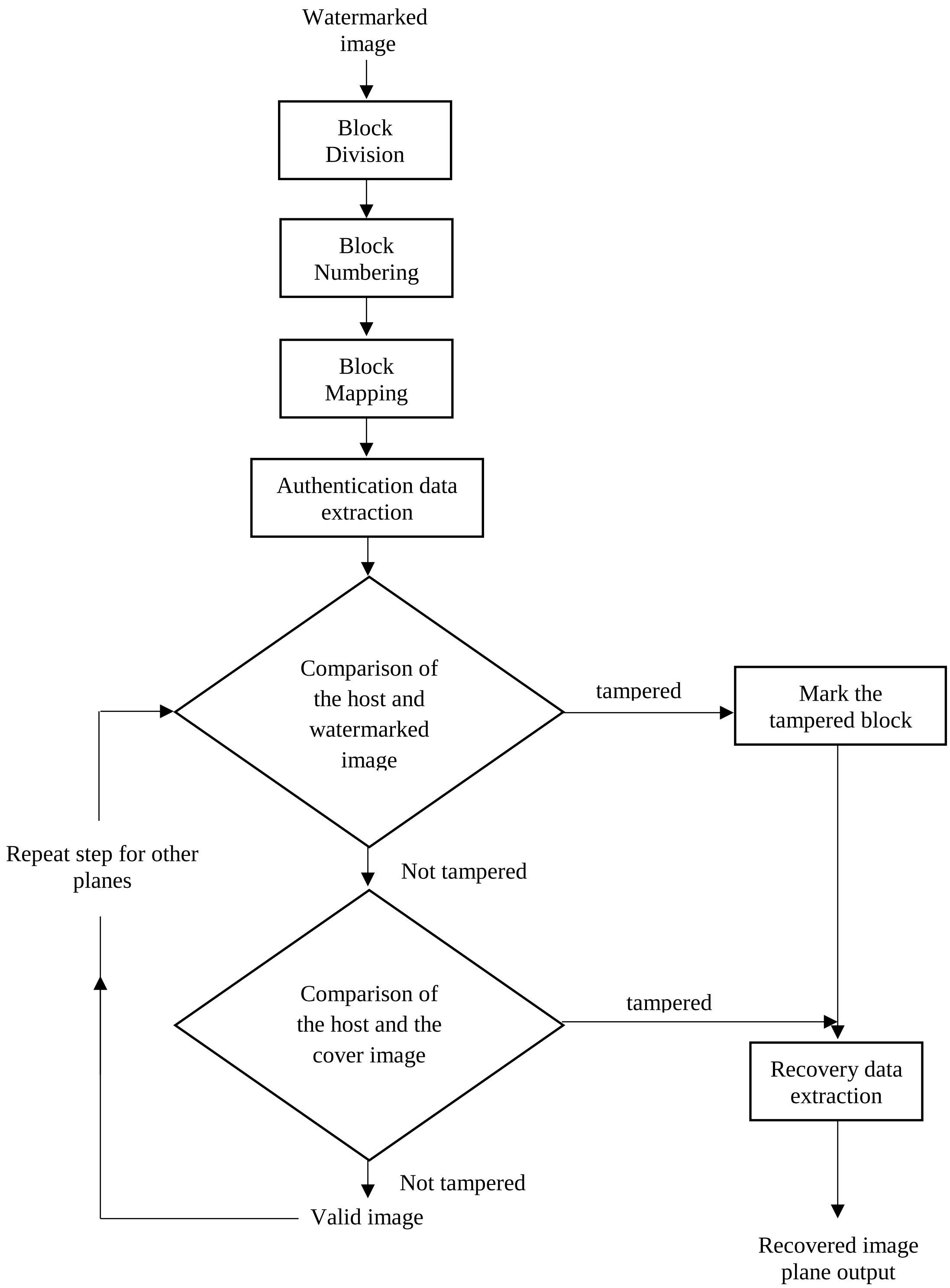

Watermarked image
Block Division
Block Numbering
Block Mapping
Authentication data extraction
Comparison of the host and watermarked image
tampered
Mark the tampered block
Repeat step for other planes
Not tampered
Comparison of the host and the cover image
tampered
Recovery data extraction
Not tampered
Valid image
Recovered image plane output

Figure 3.6 Flow Diagram for Tamper Detection in the proposed watermarking scheme

Based on Figure 3.6, the tamper detection process begins with the division of the blocks in the pixel and then each block will be numbered. This is followed by block mapping and then the extraction of the authentication data from the image. This data is the watermark information that the sender has inserted into the image for authentication purposes. This is then followed by the comparison of the host image with the watermarked image and the cover image. If the output is not tampered, then it is a valid image but if it is tampered then it will be marked as a tampered image and the recovery data extraction process will be done to recover the original image.

## 3.3 Hardware and software

In the development of this new mapping pattern, there are some hardware(s) and software(s) required. Tables below shows the hardware and software requirement and specification that will be used in this method for the testing purpose.

Table 3.1: The Hardware Requirements and Specification

| **No.** | **Hardware** | **Specification** |
|---|---|---|
| 1 | HP Pavilion Laptop PC | Processor Intel Core i5 (7th Generation)<br>Windows 10 Home Single Language |

Table 3.2: The Software Requirements and Specification

| No. | Software | Specification |
|---|---|---|
| 1 | Microsoft Office Word 2016 | Used to document the research report from Chapter 1 to Chapter 5 |

|   |   |   |
|---|---|---|
| 2 | Mendeley Desktop | Used to generate the citation of the articles, research papers and references needed for this report. |
| 3 | Microsoft Project Professional 2016 | Used to design the Gantt Chart of this research |
| 4 | Matlab | Used to run the coding |

## 3.4 Gantt Chart

Refer in Appendix

## 3.5 Conclusion

Based on the discussion above, the research already discussed about the flow of the research starting from figuring out the problem statement that this research will try to prove and from there we discussed the objectives and in Chapter 3 this research discussed mostly about the methodologies that is chosen which is the Hilbert-Peano pattern. The progress of developing the pattern there are three steps which are block numbering, block embedding and then the process to generate the Hilbert-Peano pattern itself. The most important hardware and software to run the program is by using at least a laptop with an i5 Intel Core Processor and the software is Matlab.

# CHAPTER 4

# RESULTS AND DISCUSSION

## 4.1 Introduction

In this chapter, the research materials and files that is used in the research will be presented. The results and analysis of the proposed watermarking technique for medical images and to compare the proposed watermarking technique with the Hilbert mapping pattern will be shown as well. The result of this research is expected to be helpful in order to improve the embedding time of the watermarking scheme and in the same time can be a reference to other researcher in the future.

The focus of this research is to test time taken for embedding the watermark into the image. The proposed watermarking scheme will be used and be tested based on its PSNR and MSE value and also the time taken to embed the watermark into the image.

## 4.2 Review on Watermarking for Image Authentication

Watermarking is a method that is used mainly to claim ownership of something either it is digital or physical. Watermarking in terms of authentication is also used to determine the authenticity of the image or the documents. In this research, some medical images has been used as the subject that will be tested on the proposed watermarking scheme. Watermark in medical images is important to medical officers to ensure that the medical images that they are seeing is unique and belong to the correct patient that they are treating in order for them to make the decision to make a treatment to the patient.

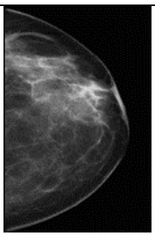
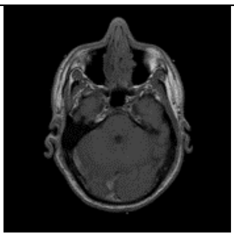
However, the watermarking are mostly not visible to the naked eye as it will affect the medical images. The watermarked images are mostly inspected if necessary such as if there is a confusion between who does the specific x-ray image belong to. The watermark is embedded in the Least Significant Bit (LSB) as any alteration in the LSB does not appear obviously in the physical image.

## 4.3 Experimental Data and Outcomes

### 4.3.1 List of Experimental Data

There are 8 images in (.bmp) format that is used to test the watermarking scheme and in the same time the collection of data of the image embedding process. The images come in different size and all are individually tested on the Hilbert watermarking scheme and Hilbert-Peano Scheme and all the outcomes are recorded.

Table 4.1 Sample Images for Testing

| No | Sample | Size |
|---|---|---|
| 1 | | Image Size: 400 X 344 Pixels<br>Data Size: 537 KB |
| 2 |  | Image Size: 328 X 504 Pixels<br>Data Size: 645 KB |
| 3 |  | Image Size: 256 X 256 Pixels<br>Data Size: 65.0 KB |

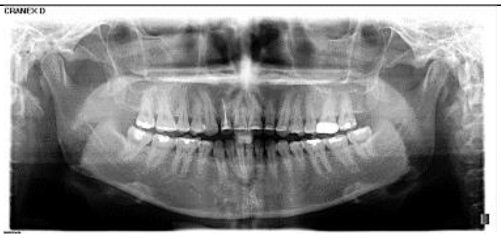
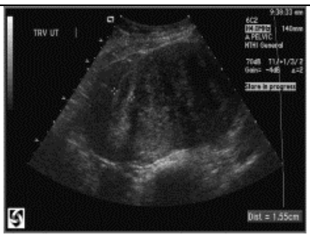
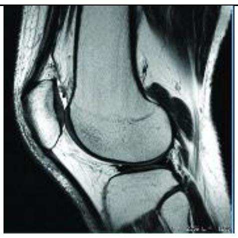
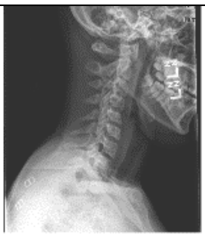
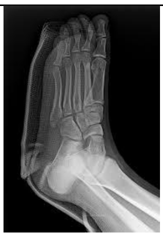
| | | |
|---|---|---|
| 4 |  | Image Size: 904 X 416 Pixels<br>Data Size: 1.43 MB |
| 5 |  | Image Size: 640 X 480 Pixels<br>Data Size: 301 MB |
| 6 |  | Image Size: 520 X 512 Pixels<br>Data Size: 101 MB |
| 7 |  | Image Size: 534 X 613 Pixels<br>Data Size: 960 KB |
| 8 |  | Image Size: 186 X 271 Pixels<br>Data Size: 5.39 KB |

Table 4.1 Shows the images that is used to test the watermarking scheme. All the images are in (.bmp) format and the data size of the image ranges from 537 KB to 301 MB.

### 4.3.2 Experimental Results and Discussion

The images displayed in Table 4.1 were tested with two watermarking technique which are Hilbert Pattern and the proposed pattern Hilbert-Peano Pattern. In this section, the results of the experiment will be displayed and will be discussed. The outcomes of this experiment is to compare the time taken for the watermark embedding process and to see which mapping pattern requires less time to embed.

### 4.3.3 Performance Analysis: Imperceptibility

The embedded watermark in medical images are not clearly visible to the naked eye at it is embedded in the Least Significant Bit (LSB). Therefore, to measure the imperceptibility of the watermarked images accurately, Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) is preferred for measurement.

#### 4.3.3.1 Peak Signal to Noise Ratio (PSNR)

PSNR is the ratio between a power of the signal noise and the signal's maximum power. It is used to measure the quality of the images that has been embedded watermark into it. If the PSNR value is high it means that the image is almost similar with the original image. Hence, each image will be embedded into two watermarking pattern and the value of the PSNR will be compared.

The following table shows the PSNR values obtained from the two watermarking pattern that is used in this research.

Table 4.2 PSNR Values between Hilbert and Hilbert-Peano watermarking pattern.

| Figure | Hilbert | Hilbert-Peano |
|---|---|---|
| | PSNR | PSNR |
| Sample 1 | 58.9348 | 58.9406 |
| Sample 2 | 58.8268 | 58.8912 |
| Sample 3 | 53.9764 | 53.6794 |
| Sample 4 | 58.3968 | 58.3872 |

| | | |
|---|---|---|
| Sample 5 | 55.4978 | 55.5138 |
| Sample 6 | 58.4014 | 58.4297 |
| Sample 7 | 58.6310 | 58.6431 |
| Sample 8 | 58.6851 | 58.6851 |
| **Average Value** | 57.6463 | 57.6687 |

Table 4.2 shows the result of PSNR values gained from both the image watermarking schemes on the medical images that is tested on 8 different samples. The amount of PSNR value is calculated based on the ration between the power of distorting noise that affects the quality of the watermarked image and the maximum possible value of a signal.

Based on the average value of PSNR, the Hilbert watermarking scheme is lower by 2 decimal places if compared to the proposed scheme. As we know, the lower the PSNR value, the better the security of the image but based on these results, there was not much difference in PSNR value in comparison between both the values.

#### 4.3.3.2 Mean Square Error (MSE)

Mean Square Error (MSE) defines as the cumulative squared error between the original image and the embedded image. The lower the MSE value, the lesser the error found in the watermarked image meaning that the alteration on the embedded image is less significant to the naked eye. The same sample images will be tested on the MSE and the outcome is recorded.

The following table shows the MSE values obtained from the two watermarking pattern that is used in this research.

Table 4.3 MSE Values between Hilbert and Hilbert-Peano watermarking pattern

| Figure | Hilbert | Hilbert-Peano |
|---|---|---|
| | MSE | MSE |
| Sample 1 | 0.0830 | 0.0831 |

| | | |
|---|---|---|
| Sample 2 | 0.0839 | 0.0852 |
| Sample 3 | 0.2787 | 0.2787 |
| Sample 4 | 0.0943 | 0.0941 |
| Sample 5 | 0.1827 | 0.1834 |
| Sample 6 | 0.0933 | 0.0940 |
| Sample 7 | 0.0889 | 0.0891 |
| Sample 8 | 0.0880 | 0.0880 |
| **Average Value** | 0.1241 | 0.1244 |

Table 4.3 shows the result of the MSE values gained from the embedding process of the images. The MSE value is calculated by taking the square of differences between every pixel in the original sample image and the corresponding pixels in the watermarked medical image, add it up and then divide it by the number of pixels.

Based on the outcome in Table 4.3, the MSE value from both watermarking schemes is low which means that the watermarking scheme managed to embed an image that is almost similar with the original image even after the watermark is inserted to the original image. The differences between the two schemes are to tiny to differ meaning that the proposed scheme doesn’t have much differences when compare with the Hilbert pattern.

### 4.3.4 Processing Time Analysis

The effectiveness of a watermarking scheme does not just depend on the PSNR and MSE value but also the time taken to embed the watermark to the original image. If the time taken is too long to embed the watermark pattern then it will only suitable for smaller size image as it will surely take more time to embed into the bigger size image. Therefore, in this section we will discuss about the embedding processing time of the two watermarking schemes. All the sample images are tested using the Hilbert Pattern and Hilbert-Peano Pattern and the time taken is recorded for every image.

#### 4.3.4.1 Embedding Processing Time

The embedding process is the process of inserting the watermark into the original image. Hilbert Pattern is a single type pattern and Hilbert-Peano is a hybrid pattern as it combines two patterns into one.

The following table shows the time taken to embed the watermark into the images. The images varies in sizes as they are different medical images.

Table 4.4 Time taken for watermark embedding

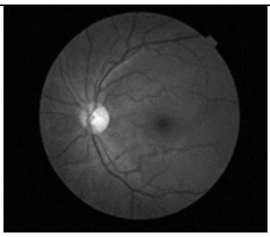
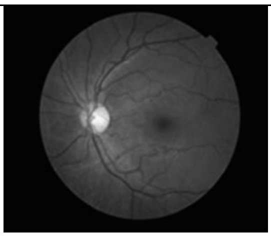
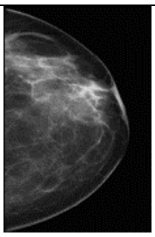
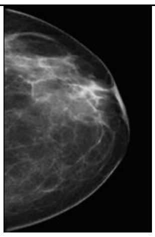
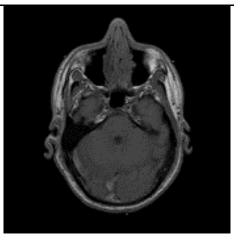
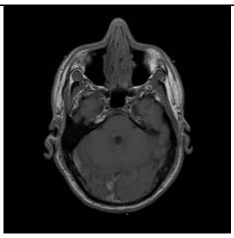
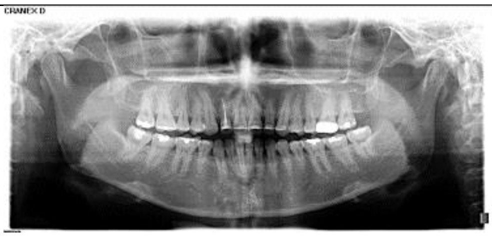
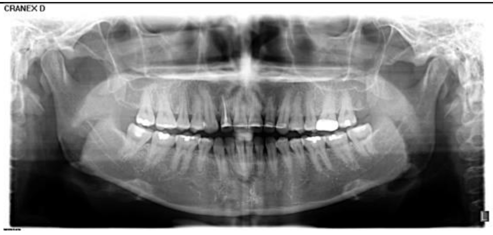
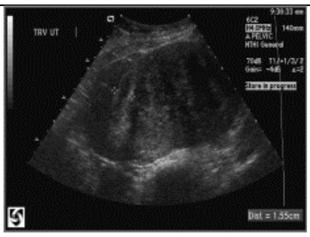
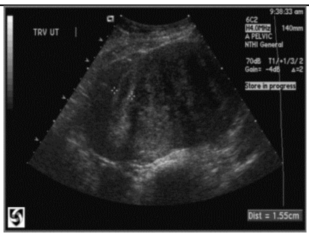
| Figure | | Hilbert | Hilbert-Peano |
|---|---|---|---|
| | Image Size | Time Taken | Time Taken |
| Sample 1 | 537 KB | 45.9219 | 37.7813 |
| Sample 2 | 645 KB | 55.8750 | 44.8906 |
| Sample 3 | 65.0 KB | 5.6563 | 4.4844 |
| Sample 4 | 1.43 MB | 510.7969 | 408.6719 |
| Sample 5 | 301 MB | 351.9219 | 338.8594 |
| Sample 6 | 101 MB | 303.0781 | 275.1406 |
| Sample 7 | 960 KB | 375.8125 | 336.0625 |
| Sample 8 | 5.39 KB | 13.8750 | 13.0313 |
| **Average Value** | | 207.8672 | 182.36525 |

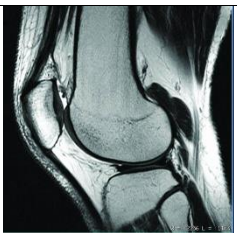
The results in Table 4.4 shows the time taken for all the images to be embedded with the watermarking scheme. The size of the images also affected the time taken for the watermark to embed into the images.

In the table, the time taken differs and the bigger the size of the image, the longer time is needed to embed the watermark. From the table, it is clear that the Hilbert pattern is taking a bit longer time to embed as compared to the Hilbert-Peano pattern. This is because of the embedding process of the Hilbert watermarking scheme requires a 2 bits information authentication data size and 7 bits for the recovery information for each pixel as compared to the Hilbert-Peano watermarking scheme which is less.

#### 4.3.4.2 Watermarked images output

Table 4.5 Before and after images after digital watermarking

| No | Original image | Watermarked Image |
|---|---|---|
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |

| | | |
|---|---|---|
| 6 | |  |
| 7 | | |
| 8 | | |

Based on Table 4.5, the outcomes of the watermarked images using the Hilbert Peano pattern does not show much significant differences. This proves that even the Hilbert-Peano pattern is a hybrid mapping pattern, it does not really affect the watermarked images and in the same time does not really affect the PSNR and MSE value meaning that the quality of the mapping pattern is proven better than the mapping pattern of only Hilbert mapping pattern.

## 4.4 Summary

In this chapter, all the outcomes of the research are shown and discussed. The proposed method was proven better in terms of it takes a shorter time to embed the watermark into the image and still manage to obtain a safe PSNR and MSE value. After testing the proposed watermarking scheme, it is obvious that the time taken to embed the Hilbert-Peano pattern is significantly faster than the Hilbert pattern. Therefore, the proposed scheme has achieved its objective.

# CHAPTER 5

# CONCLUSION

## 5.1 Introduction

In this paper, we have introduced and tested the Hilbert-Peano watermarking scheme and compared it to the current available Hilbert watermarking scheme. The main objective of proposing this watermarking scheme was to test whether the hybrid watermarking scheme can embed the watermark faster to the images as compared to the Hilbert watermarking scheme. The effectiveness of the watermarking scheme is tested by the imperceptibility of the embedded image and the time taken to generate, embed and authenticate the watermark. The proposed watermarking scheme was able to embed the watermark with a faster processing time and in the same time able to maintain the quality of the image.

## 5.2 Research Constraints

There were some constraints in the progress of completing this research. The main constraint is the short amount of time to study the currently available watermarking scheme and to understand them and this will surely affect the choosing of the watermarking pattern. There are many watermarking schemes that can be used in this research but the shortage amount of time affected the selection of the watermarking scheme.

One other constraint was the lack of knowledge on watermarking techniques. In terms of digital watermarking, there are many branches of knowledge to be learned to be able to fully understand and master the skills about digital watermarking. Both of these constraints can be overcome if there were more time to study and understand about digital watermarking.

## 5.3 Research Conclusion

The proposed watermarking scheme has proved better in terms of the time processing of embedding the watermark into the medical images.

The quality of the PSNR and the MSE value was not significantly different meaning that the quality of the image is not too much disturbed by the watermark. This proves that even though the proposed watermark is a hybrid, it does not affect much on the watermarked image.

The proposed watermarking can be used if it involves a large amount of data in order to reduce the processing time for image watermarking.

## 5.4 Future Works

The limitation of this current research will be the motivation for future improvements which is the short amount of time to understand and have more knowledge about the current available watermarking scheme. Further improvement could be done in order to achieve a shorter time for the embedding process and in the same time maintaining the quality of the watermarked image by comparing the PSNR and MSE value.

## References

Araghi, T. K., Manaf, A. B. A., Zamani, M., & Araghi, S. K. (2016). A Survey on Digital Image Watermarking Techniques in Spatial and Transform Domains. *International Journal of Advances in Image Processing Techniques– IJIPT*, *3*(1), 6–10.

Chandran, S., & Bhattacharyya, K. (2015). Performance analysis of LSB, DCT, and DWT for digital watermarking application using steganography. *International Conference on Electrical, Electronics, Signals, Communication and Optimization, EESCO 2015*. https://doi.org/10.1109/EESCO.2015.7253657

Hisham, S. I., Zain, J. M., Arshad, N. W., & Liew, S. C. (2015). HILBERT-LSB-C as authentication system for color medical images. *2015 4th International Conference on Software Engineering and Computer Systems, ICSECS 2015: Virtuous Software Solutions for Big Data*, 15–20. https://doi.org/10.1109/ICSECS.2015.7333114

Larijani, H. H., & Rad, G. R. (2008). A new spatial domain algorithm for gray scale images watermarking. *Proceedings of the International Conference on Computer and Communication Engineering 2008, ICCCE08: Global Links for Human Development*, 157–161. https://doi.org/10.1109/ICCCE.2008.4580587

Mathur, E. (2017). combination of LSB and DCT, 351–354.

Mishra, R., & Bhanodiya, P. (2015). A review on steganography and cryptography. *Conference Proceeding - 2015 International Conference on Advances in Computer Engineering and Applications, ICACEA 2015*, 119–122. https://doi.org/10.1109/ICACEA.2015.7164679

Morrissey, J. (1996). Data security, *26*(40), 32–33,35–38,40. Retrieved from http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=10161903

Nandini, D. U. (2017). Techniques, 1–4.

Pardhu, T., & Perli, B. R. (2016). Digital image watermarking in frequency domain. *International Conference on Communication and Signal Processing, ICCSP 2016*, 208–211. https://doi.org/10.1109/ICCSP.2016.7754123

Patel, M., Swati, & Chauhan, A. (2014). The study of various attacks on Digital watermarking technique. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *3*(5), 1567–1570.

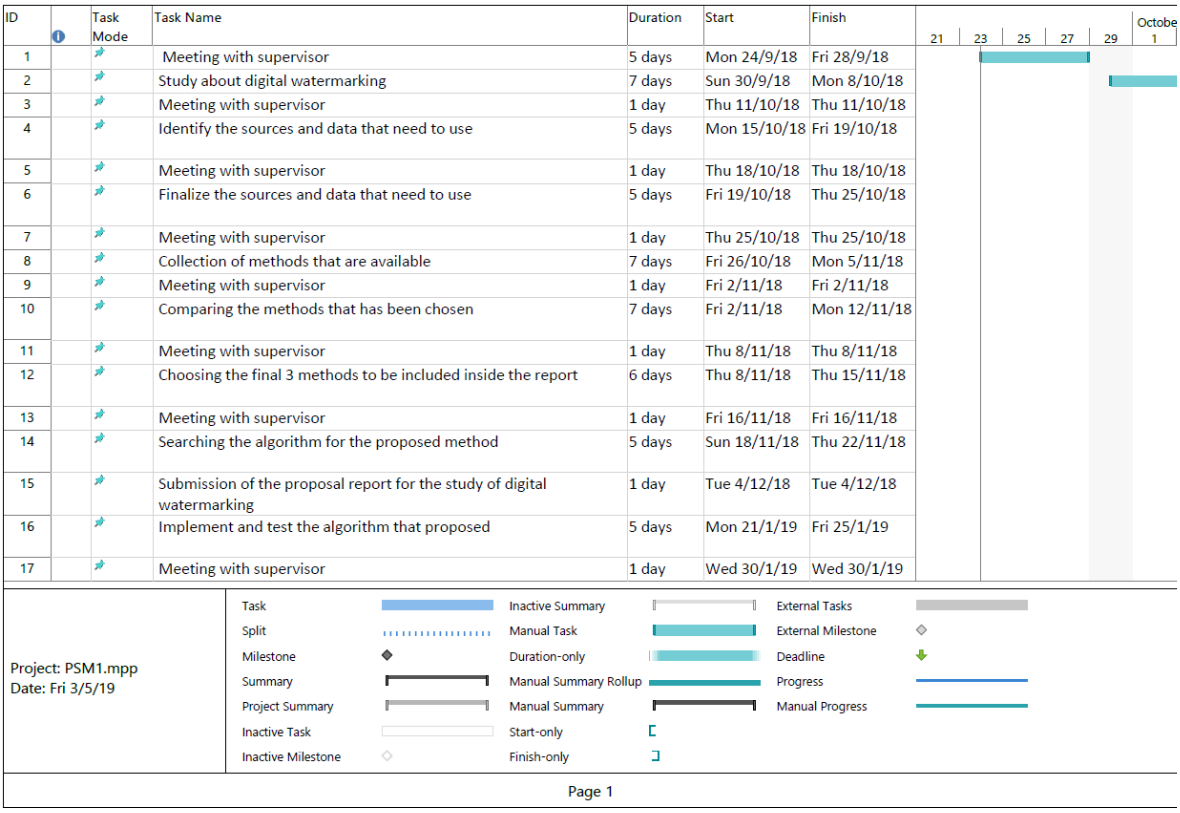
Pendyala, M., & Gokhale, A. (2016). Design of a spatial domain watermarking technique with VLSI implementation. *Conference on Advances in Signal Processing, CASP 2016*, 498–503. https://doi.org/10.1109/CASP.2016.7746223

Sharma, N. (2017). A Review on Spatial Domain Technique Based on, 24–27.

Singh, G. (2018). A review of secure medical image watermarking. *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017*, 3105–3109. https://doi.org/10.1109/ICPCSI.2017.8392297

Voloshynovskiy, S., Pereira, S., & Pun, T. (2001). Attacks on Digital Watermarks : Attacks , and Benchmarks. *IEEE Communications Magazine*, 118–126.

# APPENDIX

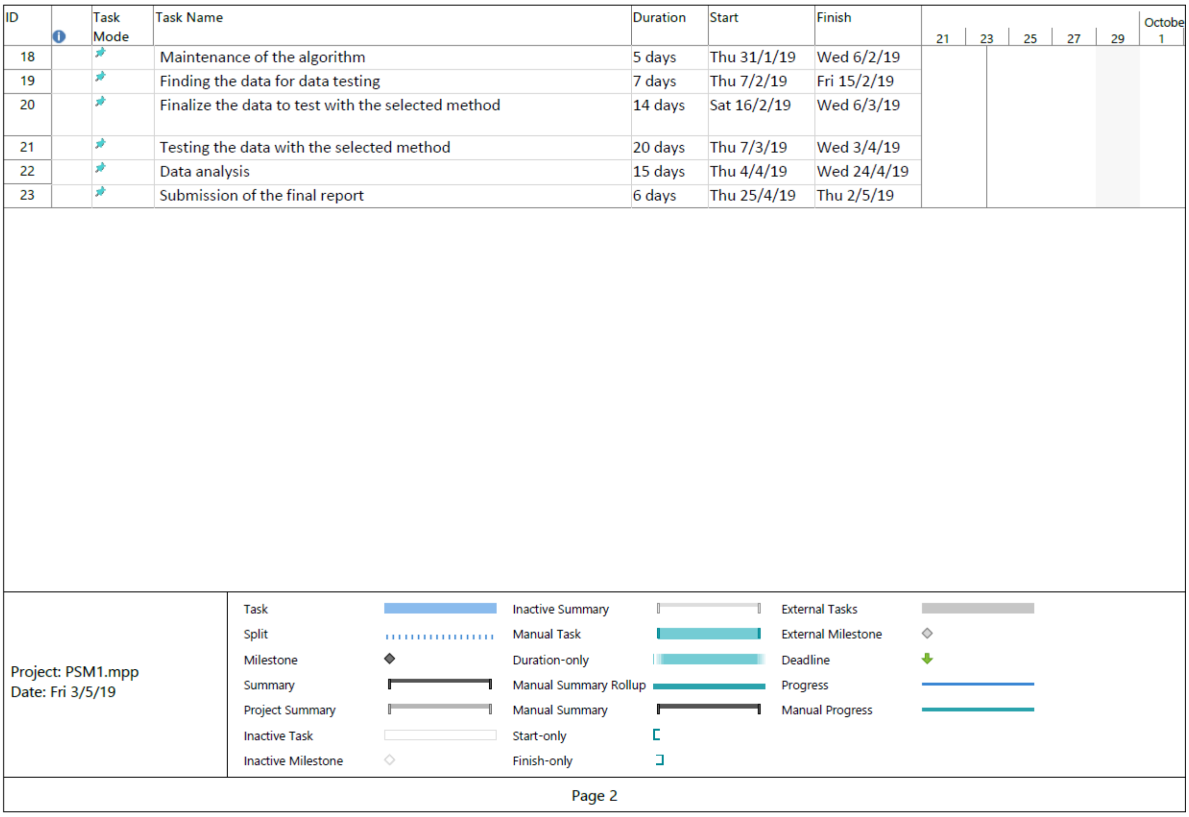


| ID | ⓘ | Task Mode | Task Name | Duration | Start | Finish |
|---|---|---|---|---|---|---|
| 1 | | 📌 | Meeting with supervisor | 5 days | Mon 24/9/18 | Fri 28/9/18 |
| 2 | | 📌 | Study about digital watermarking | 7 days | Sun 30/9/18 | Mon 8/10/18 |
| 3 | | 📌 | Meeting with supervisor | 1 day | Thu 11/10/18 | Thu 11/10/18 |
| 4 | | 📌 | Identify the sources and data that need to use | 5 days | Mon 15/10/18 | Fri 19/10/18 |
| 5 | | 📌 | Meeting with supervisor | 1 day | Thu 18/10/18 | Thu 18/10/18 |
| 6 | | 📌 | Finalize the sources and data that need to use | 5 days | Fri 19/10/18 | Thu 25/10/18 |
| 7 | | 📌 | Meeting with supervisor | 1 day | Thu 25/10/18 | Thu 25/10/18 |
| 8 | | 📌 | Collection of methods that are available | 7 days | Fri 26/10/18 | Mon 5/11/18 |
| 9 | | 📌 | Meeting with supervisor | 1 day | Fri 2/11/18 | Fri 2/11/18 |
| 10 | | 📌 | Comparing the methods that has been chosen | 7 days | Fri 2/11/18 | Mon 12/11/18 |
| 11 | | 📌 | Meeting with supervisor | 1 day | Thu 8/11/18 | Thu 8/11/18 |
| 12 | | 📌 | Choosing the final 3 methods to be included inside the report | 6 days | Thu 8/11/18 | Thu 15/11/18 |
| 13 | | 📌 | Meeting with supervisor | 1 day | Fri 16/11/18 | Fri 16/11/18 |
| 14 | | 📌 | Searching the algorithm for the proposed method | 5 days | Sun 18/11/18 | Thu 22/11/18 |
| 15 | | 📌 | Submission of the proposal report for the study of digital watermarking | 1 day | Tue 4/12/18 | Tue 4/12/18 |
| 16 | | 📌 | Implement and test the algorithm that proposed | 5 days | Mon 21/1/19 | Fri 25/1/19 |
| 17 | | 📌 | Meeting with supervisor | 1 day | Wed 30/1/19 | Wed 30/1/19 |

Project: PSM1.mpp
Date: Fri 3/5/19

| | | | | | |
|---|---|---|---|---|---|
| Task | ▬ | Inactive Summary | ▬ | External Tasks | ▬ |
| Split | ┆┆┆┆ | Manual Task | ▬ | External Milestone | ◇ |
| Milestone | ◆ | Duration-only | ▬ | Deadline | ⬇ |
| Summary | ▬ | Manual Summary Rollup | ▬ | Progress | ▬ |
| Project Summary | ▬ | Manual Summary | ▬ | Manual Progress | ▬ |
| Inactive Task | ▭ | Start-only | [ | | |
| Inactive Milestone | ◇ | Finish-only | ] | | |

Page 1



| ID | Task Mode | Task Name | Duration | Start | Finish |
|---|---|---|---|---|---|
| 18 | | Maintenance of the algorithm | 5 days | Thu 31/1/19 | Wed 6/2/19 |
| 19 | | Finding the data for data testing | 7 days | Thu 7/2/19 | Fri 15/2/19 |
| 20 | | Finalize the data to test with the selected method | 14 days | Sat 16/2/19 | Wed 6/3/19 |
| 21 | | Testing the data with the selected method | 20 days | Thu 7/3/19 | Wed 3/4/19 |
| 22 | | Data analysis | 15 days | Thu 4/4/19 | Wed 24/4/19 |
| 23 | | Submission of the final report | 6 days | Thu 25/4/19 | Thu 2/5/19 |

Project: PSM1.mpp
Date: Fri 3/5/19

| | | | | | |
|---|---|---|---|---|---|
| Task | ▬ | Inactive Summary | ▭ | External Tasks | ▬ |
| Split | ┈ | Manual Task | ▬ | External Milestone | ◇ |
| Milestone | ◆ | Duration-only | ▬ | Deadline | ⬇ |
| Summary | ┌┐ | Manual Summary Rollup | ▬ | Progress | ─ |
| Project Summary | ┌┐ | Manual Summary | ┌┐ | Manual Progress | ─ |
| Inactive Task | ▭ | Start-only | [ | | |
| Inactive Milestone | ◇ | Finish-only | ] | | |

Page 2