RECOVERY AND TAMPER LOCALIZATION FOR REVERSIBLE IRIS IMAGE WATERMARKING SCHEME USING HASH FUNCTION

MUHAMMAD ALIF AIMAN BIN ABD SAMAD

Bachelor of Computer Science (Software Engineering) with Honors

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author’s Full Name : MUHAMMAD ALIF AIMAN BIN ABD SAMAD

Date of Birth

Title : RECOVERY AND TAMPER LOCALIZATION FOR REVERSIBLE IRIS IMAGE WATERMARKING SCHEME USING HASH FUNCTION

Academic Session : SEM 2 2022/2023

I declare that this thesis is classified as:

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

____
New IC/Passport Number:
Date: 2/7/2023

____
Name of Supervisor:
Ts. Dr. Liew Siau Chuin
Date: 2/7/2023

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

UMP Universiti Malaysia PAHANG
Engineering • Technology • Creativity

SUPERVISOR'S DECLARATION

I/We* hereby declare that I/We* have checked this thesis/project* and in my/our* opinion, this thesis/project* is adequate in terms of scope and quality for the award of the degree of *Doctor of Philosophy/ Master of Engineering/ Master of Science in …………………………..

____

(Supervisor's Signature)

Full Name	:	Ts. Dr. Liew Siau Chuin
Position	:	SENIOR LECTURER FACULTY OF COMPUTING COLLEGE OF COMPUTING & APPLIED SCIENCE UNIVERSITI MALAYSIA PAHANG 26600 PEKAN, PAHANG DARUL MAKMUR TEL : 09-424 4645 FAX : 09-424 4666
Date	:	28/07/2023

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 : MUHAMMAD ALIF AIMAN BIN ABD SAMAD

ID Number : CB20165

Date : 2 July 2023

RECOVERY AND TAMPER LOCALIZATION FOR REVERSIBLE IRIS IMAGE WATERMARKING SCHEME USING HASH FUNCTION

MUHAMMAD ALIF AIMAN BIN ABD SAMAD

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Doctor of Philosophy/Master of Science/Master of Engineering

Faculty of Electrical & Electronics Engineering

UNIVERSITI MALAYSIA PAHANG

JULY 2023

ACKNOWLEDGEMENTS

First and foremost, I'd like to start by expressing my gratitude to Dr. Liew Siau Chuin, my renowned and helpful final year project supervisor, for his invaluable guidance, supervision, and ideas during the course of my PSM Final Year Project course. I also want to thank Miss Azlina Binti Zainuddin, my academic adviser, for giving me advice and support throughout my bachelor's degree despite the numerous challenges I encountered.

Furthermore, I also want to express my gratitude to the Faculty of Computing for giving me the chance to enroll in the prestigious Bachelor of Computer Science (Software Engineering) with Honours program. I also want to thank my friends, classmates, and former professors for a memorable university experience, whether it was in the classroom, lab, or other types of social situations on campus.

Last but not least, I want to express my appreciation to my family and friends who helped me out in the background by giving me unending support and morale during my bachelor's degree. Without all of them, I will not be able to complete the project. Their supports and guides mean a lot to me that I cherish them.

ABSTRAK

Watermarking digital adalah teknik untuk menanam maklumat pengenalan, seperti logo atau teks, ke dalam fail media digital, seperti imej, audio, atau video. Watermark biasanya halus dan mungkin tidak kelihatan dengan mata kasar, tetapi ia boleh digunakan untuk mengenal pasti pemilik atau pencipta kandungan tersebut, atau untuk menjejaki penyebarannya. Watermarking digital boleh digunakan untuk pelbagai tujuan, termasuk perlindungan hak cipta, pengenalan kandungan, dan penjejakan penyebaran media digital. Tamper dan penipuan adalah agak biasa terutamanya apabila ia berkaitan dengan imej digital. Tamper imej digital boleh mempengaruhi aspek keselamatan yang mengesahkan imej yang telah diubahsuai sebagai sah yang boleh menyebabkan kerugian atau data dicuri. Oleh itu, adalah penting untuk melindungi hak kekayaan intelek dan memastikan bahawa kandungan digital digunakan dengan sesuai. Jadi, kertas ini akan mencadangkan kaedah yang boleh diterapkan untuk meningkatkan imej digital untuk mengelakkan sebarang penipuan dan meningkatkan keselamatan.

ABSTRACT

Digital watermarking is a technique for embedding identifying information, such as a logo or text, into a digital media file, such as an image, audio, or video. The watermark is usually subtle and may be invisible to the naked eye, but it can be used to identify the owner or creator of the content, or to track its distribution. Digital watermarking can be used for a variety of purposes, including copyright protection, content identification, and tracking the distribution of digital media. Tamper and counterfeits are quite common especially when it comes to the digital image. The tamper of the digital image can affect the security aspect in which it authenticates the image that has been tampered as legitimate which can cause damage or data stolen. That is why, it is important to protect intellectual property and ensuring that digital content is used appropriately. Thus, this paper will propose the method that can be applied to enhance the digital images to prevent any counterfeit and improve the security.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

dB	Decibel
PSNR	Peak Signal-to-Noise Ratio
MSE	Mean Squared Error
.bmp	Device Independent Bitmap

LIST OF ABBREVIATIONS

PSM	Project Sarjana Muda
FYP	Final Year Project
ROI	Region of Interest
RONI	Region of Non-Interest
MATLAB	Matrix Laboratory
LSB	Least Significant Bit
MSB	Most Significant Bit
SHA	Secure Hash Algorithm
DE	Difference Expansion
DFRNT	Discrete Fractional Random Transform
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
DICOM	Digital Imaging and Communications in Medicine
MR	Magnetic Resonance

CHAPTER 1

INTRODUCTION

1.1 Introduction

The evolution and the rapid growth of current science and technology accommodate people around the world the convenience and much better life. At the same time, the needs to have security for protection and safety is crucial and vital. With the emergence of new technologies of information and communication, other systems have been developed such as pass codes, passwords and smart cards (Alvarez-Betancourt & Garcia-Silvente, 2014). Most of the current security nowadays relies on a security technology that has been invented and developed in recent years which is called biometric technologies in order to secure user's confidentiality and sensitive information. Over the past decades, the technology has been widely used in countless of applications, such as in a registration part of a system, attendance system and so on. Biometric technologies aids in identifying the specific personal characteristics and biophysical features of a person (Isa, Aljareh, & Yusoff, 2017). This technology has been deemed to be reliable for the security aspect up until now.

Biometrics security as of now have several types which are commonly used in security aspect. They are the voice recognition, fingerprint scanning, facial recognition, iris recognition and hear-rate sensors. These biometrics are actively used nowadays as it can provide security benefits, and it is strenuous to faked them compared to those traditional security system since they used special or unique biophysical traits of an individual. It is also used for authentication to identify a person's authorization to gain access. Iris recognition is one of a good example that can be used for both security and authentication in a system. Iris recognition is a strong biometric which has a high accuracy and fast. An individual's iris is different between both left and right eye which therefore can perform a separate recognition later on.

With the help current technology, iris recognition can be done by using a specialised digital camera. The camera will take the person's iris with the features that the camera has which are the visible and near-infrared light for a clearer picture. It will detect and identify the person's pupil, eyelids, eyelashes and so on. Then, it will divide them into blocks and converts into feature value to quantify the image. Matching process will be performed with the one that has been previously extracted for authentication and verification. Iris of a person remains unchanged despite the ageing process (Alvarez-Betancourt & Garcia-Silvente, 2014) is one of the characteristics which makes the iris recognition became more popular.

1.2 Background of the Problem

Although the biometric techniques, iris recognition supplies an effective way to identify a person’s iris feature, it still has its flaws and imperfections. This can be demonstrated by altering the initial or first image produced by the matcher from the subsequent iris image. At each phase, the manipulated iris images are combined with the current candidate's iris image created from public iris databases. The altered iris image that was input when a new candidate image was submitted will result in the highest matching score. A high matching points can be achieved which results in the successful authentication with several iterations to an altered iris image. Even with specific characteristics of iris of an individual, the iris recognition system is still vulnerable to malicious attacks. The malicious act can be done easily along with the pace of rapid evolution of technologies of computers and networks nowadays.

Furthermore, attacks may occur during the process of sender and receiver of the data. The attackers may interrupt and destroy the image at the moment when the biometric attributes are extracted by the scanner and transfer it to the component extraction module for extra devising. The channel for the transmission is vulnerable and there is no security from attacks such as brute force, eavesdropping attacks and replay attacks. If the captured iris image is destroyed by the attackers during the process of transmission, it will lead to the receiver to receive the tampered iris image. Attackers will always try to steal and get the confidential information of a targeted individuals or organization for crime motive and selfish purpose. Therefore, an action to counter or secure the biometric technology must be taken so that the security of the technology is reliable.

In this project, watermarking scheme on the iris image will be introduced to secure and shields the images of the iris data in the biometric technology. Samples of iris image will be obtained from the browser or internet with the chosen pixel sizes. The watermark is embedded or planted into the image in order to protect the person’s iris image from tampered. This project proposed the tampered detection in an image for the purpose of able to detect the exact location or area that has been altered in the image. Process of the embedment of the watermark in the iris image to fulfil with the authentication and security motive will be carried out. Furthermore, the embedment of watermarking process in this proposed scheme will use reversible watermarking technology to allow recovery and also provides tampered localization with the utilization of the Region of Interest (ROI) and Region of non-Interest (RONI).

1.3 Objective

This project consists of three objectives which involves:

1) To study the current watermarking scheme for iris images.

2) To develop a recovery and tamper localization watermarking scheme for iris images.

3) To evaluate the recovery and tamper localization watermarking scheme for the iris images.

1.4 Scope

Target User :

Authorities or the governments which uses the retinal authentication for security matters especially for the border controls and law enforcement. This retinal recognition will be used to identify passengers or travellers and grants them access to pass through. It can also be used for the crime investigation where biometrics image such as iris is required to allows better accurate identification of a personal.

Image Type : Grayscale Iris Image (8-Bit, 320 x 240 pixels)

Measurement: PSNR and MSE

Software :

- MATLAB
- Microsoft Office Word

1.5 Report Organization

Chapter 1 describes and explains the introduction of the drawbacks in digital iris security related issues. Several issues are mentioned to further explain the flaws that this technology may encounters under the background of the problem topic. This chapter also introduces the implementation of the watermarking scheme into the iris image which it can be used as an alternating method for improving the security in the biometric technologies. Then, three objectives of this project are listed including the scope with a brief explanation is given.

Chapter 2 is all about the literature reviews of this project and the previous watermarking paper works. It involves reversible watermarking schemes and also the tamper localization along with the recovery schemes for the iris image. The three chosen existing studies will be compared and explained briefly in this chapter.

Chapter 3 explains about the methodology of the thesis. In this chapter, the project proposes a solution which are the reversible tamper localization and recovery scheme for the iris image. An experiment is conducted with few samples to receive the results.

Chapter 4 discusses and talks about the results, or the outcome obtained from the experiments along with their evaluation of the proposed schemes. A table of the results is prepared to show the comparison of each sample's outcomes to give a clear view and understanding with a brief explanation,

Chapter 5 is the section where conclusions of the thesis or projects is discussed. The objectives of the project are recalled and revisited once again in this chapter. Furthermore, some other details such as the limitations of the proposed schemes and suggestions for the work for the research of this project will be discussed also.

CHAPTER 2

LITERATURE REVIEW

2.1 Introductions

In this chapter, which is chapter 2, previous related work and studies of the methods or techniques used will be discussed. These related studies will be explained briefly with some explanations and details of the techniques that the researchers have used in the research side by side. These works will be used as a reference to conduct this project’s proposed work.

2.2 Domain

In watermarking, there are numbers of way to do the watermarking embedment which are the spatial domain and transform domain. One of the simple and most direct technique would be the spatial domain technique that will be used in this research.

2.2.1 Spatial Domain

Spatial domain for watermarking uses the image as in the form of pixels. It is easily to apply into any kind of image. It embeds the information of the watermark information directly in to the pixel by manipulating the intensity and the colour of value of the certain selected pixels according to (Chitra & Prasanna Venkatesan, 2016). In Spatial domain, the simplest technique would be the usage of the algorithm method which is called as the Least Significant Bits (LSBs).

2.2.2 Transform Domain

Transform domain watermarking is a method of embedding a digital watermark into a multimedia file by transforming the content of the file from one domain (such as the spatial domain or the frequency domain) into another domain using a mathematical transformation, and then embedding the watermark in the transformed representation. The watermarked file can then be transformed back into the original domain for use. This type of watermarking is often used to protect the copyright of digital media by providing a way to trace the source of an unauthorized copy. The watermark is typically embedded in a way that is difficult to remove or tamper with without damaging the quality of the media.

2.2.2.1 Frequency Domain

Frequency domain watermarking is a type of transform domain watermarking in which the multimedia content is transformed from the spatial domain (in which it is represented as a grid of pixels) into the frequency domain (in which it is represented as a set of sinusoidal waves) using a mathematical transformation such as the Fourier transform. The watermark is then embedded in the frequency domain representation by modifying the coefficients of the sinusoidal waves. To retrieve the watermark, the content is transformed back into the spatial domain using the inverse Fourier transform.

2.2.2.2 Discrete Cosine Transform (DCT) & Discrete Wavelet Transform (DWT)

Discrete wavelets transform (DWT) and discrete cosine transform (DCT) are two mathematical transformations that are commonly used to convert images or signals from the spatial domain to the frequency domain. Both have good energy compaction properties and are used in image and signal processing, but they have some key differences that make them more suitable for different applications.

DWT represents an image or signal as a set of wavelets, which are basis functions that can be used to represent the signal or image. This allows it to provide a time-frequency representation of a signal or image, enabling it to identify features in both time and frequency. This makes it more versatile and useful for image and signal analysis, as well as transform domain watermarking. Additionally, DWT often produces sparse coefficients, which can be useful for certain types of signal processing and analysis.

On the other hand, DCT represents a signal or image as a sum of sinusoidal waves with different frequencies. This provides only a frequency representation, which means it can only identify frequency features. However, DCT is faster to compute and has better energy compaction properties, making it more suitable for image and signal compression. Furthermore, DCT is not providing multi-resolution representation, which can be a drawback in some cases.

2.3 Least Significant Bits (LSBs)

LSB is one of the watermarking techniques which is simple and direct. This will make a use of the smallest bits there is in a binary sequence. According to (Gaur & Manglani, 2015), LSB is referred as the right-most bit in which due to the convention in positional notation of writing less significant. It is much easier to understand simple to implement. This method works by selecting a specific number of LSBs of the pixel values in the image and replacing them with the watermark data. The LSBs are chosen because they are less perceptible to the human eye, making the watermark less visible and therefore less likely to be detected. Additionally, the LSBs are less sensitive to image processing operations such as cropping, rotation, and compression, making the watermark more robust.

2.4 Region of Interest (ROI) and Region of Non-Interest (RONI)

ROI and RONI are used in many areas for different purpose such as in the image. Both of the regions have their own role and functions to be used. A good example can be seen in a medical image according to (Khor, Liew, & Zain, 2017), that there will be two region which are called as the ROI and RONI. ROI is where the data is protected since it is significant on the diagnosis purpose, while RONI is the region where watermarks are embedded as it poses no significance. The ROI information will be stored into the RONI's LSB as watermark which later can be retrieved and extracted for checking its authentication and recovery.

2.5 Hash Function

Any key or string of characters can be converted into another value through hashing. The original string is often represented with a shorter, fixed-length value or key that makes it simpler to retrieve or use. A hash value, also known as a hash, is created by a hash function and is based on a mathematical hashing algorithm. A good hash always uses a one-way hashing technique to avoid the conversion of the hash back into the original key. Secure Hash Algorithm 2 (SHA-2) is one example of a hash function that includes 6 different hash function subtypes. One of the SHA-2 subcategories is SHA-512. It generates a fixed size 512-bit (64-byte) hash and is a one-way function. It is one of the strongest hash algorithms at the moment and shares a lot of structural similarities with SHA-1. Better security features make it less vulnerable to attacks.

2.6 Previous Works

According to (Zhou, Hou, Wen, & Zou, 2018), who proposed a digital watermarking scheme which can help in enhancing security of the database of images. With the concept of Transform Domain technique, the researchers proposed a technique which based on the Discrete Fractional Random Transform (DFRNT) that introduced by the combinations of the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and chaotic map (mathematical functions used to generate random sequences). DFRNT is a very effective tool for encrypting and decrypting digital images with a very fast processing time due to its inherent randomness characteristics. They took the advantage of these techniques to create a stronger security of the watermark. While the DWT with spatial frequency localization features might increase the watermark scheme's resilience, the DCT with energy-compression characteristics may provide high-performance watermarks. Watermark image is scrambled by Arnold transform which used as a scrambling step in which the number of iterations is used as a key and logistic map which is a chaotic algorithm that produce chaotic sequences. The Arnold transform is used to first scramble the watermark, and the Logistic map is used to jumble the watermark's row and column. In addition, the two-dimensional DCT produces four sub-band pictures from the host image. The low frequency sub-band images are divided into 8 × 8 small matrices, and a coefficient matrix is produced by performing the DCT on each matrix. The intermediate frequency coefficients build an intermediate matrix that is the same size as the watermark picture. The scrambled watermark is then integrated into the DFRNT domain after performing the DFRNT on the intermediate frequency coefficient matrix. According to simulation results, the suggested robust and undetectable system provides good undetectability and resistance to various image processing attacks.

As for the (Qasim, Aspin, Meziane, & Hogg, 2019), they had proposed a blind, fragile watermarking method in which the scheme also provide capability of reversibility for the Digital Imaging and Communications in Medicine (DICOM). The image segmented into two parts which are the ROI and RONI. ROI in medical images is the significant for diagnosis purpose one while RONI is the non-critical part. The scheme used ROI to hide and encode the watermark of the brain Magnetic Resonance (MR) images. Reversible watermarking based on the Difference Expansion (DE) which is a reversible data hiding method is used to encode watermark data into the ROI. When compared to other images, the majority of medical images have a sizable smooth area, which is defined as areas with little perceptible variation in the intensity values of adjacent pixels. The human eye is less likely to notice the watermark if it is incorporated into these areas. Therefore, it is embedded into the smooth region of the ROI. The proposed method can produce a watermarked image with minimal degradation for a reasonable and controllable embedding capacity, according to experimental results, despite being fully reversible. The proposed method is ideal for smaller ROI.

Besides that, (Gul & Ozturk, 2019) proposed about the usage of the Secure Hash Algorithm for the image watermarking. During the embedding procedure, the ROI is assigned a SHA-256 hash code. With the usage of the SHA-256, a novel block-based technique for embedding fragile watermarks and detecting tampering is suggested. The host picture is segmented into 32 x 32 non-overlapping parts during the watermark embedding step. The next step is to split each 32 x 32 block into four 16 x 16 non-overlapping subblocks. Using the SHA-256 hash algorithm, the whole hash value of the first three subblocks is produced as a watermark. The fourth sub-block's least significant bits (LSBs) contain the generated 256-bit binary watermark, which is then used to create a watermarked image. In the tamper detection step, the extracted watermark from the fourth sub-block of the watermarked image was compared with the hash value derived from the three sub-blocks to identify tampered blocks. Results from experiments show that the suggested technique successfully acquired watermarked images with good visual quality and recognised all tampered parts.

2.7 Comparative Analysis

Table 1: Comparison Analysis of Previous Works

Watermarking Methods	(Zhou et al., 2018)	(Qasim et al., 2019)	(Gul & Ozturk, 2019)
Methods description	- Use multiple Transform Domains based on DFRNT - Use the Transform Domain technique which are the combination of DCT, DWT, with chaotic map to improve robustness - Use Arnold transform and logistic map to improve the security of watermark that has been embedded - Extraction involves the inverse process of the watermark embedding used	- Implement the fragile watermarking scheme - Can be used for both spatial domain and transform domain - Provide the ability of image reversibility based on DE technique - Segment image into ROI and RONI - Embed the watermark in the smooth area of ROI - The higher the size of the ROI the higher the hiding capacity and distortion level. - The exact original images are retrieved after extracting the embedded watermark - Ideal for images with smaller ROI	- Proposed fragile image watermarking - Using Spatial Domain - Use SHA-256 hash functions - Divide images into 32 x 32 non-overlapped and then each of them into four 16 x 16 non-overlapped sub-blocks - Generate the hash value of the three sub-blocks as watermark - The 256-bit binary watermark embedded into LSB of the fourth sub-block to get watermarked image - Compare the hash value form the

			three sub-blocks with the extracted watermark to detect tampered blocks
Image used	Grayscale Baboon Image (512 x 512)	Grayscale Medical Image (512 x 512)	Grayscale Lena, Boat, Man and Lake Image (512 x 512)
Bits used	8 bits	8 bits	8 bits
PSNR value of watermarked image (dB)	40.9919 dB	91.18 ~ 99.94 dB (Depends on samples)	57.156 ~ 57.172 dB (Depends on samples)

2.8 Chapter Summary

In short, these three related works have been discussed in further details which shows that they have their own proposed way to solve or conduct an experiment. Some proposed a method to solve or to test an experiment based on samples or scope they have chosen, while others to improve or expand the research work that had been done before. Results were recorded to show the after effect of the experiment. PSNR value were used to check the quality of the image after embedment. From there, conclusion can be made whether the method that these researchers proposed is suitable or not. With these research works; they can be used as a reference and guidance for this project’s proposed scheme with the usage of iris image for enhancing the security.

CHAPTER 3

METHODOLOGY

3.1 Introduction

This chapter will discuss about the methodology of the proposed watermarking scheme which involve several steps and processes to achieve and get the output. Furthermore, the tools that will be used, and the attributes of the chosen samples will be explained too. Diagrams will be prepared to provide better understanding.

3.2 Research Framework

In an experiment, frameworks and the procedure structure are important to ensure it flows as planned. The first thing in a research work is the planning which is the selection of topic that a researcher wanted to immerse. By referring to the other thesis or research work that is related to the chosen subject, one can get an idea of what they can do to propose or to improve previous work. With proper understanding, one can propose a method on how to conduct the experiment. After constructing the method, data collection or samples retrieval to test the experiment is a must in order to get the results. One can interview to get more data, get previous works data results and to identify the tools needed to analyse and conduct the experiment. Once results are retrieved, conclusion can be made. Thus, same goes with this research, this section will explain about the tools or platform that will be used, type of samples or its domain and overall flow of the scheme as a guideline.

3.2.1 Tool (MATLAB)

Figure 1: MATLAB

For the process and to conduct the scheme, a tool called MATLAB will be used. MATLAB is a programming platform created especially for engineers and scientists to research, develop, and build products and systems that change the world. The MATLAB language, a matrix-based language that enables the most natural representation of computer mathematics, is the core of MATLAB. This software allows user to analyse data, develop algorithms and also create models which is the perfect choice to conduct the proposed watermarking scheme. The language used in MATLAB is called MATLAB language, which is a high-level programming language that is similar to C and C++. It is designed for numerical computing and is particularly well-suited for matrix and vector operations, which are commonly used in signal processing and image processing.

3.2.2 Samples (Iris Image Dataset)

In order to conduct the scheme, samples to test and experiment are required. This scheme will be using ten samples of iris image with the pixel of 320 x 240. These iris images dataset was collected from the iris database (MultiMedia University) on Kaggle website. The images are in .bmp format. Only the right eye will be selected from the database The samples will undergo an embedding of watermarking process. The thre example of chosen samples are as shown in Figures below.

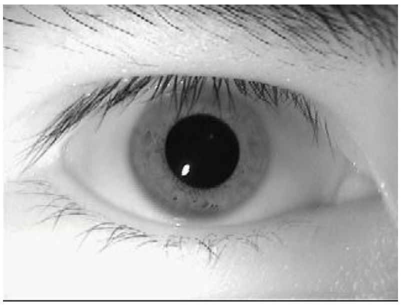


Figure 3: Sample 1

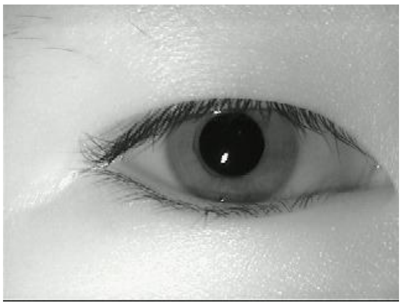


Figure 2: Sample 2

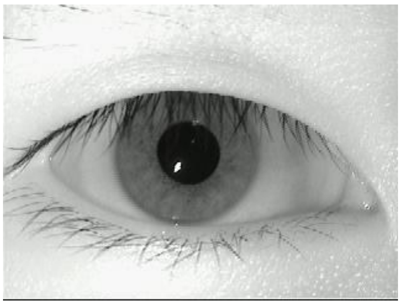


Figure 4: Sample 3

These iris image sample will undergo the same process which will be the image preparation, watermark embedding, tamper localization and recovery. The results such as the PSNR and dB will be recorded to be evaluated.

3.2.3 Methodology Overall Flow

To conduct the scheme, steps or process are proposed to ensure that proper results can be achieved. Below Figure is the overall process for the proposed scheme which covers from image preparation, watermark embedding, tampered localization, to the recovery of the iris image. Further in-depth details will be discussed in the next subtopic.

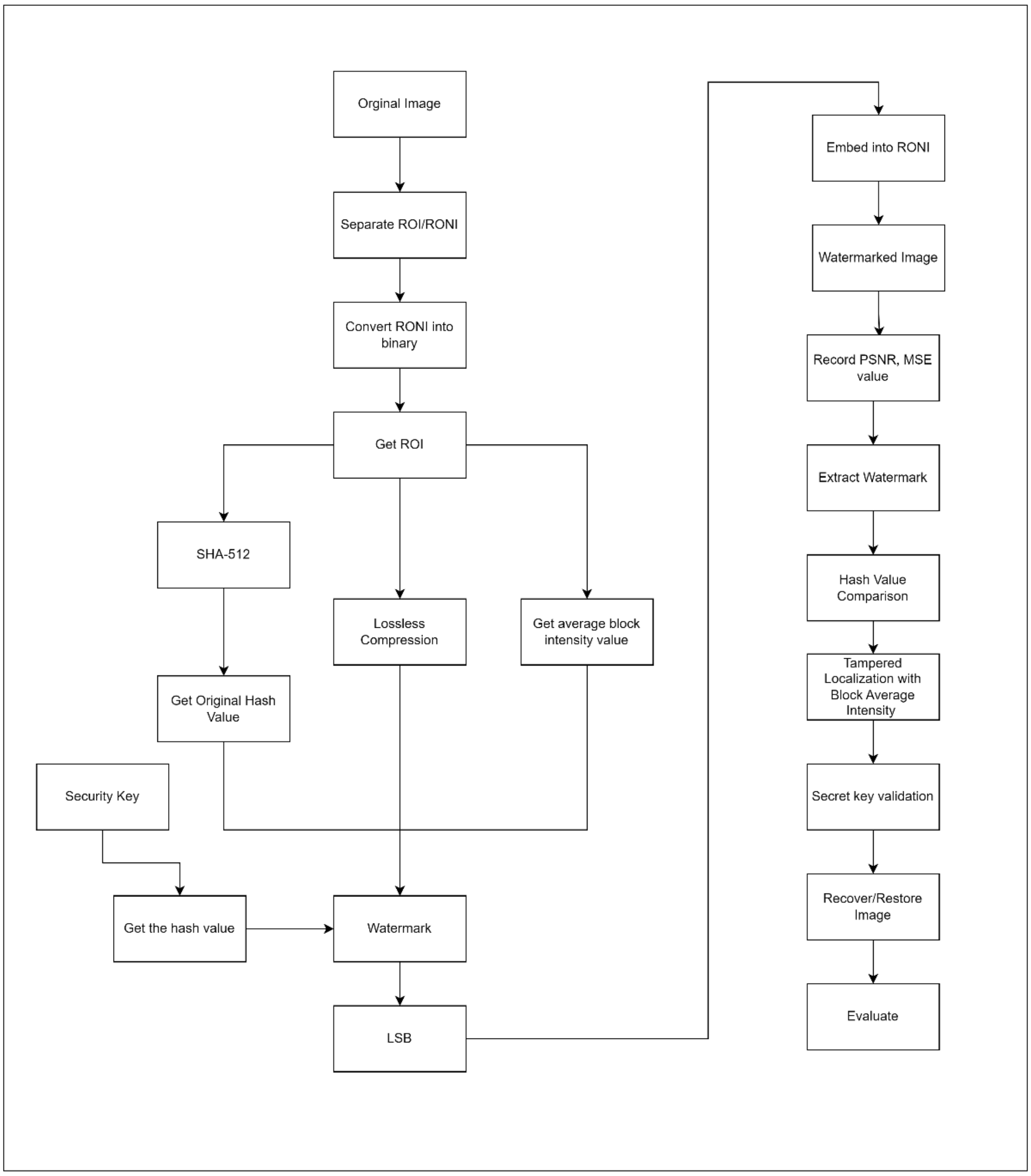


Figure 5: Overall Flow Scheme

3.3 Research Requirement

In this scheme, a procedure, or the steps will be discussed and explained even further to fulfil the research requirement. Diagrams may be provided for clearer explanation. The proposed scheme will cover several phases. Each phase will have their own procedure. The phases involve are the image preparation, watermarking embedding, extraction, tamper localization, and image recovery.

3.3.1 Hardware Requirement

Laptop

- Asus VivoBook A542U
- Intel® CoreTM i5-8250U CPU @ 3.4 GHz
- 12GB RAM memory
- 1TB HDD
- 128GB SDD

3.3.2 Proposed Method

3.3.2.1 Image Preparation

The collected samples are used to embed the watermark. As discussed, the samples of each iris image are 320 x 240 pixels. First and foremost, the images will be divided into two separate region which are the ROI and the RONI with the labels ROIA, RONIA, RONIB, RONIC, and RONID. The ROI region of the samples will cover the important or the significant area which is in this case is the iris part. Figure below shows the ROI and RONI segments of the iris image with the rectangle at the centre as the ROI and the eight rectangles around it are the RONI.

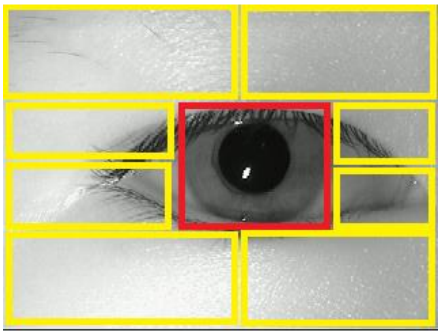


Figure 6: ROI/RONI Segments in Sample

The ROI segments has a size of 106 x 85 pixels. The total of final bits required to be embedded is based on the effectiveness of the compression method applied. The image ROI will further divide into 4 x 4 sectors which are non-overlapping blocks of 16 sectors with the size of 70 x 55 pixels. Use the SHA-512 to get the hash value in hexadecimal of the ROI of the original iris image and named it as HASH1_A. Then, the ROI will undergo lossless compression and named as SAMPLE1_A to prevent degradation of the image and reduce payload.

3.3.3 Embedding Watermark

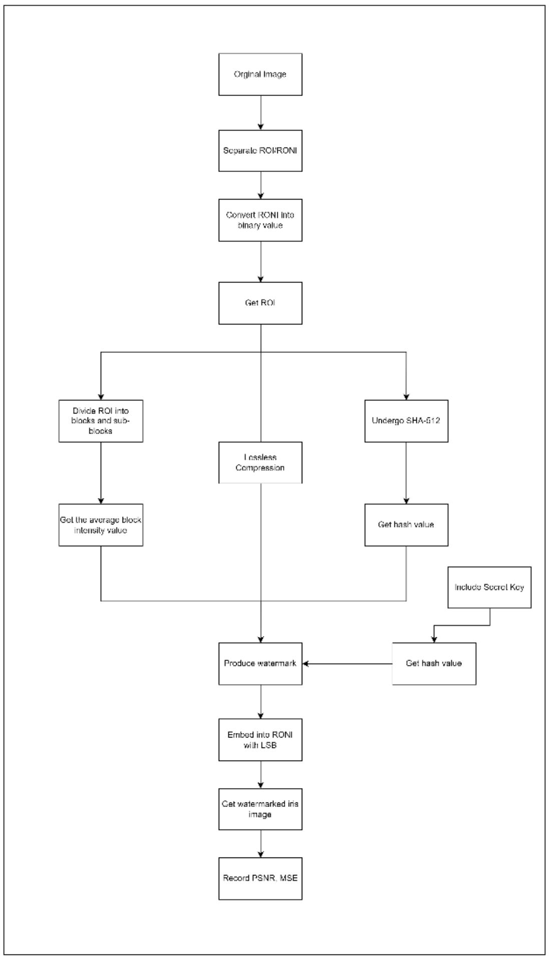


Figure 7: Watermark embedding process

After separating ROI and RONI, will be converted into binary. To further increase the storage, the watermark will be embedded in the two least significant bits of each pixel of the RONI. This is to achieve lower distortion level of the watermarked iris image which also means the watermark embedment does not reduce the quality of the image while maintaining the data. The bits in the watermarked value were changed one at a time, starting with the least significant bit and moving up to the next least significant bit, all before the second pixel value. Figure below shows example of the flow of replacing the watermark value into the LSB of the RONI section.

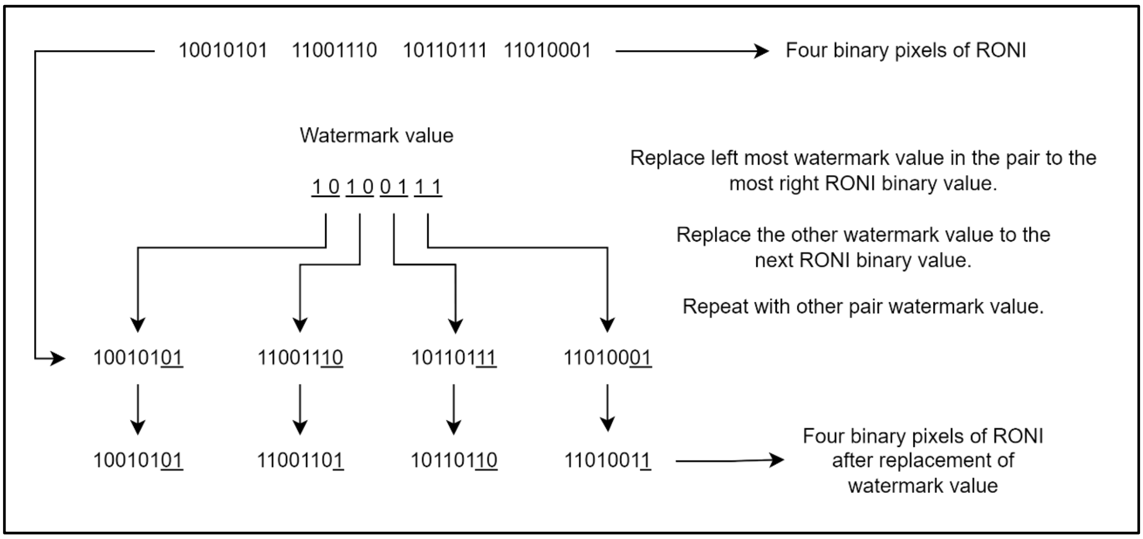

10010101 11001110 10110111 11010001
Four binary pixels of RONI
Watermark value
1 0 1 0 0 1 1 1
Replace left most watermark value in the pair to the most right RONI binary value.
Replace the other watermark value to the next RONI binary value.
Repeat with other pair watermark value.
10010101 11001110 10110111 11010001
10010101 11001101 10110110 11010011
Four binary pixels of RONI after replacement of watermark value

Figure 8: Demonstration of LSB Implementation

With the LSB method, watermark that contains the hash value of the ROI, the original ROI of the iris that has been compressed previously, and authentication information or the average block intensity of the original iris image which will be explained even further in the next phase of how to compute or retrieve, including a secret key for better security are used to further improve the security aspect which led to successfully produced watermarked iris image will also be included in the watermark with its hash value. The PSNR and MSE is recorded including the update of the RONI size used to embed the watermark.

3.3.4 Watermark Extraction and Tamper Localization

To detect if there is any tamper, the watermark is then extracted to retrieve the data stored in RONI. This time, the iris image is still segmented into ROI and RONI. The original ROI, the original hash function and authentication information is retrieved and will be used to compared. The current iris image will undergo the same hash function SHA-512 to produce hash value that is named as HASH1_B. To check the iris image validity, the extracted HASH1_A from RONI will be compared with the current generated hash value which is the HASH1_B. If the hash value is equal, the current iris image is valid. Otherwise, the iris image is invalid and indicates the iris image has been tampered since its hash values are not matched. The validity of the iris image may be identified, but the tamper localization has yet to discover if its tampered. Therefore, to know where the area of the tamper is, the usage of the average block intensity comes in handy.

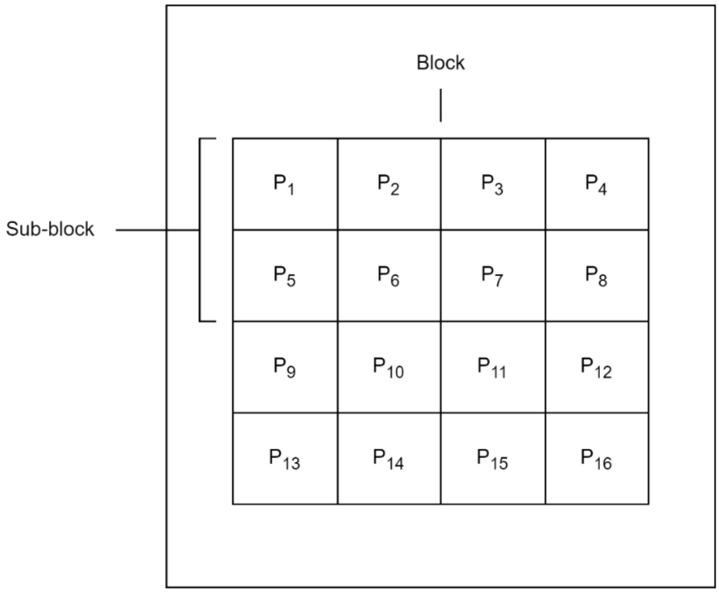
Average block intensity method developed by (Liew & Zain, 2011) is used to conduct this experiment. This method divides and separates the iris image into blocks or sectors and is further divided into sub-blocks. The average intensity of the divided blocks including the sub-block's average intensity will be used to detect tamper localization. The formula can be defined as below.

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

P_1 to P_{16} in the formula refers to the intensity of the pixels in a block.

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

P_1, P_2, P_5, P_6, in the formula refers to the intensity of the pixels in a sub-block.



P_1	P_2	P_3	P_4
P_5	P_6	P_7	P_8
P_9	P_{10}	P_{11}	P_{12}
P_{13}	P_{14}	P_{15}	P_{16}

Figure 9: Division of block into four sub-blocks

There will be two bits for each block which are one bit for the authentication bit and one bit for the parity check bit as the authentication information. The block's average intensity will be denoted as the b1 and b1s for its sub-blocks are calculated and then denoted as average_b1 and average_b1s respectively. For example, as shown in Figure below, which shows the average_b1 with value 86 and its sub-blocks, average_b1s with the values of 87, 95, 79, and 84 respectively

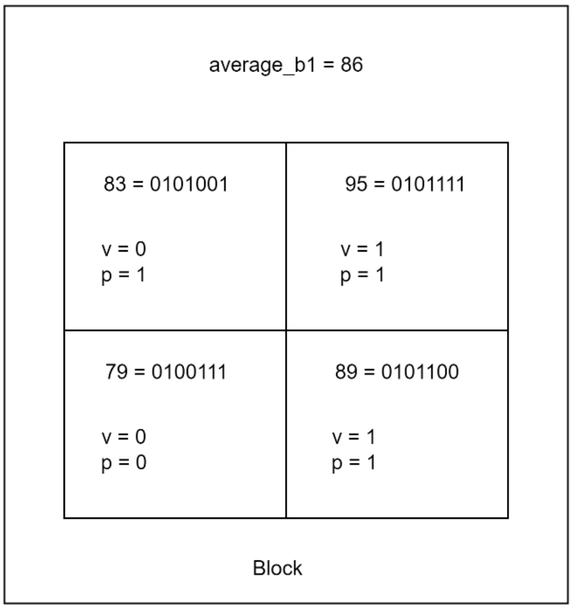


Figure 10: Block b1 that is divided into sub-blocks with its calculated average intensities to get the v and p value

After getting the average_b1 and average_b1s values, the bits for the authentication, v and parity check bit, p of each sub-blocks are generated as below.

a) v = {1: if average_b1s ≥ average_b1} OR {0: Otherwise}

b) p = {1: if number is odd, where number = total of 1s in the 7 most significant bits} OR {0: Otherwise}

The authentication information can be embedded as watermark too for tamper localization. The original authentication information of ROI will be then compared its average block intensity with the current one to detect the area of tamper.

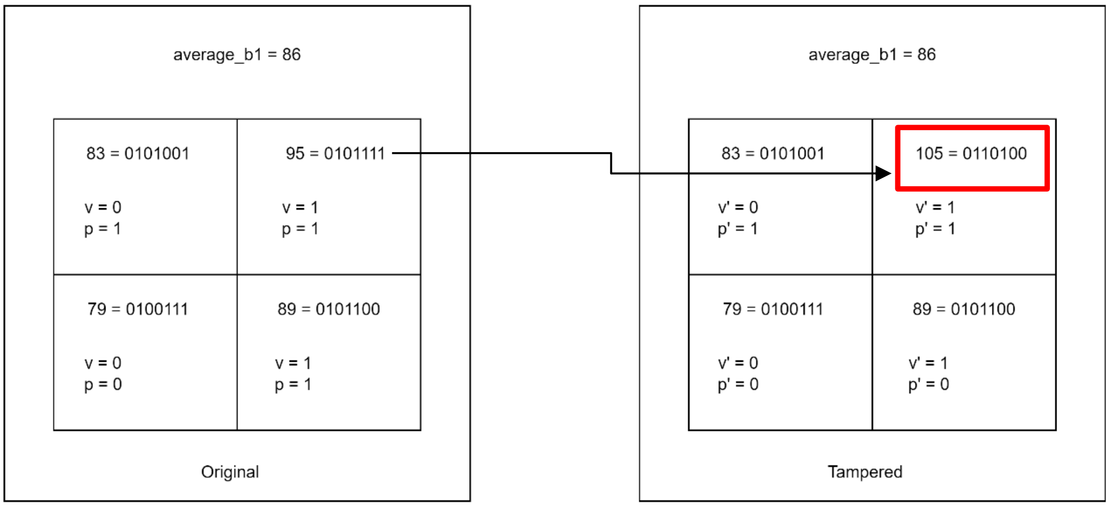


Figure 11: Comparison of the original and tampered

Figure above shows how the comparison, and the tamper localization is done. From the original (left), the average block intensity is shown and compared with the tampered one (right). Each sub-block will have its own value and if its tampered, the value would not be match. The sub-block that is different is the area where it is tampered. For example, as shown in Figure above, the average_b1s are 83, 95, 79 and 89 while tampered one have the average of 83, 105, 79 and 89 respectively. In this case the tampered value of 105 is not equal to the original value of 95 and the area of tampered is found. Therefore, tamper localization using average block intensity is a good approach. Figure below shows the flow of the extraction and tamper localization process.

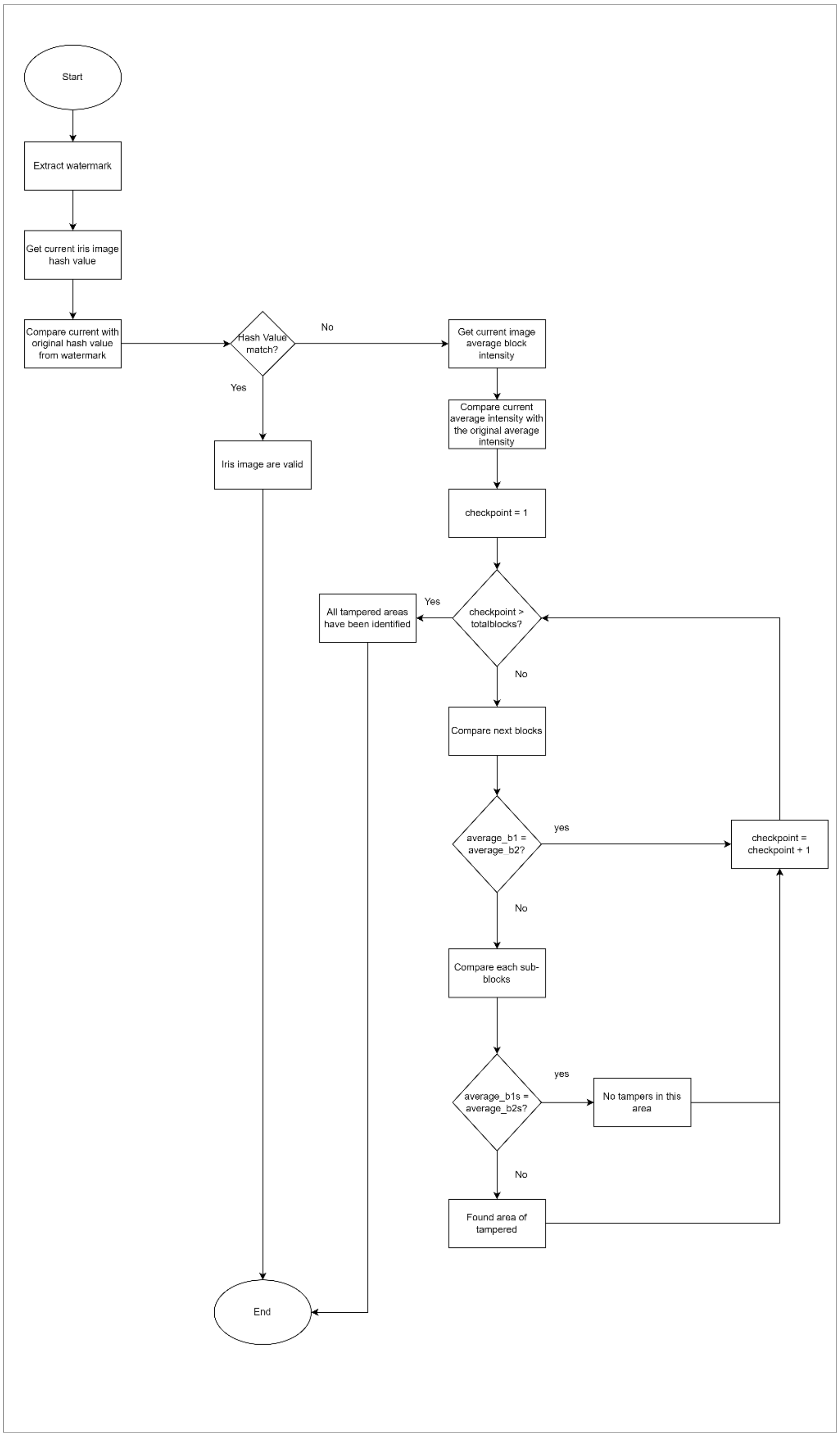

Start
Extract watermark
Get current iris image hash value
Compare current with original hash value from watermark
Hash Value match?
No
Yes
Iris image are valid
Get current image average block intensity
Compare current average intensity with the original average intensity
checkpoint = 1
checkpoint > totalblocks?
Yes
All tampered areas have been identified
No
Compare next blocks
average_b1 = average_b2?
yes
checkpoint = checkpoint + 1
No
Compare each sub-blocks
average_b1s = average_b2s?
yes
No tampers in this area
No
Found area of tampered
End

Figure 12: Extraction and tamper localization procedure

3.3.5 Recovery

After detecting the area where it is tampered will be replaced with the retrieved original ROI pixel value after decompressing. The user must enter the secret key and it will be converted into hash value. The hash value will be then compared with the secret key’s hash value that has been embedded and extracted the watermark. If they are the same, then it will proceed with the recovery, otherwise it will not proceed. By checking each block whether its valid or not, an initial point is updated if invalid. To recover, the process is almost the same with tamper localization using the average block intensity. Each block and its sub-blocks will be checked one by one. The blocks with the difference of average intensity value are the area where it will be recovered. The bits of block of the current tampered iris image will be replaced with the original bits retrieved from the original iris image average block intensity. The process of the recovery will proceed until all blocks checked and the average intensity are equal which indicates that the current iris image has been fully recovered just like the original one.

3.3.6 Evaluation

The watermarked iris image can be measured by their quality level with the usage of means-square error (MSE) and also the PSNR values. This is to know whether any distortion or the aftereffects can be seen or not.

PSNR is the value in which is used to quantify the indistinguishable of the watermarked image. The higher the PSNR value deems that the watermark in the image is difficult to be detected and high invisibility which makes it hard for a human to be able to identify with their naked eyes. Below is the mathematical formula of PSNR (Halawa, Wibowo, & Ernawan, 2019).

$$PSNR = 10 \log \frac{(\max(f))^2}{MSE}$$

The term f refers to the original pixel value. As for the MSE, the distortion can be calculated to quantify it. MSE is a measure of the difference between two images, the original image and the watermarked image. The smaller the MSE value, the closer the two images are to each other, indicating that the watermark has not caused significant degradation to the quality of the original image. Below is the MSE that can be defined as (Isa et al., 2017).

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left(f(i,j) - g(i,j) \right)^2$$

The f(i,j) refers to the original image while the g(i,j) defined the watermarked image with M and N denotes the sized of the image. These values will be recorded for each sample to be evaluated. The results will be compared in a table to see any difference between iris image samples with the elapsed time required to undergo the embedding of the watermark process.

3.4 Potential Use of Proposed Solution

As previously explained, in this current era, technologies are getting advanced with the continuous rapid growth and evolutions. Counterfeits and tampers that occurs within the community or organization with the usage of the technologies is getting to concern as time pass. Data steal and exploitation can happen with these actions which can bring harms to an individual or an organization. This same goes for the image of iris for the biometric authentication, iris recognition. They can intentionally or unintentionally alter and tampers the iris image which makes the security quality questioned.

The malicious intents may be done intentionally to deceive or mislead others. Iris images may be tampered with in order to create a fake identity or to impersonate someone else. Iris image tampering may also be done in an attempt to bypass iris recognition systems, which are used for security purposes in a variety of settings, including airports, government buildings, and financial institutions. Furthermore, Iris image tampering may also be done with malicious intent, such as to harass or defame someone by altering an iris image to make them appear in a negative light. Besides that, in some cases, iris image tampering may occur unintentionally, such as when an iris image is edited or resized, and certain details are lost or distorted as a result.

Regardless of the reason for iris image tampering, it is important to be aware that altered iris images may not accurately represent the original iris, and care should be taken to verify the authenticity of any iris images that are used. That is why, watermarking technique is implemented. The goal of implementing watermarking is to countermeasure these malicious actions and improve the security. Watermarking will be embedded into the iris image in a region which it can later be extracted to detect tamper localization and recovery. To reduce the distortion of the iris image, it is embedded in a place where there is a space for it to store. Therefore, a procedure to improve the security for the iris image authenticity, is proposed with the use of techniques or methods that is acceptable and suitable. When there is a problem, a solution must be proposed to solve them for the sake of bringing ease and convenient to all.

CHAPTER 4

IMPLEMENTATION, RESULT AND DISCUSSION

4.1 Introductions

In general, the fourth chapter of the paper focuses on the research's implementation, results, and analysis. This chapter is an essential component of the research paper because it provides detailed information on the study's procedure, results, and outcomes. In addition, the conclusion emphasises on the method’s strength and limitations, as well as the potential for future research. In this chapter, readers can obtain a deeper comprehension of how the research was conducted, the results' reliability, and the study's contribution to the field.

4.2 Implementations

This sub-topic will focus on how the method is implemented to produce results. The implementation involves several steps, such as image pre-processing, block-based tampering localization, and feature extraction. It also provides a brief detail of each step and the tools and techniques used to perform the implementation including the parameters used in the implementation and the justification behind them.

4.2.1 Input

Figures provided below are the samples used as input to produce results for the methods implemented. 3 samples are used for this experiment. Each of the samples is an iris image in .bmp format represented in grayscale with 8-bit values. The samples have been carefully selected to represent a diverse range of iris images with varying levels of complexity and features. The images were pre-processed to ensure consistency in size and format, and their sizes were also checked before and after embedding to ensure that the techniques did not result in any significant increase in file size.

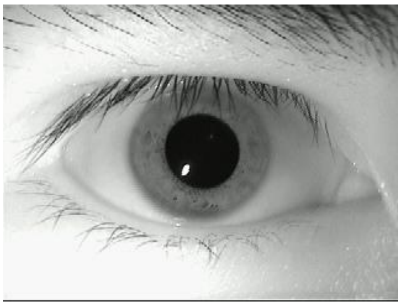


Figure 13: Sample 1

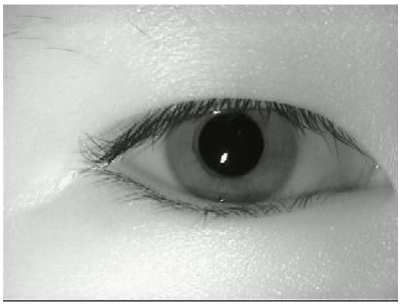


Figure 14: Sample 2

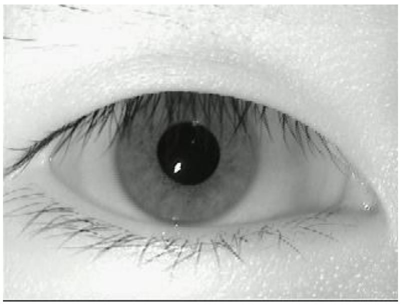


Figure 15: Sample 3

4.2.2 Output

The main outputs of this experiment are the watermarked images, which are the original images with the embedded watermark, and the recovered watermark images, which are obtained after detecting any tampering. In addition, various metrics are used to evaluate the quality of the watermarked images, such as the Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR).

4.2.3 Process Description

The proposed iris image watermarking technique consists of two phases, namely watermark embedding and watermark detection. The pre-processing step involves segmentation, and hashing (SHA-512) which are essential to ensure the robust and secure embedding of the watermark. A unique watermark is generated based on a secret key provided by the user. The watermark is then embedded into the iris image using a block-wise embedding technique that involves dividing the iris image into blocks of equal size and embedding the watermark using the Least Significant Bit (LSB) substitution technique. The embedded watermark is encrypted using a secret key provided by the user to ensure its security and robustness against potential attacks. The final output of the watermark embedding phase is the watermarked iris image that contains the encrypted watermark. Measurements of the quality of the watermarked images are also recorded to be evaluated.

The watermark detection phase involves the extraction of the watermark from the watermarked iris image. The watermarked iris image is divided into blocks of equal size, and the watermark is extracted from each block using the LSB extraction technique. The decrypted watermark is then compared with the original watermark to authenticate the watermarked iris image. If the decrypted watermark matches the original watermark, the watermarked iris image is considered authentic; otherwise, it is considered tampered. The watermark detection phase aims to detect any unauthorized modifications made to the watermarked iris image.

After detection, the tampered blocks, will then be replaced with the original one to produce a reversed watermarked image. Which also means, it can have the recovery of the original images. But, to do the recovery, a secret key must be authenticated. If its match, then the recovery can be proceeded.

4.2.4 Case Study

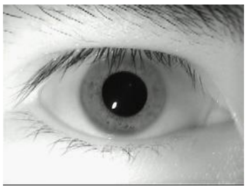
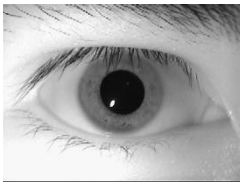
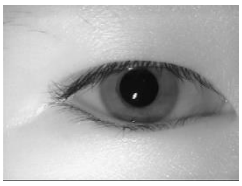
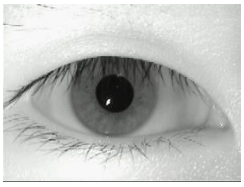
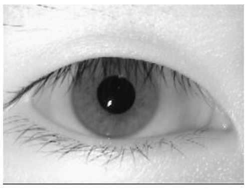
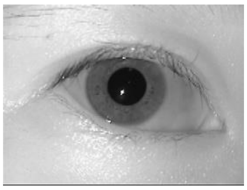
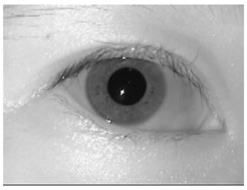
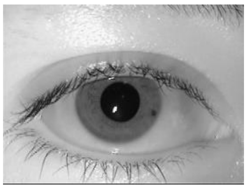
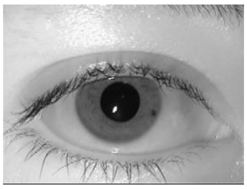
One potential application of the proposed iris image watermarking technique is in biometric authentication systems. Biometric authentication involves the use of unique physical characteristics, such as fingerprints, facial features, or iris patterns, to verify the identity of individuals. These systems are widely used in various industries, including banking, healthcare, and law enforcement. In addition, the proposed iris image watermarking method can also be applied in forensic investigations. Forensic investigators often rely on biometric data, such as fingerprints or iris patterns, to identify suspects or victims. By watermarking iris images, investigators can ensure that the biometric data is not tampered with or altered in any way. In a criminal investigation, the iris images of a suspect can be watermarked with their personal information. If the suspect attempts to alter or replace their iris image, the watermark will not match the original information, revealing that the image has been tampered with. This can provide valuable evidence in the investigation and help to ensure that justice is served.

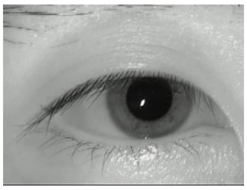
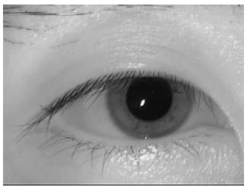
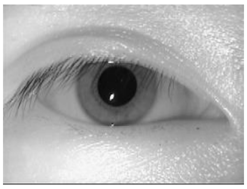
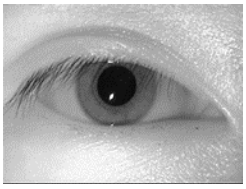
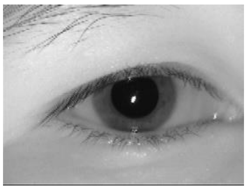
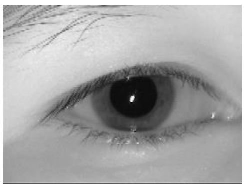
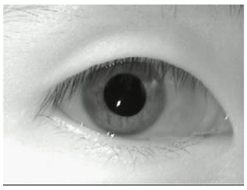
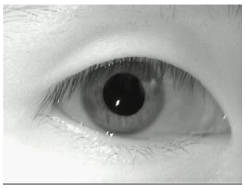
4.3 Result

The results obtained from the implementation of watermarking methods on the ten samples were evaluated in terms of image quality. The visual inspection of the watermarked images showed that the watermark was successfully embedded without significant distortion in all the samples. The recovered watermark images after tamper detection indicated that the proposed methods were able to detect and localize the tampered regions accurately. The performance was also evaluated using metrics such as MSE and PSNR, which indicated that the watermarking methods had high robustness and were able to detect various image processing attacks such as Gaussian noise, salt and pepper noise, and blurring effect.

4.3.1 Embedding

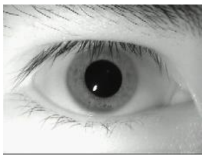
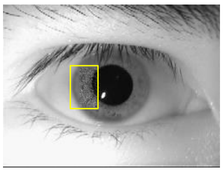
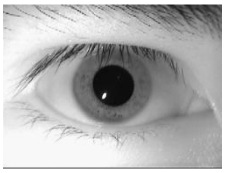
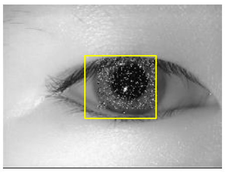
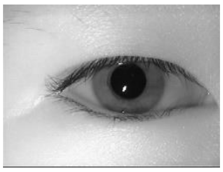
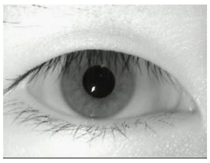
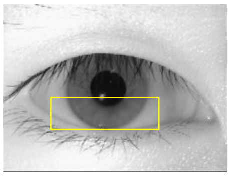
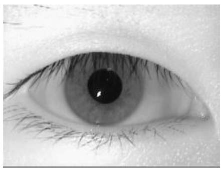
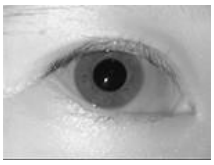
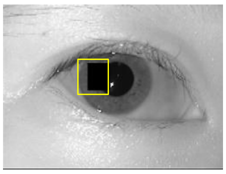
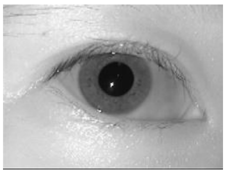
Table 2: Watermarked image results

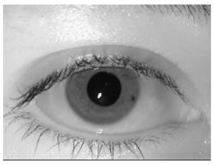
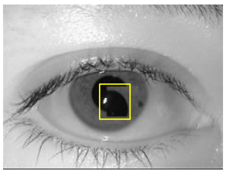
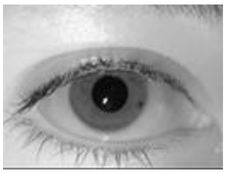
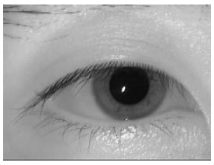
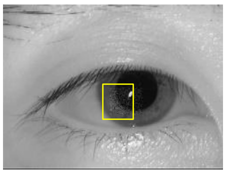
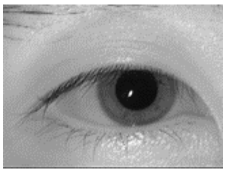
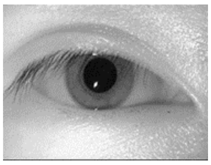
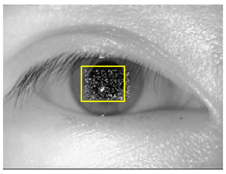
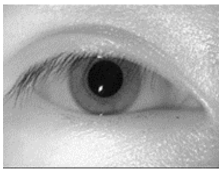
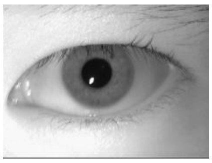
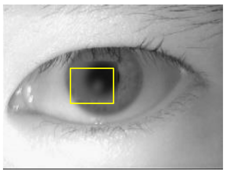
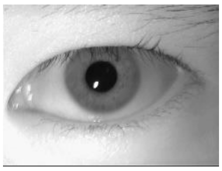
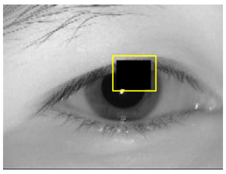
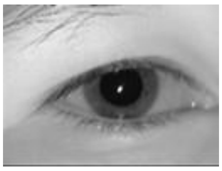
Samples	Elapsed Time	PSNR (dB)	MSE	Size Before Embed	Size after Embed	Output
 sample1.bmp	2.7500	47.2489	1.2252	75.1 KB	76.0 KB	 sample1_watermarked.bmp
 sample2.bmp	1.6719	49.5927	0.7142	75.1 KB	76.0 KB	 sample2_watermarked.bmp
 sample3.bmp	2.7813	47.3267	1.2043	75.1 KB	76.0 KB	 sample3_watermarked.bmp
 sample4.bmp	2.4531	48.9271	0.8325	75.1 KB	76.0 KB	 sample4_watermarked.bmp
 sample5.bmp	2.0313	48.4988	0.9188	75.1 KB	76.0 KB	 sample5_watermarked.bmp

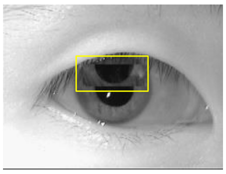
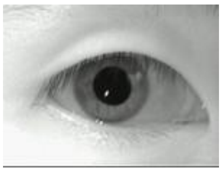
 sample6.bmp	1.7031	48.8190	0.8535	75.1 KB	76.0 KB	 sample6_watermarked.bmp
 sample7.bmp	1.8281	48.8368	0.8500	75.1 KB	76.0 KB	 sample7_watermarked.bmp
 sample8.bmp	2.8438	48.4064	0.9385	75.1 KB	76.0 KB	 sample8_watermarked.bmp
 sample9.bmp	2.4375	49.5851	0.7154	75.1 KB	76.0 KB	 sample9_watermarked.bmp
 sample10.bmp	2.7188	48.2927	0.9634	75.1 KB	76.0 KB	 sample10_watermarked.bmp
Average	2.32189	48.55342	0.92158	75.1 KB	76.0 KB	

4.3.2 Tamper Localization and Recovery

Table 3: Tamper Localization and Recovery

Samples	Tampered Blocks	Tampers	Tampered Area	Recovery
 sample1_watermarked.bmp	1677	Gaussian Noise	 sample1_watermarked_tampered.bmp	 sample1_watermarked_recovered.bmp
 sample2_watermarked.bmp	876	Salt and Pepper	 sample2_watermarked_tampered.bmp	 sample2_watermarked_recovered.bmp
 sample3_watermarked.bmp	2747	Gaussian Blur	 sample3_watermarked_tampered.bmp	 sample3_watermarked_recovered.bmp
 sample4_watermarked.bmp	1280	Cropping	 sample4_watermarked_tampered.bmp	 sample4_watermarked_recovered.bmp

 sample5_watermarked.bmp	1804	Flip/Invert	 sample5_watermarked_tampered.bmp	 sample5_watermarked_recovered.bmp
 sample6_watermarked.bmp	1891	Gaussian Noise	 sample6_watermarked_tampered.bmp	 sample6_watermarked_recovered.bmp
 sample7_watermarked.bmp	708	Salt and Pepper	 sample7_watermarked_tampered.bmp	 sample7_watermarked_recovered.bmp
 sample8_watermarked.bmp	3422	Gaussian Blur	 sample8_watermarked_tampered.bmp	 sample8_watermarked_recovered.bmp
 sample9_watermarked.bmp	1699	Cropping	 sample9_watermarked_tampered.bmp	 sample9_watermarked_recovered.bmp

sample10_watermarked.bmp	2818	Flip/Invert	 sample10_watermarked_tampered.bmp	 sample10_watermarked_recovered.bmp

4.3.3 Result Analysis

From the results, it proves that the scheme able to embed the ROI in RONI as watermark and produced watermarked image and achieved average PSNR of 48.55 dB PSNR and average MSE of 0.92158 which are acceptable. Five attacks have been tested on the ROI region of the watermarked samples for tamper localization and recovery. The recovered image can be produced after tamper localization is done. The secret key will increase the security of the scheme as it can only allow the authorized user to do the extraction of the original ROI to recover the original image if there are any tampers since the secret key needed to be matched to proceed.

CHAPTER 5

CONCLUSION

5.1 Introduction

The conclusion chapter presents a comprehensive overview of the research findings and insights obtained throughout the study. The main objectives of the research are summarized and assessed for their accomplishment. The significance of the research outcomes is discussed, shedding light on their implications within the broader context of the subject matter. Limitations of the study are acknowledged, and potential avenues for future research are suggested. Ultimately, the chapter concludes by summarizing the key contributions of the study and emphasizing its impact in advancing knowledge and practical applications.

5.2 Objective Revisited

The first objective was to investigate the present watermarking approach for iris image. In order to achieve this aim, a thorough literature research was done in order to investigate existing methodologies in iris image watermarking. The study took into account variables including resilience, security, imperceptibility, and computing efficiency. By analysing the schemes' strengths and drawbacks, an overview of the present environment of iris image watermarking was established, laying the groundwork for future study and improvement.

The second objective was to create a recovery and tamper localisation watermarking method tailored exclusively for iris image. A watermarking technique was devised and deployed based on the insights acquired from researching current schemes. The goal of this technique was to restore the original iris image in the event of tampering or assaults while precisely localising the tampered regions. Extensive study and testing were carried out to develop appropriate methods and approaches for embedding and retrieving the watermark.

The third objective was to assess the effectiveness of the recovery and tamper localisation watermarking technique for iris images. To examine the scheme's efficacy and appropriateness for practical usage, rigorous assessment processes were conducted. For testing and benchmarking, a wide range of iris images, including both genuine and altered samples, was used. Performance parameters were measured and analysed, including recovery accuracy and tamper localisation precision. The scheme's resistance to typical assaults was also assessed. The outcomes of these evaluations gave useful insights into the suggested watermarking scheme's strengths and limitations, improving overall understanding of iris image watermarking approaches and directing future research paths.

5.3 Limitation

One of the scheme's limitations is the watermarking approach only protects the ROI region and does not provide complete security for the full iris image. While protecting the ROI region is critical in iris image, it is also critical to protect the overall image's integrity and security. Attacker may attempt to meddle with locations beyond the ROI, which the existing scheme may miss.

Second, is its inability to identify tampering in the area of Non-Interest (RONI) area. While the technique concentrates on embedding and detecting watermarks in the Region of Interest (ROI), it ignores the potential of tampering or unauthorised changes in the RONI region. This restriction creates a concern since manipulation in the RONI area may go unnoticed, jeopardising the whole image's integrity and validity.

Finally, the scheme is vulnerable if the watermark in the RONI area is damaged or lost due to attacks such as image compression, noise, or purposeful assaults. Once the RONI region watermark is compromised, the system lacks a recovery mechanism, rendering the tamper localization and recovery procedure worthless.

5.4 Conclusion and Future Work

The research successfully achieves the objectives by using the proposed watermarking scheme. It produces an acceptable imperceptible watermarked image, ability to detect tamper localization from various attacks to the ROI and able to extract for the recovery of the original image. With the addition of the secret key, can increase the security of the iris image as it can prevent any authorized user from recovering the original image. Regardless, there are room for improvements of the scheme for future work to improve the scheme.

Future research in the area of watermarking for iris image protection and tamper detection has a number of potential directions that might improve the technique's overall efficacy. The extension of tamper detection capabilities to encompass the entirety of the image, including the Region of Non-Interest (RONI), is a vital component that requires attention. The Region of Interest (RONI) is now exposed to undetected manipulation since the watermarking method only protects the Region of Interest (ROI). Future research should examine methods and algorithms to expand the tamper detection systems to include the RONI region as well, guaranteeing thorough security over the full image.

Addressing the limitation of possible loss or destruction of the watermark in the RONI zone is another subject for future development. This restriction makes it difficult to collect and remove tamper evidence from that particular place. To get over this limitation, it is crucial to provide reliable recovery techniques that can fix the watermark or make it possible to retrieve tamper evidence even when the watermark in the RONI area has been damaged. Improving the overall robustness and efficiency of the watermarking strategy will need investigating cutting-edge algorithms and strategies that can rebuild or recover the watermark information from deleted or damaged sections.

The improvement of tamper detection capabilities for the entire image, including the RONI region, should be prioritised in future watermarking development. Additionally, work should be put towards creating powerful recovery techniques that can get beyond the RONI's limits caused by damaged or destroyed watermarks. These will help create a watermarking strategy that is more thorough and robust, protecting the integrity and authenticity of the iris images from any manipulation.

REFERENCES

Alvarez-Betancourt, Y., & Garcia-Silvente, M. (2014). An overview of iris recognition: a bibliometric analysis of the period 2000–2012. *Scientometrics*, *101*(3), 2003–2033. https://doi.org/10.1007/s11192-014-1336-1

Chitra, K., & Prasanna Venkatesan, V. (2016). Spatial domain watermarking technique: An introspective study. *ACM International Conference Proceeding Series*, *25-26-Augu*, 1–6. https://doi.org/10.1145/2980258.2980363

Gaur, P., & Manglani, N. (2015). *Image Watermarking Using LSB Technique*. *3*(3), 1424–1433.

Gul, E., & Ozturk, S. (2019). A novel hash function based fragile watermarking method for image integrity. *Multimedia Tools and Applications*, *78*(13), 17701–17718. https://doi.org/10.1007/s11042-018-7084-0

Halawa, L. J., Wibowo, A., & Ernawan, F. (2019). Face Recognition Using Faster R-CNN with Inception-V2 Architecture for CCTV Camera. *ICICOS 2019 - 3rd International Conference on Informatics and Computational Sciences: Accelerating Informatics and Computational Research for Smarter Society in The Era of Industry 4.0, Proceedings*, (October). https://doi.org/10.1109/ICICoS48119.2019.8982383

Isa, M. R. M., Aljareh, S., & Yusoff, Z. (2017). A watermarking technique to improve the security level in face recognition systems. *Multimedia Tools and Applications*, *76*(22), 23805–23833. https://doi.org/10.1007/s11042-016-4109-4

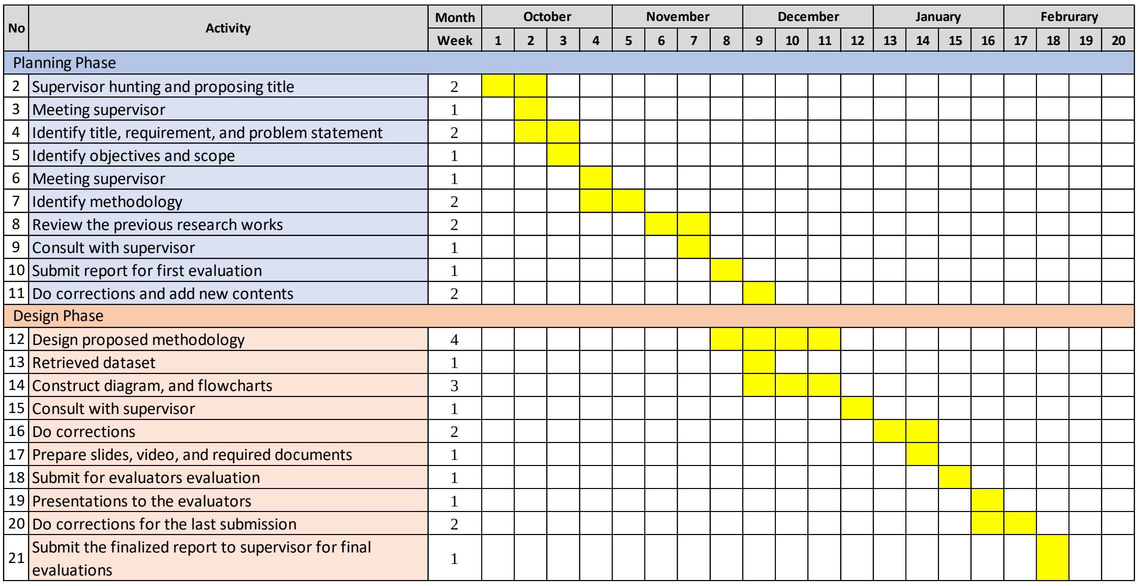
Khor, H. L., Liew, S. C., & Zain, J. M. (2017). Region of Interest-Based Tamper Detection and Lossless Recovery Watermarking Scheme (ROI-DR) on Ultrasound Medical Images. *Journal of Digital Imaging*, *30*(3), 328–349. https://doi.org/10.1007/s10278-016-9930-9

Liew, S. C., & Zain, J. M. (2011). The usage of block average intensity in tamper localization for image watermarking. *Proceedings - 4th International Congress on Image and Signal Processing, CISP 2011*, *2*(October), 1044–1048. https://doi.org/10.1109/CISP.2011.6100301

Qasim, A. F., Aspin, R., Meziane, F., & Hogg, P. (2019). ROI-based reversible watermarking scheme for ensuring the integrity and authenticity of DICOM MR images. *Multimedia Tools and Applications*, *78*(12), 16433–16463. https://doi.org/10.1007/s11042-018-7029-7

Zhou, N. R., Hou, W. M. X., Wen, R. H., & Zou, W. P. (2018). Imperceptible digital watermarking scheme in multiple transform domains. *Multimedia Tools and Applications*, *77*(23), 30251–30267. https://doi.org/10.1007/s11042-018-6128-9

APPENDIX



No	Activity	Month	October				November				December				January				Februrary			
		Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Planning Phase																						
2	Supervisor hunting and proposing title	2	🟨	🟨																		
3	Meeting supervisor	1		🟨																		
4	Identify title, requirement, and problem statement	2		🟨	🟨																	
5	Identify objectives and scope	1			🟨																	
6	Meeting supervisor	1				🟨																
7	Identify methodology	2				🟨	🟨															
8	Review the previous research works	2						🟨	🟨													
9	Consult with supervisor	1							🟨													
10	Submit report for first evaluation	1								🟨												
11	Do corrections and add new contents	2									🟨											
Design Phase																						
12	Design proposed methodology	4								🟨	🟨	🟨	🟨									
13	Retrieved dataset	1									🟨											
14	Construct diagram, and flowcharts	3									🟨	🟨	🟨									
15	Consult with supervisor	1												🟨								
16	Do corrections	2													🟨	🟨						
17	Prepare slides, video, and required documents	1														🟨						
18	Submit for evaluators evaluation	1															🟨					
19	Presentations to the evaluators	1																🟨				
20	Do corrections for the last submission	2																🟨	🟨			
21	Submit the finalized report to supervisor for final evaluations	1																		🟨		

Appendix 1: Gantt Chart