CHAPTER I
INTRODUCTION

This chapter provides a brief overview of the research. Consist of six sections; the explanation starts with background, problem identification and objective, scope of work, research methodology, and structure of this thesis. A more detailed explanation will be later in the next chapter.

1.1 Background

Communication using digital media to transmit data can be a threat to users. One of them is about the authenticity of the data they send or receive via digital media. There will be a very high need, especially for the security sector. With various developments across sectors, research and educational institutions are intensively exploring the field of quantum computing. The acceleration of progress in quantum computing has significant implications for the sustainability and efficiency of information systems. Therefore, the need for more proactive measures to secure information becomes a crucial key in maintaining the sustainability of this technological advancement [1]. An important aspect in the communications sector is data security. One way to secure transmitted data is to use watermarking. Unlike cryptography, watermarking aims to hide the existence of information within otherwise seemingly harmless data, making it less likely to be detected or suspected [2]. Watermarking can be used to secure our data and minimize modification by irresponsible people. The domains that are often used for watermarking are the spatial and frequency domains [3]. Domains that are currently being actively developed is quantum watermarking [4]. Steganography research is becoming more and more fascinating with advances in quantum technology. Quantum steganography focuses on developing information hiding techniques in quantum data that are resistant to attacks and of high quality. In quantum steganography, security is enhanced compared to classical steganography. The physics principles applied are superposition and entanglement. This second principle is the main point in using quantum watermarking.

Chandana and Geetha, proposed quantum images steganography using grayscale images with the Least Significant Bit (LSB) method, resulting in a scheme with a Peak Signal to Noise Ratio (PSNR) of 43.74 dB [5]. But in Chandana's research, there was no mention of any attacks conducted during the testing phase. This study solely focused on the utilization of the Arnold images scrambling method, aiming to enhance capacity and achieve a yield of 2 bits per pixel. In the same year, using the same method as Chandana, Geofeng proposed a steganography scheme uses boundary pixels LSB steganography by resizing the images with a higher imperceptibility value 55 dB. However, when tested using salt and pepper noise, the PSNR dropped to 29 dB and does not include the payload value [6]. In [7] proposed the algorithm used the LSB method with RGB images. The advantage of this quantum watermarking scheme was the testing against attacks in the quantum domain. The results were good, with PSNR above 40 dB.

Sangeeta Dhall et al. proposed quantum steganography using LSB and Arnold transform with Red Green Blue (RGB) images, resulting in a scheme with high imperceptibility, measuring 80 dB. Combining quantum computing and images encryption, quantum images hiding techniques are gradually attracting attention [8]. In [9], Xiande Liu et al. made a technique for encoding RGB images using FRQI representation and qubit rotation, resulting in a highly imperceptible scheme. The information presented in this study is quite complete. Starting from the steps for each part to the quantum circuit used. However, there is a lack of information regarding the capacity of the proposed watermarking scheme. In [10], quantum watermarking implemented in a mobile application using Quantum SS, DCT, and Wavelet embedding techniques was proposed. The application developed is good because it can produce PSNR values. However, the application does not provide any capacity.

In [11], Hu et al. proposed method in using the FRQI representative also gives good imperceptible value PSNR 54-64 dB. In this paper, the images used grayscale and binary for host and watermark. The host images is a grayscale and the watermark image is a binary. A weakness in this watermarking scheme is that it still has a small capacity, amounting to 0.25 bits per pixel. Astuti et al., proposed LSB steganography for colour images. Schematic of Bit-flipping used for change the wevelet coefficient slightly of carrier images. This steganography appropriate for grayscale and color images. It utilized RGB host images and grayscale watermark images and get PSNR 55 dB. The drawback in this study is there is no mention of the level of decomposition in the wevelet transformation [12].

Study of Quantum watermarking using LSB and representation Novel Enhanced Quantum Representation (NEQR) by applying principle of the nearest neighbor interpolation was written by WenWen et al. proposed scheme exhibits good visual quality. However, the journal focuses only on imperceptibility and capacity as discussed parameters, with no mention of robustness. Using RGB for host image and binary image for watermark image the scheme of watermarking get result PSNR 55 dB and capacity 0.25 bits per pixel [13]. With same method with [13], Zhiguo Qu et al. resulting PSNR 44 dB using host image grayscale in [14]. Confidential information that has been damaged can be recovered and the location of the damage can be found. The drawback of this journal is that it does not mention the capacity of the proposed steganography scheme. In [15] Zhiguo Qu et al., proposed a study of quantum watermarking technique using NEQR with increase the range of dynamic subgroup modification and sharing technique. This research resulted a good imperceptibility with PSNR above 50 dB and a capacity of 1 bits per pixel.

In another paper, Zhiguo Qu et al. used quantum steganograhy based matrix coding for quantum colour images [16]. The proposed method in this paper is two qubits of secret information into three LSQbs of quantum images carrier. The scheme of quantum steganography produce high capacity. In same years Zhiguo Qu et al. proposed grover search algorithm and images expansion based quantum. This algorithm adopts quantum log-polar images (QUALPI) representation [17]. The result of this scheme is have good coding scalability. In [18], Marius Nagy et al. proposed quantum steganography using entanglement domain for information.

The method used in this study is the application of amplitude (elevation) encoding using the Taylor Series for the information embedding process. The images will be changed, which was previously in the classical domain, into the quantum domain using Flexible Representation of Quantum Images (FRQI) using Taylor series. The angle of watermark image in quantum domain will be included in host images in the quantum domain. The embedding results will be entered into the rotation gate. This algorithm is non-blind, thus requiring the host images to reconstruct the watermark images.

1.2 Problem Identification

With the advancement of quantum technologies for information hiding, a critical issue remains the lack of techniques tested within the quantum domain. Most existing approaches are validated only in classical contexts, overlooking the unique threats and vulnerabilities present in quantum environments. Furthermore, there is an absence of information hiding methods that explicitly demonstrate the distinctive advantages of quantum information hiding, which limits the potential to fully exploit quantum mechanics for enhanced data security and robustness.

1.3 Objective and Contributions

The objective of this research is to develop a quantum watermarking scheme by utilizing a modified Taylor series approach and employing rotation gates to manipulate quantum state angles during watermark embedding. The research focuses on analyzing the imperceptibility and capacity of the watermark by adjusting the order of the Taylor series, as well as assessing its robustness against potential quantum channel attacks. The contributions of this research is the robustness evaluation of quantum information hiding using Taylor series and rotation gate.

1.4 Scope of Work

To keep the experiment from being too long, this thesis limits the works as follows:

1. The method used for quantum watermarking is Taylor Series modification and Rotation Series.
2. The representation used is FRQI.
3. The host image used is a grayscale image.
4. The watermark image used is a grayscale image.
5. The host ad watermark image using *L*=64.
6. The rotation gate used in the watermarking scheme employs the X rotation gate.
7. Attacks were performed in the quantum domain using Pauli X, Y, and Z gates applied randomly.
8. The analyzed parameter values include Peak Signal Noise Ratio (PSNR), representing the similarity value between the host image and the watermarked image and Payload.

1.5 Research Methodology

In this thesis, we use fundamental study and experiment based on work-packages (WP). These are the following WP for this thesis:

- WP 1: Study Literature
  In this stage, research is conducted to search for and comprehend the concepts of the Taylor Series modification and rotation gate. Representative FRQI that have been investigated in previous studies. Information sources are obtained from various books, journals, and articles related to quantum watermarking. The literature review is carried out with the aim of understanding and keeping up with developments in watermarking, which will serve as the foundation for the research.

- WP 2: System Design and Simulation
  This process involves the creation of a quantum image watermarking system using the representative FRQI method. The embedding process is performed using the Taylor Series modification and rotation gate. The designed system will be simulated using MATLAB software.

- WP 3: Testing and Analysis
  Analyzing the performance of the technique based on the values of PSNR, and payload. The system will be subjected to various types of quantum domain attacks. Simulation results will demonstrate that the quantum image watermarking system possesses a high level of security, imperceptibility, and good capacity.

1.6 Organization of The Thesis

The structure of this thesis is as follows:

- CHAPTER 1: INTRODUCTION

  The introduction includes the background, problem formulation, research objectives, scope of the study, research methodology, and the structure of the thesis.

- CHAPTER 2: BASIC CONCEPTS

  The theoretical framework provides explanations of the methods used in this thesis. Reviews the existing literature on quantum information processing, quantum image representations, and related watermarking techniques.

- CHAPTER 3: SYSTEM MODEL AND THE PROPOSED DESIGN

  Outlines the system model and introduces the proposed quantum image hiding design. Highlights the design's proposed and its impact on quantum information hiding, setting the stage for later performance evaluations and results.

- CHAPTER 4: PERFORMANCE EVALUATION

  Results and discussion present the data obtained from the system and the analysis of the results.

- CHAPTER 5: CONCLUSIONS AND FUTURE WORKS

  The conclusion summarizes the research findings in relation to the research objectives and offers recommendations for further development.