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

In digital era, multimedia plays an important role in disseminating information around the world. Multimedia content such as audio, video, and images can be easily accessed and shared with anyone around the world. However, behind this convenience lies a great risk of information misuse and copyright infringement. Manipulation, unauthorized distribution, and illegal copying are major challenges for multimedia content owners. Digital image tagging is an effective solution to protect the authenticity and copyright of information contained in multimedia content [1].

Generally, watermarking has two area classifications, it is spectrum domain and space domain. Spectrum domain is a domain where the watermark embedding process involves manipulating the coefficients of the original image. While space domain is processing watermark hiding which is carried out directly into the picture or other media in the form of image pixels. This hiding process uses low computational complexity, but the process cannot withstand digital signal processing .

Image watermarking is a method to protect multimedia content with secret information embedded into carrier images. The inserted secret information is called a watermark or label. Watermarking is used to protect copyright, so watermarking must be embedded and extracted by the owner with ease, thus need Exactly embedding process [2]. Along with the increasing uses of digital images, then the research area in watermarking is more extensive. Data authentication and copyright protection is an important application scope in the use of image watermarking. These applications include ownership identification, broadcast monitoring, usage control, forgery detection and authentication, copy control, medical applications, and copyright protection [3].

Although digital image watermarking is an effective method to protect multi-

media content, it also faces challenges, especially from attacks that aim to damage or remove the watermark. Geometric distortion, compression, low pass filter, and Gaussian noise are some type of attack at image watermarking [4]. Therefore, to protect multimedia content from attacks, a robust watermarking algorithm scheme is required. In [5], Chang et al. first proposed a turtle shell-based information hiding scheme. Then, in [6], Liu et al. redeveloped the research of Chang et al. [5] to improve the insertion capacity and image quality using the turtle shell scheme.

Over the past five years, research on turtle shell schemes has continued to develop. Lin et al. [7] proposed a real-time dual-image-based reversible data hiding scheme using turtle shells, achieving a PSNR of 49.38 dB, though it lacked testing against image attacks. Lin et al. [8] introduced a fragile watermarking scheme with the turtle-shell technique, improving embedding capacity and reducing distortion, with a PSNR of 46.8 dB, but also lacking attack testing. Chang and Liu [9] proposed two real-time turtle-shell-based data embedding mechanisms to reduce computational complexity and enhance visual quality, achieving a PSNR above 45 dB, yet without testing for attacks. Xieo et al. [10] presented a modified 2D histogram-based turtle shell scheme, expanding the embedding area and achieving a PSNR around 30 dB, but this study also did not include attack testing and reported lower PSNR values. Lastly, Li et al. [11] proposed a scheme for sharing secret images with easy authentication using a turtle shell structure, achieving a PSNR of 47.87 dB. In this study [11], the PSNR value is good and has explained the attack,but the variety of attacks is slight.

In this paper, we propose a secret information hiding scheme based on a turtle shell technique. This research not only examines imperceptibility and capacity but also addresses robustness, unlike previous studies [7] [8] [9] [10] that did not discuss robustness. The inclusion of attack testing is a significant advantage of this paper, demonstrating that the proposed scheme can not only effectively embed information but also protect it against various types of attacks.

This research is organized into five chapters to discuss this research comprehensively. Chapter 1 is the introduction, explaining the background, problem identification, objective, scope of work, and research methodology. Chapter 2 discusses the theoretical foundation, presenting theories related to the turtle shell scheme and data hiding techniques. Chapter 3 outlines the methodology, describing the system model, embedding process, extraction process, attacks, and performance parameters used for evaluation. Chapter 4 presents the results, presenting the experimental findings and analysis. Finally, Chapter 5 contains conclusions and suggestions for future research.

1.2 Problem Identification

In various previous studies [7] [8] [9] [10] [11], turtle shell-based watermarking methods have generally achieved PSNR values above 40 dB, which typically indicates that the watermark is not visible to the human eye. However, there is a study that reported a PSNR value as low as 30 dB [10]. A PSNR value below 40 dB indicates that watermarking may cause significant visual distortion, thereby reducing imperceptibility and potentially compromising the visual quality of the image [12]. The presence of such low PSNR values indicates a gap in the development of methods to improve imperceptibility.

In previous research, several studies have tested the robustness of watermarks against certain attacks, such as Gaussian noise, Salt and Pepper, Speckle noise [11]. However, there are still studies that have not discussed resilience against attacks [7] [8] [9] [10]. The turtle-shell technique itself is still limited in terms of testing variations against attacks, which generally include various types of attacks such as noise, filtering, and compression. Attack resistance is a crucial aspect in assessing the effectiveness of watermarking methods, so further research is needed that includes testing against a more diverse range of attacks to ensure the validity and strength of the proposed scheme. A wider variety of attacks is needed to test the robustness of the watermark more thoroughly, especially on the turtle-shell method, which is still little discussed. This opens up opportunities to develop further tests to improve watermark robustness against various types of attacks.

1.3 Objective

The objectives of this research are as follows:

1. To propose a watermarking scheme using the Turtle-Scheme on Neighborhood Pixel method that aims to enhance image quality, ensuring higher imperceptibility and achieving superior PSNR compared to previous approaches.

2. To evaluate the robustness of the proposed Turtle-Scheme on Neighborhood Pixel watermarking method against a range of attacks, including but not limited to Gaussian noise, Salt and Pepper noise, compression, low-pass filtering, rescaling, speckle noise, and median filter with the potential to include additional attacks as the research progresses.

1.4 Scope of Work

To maintain focus and prevent the experiment from becoming overly extensive, this thesis limits the scope of work as follows:

1. The watermarking method implemented in this research is the Turtle-Scheme on Neighborhood Pixel, a modification of the Turtle shell algorithm.
2. The images used in the experiments are grayscale images to standardize the testing conditions.
3. The watermark used in all experiments is a randomly generated binary image
4. The imperceptibility of the proposed method will be evaluated using the following parameters: Peak Signal to Noise Ratio (PSNR), Payload, and Mean Opinion Score (MOS).
5. The robustness of the proposed method against various attacks will be assessed using the Bit Error Rate (BER) as the primary performance parameter.

1.5 Research Methodology

This thesis is divided into 3 work packages (WP) to produce high quality results.

- WP 1: Study of Literature
  This thesis studies the basic concepts and theories related to Digital Image, Watermarking, Binary Representation, Least Significant Bit (LSB),and Turtle shell algorithm.
- WP 2: System design and simulation
  Make a system design for the image watermarking process, embedding process, and perform extraction using a modified turtle scheme. After that, simulate based on the previously designed embedding to extraction system model into the MATLAB program.
- WP 3: Testing and Analysis
  This final project tests the system and analyzes the data obtained from the testing process to determine the performance results produced by the system.