AN ENHANCED METHOD BASED ON INTERMEDIATE SIGNIFICANT BIT TECHNIQUE FOR WATERMARK IMAGES

GHASSAN NASHAT MOHAMMED

DOCTOR OF PHILOSOPHY
UNIVERSITI UTARA MALAYSIA
2015

Permission to Use

In presenting this thesis in fulfilment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the Universiti Library may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence, by the Dean of Awang Had Salleh Graduate School of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Awang Had Salleh Graduate School of Arts and Sciences
UUMCollege of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok

Abstrak

Digital Watermarking Intermediate Significant Bit (ISB) adalah satu teknik baru penerapan *watermark* dengan menggantikan piksel imej asal dengan piksel yang baru. Ini dilakukan dengan cara memastikan persamaan yang nyata antara piksel baru dengan piksel asal dan pada masa yang sama, data *watermark* di dalam piksel baru tidak di ubahsuai. Salah satu teknik yang popular dalam *watermarking* adalah mengunakan *Least Significant Bit* (LSB). Ia menggunakan spatial domain yang diselitkan dalam imej LSB. Masalah yang biasa dihadapi dengan kaedah ini ialah imej tersebut mudah di ubahsuai dan, kemungkinan berlaku gangguan pada imej setelah *watermark* diterapkan. LSB boleh digunakan dengan menggantikan satu, dua, atau tiga bit; ini dilakukan dengan menukar bit tertentu tanpa apa-apa perubahan lain dalam bit piksel tersebut. Objektif tesis ini adalah untuk merangka algoritma baru bagi meningkatkan kualiti dan *robustness* imej digital *watermarking* dengan menerapkan dua bit imej *watermark* ke dalam setiap piksel. Ini dapat meningkatkan *robustness* kedua-dua imej tersebut di samping meningkatkan keupayaan *watermark* berasaskan pada teknik ISB. Walau bagaimanapun, *tradeoff* antara kualiti dan *robustness* perlu dilakukan untuk mendapatkan keseimbangan kedudukan yang terbaik untuk kedua-dua bit *watermark* yang di ubahsuai. Teknik *Dual Intermediate Significant Bits* (DISB) telah dicadangkan dalam kajian ini untuk mengatasi masalah dalam LSB. Keputusan ujian yang diperolehi daripada teknik yang dicadangkan adalah lebih baik berbanding dengan LSB dari segi *Peak Signal to Noise Ratio* (PSNR) dan *Normalized Cross Correlation* (NCC). Kajian ini juga menyumbang pada pembinaan persamaan matematik yang baru bagi tujuan untuk mengubah enam bit piksel *watermark* selepas menerapkan dua bit yang baru.

Kata kunci: Watermark, Intermediate Significant Bit, Kualiti, Robustness, Least Significant Bit.

Abstract

Intermediate Significant Bit digital watermarking technique (ISB) is a new approved technique of embedding a watermark by replacing the original image pixels with new pixels. This is done by ensuring a close connection between the new pixels and the original, and at the same time, the watermark data can be protected against possible damage. One of the most popular methods used in watermarking is the Least Significant Bit (LSB). It uses a spatial domain that includes the insertion of the watermark in the LSB of the image. The problem with this method is it is not resilient to common damage, and there is the possibility of image distortion after embedding a watermark. LSB may be used through replacing one bit, two bits, or three bits; this is done by changing the specific bits without any change in the other bits in the pixel. The objective of this thesis is to formulate new algorithms for digital image watermarking with enhanced image quality and robustness by embedding two bits of watermark data into each pixel of the original image based on ISB technique. However, to understand the opposite relationship between the image quality and robustness, a tradeoff between them has been done to create a balance and to acquire the best position for the two embedding bits. Dual Intermediate Significant Bits (DISB) technique has been proposed to solve the existing LSB problem. Trial results obtained from this technique are better compared with the LSB based on the Peak Signal to Noise Ratio (PSNR) and Normalized Cross Correlation (NCC). The work in this study also contributes new mathematical equations that can study the change on the other six bits in the pixel after embedding two bits.

Keywords: Watermarking, Intermediate Significant Bit, Quality, Robustness, Least Significant Bit.

Acknowledgement

It gives me great pleasure to express my gratefulness to everyone who contributed in completing this thesis. It was my pleasure to study under Associate Professor Dr. Azman Yasin's supervision. I'm so grateful for his support during the last four years; who was also my supervisor during my Master's study at UUM. He is like a brother to me, and for all of these, there are no words to express my gratitude for his guidance in helping me to achieve my goal. Without his valuable support, my thesis would not have been possible. I would like to thank my co-supervisor Associate Professor Dr. Akram M. Zeki for his advanced ideas and his noble mind. His continuous advice and important comments helped improve my work successfully.

To my father, whose surname I proudly carry – I am forever appreciative. I hope he is proud of me even if he is no longer with us. To my mother, who gave me life and prayed for me all the time, may Allah continuously bless her with good health. To my sisters and brothers, thanks for their love and support. To my wife Suha, who gave her time and patience during the last four years of study, I thank her from the bottom of my heart. I would also like to thank my two young babies Mohammed and Zainab, without whom my goal would not have been achieved. I dedicate this work to my family.

I'm so glad to study at Universiti Utara Malaysia (UUM). I completed both my Master's and PhD at the same university and spent a total of about five years there. During my time in UUM, I have gained a lot of friends, and studying there was like being in my hometown. My sincere gratitude to all of them for all the encouragement during my study.

Table of Contents

List of Tables

List of Figures

List of Appendices

CHAPTER ONE
INTRODUCTION

1.1 Background

Currently, digital watermarking and information hiding have become important topics of computer science due to the increasing popularity of the Internet and the critical need of data security (Chin et al, 2004).

Digital watermarking is a special case of general information hiding problem. It inserts a perceptually transparent pattern known as a watermark into an image called original or cover using an embedding algorithm in which it is undetectable to human eyes, but visible to computer processes for data declaration (Modaghegh et al, 2009).

In other words, digital watermark is a signal which is permanently embedded into digital data (audio, images, videos, and text) which can be detected or extracted later by means of computing operation to make assertion of the data. The watermark is hidden in the original data, in such a way that it is inseparable from the data and so that it is resistant to many operations which do not degrade the original data. Thus, by means of watermarking, the work is still accessible but permanently marked (Lu, 2005). This method successfully shields the copyright of the originality for media which is organization mark, for instance, in the original media. The image quality has not been corrupted through the watermarking system, and the inserted watermark should recover dependably. It is also essential for the embedded watermark to be resilient against noise and other typical image processing attacks. These attacks may be blurred

images, sharpened images, compressed images, and cropped images (Peungpanich et al, 2010).

Digital watermarking provides the owner of a piece of digital data the means to invisibly mark the data. The mark could be used to serialize a piece of data as it is sold or used as a method to mark a valuable image. For example, this marking allows an owner to safely post an image for viewing, but legally provides an embedded copyright to prohibit others from posting the same image (Lu, 2005).

Since the beginning of human communication, the desire to communicate in secrecy has existed. There have been many solutions to this problem, and the most widely used and investigated is cryptography (Schneier, 1996; Massey, 1988; Simmons, 1992). The use of cryptography in communication makes it obvious to an intruder that the communication is secret because of the encryption used. However, the digital watermarking problem requires that the very existence of communication (i.e. the watermark itself) is kept secret. This can be achieved by embedding the watermark in the media imperceptibly and detecting it whenever required. Such a digital watermark may carry any information, depending on the application (Adrian, 2003).

The difference between cryptography and watermarking is more intuitive. Cryptography encodes a normal message into a secret message. If an encrypted message is intercepted, it may immediately arouse suspicion. Once the encoded data is decoded, the data becomes totally unprotected. On the other hand, watermarking

hides the existence of a message; so if the original is intercepted, the message may remain concealed (Qi, 2005).

Any algorithm for watermarking should consist of three_ parts. The first, which is exclusive to the owner, is the (Watermark). The second one is the (Encoder) for embedding the watermark into the data, and the third one is the (Decoder) for extraction and verification (Abdullatif et al, 2013). Figure 1.1 demonstrates both the encoding and decoding processes. In the first state, the watermark is embedded into an original image through a key file, either for visible or invisible watermarking. Thus, the watermarked image can be obtained. While the decoding state entails reading the image that was watermarked and the key file used to extract the watermark. The watermark will be extracted using the same key used in the embedding/encoding stage (Abdullatif et al, 2013).

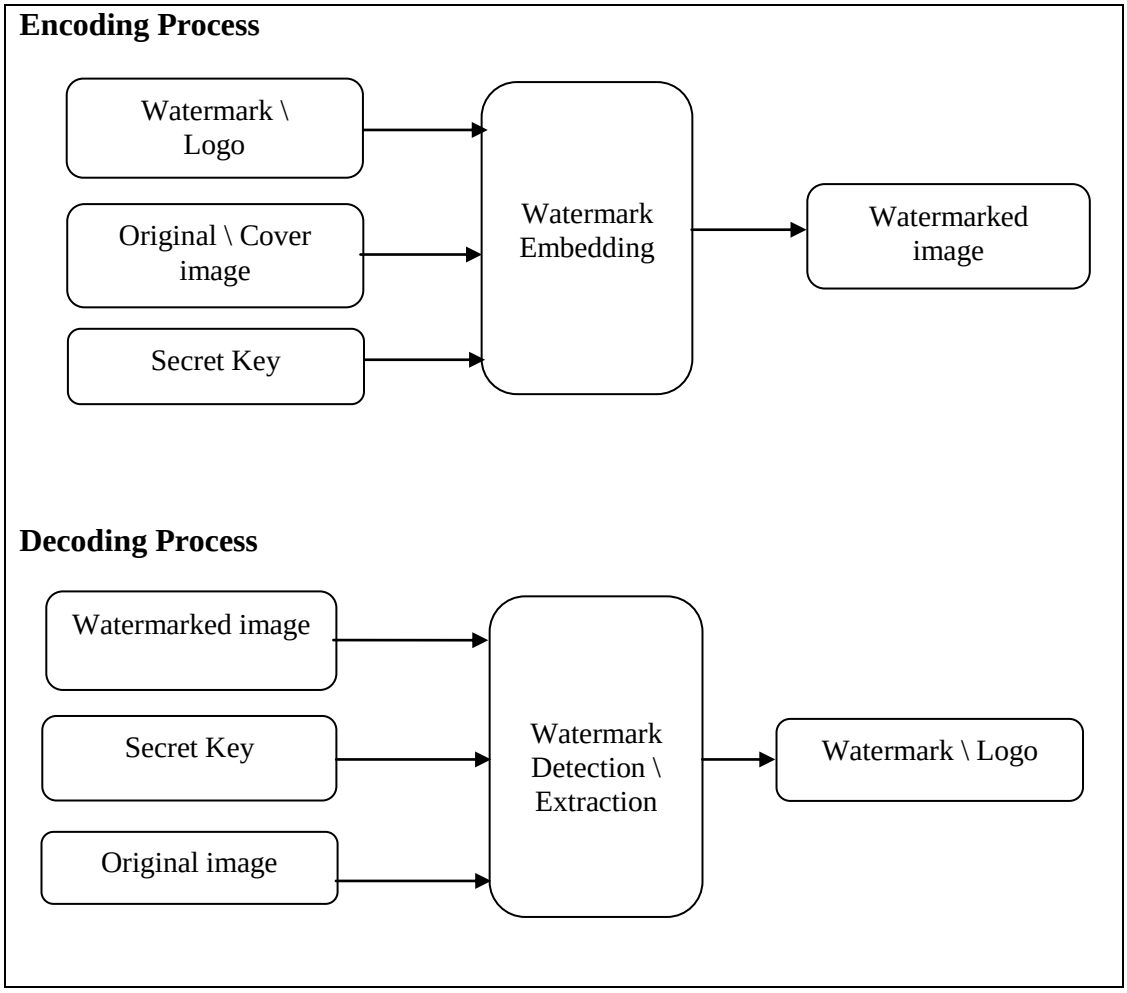


Figure 1.1. Embedding and Detection processes (Abdullatif et al, 2013)

In detail, there are different types of watermarking images depending on human perception, or according to the types of documents to be watermarked. The four watermarking procedures for documents are identified, which are (Text, Image, Video, and Audio) Watermarking (Singh & Gupta, 2011).

Meanwhile, there are two types of watermarking techniques depending on human perception: (Visible Watermark), and (Invisible Watermark). Visible watermark is visible to the viewer since it is translucent and covers an image. This is for the sole

purpose of ownership and copyright security. An invisible watermark, on the other hand, is embedded in the data so carefully that any adjustments done to the pixel values are not realized. The process of extracting watermark can be of one of the three types: the first one is non-blind, while the second one is semi-blind, and third one is blind. In the non-blind watermarking scheme, two important things for watermark discovery are needed, the original image, and the secret key (Mabtoul et al, 2007).

For the purpose of extraction, the semi-blind scheme requires a secret key and a sequence of watermark bit. Meanwhile, the blind scheme needs only a secret key for extraction, which is why the retrieval of the logo (watermark) does not need the original image (Hongqin & Fangliang, 2010).

Generally, the most common techniques of watermarking are: The Spatial Domain Watermarking Technique (Chan, et al., 2004; Wang et al, 2001; Schyndel et al, 1994), and Transform Domain Watermarking Technique (Dubolia et al, 2011; Anwar et al, 2010). In the spatial domain technique, the main idea is to make the insertion process for the watermark image into the original one by changing certain amounts of pixels in the original image (Dejun et al, 2009). The main advantages to this are the implementation is easier and investigate simplicity. On the other hand, the dis-advantages is there is a possibility to discover the inserted watermark through computer programs (Shih, 2010; Yang & Zhang, 2009).

The simplest and the most common method used in the spatial domain watermarking technique is the Least Significant Bit (*LSB*) coding (Lin et al, 2010). The value of the image is not influenced by the insertion of a watermark into a particular image (Peungpanich et al, 2010). The process entails the insertion of the watermark by exchanging the *LSB* of image information by the new information from the watermark. However, one of the main disadvantages of this technique is that it is not recommended for copyright authentication since it can be removed from the original image easily, and it can easily be replaced by an enormous amount of embedded bits, as it has not included important data. Hence, this technique can easily be destroyed and is unsafe (Megalingam et al, 2010).

Furthermore, Genetic Algorithm (*GA*) is used by other studies to enhance the (image quality) and (robustness) (Mohamed et al, 2011; Zamani et al, 2009), as well as it is considered as one of the important methods which support the quality enhancement of the watermarked image and it is represented widely as an optimization technique (Goyal et al, 2009).

A technique called Intermediate Significant Bit (*ISB*) tried to solve *LSB's* weaknesses. The study developed a solid watermarking model using the spatial domain technique, whilst retaining the significant watermarking needs of picture quality and reasonable capacity by embedding only one bit. The technique proved that the edge of the range gives the highest quality for watermarked image, while the middle of the range gives the highest robustness against image attacks. This is done via using new pixels in the place of watermarked image pixels which help to secure

the watermark data from attacks, at the same time keeping the quality for the watermarked image (Zeki & Manaf, 2009).

The work in this research sets a new direction for *ISB* by enhancing it via embedding two bits that can handle many limitations, and by embedding two bits in *LSB* method. This new direction will be used in this research to enhance the image quality using derivative mathematical equations which study the effect of all bits in the embedding process.

1.2 Problem Statement

The problem with digital watermarking is that it requires quality and robustness to be met. However, they are almost always in conflict with one another (Emami et al, 2012; Chetouani et al, 2010; Aliwa et al, 2013; Zeki & Manaf, 2009; Bedi et al, 2009; Langelaar et al, 2000). For example when the quality is high, the robustness decreases and vice versa. Therefore, there is a need to have a balancing mechanism for handling quality and robustness together.

The watermarking algorithm must embed the watermark so that it does not affect the quality of the underlying original data. The watermark is truly invisible if the original data cannot be distinguished from the watermarked information. However, since users of watermarked data normally do not have access to the original data, they cannot perform this comparison. Therefore, it is sufficient that the modifications in the watermarked data go unnoticed, as long as the data is not compared with the original data (Gulati, 2003; Shelby, 2000).

The second important requirement of watermarking schemes is robustness. Robustness refers to the ability of the inserted information to withstand image modifications (intentional or unintentional). The watermark should be difficult to remove or alter without the degradation of the original image (Voyatzis and Pitas, 1998; Chen, 2003). However, it is important to note that the level of robustness required varies with respect to the application at hand (Zeki, 2009). Improving the robustness of a watermark so as to withstand attacks has been one of the main study objectives in digital image watermarking (Hemahlathaa & Chellppan, 2012).

The common watermarking technique that turns out well in the Spatial Domain is the *LSB* (Chan et al, 2004; Wang et al, 2000). Many studies that used the *LSB* method have been developed by embedding two bits from every pixel taken from the watermark image into each pixel of the original image (Aarthi et al, 2012; Bamatraf et al, 2010; Thapa & Sood, 2011).

One of the *LSB* method limitations is the watermarked image distortion after the embedding process (Chan et al, 2004; Maity and Kundu, 2002). This is because the main idea of the LSB replaces the embedding bits with original bits directly (Jadav, 2013; Zeki & Manaf, 2009; Schaynedel, 1994), therefore, this will lead to ignoring the effectiveness of other bits.

To overcome this problem is to find a new way for embedding two bits in digital watermarking for the purpose of studying the effect in changing all other bits in the same pixel after the embedding process.

Another limitation of the existing *LSB* method is that it is not robust enough against possible attacks. Robustness relates to how much the inserted information can resist any form of image alterations. The disadvantage of this technique is that it can easily be replaced by an enormous amount of embedded bits; since it does not consist of vital information presented visually, so this technique can easily be destroyed and is unsafe (Wu, 2001).

To overcome this limitation, a new way for embedding two bits in digital watermarking is needed to get a strong watermarked image and for it to be more robust against possible attacks.

The two requirements of quality and robustness always conflict with each other (Emami et al, 2012; Chetouani et al, 2010; Aliwa et al, 2013; Zeki & Manaf, 2009; Bedi et al, 2009; Langelaar et al, 2000).

To overcome this problem, a new way by making a balance between image quality and robustness has to be done.

1.3 Research Questions

Based on the problems that deals with embedding two bits described in the previous section, the study tries to answer the questions as below:

1. Can adding another bit improve the quality of watermarking image?
2. How can the enhanced algorithm be used to handle image distortion?

3. Can the enhanced algorithm resist all attacks?
4. How can the enhanced algorithm make a tradeoff between quality and robustness?

1.4 Research Objectives

This study is carried out in response to solving the described problems and to answer the research questions as defined in the previous section. Hence, the main objective of this thesis is to propose new algorithms that simultaneously enhance both image quality and robustness based on the existing technique *ISB*. The following specific objectives should be achieved:

i. To develop an enhanced algorithm based on *ISB* so that the new algorithm could add another bit and improve the quality of watermarking image.
ii. To develop an enhanced algorithm based on *ISB* technique that can handle image distortion.
iii. To develop an enhanced algorithm based on *ISB* that can resist image attacks and increases the robustness.
iv. To develop an enhanced algorithm based on *ISB* which can make a tradeoff between image quality (quality) and resistance against image attacks (robustness).

1.5 Scope of the Study

This study emphasizes on using a blind technique for watermarking image in the spatial domain to embed two bits of the watermark image into each pixel of the

original image. The thesis focuses on using *ISB* technique to embed two bits of watermark into the original image. The important thing is that the watermarked image cannot be noticed by the third party to maintain the safety of the secret message. The other important thing is that the watermarked image has to be robust against attacks which try to remove the new pixels after the embedding process.

The study uses the dataset from Grayscale Standard Images (http://www.dip.ee.uct.ac.za/imageproc/stdimages/greyscale/), and Dataset of Standard 512×512 Gray scale test images (http://decsai.ugr.es/cvg/CG/base.htm). Twelve gray scale images (256×256 pixels) are used. In addition, six watermark gray scale images (128×128 pixels) are used in this study.

Practically all images can be digitally watermarked; however, some types will yield to obtain the best results from using this powerful technology. This study uses the images of various types of format like, *TIFF*, *GIF*, and *PNG*. Besides that, the study test the images with uncompressed format (*BMP*) and (*JPEG*).

1.6 Significance of the Study

The work in this research sets a new direction for *ISB* via enhancing it by embedding two bits that can handle many limitations, and by embedding two bits in *LSB* method. This new direction will be used in this research to enhance the image quality using derivative mathematical equations which study the effect of all bits in the embedding process. This new direction will then be used to obtain the best robustness against attacks by using new sets of derivative equations. The study suggests making a tradeoff between image quality and robustness using *DISB*

technique to get a strong image, besides keeping image quality for the watermarked image as much as possible. The outcome of this research is a new technique, *DISB,* which can enhance the image quality and find the best robustness against watermarking attacks by embedding two bits.

1.7 Thesis Organization

This thesis is partitioned into six chapters. Chapter One focuses on digital watermarking and provides a brief description of the types of watermarking. The watermarking terminology and preliminary definitions are introduced. Furthermore, the chapter clarifies briefly the watermarking algorithm process of embedding and extracting. In addition, in the problem statement is elaborated and the objectives of the study are outlined, the scope of the study is also explained and the data set introduced, finally the significance of the study clarifies the contributions and the goals of the study.

Chapter Two reviews the previous works related to watermarking techniques. Since the number of related studies is numerous, only the most related studies with image quality and how to enhance the quality and lessen image distortion after embedding the watermark image are discussed. The robustness requirement is also reviewed in this chapter. Later, its narrows down to focus on the most common studies explaining the various models that used tradeoff between image quality and robustness. Moreover, the evaluation for image quality and robustness is discussed along with the measurement criteria that used for testing.

This is followed by the technique chosen for this study, which is called *ISB*, the review of this technique is focused on the mathematical equations, the image quality measurement which is called *PSNR*, *MSE*, and image robustness against attacks which is called *NCC*, *BER*. The optimal pixel value that uses *GA* is also clarified by several studies. In addition, the related works that deals with image quality, robustness, and the tradeoff between them are also reviewed. Finally, the summary of the reviews is at the end of this chapter.

Next, the proposed methodology in this work is elaborated in Chapter Three. This chapter explains the structure for the new technique and presents the methodology for this thesis to enhance algorithms for embedding two bits of the digital watermark image based on the *ISB* technique. In addition, this chapter introduces the data-sets and the tools that are used in this study. Besides that, it presents the enhancement of the *ISB* technique by using two bits, and clarifies the proposed methodology that is used to enhance the image quality by embedding two bits of the watermark image. Image robustness is also discussed. A tradeoff between image quality and robustness is presented. Also, the evaluation for the proposed algorithm is discussed and the measurements criteria are presented in detail. Finally, the summary of this chapter is presented.

Then, Chapter Four presents the proposed Dual Intermediate Significant Bits (*DISB*) method. First, the chapter presents the enhancements of *LSB* method and presents the *ISB* method by embedding two bits of watermark image. It also presents and explains in detail the *ISB* technique, and the proposed Dual Intermediate Significant Bits

(*DISB*) technique. In addition, the chapter presents the image quality algorithm based on the proposed *DISB* technique which is called *Quality_AGA* algorithm. Besides that, it presents the proposed image robustness algorithm based on *DISB* technique which is called *Robust_AGA* algorithm, then presents proposed the tradeoff algorithm between image quality and robustness which is called *Tradeoff_AGA* algorithm. The chapter also includes the mathematical Equations for *ISB* technique and *DISB* technique with flow-charts and pseudo codes for each of them. Finally, the summary of the chapter is presented.

This is followed by Chapter Five which presents the actual embedding of the watermark images based on the proposed *DISB* method, and the experimental results. Besides that, all the tables and figures that presents the results of the proposed technique are clarified. The experimental results of the image quality by finding the *PSNR* and *MSE* values for all embedding bits based on the proposed method are revealed. In addition, the results of the proposed algorithms compared with the existing *LSB,* and *GA* are presented through tables. The experimental results of the embedding process of the proposed image robustness and the calculating of *NCC* and *BER* to evaluate the image robustness are presented and clarified in tables and figures. Furthermore, the tradeoff between image quality and robustness is also included. The analysis of the proposed algorithms are included in this chapter through figures that explain the results.

Finally, Chapter Six includes the conclusion of this study, and the proposed future work with hopes of unlocking new ideas that can be developed and applied from this study.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

The art and science of transmitting undisclosed information in suitable carrier such as text, image, audio and video files is also known as data hiding (Thanikaiselvan et al, 2011). In the present digital world, it may be used in a considerable formulation to the data. The most popularly used format on the Internet (according to their reputation) are, *.txt*, *.bmp* and *.jpeg* (Brabin & Tamilselvi, 2013).

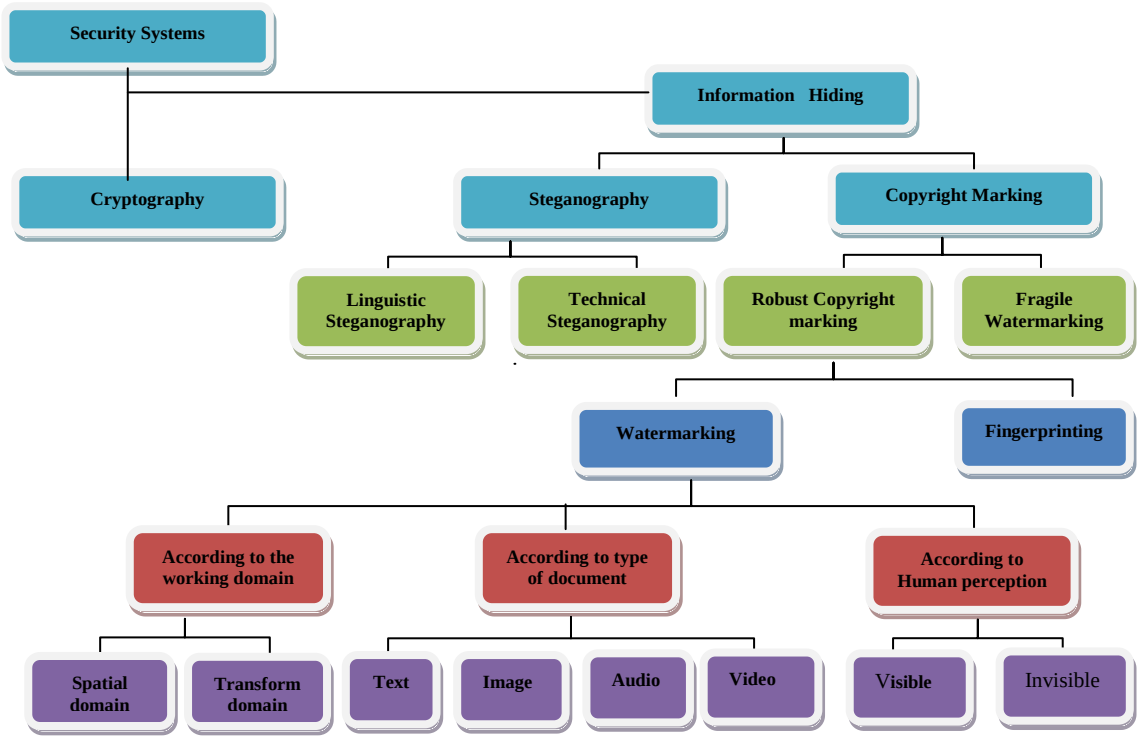


Figure 2.1. Classification for information hiding techniques (Petitcolas et al,1999)

As demonstrated in Figure 2.1, information hiding can be presented as a tree with branches. Watermarking and steganography are almost the same in the sense that

they both aim to use as little to almost no degeneration of the cover object in the process of inserting the information in the cover message. The only difference is that watermarking increases the image's resilience.

For the purpose of avoiding any form of illegal copying of data (piracy of data), the watermark is integrated. Thus, watermarking is also becoming a subject of argument. Watermarking has the ability to maintain the original image by keeping it intact and recognizable, which is different from steganography or encryption. Moreover, image watermarking can be divided into two that are noticeable (visible) and unnoticeable (invisible). Watermarking that is noticeable carries with it an image message that states the possession of that image specifically. On the other hand, an invisible watermarked image may seem the same except that it may not be like the original unmarked image (Ramani et al, 2008).

In relation to the problem in general information hiding, four significant parameters are usually used to ascertain that the watermarking scheme is of great value. They are robust, quality, (capacity) payload, and security. A tradeoff is involved between them as illustrated in Figure 2.2 (Al-Ataby & Al-Naima, 2010; Gunjal & Mali, 2013).

Digital watermarking is a method used to insert copyright details or other data into the underlying data; hence, the inserted or embedded information should preserve the original signal's value with respect to the two other requirements - robustness and capacity.

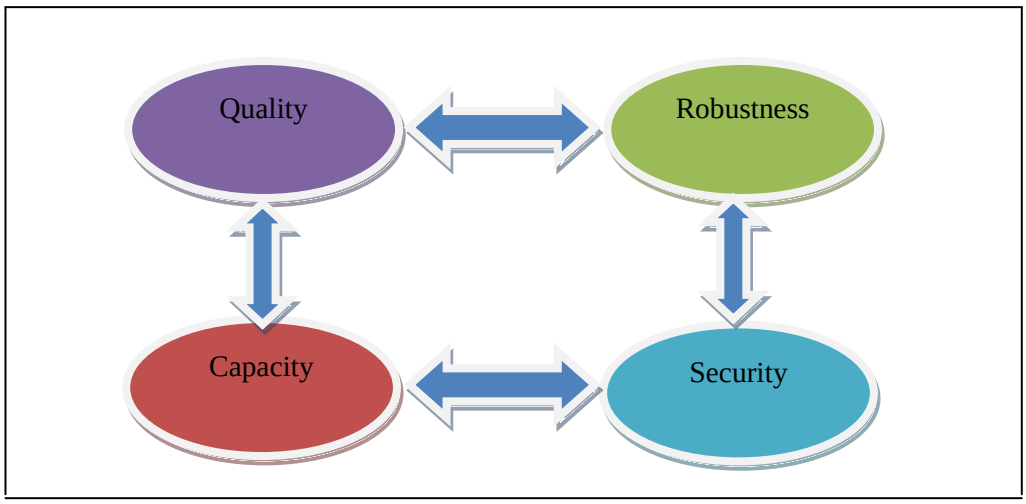


Figure 2.2. Watermarking Requirements (Al-Ataby & Al-Naima, 2010)

The first requirement is quality, which means that the value of the original signal should not be influenced by the watermark. The watermarking embedding is a kind of distortion of the host image. The perceptual invisibility of the distortion of the watermarking is the preliminary condition for common watermarking schemes (De-Santis, 2008). The second requirement is robustness, in which the watermarked data should be resilient to removal or elimination by unofficial distributors. Hence, it has to be resilient to certain signal processing operations, namely filtering, compression, and filtering with compression. Capacity is also required. This refers to how many bits are inserted at one go. In addition, the capacity of watermarking should be closely related to the image's content, whereby different watermarking apply to different images. Finally, security refers to the inability of the hacker to extract hidden information (Zhang and Zhang, 2004).

Quality and robustness have made watermarking a popular topic of discussion (Li and Yang, 2003; Podilchuk & Delp, 2001; Podilchuk & Zeng, 1998) that is why the study will focus on them. This study is focused on two requirements that are image quality and robustness.

In addition, many studies in the past used different datasets in terms of number of images, size of images, and the type of images etc., Saxena (2008) used four original gray and colored digital images with the size of 256×256 pixels for testing his proposed watermarking schemes, Peungpanich et al, (2010) used seven color images with the size of 256×256 pixels, on the contrary Hongqin and Fangliang (2010) used seven original grayscale images with the size of 512×512 pixels, Anwar et al, (2010) used ten standard images as cover images and the secret image, while Ishtiaq et al, (2010) used four standard images as the cover image to check the quality and the robustness of their proposed watermarking method, Lin et al, (2010) used four grayscale images as original images which are downloaded from USC-SIPI Data-base with size 512×512 pixels, Yang and Zhang (2009) used two grayscale images as original images with the size of 512×512 pixels and two images as watermarks with the size of 128×128 pixels.

2.2 Enhancing Quality of Watermarked Images and Handling Distortion

With the aim of ascertaining the proprietorship of a range of multimedia such as images, audio, and video, the method of digital watermarking is applied. Digital watermarking attains the exclusive rights protection of inserting a signal with certifiable data for originality (Peungpanich et al, 2010). Generally, the image quality

should be kept as much as possible and cannot corrupt by the watermarking system, whereas the inserted watermark should be recovered dependably.

In most cases, the watermark should be inserted using the chosen algorithm that does not affect the original data's value. If a distinction between the original data and watermarked information cannot be seen, the watermark becomes undetectable (Gulati, 2003).

Various studies on image watermarking have been done continuously in previous years. These studies can be categorized as spatial domain, transform domain, or both (Peungpanich et al, 2010).

2.2.1 The Transform Domain Techniques

In transform domain, many of the techniques of transformation are first implemented to the original image. Then the insertion process can be done by changing the coefficients of the transform field. The change that is used may be Discrete Cosine Transform (*DCT*) (Ahmad & Gaydecki, 2009; Dejun et al, 2009; Gunjal & Mali, 2011; Gupta & Jain, 2010), or Discrete Fourier Transform (*DFT*) (Ansari et al, 2012; Dubolia et al, 2011; Jun & Jun, 2009), Discrete Wavelet Transform (*DWT*) (Tripathi et al, 2010; Yongqiang et al, 2009).

In relation, Cox et al, (1997) proposed a watermarking technique by embedding a watermark in the *DCT* domain using the concept of spread spectrum communication. The authors realized that, in order to obtain a robust watermark, the watermark

should be embedded in low-frequency components of the image, and does not need the original data for extracting watermarks. The method adds the watermark to the image by modifying the 1000 largest coefficients of the *DCT* (excluding the *DC* term). These components are heuristically and perceptually more significant than others. An important open problem is the construction of a method that would identify perceptually significant components from an analysis of the image and the human perceptual system. Such a method may include additional considerations regarding the relative predictability of a frequency based on its neighbors. The latter property is important in combating attacks that may use statistical analyses of frequency spectra to replace components with their maximum likelihood estimate. The study showed that by using the Bavarian couple image, the proposed algorithm can extract a reliable copy of the watermark from imagery that is degraded with several common geometric and signal processing procedures. An important caveat here is that any affine geometric transformation must first be inverted.

A Discrete Wavelet Transform (*DWT*) based watermarking scheme proposed by Tripathi et al, (2010) makes use of both blind and non-blind algorithms. The highlight of the algorithms is that besides protecting the copyright of the Original image, they also protects the watermark from any misuse. Since the embedding process uses data from the source image, the extraction of the watermark by an unauthorized person is not possible. It thus serves the twin purposes of providing copyright protection to the watermark and increasing the security of the whole process. For this purpose, a new pseudo random generator based on the mathematical equations has been developed and used successfully at various stages in the

algorithm. The new concept of applying pseudo randomness in selecting the watermark pixels makes the process more resistant to attacks. In conjunction, the randomness is also incorporated in selecting the location to embed the watermark. Furthermore, the watermarked image was tested under various attacks and they found that the proposed technique is better than the contemporary techniques. The dependency of the watermark on the cover image makes the technique resistant to copy the attacks. It was found that the method is resistant to most of the commonly occurring attacks.

Finally, the proposed technique can be made more robust by introducing the concept of Fuzzy Logic, Adaptive Fuzzy Logic, or Neural Networks. Furthermore, Fuzzy Logic can be used instead of pseudo-random approach, in the selection of the sub-blocks, where the watermark pixels are to be embedded.

Besides a number of disadvantages of the transform domain have been discussed by Kao and Hwang (2005). In particular, while the transform domain is regularly more robust than the spatial domain techniques, it still loses some embedded data after performing the lossy compression process to the watermarked image (Langelaar et al, 2000; Wang & Pearmain, 2004). Therefore, users are not able to hide the text information in it (Chung et al, 2001). Earlier, Swanson (1996) cleared that the process of compression and hiding is extremely complex than the spatial domain.

On the other hand, Bhatnagar and Raman (2008) presented a semi-blind reference watermarking scheme based on *DWT* and Singular Value Decomposition *SVD* for

copyright protection and authenticity. They used a gray scale logo image as the watermark instead of the randomly generated Gaussian noise type watermark. In embedding the watermark, the original image is transformed into a wavelet domain and a reference sub-image is formed using directive contrast and wavelet coefficients. To embed the watermark into reference image by modifying the singular value of reference image, the singular value of the watermark is used. The reliable watermark extraction scheme is developed for the extraction of the watermark from distorted images.

2.2.2 The Spatial Domain Techniques

On the other hand, the watermark could be simply inserted into the original image through the other domain which is called spatial domain. This is done by modifying the gray levels of certain pixels that are present in the original image (Shih, 2010). The benefits are low complication and easy execution; however, this also makes the embedded data more vulnerable to detection through a computer analysis or attack. This is one area that an image is symbolized through the strengths at the known points in space, and the demonstration of image data usually uses it (Wu & Hwang, 2007; Chen et al, 1999).

The watermark has to be inserted this way since these methods are in accordance with direct alteration of the values of the image pixels. They are straightforward and computationally competent. They do not require difficult application and need very little computational power due to their ability to change the color, luminance or brightness values of a digital image's pixels (Asatryan & Asatryan, 2010).

A number of studies, (Bamatraf et al, 2010; Fridrich & Goljan, 2003; Hajisami et al, 2011; Maity & Kundu, 2002; Mohammad & Asad, 2006; Mukherjee et al, 2004; Nasir et al, 2007; Seddik et al, 2003; Singh & Gupta, 2011; Zeng & Wu, 2010) have used the spatial domain techniques.

Predictable spatial domain watermarking is the least dependable; hence, it is not widely used. It is here that changes are made to the pixels of indiscriminately chosen areas based on the signature of logo. Based on a predefined algorithm that might have different complexities in practical systems, the chosen image data are prevented slightly. The main drawback to this conventional watermarking is that removal from the initial image is made simple, which makes this method unsuitable for the authentication of copyright (Megalingam et al, 2010).

In this case, the transform domain watermarking method has shown better effectiveness in attaining the quality and resilience in comparison with the spatial domain method. However, too much data cannot be inserted in the transform domain since this will lead to a considerable deformation of quality of the original image (Dejun et al, 2009). Some disadvantages of this transform domain were presented by (Kao & Hwang, 2005). Although the transform domain is usually more robust than the spatial domain technique, it still loses some embedded data after performing the lossy compression process to the watermarked image (Wang and Pearmain, 2004; Langelaar et al, 2000).

In the spatial techniques, *LSB* is used to embed the watermark into the original image, so that the watermark can be embedded into an image without influencing the image's significance (Jain & Rai, 2012). The advantages of using this technique are it is very easy, fast, efficient, and the watermarked image quality might be simply controlled (Thapa & Sood, 2011). Furthermore, this method makes it possible for the insertion of small objects several times so that in the .event that there may be any loss of image that may occur through attacks, one remaining watermark would still be considered an achievement. This technique contains a range of variations. Generally, it includes logo insertion by substituting the *LSB* of the original image data with the information from the logo. The most common way used in watermarking utilizes a spatial domain, which involves the insertion of the watermark in the *LSB* of the image.

2.2.2.1 Enhancing Image Quality Using Least Significant Bit

Many studies have been carried out in this field using the traditional *LSB* or by embedding two or three bits as well as to enhance the quality (Aarthi et al, 2012; Bamatraf et al, 2010, Thapa & Sood, 2011), while other studies try to make the enhancement by using Genetic Algorithm (*GA*) (Mohamed et al, 2011; Zamani et al, 2009). It is considered as one of the important methods which support the quality enhancement of the watermarked image and it is represented widely as an optimization technique (Goyal et al, 2009).

When inserting information or data in a cover image, the *LSB* method is applied. Modifications are made to the pixels inside the cover image by bits of the secret

message. Based on the message, the 4 to 1 least bits have to be modified even with the inserted first 8 bytes of the grid. Generally, for the purpose of concealing a secret message with a cover image, only half of the bits in an image are modified. The low quality of the watermarked image (less than the 4-bit *LSB*) makes any change to the *LSB* of a pixel result in small changes in the intensity of the colors. However, these modifications are not apparent to the human eye. The changed bits can be obtained by a passive attacker due to this simple procedure (Bamatraf et al, 2010).

The first *LSB* has been recommended widely. In contrast, this proposed watermarking algorithm uses the third and fourth *LSB* to the data. As a response to the security reason, it is anticipated that the existence of the hidden data in the third and fourth *LSB* will not be anticipated. In accomplishing that, first, the image in grayscale is selected and the algorithm transfers the data into binary values after they are typed. Then, it hides the data in the image, and the watermarked image is obtained. Later, the data will be obtained by the receiver and removed from the watermarked image (Bamatraf et al, 2010).

A bit plane can be defined as – a set of bits with the same position in relevant binary numbers, which is also known as a bit-plane of digital images (Zeki & Manaf, 2009). For image penetration, eight similar bits are formed from the grayscale of every pixel; the first bit-plane includes a set of the most important bits and the 8th bit-plane includes the least important bits. Computation and the insertion of a load of data which help maintain a good level of quality are made easier with *LSB*. For any insertion, the added LSBs are used that cause further deformed results. Not all pixels

in an image can tolerate a huge quantity of modifications without making it obvious. The main number of the *LSB*s with modified gray values that do not produce a detectable artifact in each pixel is distinctive. Apart from that, according to Wu and Tasi (2003), the modifications of the gray values of the pixels in the images' smooth areas are further easily noticed by human eyes (Zeki et al, 2011).

Yet another easy and resilient watermarking method with random mapping features is proposed. This algorithm carries with it the idea that watermark embedding can be more resilient compared with the traditional *LSB* method. It makes the secured random coordinate of the cover image enhance the resilience of the watermarked image. It has been found that the watermarked image contains a higher quality in the case of the proposed scheme compared to the use of the *LSB* method (Lee et al, 2008).

Furthermore, a study by Kumari et al, (2009) used an *LSB* method via inserting the watermark. The study showed that there are three possibilities after the embedding process: i) no changes on the value of the pixel, ii) the value of the pixel increases, and iii) the value of the pixel decreases to one. The study divides the image into a non-overlapped window of a predefined size. Any window of the size (*m x m*) will be having (m^2) pixels. Each pixel in the window is represented by a location (xi, yj) and a gray level value of *pi*. By embedding a bit in *LSB*, the *pi* value will have the following three cases. Case 1: *pi* values may be the same, if the corresponding *LSB* of *pi* and embedded bit are the same i.e., 1 or 1 and 0 or 0. Case 2: *pi* values may be incremented by one, if the LSB of *pi* is zero and embedded bit value is one. Case 3:

pi values may be decremented by one if *LSB* of *pi* is one and embedded bit value is zero. If the *pi* is even, its *LSB* is zero; therefore, its value will be changing as represented in Case1 or Case 2. If the *pi* is odd, its *LSB* is one; therefore, its value will be changing as represented in Case1 or Case 3. Based on the above three cases, the present method found that the ambiguity of pixel values will be rising at the time of reconstruction between successive even and odd values. To overcome this present method, it is essential to treat the successive even and odd values of the window as the same, i.e., *ni* and *ni+1*, where *ni* is an even number, and the difference of *ni+1* and *ni* is always one. The method is applied on more than 32 different images with different sizes. However, the present work shows four of them are of the size of 100 × 100, and converted each character of the watermarked text as 12 bit code by dividing each character value by mod 9. The four-bit remainder is appended to make 8 bit text character, as 12 bit character. The method identified would overcome with a solution for the ambiguity of gray level values, which arose between successive even and odd values after inserting the watermark using *LSB*.

Bamatraf et al, (2010) produced an easy and resilient watermarking algorithm the 3rd and the 4th *LSB* method. This is for the sole purpose of defense, so that the hidden data is not expected to be in *LSB*s three and four. First, the image in a grayscale image is selected and the data is transferred to a binary value after being typed. Then, the data is concealed in the image with the algorithm. The watermarked image is then received, data retrieved back, and that data is extracted from the watermarked image. Four cover images of 512 × 512 pixels grayscale images were utilized. The first was for the insertion of secret information containing 128 bytes in determined pixels in

LSB three and four, and then the retrieval of watermarked images without visible deformation and subtracting the watermarked image from the initial image to contrast. The second was for the insertion of similar secret data containing 1023 bytes in the four images, then retrieving the watermarked images with no obvious deformation and deducting the watermarked image from the initial image to discern them. Because of the modification in *LSB* three and four, a black image will be noticed as a distinction between the initial image and the watermarked image. The values of the 3rd and 4th *LSB* are 4 and 8 respectively, and 12 is the ultimate distinction of the pixels between the two images, the value 12 in grayscale images is nearly black.

Another block-based multiple-bit spatial domain spread spectrum image watermarking system was proposed by Ghosh et al, (2009) where a gray scale watermark image is represented by less number of binary digits using channel coding and spatial bi-phase modulation principle. The method developed an image-watermarking algorithm that can serve the purpose of media authentication as well as secure the communication of an image like a message signal in real time environment. This has been accomplished by exploiting the strong spatial correlation of the neighboring pixel values of the cover image. The method is made here for the cover image of the size 256 × 256 with 8 bits per pixel. On the other hand, the watermark image size taken was 64 × 64 with 4 bits per pixel. The cover image is partitioned in 8 × 8 non-overlapping blocks, and watermark image in 2 × 2 non-overlapping blocks. The proposed watermarking is based on the combination of channel coding and spread spectrum technique. The binary of watermark image of

the size 32 × 32 is obtained using spatial bi-phase modulation by assigning a binary digit for a substring consisting of 64 symbols. The algorithm is simple with low computation cost and can be easily implemented in hardware. Digital design of the proposed algorithm is also developed and thus makes it suitable for real time authentication as well as secured communication.

A modified *LSB* embedding approach has been proposed recently. The main goal for this study is to make enhancement for the common *LSB* by using two bits from the watermark into each pixel of the original image (Aarthi et al, 2012). To make the embedding process for data into a cover image, the *LSB* method is applied. The application of the *LSB* method means that the pixels which are inside the original image will be replaced with bits from the watermark; these bits represent the secret need to be hidden. These modifications are not apparent to the human visibility system, but can easily be detected by several types of image attacks. The proposed method used one cover image with the size 256 × 256, while the size of the watermark image applied with many size in each time of embedding is, 50 × 50 and 100 × 100. The *LSB* scheme is chosen for the proposed work. The conventional *LSB* scheme provides low embedding rate and low distortion and is irreversible. However, the conventional *LSB* scheme uses only one bit in every pixel for embedding. The proposed scheme presents a modified *LSB* embedding strategy that satisfies the reversibility and improves the embedding rate by using two bits in every pixel for embedding. The higher the *PSNR* values, the better the quality of the image. Since the secret data is embedded in the 3rd and 4th *LSB* bits of each pixel, it has been noticed that there are some changes with the value of the pixels. Because of this, the

proposed algorithm's imperceptibility went down. That is why the conventional *LSB* scheme cannot be used for critic applications where reversibility is mandatory.

Khodaei & Faez (2012) suggested an adaptive data-hiding technique based on *LSB* replacement and pixel and value differencing (*PVD*) for grayscale images. The method divides the cover image into some non-overlapping blocks containing three consecutive pixels, and picks the second pixel of each block as the central pixel (called base-pixel). Then, *LSB* replacement is applied to insert k-bits of secret data in the base-pixel by using optimal pixel adjustment process (*OPAP*). The quantity of secret bits that can be inserted in the two pixels is decided through the dissimilarity between the base-pixel value and other pixel values in the block. In this procedure, the differences are classified into lower level and higher level with a number of ranges. Then, the number of secret bits that are to be inserted into each block is gained based on the range which the different values belong to. A huge quantity of secret information can be implanted with this procedure while maintaining a high visual quality of the stego-images. Compared to other three data-hiding methods which are investigated in this study, the *PSNR* values and the embedding capacity of the proposed technique are greater. In the experiments, ten grayscale images with the size of 512 × 512 are used as test cover images. Moreover, the secret data bits are generated by a random number generator. Generally, for evaluating the performance of data hiding method, four criteria are utilized: the distortion and the visual quality of the stego-images, the embedding capacity, the complexity and the security of the embedding hiding algorithm. These factors are conflicted together and the data-hiding methods rarely can prepare all these factors at the same time. The proposed

method tried to satisfy these performance criteria. Their algorithm can embed a large amount of secret data while maintaining acceptable image quality. However, their proposed algorithm only has fixed embedding capacity. In addition, the derivation for three consecutive pixels in the boundary region is poorly manipulated using raster scan order, resulting in inaccurate pixel differences.

Another study proposed by (Chan & Cheng, 2001) is for an improvement to efficiency and an enhancement to image quality. The *MSB* is called the first bit, while the *LSB* is called the eighth bit. With the use of the optimal substitution process and local pixel adjustment process, the image quality of the resulting stego-image is much better than that of the simple replacement method. However, the optimal substitution process may require a huge computational cost for the *GA* to find an optimal permutation matrix. Moreover, the local pixel adjustment process operates only on the last three bits (bits 6-8) and the fourth bit but not on all bits. As a result, the local pixel adjustment process may not be optimal. The *GA* is not required and the local pixel adjustment process is modified to operate on all of the bits except the fifth bit, which is used to embed the data, and the bit location will be rearranged according to a key to avoid possible attack.

A study proposing an adaptive data hiding algorithm based on *LSB* substitution and *PVD* for gray-scale images has been conducted by Tsai et al, (2014). The main point of this algorithm is to use a dynamic block subdivision to replace pixel traversal. This algorithm also consists of three phases: the range division, data embedding, and data extraction. The study used 8 gray scale images as cover image with different

sizes of blocks. The experimental results are obtained from eight commonly used grayscale images. Furthermore, the pixels in the boundary region can be manipulated, allowing accurate pixel differences to be derived for data embedding. The embedding capacity and image quality in the proposed algorithm can be adjusted according to the block size. This study demonstrates the feasibility of this technique for adaptive data hiding with the support of experimental results. In time ahead, they hope to integrate the image interpolation scheme and then perform pixel difference calculations to consider both the embedding capacity and image quality.

Another method using 3 *LSB* watermarking techniques has been proposed by Dadkhah et al, (2012), which is able to authenticate the digital image and detect the tamper locations accurately. The proposed method improved tamper detection technique. In the proposed algorithm a 12-bit watermark key is created from each block of original image, which is embedded to the last three significant bit of each block. The proposed tamper detection method consists of two parts which both are the comparison of the content of the 12-bit that has been watermarked to original image. In the first level, the average intensity bits are compared, which are the last 2 bits of the 12-bit, whereas the second level is the comparison of the remaining 10 bits, in which all have to be identical, otherwise tampering will be occur. The experimental result clearly proved the efficiency of the proposed method.

Hsieh et al, (2000) introduced a general concept called *(n+k)/n* method to improve the cover image quality for all traditional watermarking techniques, and another special case for *(n+1)/n* method is also proposed. In *(n+1)/n* method, an intermediate

set is derived from the information set by a simple Exclusive-OR operation. In the algorithm, the intermediate set is embedded rather than embedding the information set directly. As a result, the number of feature modifications for embedding the intermediate set was found 25% less than that for embedding information set directly. Additionally, the quality of the cover image applying the proposed *(n+1)/n* method was 2.5db better than the traditional one.

Yin et al, (2002) proposed an embedded annotation data, museum copyright logos, and fragile watermarks simultaneously within an archive image. In their works, the annotation data are embedded within eight surrounding pixels of each 3 × 3 image block using the *LSB* replacement method. The multiple copies of annotation are also embedded, in which each copy of the annotation was separated by boundary line signals that are embedded together with the fragile watermark. The annotation data within the cropped images could always be extracted if any two consecutive vertical and horizontal boundary lines (which embraced a square area) could be found. On top of that, a museum copyright logo is also embedded to prove the ownership of the archived images. Furthermore, a fragile watermark, based on the *HVS*, is embedded in the central pixels of 3 × 3 blocks imperceptibly. Hence, any alteration to the watermarked image could be detected and located with a high probability.

Al-Jaber and Aloqily (2003) then introduced an algorithm which makes use of the *LSB* method to embed the information within the inhomogeneous areas of the cover image. In the algorithm, an error correction code is used to increase the probability of retrieving the message, and to enable the receiver to detect any alterations in the

cover media. In this case, the receiver informs the sender about such alterations. This model makes use of the *HVS* properties and embeds the message in the most important areas of the image. Experimental results prove that this method is efficient and effective to be used, in addition to the finding which reveals that it produces high quality images.

Another study for watermarking colored images (such as cartoon images, line-draw images, binary images, maps and the like) was proposed by Pan et al, (2002). The main idea of this algorithm is to use the prioritized sub-blocks by pattern matching in selecting the pixels with the least visual quality reduction of embedding. In the algorithm, a sub-block with the size of 3×3 is employed to evaluate the embeddable priority of its central pixel by examining its eight neighbors. Each sub-block is associated with a rank, indicating the effect on its visibility by assuming the change of the central pixel. The higher rank implies that the alteration of the central pixel reduces less visual quality, and it should have a higher priority for embedding. It was found that the algorithm performs well.

In the scheme proposed by Kailasanathan (2003), the polarity of the central pixel of an image block is determined by calculating the differences between the center pixel of the image block and the means of the image block pixels. Additionally, a fragile watermarking scheme, which embeds the marks on the central pixels of the image blocks based on the polarity of the pixels, has also been proposed. Then, the security level of the scheme and the possible extension to multiple watermarking schemes are investigated.

In detail, the most common way used in watermarking utilizes a spatial domain that involves the insertion of the watermark in the *LSB* of the image. This enables the logo to be inserted into the original image by trying to keep the quality of watermarked image as much as possible. On the other hand, the *LSB* is not resilient against attacks.

2.2.2.2 Enhancing Image Quality Intermediate Significant Bit (ISB)

The main idea for the proposed technique depends on bit plane model which means "takes a bit-plane of digital images as a set of bits having the same position in the respective binary numbers". According to this study, grayscale image depiction contains eight bit-planes, a group of the Most Significant Bits (*MSB*) being in the first, and the *LSB* in the 8th. The Intermediate Significant Bits (*ISB*) are placed from the 2nd to 7th bit-planes (Zeki and Manaf, 2009).

The important thing when the embedding process has been done is to keep the quality of watermarked image as much as possible. If the original image and watermarked image cannot be differentiated, the watermark becomes unnoticeable. Nevertheless, because the original image of the watermarked image is not easily attainable, comparisons cannot be made. Hence, it is essential the changes in the watermarked image are imperceptible since it is not compared with the original image (Gulati, 2003; Shelby, 2000). In the meantime, the highest value of the input signal (frequently 255 for 8 bit grayscale images) is the Peak Signal to Noise Ratio (*PSNR*) (Eggers et al, 2000). After inserting the logo, the *PSNR* is applied for the watermarked image's quality assessment. No typical significance is contained in the

PSNR; nevertheless, the image property gets better as the *PSNR* gets bigger. An adequate quality of watermarked image regarded by many is when the *PSNR* is greater than 30 db (Zeki, 2009; Bennour, Dugelay; and Matta 2007), some need it to be 34 db (Cheung, 2000; Eggers, Su, & Girod, 2000), and others require 38 db as an adequate image quality (Hosinger and Rabbani 2000). According to these illustrations, an adequate image quality for this research is a *PSNR* value equal or larger than 30db.

In accordance with the parameters of every bit-plane, Zeki and Manaf, (2009) evaluated the position of the watermarked pixel. Hence, if it is located in the middle, when the pixel is affected by any attacks, this causes complexity in the moving of a chosen bit to a new location. The study used watermark object (logo image) which is in grayscale level image. It contains 90 × 90 pixels and will be embedded within the original grayscale level image which contains 256 × 256 pixels. The embedding is done with all bit-planes and few different types of attacks have been applied to the watermarked image in order to test the robustness of the proposed technique. However, any minor modification by attacks on the pixel value that is positioned on the outer range will move the pixel from one range to another. The result showed that the 4^{th} bit-plane, in which the distance from the edge of the range for the position of the watermarked pixel was 6, was where the best-obtained logo from the undistorted watermarked image can be found. To conclude, the study contributes to the body of knowledge by replacing the classic *LSB* method with a new one called *ISB*, which develops the resilience and makes sure the value of the watermarked images is intact. The *ISB* assisted in locating the threshold values for the greatest embedding status.

Another proposed wavelet based Digital Watermarking approach with two steps is by Perumal & Kumar (2011). In the first step, a Threshold based on Intermediate Bit Values (*TIBV*) of image pixels is proposed by selecting the image pixel for inserting the watermark. In the second step, Al-attar's method is used for inserting the Digital Watermark bits in the selected pixels of the first step. These two steps make the proposed *TIBV-DW* method more efficient and hard to break. To test the efficacy of the proposed *TIBVDW* method, various statistical measures which indicate a high quality, un-ambiguity, confidentiality and integrity of the present technique. The proposed method embeds more than one bit by using Al-attar's method in the selected pixels based on *TIBV* approach in a single pass using wavelet decomposition and also derives high embedded image quality.

Finally, an approximation approach is proposed by Emami et al, (2012) for identification of the rightful owner of the property by utilizing the remaining information of the attacked watermarks regardless of the attack behavior. Here, the ownership of the property is identified by coupling the *BiISB* (Duo-ISB-Bit-Plane) watermarking algorithm with the *HI* (Histogram Intersection) technique. In *BiISB* approach, while the main watermark delivers the ownership identification information, the sub-watermark, which is a bit-pattern histogram, is the statistical information regarding the main watermark. In addition, three bit-pattern histograms, namely - original, extracted and computed sub-watermarks have been used for approximation purpose. An investigation has been achieved using a standard Lena grayscale original image of 512 × 512 pixels, a trademark image of 38 × 89 pixels as a sub-watermark. The proposed approach was successfully achieved by preserving

the quality of the watermarked image and, simultaneously, identifying the ownership of the property.

2.2.2.3 Enhancing Image Quality Using Genetic Algorithm (GA)

One of the most important algorithms used to enhance the image quality and robustness is *GA*, in which can be found an appropriate position in the original images to embed a watermark in a way that retains the image quality. Particularly, spatial domain techniques are known for poor values of fidelity, although they are simpler to implement. The study proposed a technique which employs *GA* that used normalized correlation of the cover image and watermarked image as the basis of fitness function that needs to be optimized and works by searching appropriate embedding locations of watermarks within the cover image which are treated as the population of the *GA*. This is the reason of the wide application of *GA* in optimal areas. Figure 2.3 describes a simple *GA* in its simplified form (Goyal et al, 2009).

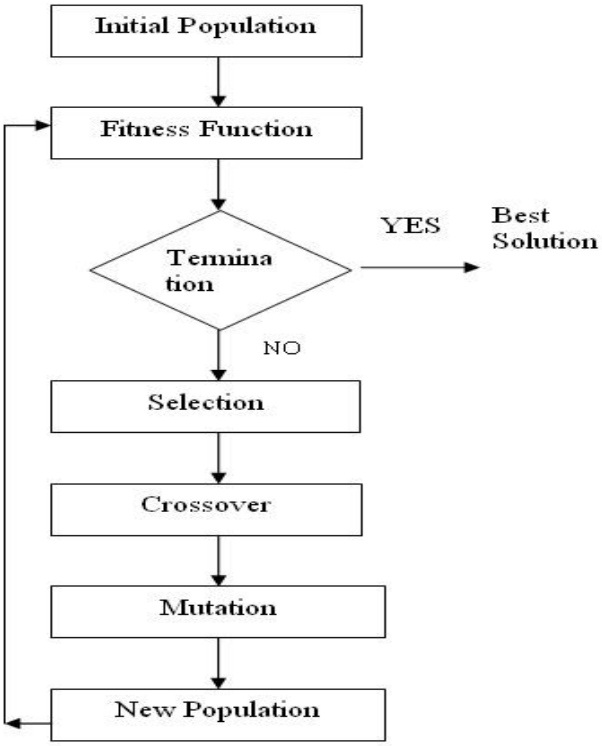


Figure 2.3. Genetic Algorithm process (Goyal et al, 2009)

Another study introduces a method of adaptive blind digital image watermarking in the spatial domain (Anwar et al, 2010). In this study, both cover and secret images are partitioned into equally-sized blocks. Then, the original for each secret image block is intelligently selected through *GA* which helps in identifying the target blocks of the cover image such as that with the *LSB* embedding, the visual quality of the cover image and quality of secret image remain less affected. At the watermark extraction phase, only the watermarked image is required in which using Jigsaw Puzzle Solver (*JPS*), the secret image is reconstructed. For experimental purpose, the study used some of the standard images as cover images and secret image. While embedding watermarks, the sizes of both the cover and the secret image were kept similar. The results are first calculated by embedding the secret image into the cover

image by using conventional single *LSB* replacement method and then the same experiment was repeated by doubling the payload of the secret data into the cover image i.e. replacing 2 *LSB*s of the cover image by the secret image bits. While in watermark detection process, a random image is extracted by extracting linear *LSB*s of the stego-image the method increases the payload 2 times and keeps the quality.

Wang et al, (2000) proposed a data hiding technique in storing and transmitting important data. Their technique embeds the important data in the Moderately Significant Bit (*MSB*) of an image, and applies a global substitution step, as well as a local pixel adjustment process to reduce any image degradation using the Local Pixel Adjustment Process (*LPAP*). In the first step, a polynomial transformation (Rhee, 1994) is applied to cipher the watermarked image and obtain a perturbed image. In the second step, the MSB (the fifth bit) of all the pixels of the original image is extracted to form a (binary) residual image. In this step, the *MSB* is called the first bit while the *LSB* is referred to as the eighth bit.

Wang et al, (2001) incorporated a *GA* to solve the problem of hiding important data in the rightmost *LSBs* of the original image, which involves a huge computation time to find the optimal result when k is large. The disadvantage regarding to computational time is also explained by Chan and Cheng (2001). It should be noted that the optimal substitution process requires a huge computational cost for the *GA* to find an optimal permutation matrix. Moreover, the local pixel adjustment process operates only on the last three bits (bits 6-8) and the fourth bit, but not on all the bits. Hence, it was found that the local pixel adjustment process may not be optimal.

Further, Chan and Cheng (2001) proposed an improvement to the scheme introduced by Wang et al, (2000) to improve its efficiency and enhance the quality of the image.

In relation, Chan et al, (2004) also obtained results for data hiding scheme in embedding the k number of bits together within the *k* bit-planes, by an optimal *LSB* substitution and *GA*. Using the proposed algorithm, the Worst Mean Square Error (*WMSE*) between the cover-image and the watermarked image, is shown to be ½ of that obtained by the simple *LSB* substitution method. As a result, the quality of the watermarked image could greatly be improved, with low extra computational complexity.

Previously, Changa et al, (2003) proposed an optimal *LSB* substitution in image hiding using the dynamic programming strategy. Although the method proposed by Wang et al, (2001) was proven to reduce the computation time, the results it achieved were not optimal, but they were rather "approximately" optimal solutions. Changa et al, (2003) made use of a dynamic programming strategy to solve the optimal *LSB* substitution problem. In accordance, it was found that the method significantly reduced the computation time and also achieved an optimal solution.

On the contrary, Hala and Zayed (2005) implemented a technique for hiding secret data in images. Their technique combines two methods to improve the quality of images, namely the optimum substitution matrix and pixel adjustment process. The optimum substitution matrix replaces the *K-LSBs* of the data by other optimum values to minimize the difference between the carrier image and the secret data. It

was found that the optimum substitution matrix is a computationally expensive process. In addition, they implemented a dynamic programming strategy to find the optimum substitution matrix. After applying the optimum substitution matrix and the secret data was hidden in the image, a pixel adjustment process was used to decrease by about half of the Mean Square Error (*MSE*) between the watermarked image and the carrier (original) image.

2.3 Enhancing Robustness of Watermarked Image

The second important requirement of watermarking schemes is robustness against image attacks. Copyright authentication or secret communication can be achieved through digital image watermarking.

Watermarking attacks are, in fact, exploitations of image, whereby different processes can be implemented to images, which then cause geometric alterations, and remove and change watermark objects from the image (Juergen, 2005).

Watermark attacks can be classified into four types, which are protocol attacks, geometric attacks, removal attacks and cryptographic attacks (Geetha et al, 2011).

Removal attacks try to remove the watermark signal from the watermarked image by not breaking the protection of the watermark algorithm. It is not concerned with the encryption methods used or how embedding was performed (Song et al, 2010). The classifications of removal attacks can be comprised of blurring sharpen attacks, noising, and histogram equalization (Geetha et al, 2011).

Geometry attacks, on the other hand, differ from removal attacks, whereby the goal is to alter the watermark signal instead of damaging it. However, there is still the probability of recovery of the original watermark by the detector if there is a way to determine the geometry attack and apply counter measure. This correctional procedure is called synchronization, which can be extremely costly and time consuming. Image rotation, scaling, and translation and skewing are classified under watermark attacks.

Cryptographic attacks are aimed at breaking the procedure used for security in any watermarking schemes and finding reliable methods to eliminate inserted watermark data or to embed confusing watermarks. The brute-force method is one example, which tries to break the defense of the watermark by applying a huge number of ways to look for any meaningful secret data (Song et al, 2010).

Another type of watermark attack is known as protocol attacks. Protocol attacks make the attacker's own watermark signals available in the data that is questioned, which causes the real ownership of the data to be vague and doubtful. This totally differs from other attacks, which only destroy, distort or extract the watermark signal. Protocol attacks go for the whole idea of applying watermark techniques as a resolution to copyright protection.

Copy attack is yet another form of protocol attack that takes an estimation of a watermark from watermarked information and copies it to another data known as target data. In order to satisfy its vagueness, the watermark estimation that is derived

is modified to the features of the target data. These classifications of watermark attacks are summarized in Figure 2.4 (Song et al, 2010).

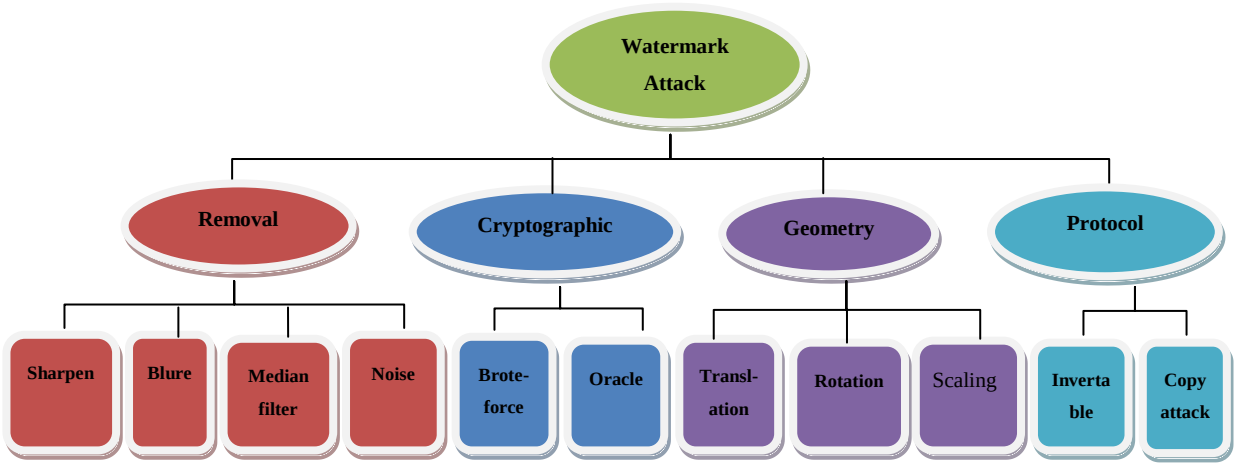


Figure 2.4. Watermark attacks classification (Song et al, 2010)

There is always the possibility of a watermarked image being exposed to certain deliberate and unintended exploitations, for example, *JPEG* compression, Speckle noise, cropping, blurring, Rotation and Gaussian filter. The attacks of watermarking refer to the exploitation of an image, whereby various processes are applied to images. This leads to geometric deformation as well as elimination or change of the watermarked objects from the image.

Ample numbers of watermarking methods that can be subdivided into different practical and difficulty stages have been generated by studies in watermarking areas. They all aim at lowering the weakness in numerous attack situations.

A variety of image watermarking techniques have been proposed to focus on the robustness to common attacks like compression, noise, cropping, and geometric (Gao et al, 2010; Kumari et al, 2009; Megalingam et al, 2010)

This study has chosen five attacks, which apply to the watermarked image. The attacks are *JPEG* compression, Speckle noise, blurring, Wiener and Gaussian filter, respectively.

2.3.1 Enhancing Image Robustness Using LSB

A study on a robust method for digital watermarking in spatial domain has been discussed (Megalingam et al, 2010). The technique manages an image in the spatial domain which is watermarked at different intensity subsections. Moreover, provided is the evaluation of the projected spatial domain technique with the frequency domain technique. By deducting the original image from the watermarked image, the normal watermark can be removed from the conventional spatial domain watermarked image. Only the expected user using the same key at the receiver's end can remove the watermark. This would avoid any eavesdropper from removing the data embedded in the watermark, which makes the method suitable in the security aspect as well. The resilience of this watermarking method can also be authenticated with pseudo random noise with the watermarked image. Hence, an intruder is not able to remove the watermark if he does not have the appropriate key that is multiplied by the image.

Another study proposed an alternative watermarking technique based on spatial *LSB* modification (Chen & Lu, 2012). It is robust against moderate *JPEG* compression, while keeping all the features of LSB. The study used quantization to resist *JPEG* compression, and used *DCT* based *JND* model to reduce image quality deterioration. The embedded watermark is more robust against usual spatial *LSB* based watermarking techniques. However, it may still suffer from deliberate attacks and color level manipulation.

In addition, a spatial domain watermarking scheme using simple error control coding technique has been proposed (Rohith & Bhat, 2012). The idea of this scheme is to embed an encoded watermark using (5, 1) repetition code inside the cover image pixels by *LSB* embedding technique. The proposed algorithm is simple, more robust against salt and pepper noise than *LSB* only watermarking techniques. In this study, a comparison is made between embedding different watermark encoding schemes such as (7, 4) Hamming code, (3, 1) repetition code, (5, 1) repetition code, and without encoding for different noise density of salt and pepper noise. The watermark encoding scheme using (5, 1) repetition code provides better robustness towards random error compared with other said schemes, without much degradation in the cover image.

Another technique proposed by Maity and Kundu (2002) describes the robust and blind digital image watermarking in spatial domain which is computationally efficient. The embedded watermark is meaningful and recognizable rather than a sequence of real numbers that are normally distributed or a Pseudo-Noise sequence.

Also, this proposed technique has been tested over a large number of benchmark images as suggested by the watermarking community, in which the results of robustness to different signal processing operations are found to be satisfactory. Currently, investigations are being carried out to insert the same watermark symbol in other region of the cover image. It is also to make the present scheme more resilient to other types of external attacks.

Hajisami et al, (2011) proposed a blind watermarking idea for copyright protection in which the embedding is implemented in a cumulative form with different embedding strengths, and the watermark extraction uses two watermark images and applies the Independent Component Analysis (*ICA*). Extracting the watermark in this method requires no needs for the original image, because the watermark or the key and the extraction are completely blind. Furthermore, the *ICA* is applied in the extraction results in robustness of this method against a variety of attacks, including noise addition, resizing, low-pass filtering, multiple marks, grayscale reduction, rotation, *JPEG* compression and cropping parts of the image.

Darmstaedter et al, (1998) designed an approach for embedding a code into an image. The technique is based on the image spatial decomposition in blocks and the classification of the pixels in homogeneous luminance zones. In detail, one bit is embedded into one block of 64 pixels (8 × 8 pixels); in which the code is embedded in the relationship order between the mean values inside the zones. Additionally, the influence of the different embedding parameters on the visibility and the resistance of the code were also studied.

Another study which introduced, a fast two-layer image watermarking was proposed by Liu (2001). This two-layer watermarking means that two types of watermarking techniques are simultaneously employed to hide the same watermarks in the spatial domain, more specifically the first layer watermarking which resists high-frequency destruction, while the second layer which resists the low-frequency destruction. Although the image was modified through the two-layer watermarking, the watermark was still invisible.

Pieprzyk et al, (2000) described a robust spatial domain watermarking algorithms for the image copyright protection. The method is robust against compression, filtering and cropping. Agreeing with the all published crop-proof algorithms, the proposed method requires the original image for the mark recovery. In particular, the robustness against compression and filtering is obtained using the *JPEG* algorithm to decide on the marked location and magnitude (the method compresses the image many times and maintains the embedded information every time); while the robustness against cropping is achieved through a repetition code.

Lin and Tsai (2004) presented a robust watermarking method against *JPEG* compression, which is difficult for collusion attack. The technique of block-oriented and modular-arithmetic-based watermark embedding and extraction were found to be robust enough against image processing such as lossy compression, filtering, and cropping. Meanwhile, the random perturbation of the pixels within the marked block, as well as the unique and fused watermark information, resulted in different images with irregular-shape and uneven-luminance blobs, which greatly increased the

difficulty of collusion attack. Although the method can embed the watermark within good image quality, it is not able to survive in front of the lossy compression attack. In addition to this, the system needs to use the original image during the extraction process because the attacks change the contrast of the image.

2.3.2 Enhancing Image Robustness Using ISB

A developed robust watermarking model using the spatial domain technique, and at the same time maintaining important watermarking requirements of picture quality and reasonable capacity is proposed by (Zeki, 2009). This model was generated based on the intermediate significant bit (*ISB*) to substitute the watermarked image pixels with new pixels. This can shield the watermarked information against attacks while maintaining the new pixels very close to the originals. The technique was done in accordance with the testing of the value of the watermarked pixel based on the range of each bit-plane and positioning the watermarked pixel away from any of the edges of the range. The best pixel value that lies from the middle to the edge of the range that is also known as threshold value was developed to secure the watermarked object from various types of attacks and maintain the minimum distortion of the watermarked image.

The technique embedded one bit-plane of the watermarked image into each pixel of the original image. After selecting one bit-plane for embedding, comes creating sets of ranges for the selected bit plane.

The length of range is calculated according to Equation 2.1:

$$L\_range = 2^{k-1}. \quad (2.1)$$

where *k* is the selected bit plane.

Therefore, the number of ranges in each bit-plane can be found according to Equation 2.2:

$$N\_range = 256/L\_range \quad (2.2)$$

This is followed by dividing each range into two equal groups. The length of each group is calculated using Equation 2.3:

$$L\_group = L\_range/2. \quad (2.3)$$

The proposed technique above can be explained by dividing each range into two equal groups, as seen in Figure 2.5 below.

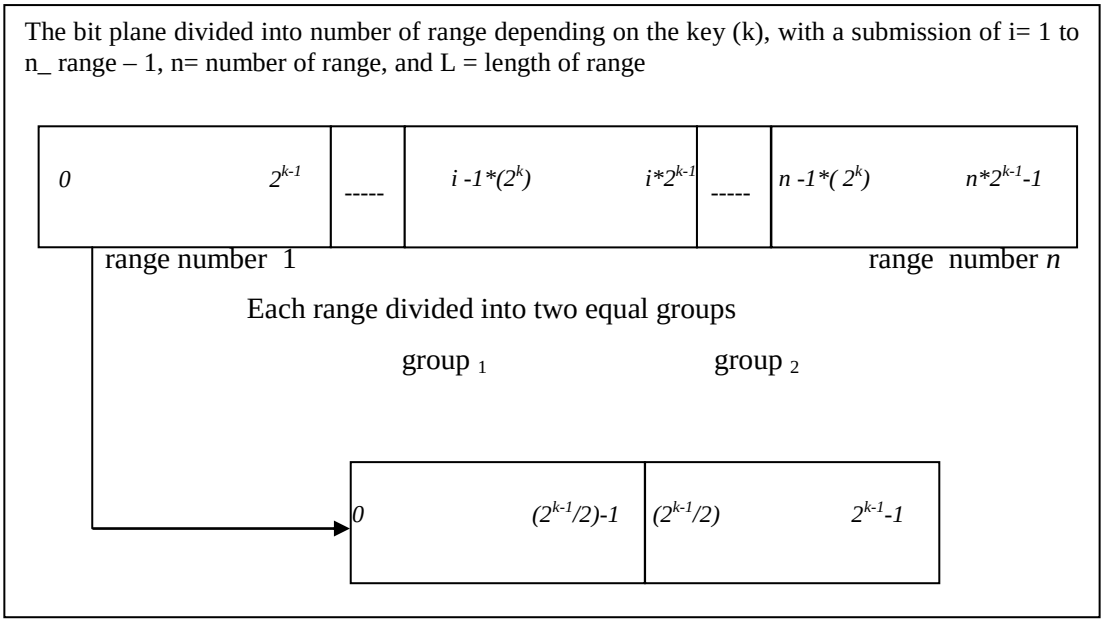


Figure 2.5. The general ISB technique

This means that there is a change of bit between 0 and 1 in each range. For the first bit plane, two is the only number of ranges, either [0:127] or [128:255]. This means that the first range has a bit of 0, whereas the second range has a bit of 1 with a length of 128 for each range of the first bit-plane. In contrast, there are 4 ranges for the second bit-plane: [0:63] [64:127] [128:191] [192:255], and the length of the ranges is 64, and so on, as shown in Table 2.1.

Table 2.1

Ranges of each Bit-Plane with the length

Bit –Plane	Length of the ranges	Number of ranges	Ranges
1	28	2	[0:127] [128:255]
2	64	4	[0:63] [64:127] [128:191] [192:255]
3	32	8	[0:31] [32:63] … [192:223] [224:255]
4	16	16	[0:15] [16:31] … [224:239] [240:255]
5	8	32	[0:7] [8:15] … [240:247] [248:255]
6	4	64	[0:3] [4:7] … [248:251] [252:255]
7	2	128	[0:1] [2:3] … [252:253] [254:255]
8	1	256	[0] [1] … [254] [255]

From the above table, it is obvious that the proposed technique used a new way to make sure to reach the existing bit in the pixel of the embedded.

A robust blind watermarking method based on correlation detector is proposed by Gong et al, (2011). A random binary watermark is generated by a secret key and bit-wisely embedded into one sub-band of the *DWT* domain of the image. A correlation-based detector which does not need an original image is used to determine whether a watermark exists or not in an image. The scheme is also secure with two secret keys. Future research is to improve the robustness against geometrical distortions.

The efficiency of digital watermarking algorithm is, is demonstrated by the strength of implanted watermarks against various attacks (Hemahlathaa & Chellppan, 2012). Improving the robustness of a watermark so as to withstand attacks has been one of the main study objectives in digital image watermarking. The two issues of existing feature-based schemes that have to be addressed are: i) is avoiding repeated selection

of robust regions for watermarking to resist similar attacks, and ii) is the difficulty of selecting the most robust and smallest feature region set to be watermarked. To achieve resilience, an overall architecture for a feature-based robust digital image watermarking system is planned. A simulated attacking procedure is performed using predefined attacks to assess the strength of every candidate feature region chosen. In comparison with some well-known feature-based methods, the proposed method demonstrates better performance in robust digital watermarking.

Recently, a digital watermarking method through bit replacement technology has been proposed by Pal et al, (2012), which stores multiple copies of the same data that is to be hidden in a scrambled form in the cover image. In their study, the method is described for recovering the data from the damaged copies of the data under attack by applying a majority algorithm to find the closest twin of the embedded information. A new type of non-oblivious detection method is also proposed. The improvement in the proposed algorithm for digital watermarking aims at obtaining a solution to the several problems of digital communication and also for data hiding. It is seen that the proposed algorithm is robust against compression and salt and pepper noise attacks where a private key is required for the recovery of the hidden information and which enhances security of the algorithm. Since digital watermarking has many applications in the digital world today, it can be thought of as a digital communication scheme where an auxiliary message is embedded in digital multimedia signals and is available wherever the latter signals move.

2.4 Tradeoff between Image Quality and Robustness

The relationship between the two requirements of image quality is opposite. In other words, the increase of image quality leads to decreasing the robustness of the image against possible attacks. For this reason, there is the need to make a balance between the two requirements which is called tradeoff. Recently, many studies have tried to improve both of image quality and robustness by making a tradeoff between them.

A digital watermarking is proposed to make tradeoff between quality and robustness (Fazli and Khodaverdi, 2009). In their proposed algorithm, significant bit planes of the watermarked image, not lower bit-planes of the asset picture, are positioned instead. The effect of image compression on the watermark is studied, and an evaluation of the robustness and quality which measures the distortion due to watermarking using two quality metrics: *MSE* and 1- structural similarity (*SSIM*), is made. Then, one that is close to the human visual system (*HVS*) is to be found. *SSIM* measures the similarity between its two input images (asset and watermarked images) and is in the range of [0, 1]. *SSIM* of 1 means perfect similarity (identical), and lower than that means less similarity. A tradeoff between quality and robustness has been done using the *LSB* watermarking with few bit-planes of the asset image. Its robustness is very low.

A tradeoff algorithm between image quality and robustness has been proposed by Zeki (2009). The study embedded only one bit of the watermarked image into the original image. The relationship between quality and robustness is opposite. For this reason, there is a need to create a balance between them. The middle and the edge of

the range is where the greatest pixel value would be identified, so that it could survive a range of attacks, whilst keeping image deformation to the lowest possible. Positioning the watermarked pixel away from the edge of the ranges does this. It is supposed by the research that the bias value *X* is the least distance from the location of the watermarked pixel *P`* to the edge of the range, which is nearer to the original pixel. In other words, in the case that the distance from the pixel to the edge of the range is greater than the bias value, the location of the pixel will not be modified. On the other hand, if the distance from the pixel to the edge of the range is smaller than the bias value, the position of the pixel will be modified to be equal to the bias value. The study proves that the 4^{th} bit in the pixel has the best robustness and at the same time investigates good image quality.

Recently, a tradeoff between quality and robustness has been proposed by Emami et al, (2012). Their study proposes an approximation approach for identification of the legal owner of the property utilizing the remaining data of the attacked watermarks regardless of the attack behavior. They coupled the *BiISB* (Duo-ISB-Bit-Plane) watermarking algorithm together with the *HI* (Histogram Intersection) technique in order to identify the ownership of the property. Their study tried to keep the quality of the watermarked image and, at the same time, identify the ownership of the property even though the attack totally corrupted the embedded watermarks. A tradeoff has been done between the quality and robustness to find an acceptable image quality with strong image against attacks. The study used two watermarks for embedding concretely by using only one bit each time based on *ISB* technique.

Another digital watermarking performance *tradeoff* measurement technique by Emami et al, (2012) to evaluate image watermarking has been proposed. The method attempts at assessing the tradeoff balance degree among these three; picture quality, resilience, and capability. This has included three factors: quality effect 'before attack and after watermarking', perceptibility effect 'after attack', and robustness 'after attack'. The study that used the bit-plane watermarking algorithms under several intensities of Reset Removal Attack revealed that the 3rd bit-plane algorithm showed better coordination between strength (resilience), picture quality, and capability. Performance evaluated at least three major metrics: quality, resilience and capability, of which have been widely used by researchers to analyze the performance of watermarking schemes; however, they constantly conflict with each other. An efficient system to assess the tradeoff balance degree among these procedures using three threshold conditions is suggested. These thresholds comprise three factors: quality effect 'before attack and after watermarking', perceptibility effect 'after attack', and robustness 'after attack'. As a result of this study, the performance tradeoff of a watermarking scheme can be stated based on degrees. Moreover, the study proposed reset removal attack as a severe geometric attack. Finally, the experimental investigation of the proposed technique using the bit-plane watermarking algorithms under several intensities of reset removal attack revealed that the 3rd bit-plane algorithm behaved a better compromise among resilience, picture quality, and capability.

2.5 Evaluation

The most common way used in watermarking utilizes a spatial domain that involves the insertion of the watermark in *LSB* of the image. This allows a watermark to be inserted into an image, without affecting the value of the image. On the other hand, the *LSB* is not robust enough against attacks.

A new developed technique called *ISB* technique has enhanced the image quality and image robustness against attacks (Zeki, 2009). The technique is based on a bit plane model by embedding one bit of each pixel in the watermarked image into each pixel of the original image.

This technique tries to solve the problems with the *LSB* method by enhancing the watermarked image's imperceptible distortion and improving the image robustness against possible attacks. In addition, the new technique tries to find the best pixel value by making a balance between the two requirements; image quality and robustness. *ISB* is a method to substitute the watermarked image pixels with new pixels to enhance image quality and robustness. This secures the watermarked images against attacks, and at the same time, keeps the new pixels very close to the original pixels.

2.6 Summary

Digital watermarking is one of the general information-hiding problems. Many studies have tried to solve this problem by using various techniques and methods.

Spatial technique and frequency technique are the most used among the other techniques. The most common way used in watermarking utilizes a spatial domain that involves the insertion of the watermark in *LSB* of the image. This allows a watermark to be inserted into an image, without affecting the value of the image. On the other hand, the *LSB* is not robust against attacks. Two important requirements should be available in watermarking image; which are quality, and robustness. Therefore, this research tried to enhanced image quality and robustness by embedding two bits of watermark image into each pixel of original image.

Furthermore, *ISB* is a method to substitute the watermarked image pixels with new pixels to enhance image quality and robustness. This secures the watermarked images against attacks, and at the same time, keeps the new pixels very close to the original pixels. The relation between the two requirements are opposite all the time. That is why, there is a need to make a balance between them to keep the watermarked image quality and robust against possible attacks. Since *ISB* proved to be more secure as compared with *LSB*, there is a need to embed more information as a secret image and keep the quality and robustness for watermarked image. However, the existing method *ISB* uses one bit for embedding. In this research two bits of watermark image are used to embed into each pixel of the original image, so that more information of the secret image can be embedded into the original image, and at the same time, keep the quality of the image and lessen the distortion that's happens after embedding the secret image.

CHAPTER THREE
RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the phases and methodology. Section 3.2 introduces the data preparation that are used in this study. Section 3.3 demonstrates the enhancement of ISB to improving image quality. Section 3.4 presents the enhancement of ISB for improving image robustness. Section 3.5 presents the enhancement of ISB for tradeoff between image quality and robustness. Section 3.6 presents the evaluation of tradeoff. Section 3.7 presents the summary of this chapter. Figure 3.1 shows the phases of the research.

Figure 3.1. Research phases

Based on Figure 3.1, there are five sequential phases. Each phase has a set of steps. The following sections explain the phases.

3.2 Phase 1 - Data Preparation

This study used twelve original gray scale images with sizes of 256 × 256 pixels. These original images were downloaded from two websites, the first one is Grayscale Standard Images data set:

(http://www.dip.ee.uct.ac.za/imageproc/stdimages/greyscale/), and the second one is the Dataset of Standard 512 × 512 Gray Scale Test Images, (http://decsai.ugr.es/cvg/CG/base.htm). The names of these original images are Bridge, Columbia, Boats, Lake, Plane, Camera, Peppers, Bird, Milk drop, Baboon, Dock, and Waterfall. Many studies in the past used different datasets in terms of number of images, size of images, and the type of images etc., Saxena (2008) used four original gray and colored digital images with the size of 256×256 pixels, Peungpanich et al, (2010) used seven color images with the size of 256×256 pixels, Hongqin and Fangliang (2010) used seven original grayscale images with the size of 512×512 pixels, Anwar et al, (2010) used ten standard images as cover images and the secret image, Figure 3.2 shows the twelve images used.

In this phase, the images were prepared as follows:

a. Convert the *BMP* image with size of 512 × 512 pixels to image size of 256 × 256 pixels. This was done using Photoshop *C56* software.
b. Convert the *BMP* image with size of 256 × 256 pixels to *TIFF*, *GIF*, and *PNG* format. This was also done using Photoshop *C56* software.
c. Convert the *BMP* image with size of 256 × 256 pixels to *JPEG* format. This was also done using Photoshop *C56* software.

Images in *BMP*, *TIFF*, *GIF*, and *PNG* are uncompressed format and *JPEG* are in the form of compressed.

In addition, the study used six watermark images with the size of 128 x 128 pixels. The watermark images were taken from different websites, one of them is http://uum.edu.my/index.php/en/, and Figure 3.3 shows the six images.

For these images, the preparation were as follows:

a. Convert the BMP image with the size of 512 × 512 pixels to image with the size of 128 × 128 pixels. This was done using Photoshop *C56* software.
b. Convert the BMP image with the size of 128 × 128 pixels to *TIFF*, *GIF*, and *PNG* format. This was also done using Photoshop *C56* software.
c. Convert the BMP image with the size of 128 × 128 pixels to *JPEG* format. This was also done using Photoshop *C56* software.

Original 1 (Bridge)

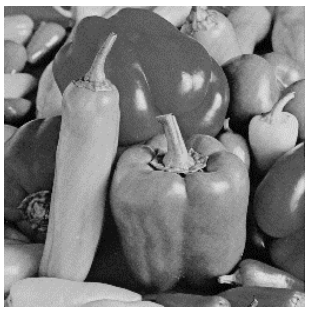
Original 2 (Columbia)

Original 3 (Boats)

Original 4 (Lake)

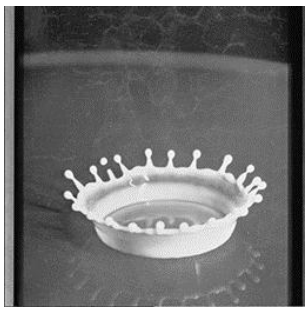
Original 5 (Plane)

Original 6 (Camera)

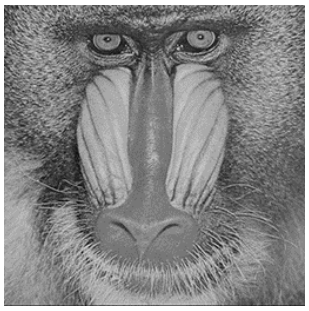


Original 7 (Peppers)

Original 8 (Bird)



Original 9 (Milk drop)



Original 10 (Baboon)

Original 11 (Dock)

Original 12 (Waterfall)

Figure 3.2. The grayscale original images with size 512 × 512 pixels

Watermark 1

Watermark 2

Watermark 3

Watermark 4

Watermark 5

Watermark 6

Figure 3.3. The grayscale watermark images with size 512 × 512 pixels

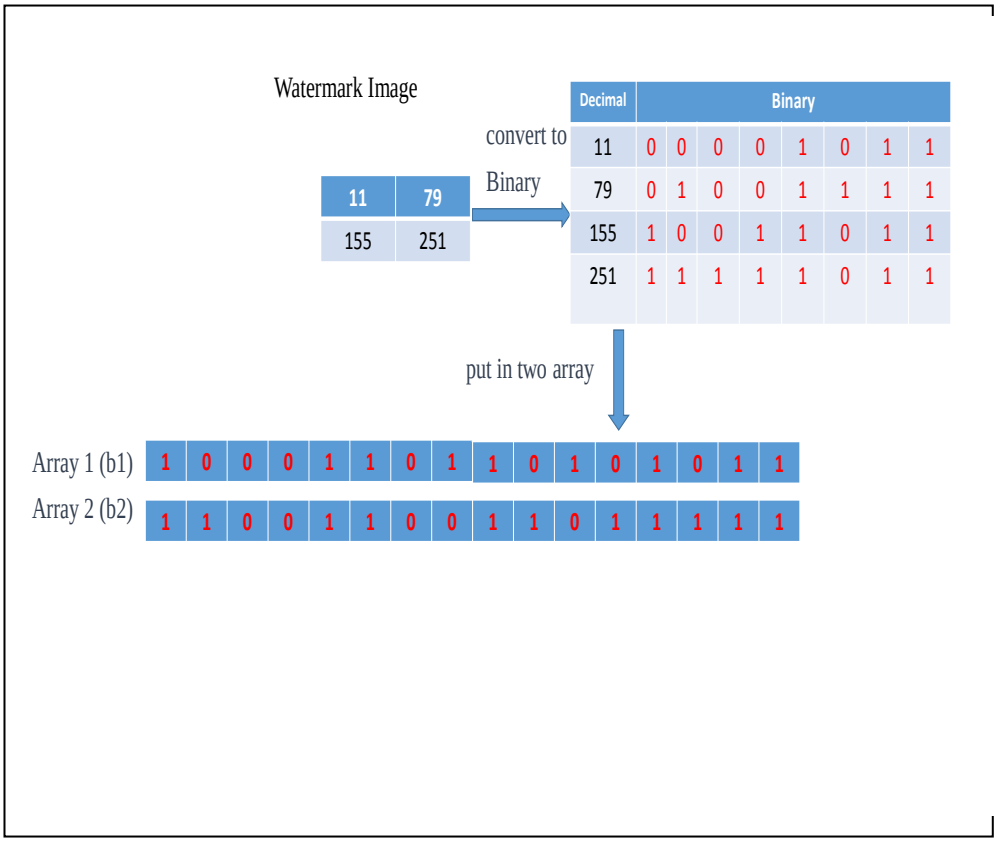
The output for this phase are original images *TIFF*, *GIF*, *PNG* and *JPEG* with size 256 x 256 pixels. Besides watermark images *TIFF*, *GIF*, *PNG* and *JPEG* with size 128 x 128 pixels.

3.3 Phase 2 - Enhancement of ISB for Improving Image Quality

In this phase, the *ISB* algorithm was enhanced to improve image quality. The steps involved are:

Step 1: The six watermark images from Phase 1 were converted into binary.

An example of the images in binary is shown below:



Step 2: Divide the host images (pixels) into a number of ranges. Figure 3.4 shows the flowchart:

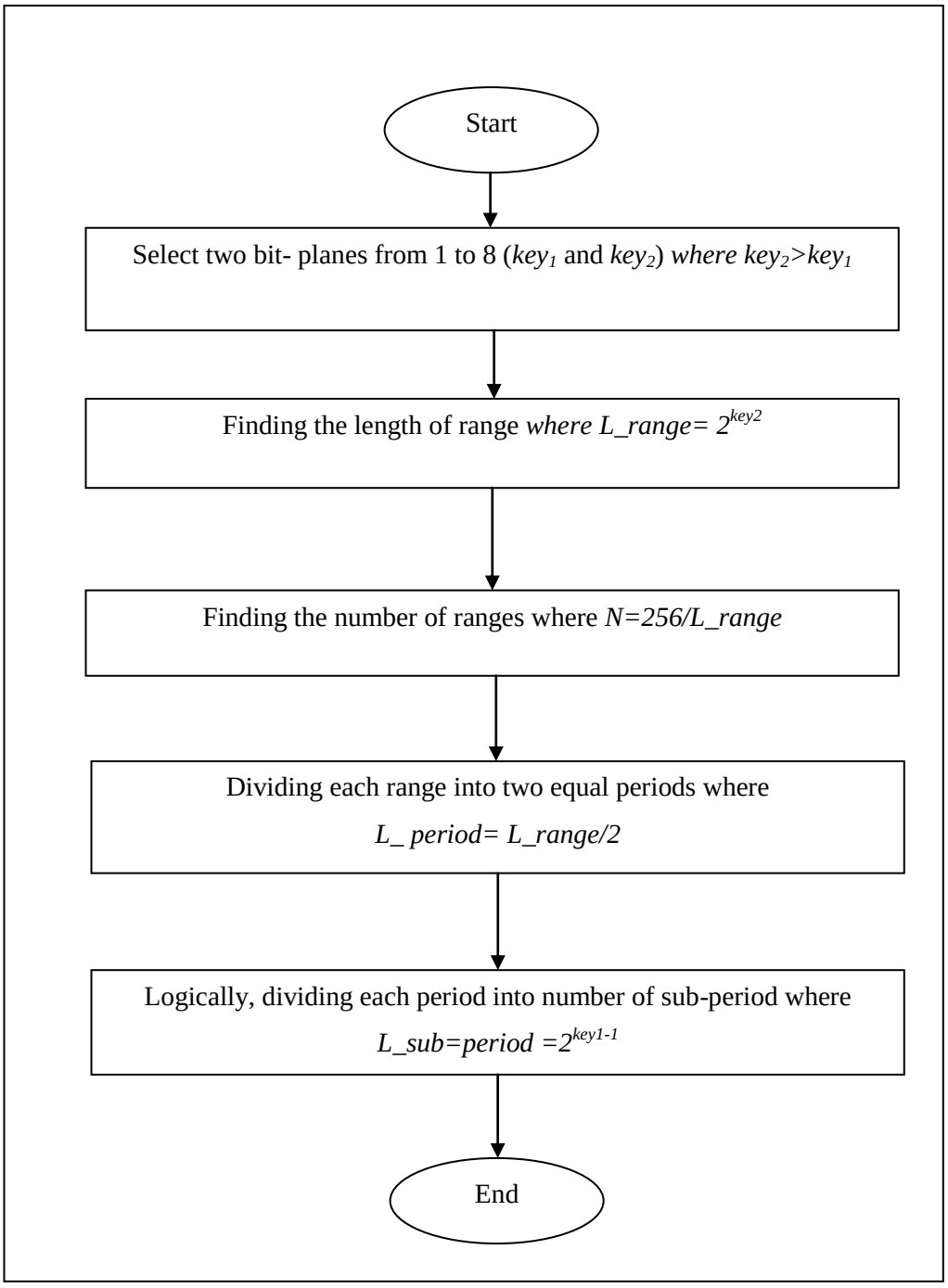


Figure 3.4. The division process flowchart

The specific steps are:

a) Select two bits-plane from 1 to 8 (key_1 and key_2) where $key_2 > key_1$.

b) The length of each range depends on the value of key_2, so the length of the range is $L\_range = 2^{K2}$.

c) Divide each range into two equal *period1* and *period2*. Particularly, *period1* is on the left and *period2* is on the right, so the length of each period will be $L\_period = L\_range/2$.

d) Arrange for a table of all the ranges for the two selected bits-plane (and the number of ranges (N) is $256/L$).

e) Divide each period into *sub-period* and this *sub-period* depends on key_1, while the length of each *sub-period* is $L\_group = 2^{key1-1}$.

So, the number of *sub-period* in each period is determined by the length of period divided by the length of *sub-period* ($N\_sub\text{-}period = L\_period / L\_sub\text{-}period$).

f) Input two embedded bits (b_1, b_2) into two original bits, where b_1 is embedded in $ykey_1$ and b_2 is embedded in $ykey_2$.

g) If the two original bits are equal to the two embedded bits where ($b_1 = ykey_1$ and $b_2 = ykey_2$), then the pixel will not be changed. The watermarked pixel is then equal to the original pixel, $p` = p$.

h) In case the two original bits are different from the two embedded bits, then the other 6 bits will be changed to closely assimilate the original pixel, as follows:

In the event the two embedded bits are ($b_1 \neq ykey_1$), and ($b_2 = ykey_2$), then the watermarked pixel can be found by calculating the minimum distance between the next or previous *sub-period* from the pixel.

If the two embedded bits are ($b_1 = 0$), and ($b_2 \neq ykey_2$), then the watermarked pixel can be found by calculating the minimum distance between the next or previous *period* from the pixel.

If the two embedded bits are ($b_1 = 1$), and ($b_2 \neq ykey_2$), then the watermarked pixel can be found by calculating the minimum distance between the next or previous *period* from the pixel, the watermarked pixel in this case will be in different period based on the value of key_2.

Figure 3. 5 shows how the division has been done.

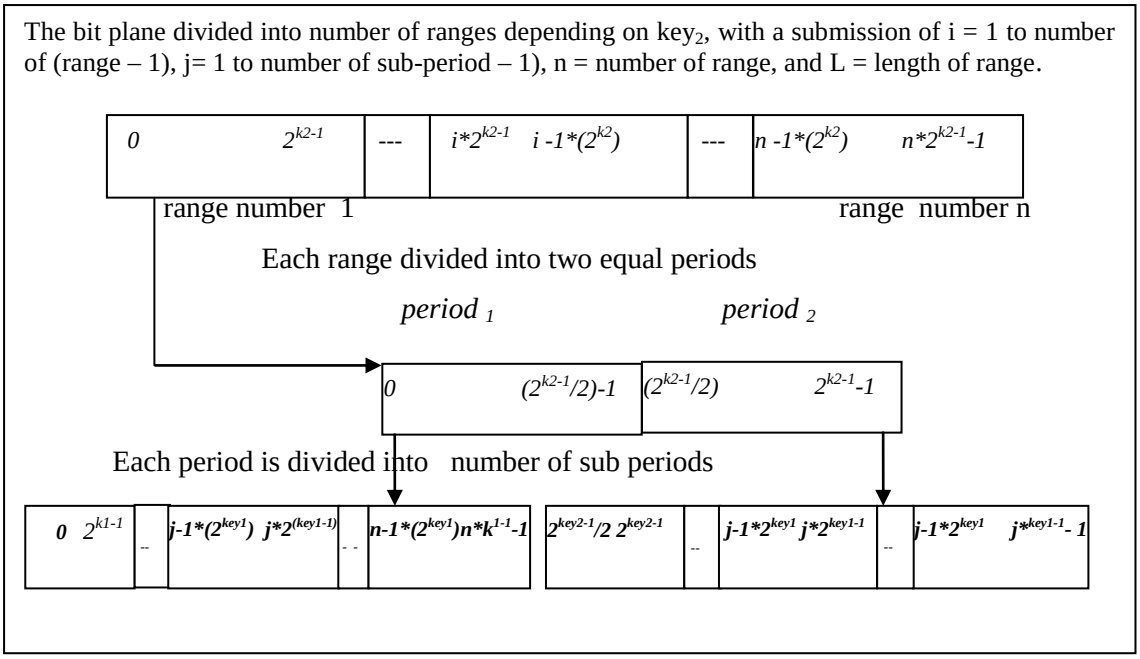


Figure 3.5. The division process

Step 3: Derive 10 mathematical equations based on *ISB*. The equations are shown in Chapter 4, Section 4.3. These equations help to determine the best value for embedding two bits and maintain the quality of the watermarked image.

Step 4: The *ISB* algorithm was enhanced by embedding two bits of watermark image into the existing pixels of the original images.

Step 5: The enhanced algorithm from Step 2 was tested on twelve original images.

Step 6: The *LSB* was also tested using the twelve original images.

Step 7: The *GA* algorithm was enhanced by incorporating 1 equation. The enhanced *GA* is known as *Quality_GA*. The equation and enhanced *GA* are presented in Chapter 4.

The enhancement steps are as follows:

a) Selecting any two bit-planes. “A bit-plane of digital images is a set of bits having the same position in the respective pixels of the digital images from 1 to 8, which are called (key_1, key_2) where ($key_2 > key_1$)”.

b) The two embedded bits are b_1 and b_2, in which b_1 is embedded into key_1, and b_2 is embedded into key_2. However, $ykey_1$ & $ykey_2$ represents the binary value of the original bits. Two bits that have been selected are used for the watermarked object to be inserted.

C) In case the two embedded bits are equal to the original bits, no change will be seen to the other remaining bits.

d) *GA* is then brought in to solve this problem in case the original value is not equal to the embedded one. The first phase in this algorithm is generating the population (pop) with a size of 256. The representation of the chromosome is a one dimension array, each chromosome contain 8 bits from 0-255, then each chromosome into binary (*GA*_ chromosome) is converted in one dimension array.

e) In the case of *GA*_ chromosome (key_1) = b_1 and *GA*_ chromosome (key_2) = b_2, the method will calculate fitness for chromosome. It symbolizes the total value of the pixel minus that of the chromosome. This means that the procedure checks all possibilities by taking the first two embedded values and considering these values as the fitted values. This is also done for the second, third, and so forth.

f) After embedding all values, the method will calculate the *PSNR* and *MSE* values and the time value. *GA* is used to find the best value by embedding two bits of watermarking data within each pixel of the original for all the bit-planes, starting from ($key_1=1$, $key_2=2$) to ($key_1=7$, $key_2=8$).

The *PSNR*, *MSE* and the time are presented for each embedding. The method clearly indicates the quality of the watermarked images of *PSNR* value using the proposed method showing gradual increase for all bit-planes.

Step 8: The algorithm was tested on twelve original images.

Step 9: Results from Steps 4, 5 and 6 were compared and recorded.

The output of this phase are 10 equations, an enhanced *ISB* algorithm (*Quality_AGA*) with two embedded bits procedure, and an enhanced *GA* (*Quality_GA*).

3.4 Phase 3 - Enhancement of ISB for Improving Image Robustness

In this phase, an enhanced *ISB* algorithm to improve image robustness was constructed. The steps involved are:

Step 1: Based on *ISB*, 7 mathematical equations were incorporated. The 7 mathematical equations are shown in Chapter 4, Section 4.4. These equations help to determine the best value for embedding two bits and maintain the quality of the watermarked image. The procedure undertaken to produce the mathematical equations are:

a) Selecting two bits of the watermark sequentially (b_1, b_2) and comparing them with the original bits ($ykey_1$, $ykey_2$) from pixel (p), where $key_2 > key_1$.

b) The length of each range depends on the value of Key_2, so the length of the range is $L\_\ range = 2^{k2}$.

c) Divide each range into two equal periods; *period1* and *period2*. *Period1* is on the left and *period2* is on the right, so the length of each period will be $L\_\ period = L\_\ range/2$.

d) Arrange for a table of all the ranges for the two selected bits-plane (in which the number of ranges (N) is 256/L).

e) Divide each period into *sub_ periods* and these *sub_ periods* are subjected to key_1, hence the length of each *sub_ period* will be $L\_\ sub\_\ period = 2^{k1-1}$. So the number of

sub_ periods in each period which is equal to the length of the period divided by length of the *sub_ period* (*N_ sub_ period = L_ period / L_ sub_ period*).

f) Input two embedded bits (b_1, b_2) into two original bits, where b_1 is embedded in key_1 and b_2 is embedded in key_2.

g) In case the two original bits and the two embedded bits are equal, this means *b1*equals $ykey_1$ and b_2 equals the corresponding value $ykey_2$. The watermarked pixel (*p`*) can be found by calculating the maximum distance between the next or previous *sub-period* from the pixel.

Hence, the new pixel will be found by choosing the nearest pixel to the original, which contains the two embedded bits, then by moving towards the other edge of the *sub-period* that contains this pixel. This means that the best robustness can be found on one of the sub-period edges.

h) In the case of the embedded bit b_1 being not equal to the corresponding original bit $ykey_1$ and the other embedded bit b_2 being equal to the corresponding original bit $Ykey_2$, there are two possible ways to find *p`*.

The first possibility is the pixel is less than minimum distance between previous and next pixel which are located in the same period.

The second possibility is the pixel is greater than minimum distance between previous and next pixel which are located in the same period.

i) Otherwise, in case the embedded bit b_1 is equal to zero and the other bit b_2 is not equal to the corresponding original $ykey_2$, therefore there are two possible ways to find the new pixel, which are:

The first possibility is the pixel is less than minimum distance between previous and next pixel which are located in the different period.

The second possibility is the pixel is greater than minimum distance between previous and next pixel which are located in the different period.

j) Another probability is that when b_1 is equal to one and $ykey_2 \neq b_2$, there are two ways to find the new pixel. These two probabilities are as shown below:

The first possibility is the pixel is less than watermarked pixel and equal to minimum distance between previous and next pixel which are located in the different period.

The second possibility is the pixel is greater than watermarked pixel and equal to minimum distance between previous and next pixel which are located in the different period.

Step 2: The enhanced algorithm from Step 1 was tested on twelve original images.

Step 3: The enhanced algorithm was applied to five chosen attacks, Blurring, Gaussian filter, Wiener filter, Speckle noise, and *JPEG* compression on the watermarked image. The proposed algorithm applied the five chosen attacks as mention above on the watermarked image after embedding two bits from each pixel of the watermark image into each pixel of the original image. Then, a calculation of the *NCC* and *BER* value for all bit planes and a comparison of the results with the *LSB* embedding two bits, were done.

In this section, the best robustness of the bit-planes model is proposed by understanding the effects of the attacks on the images. Simple watermark attacks attempt to eliminate the watermark information by manipulating the whole image and its components, without changing the geometry of the images and not making any use of the prior information about the watermark. The attacks change the value of the pixel, using the formula of each attack. In most cases, the effectiveness of the attacks on the image is rather small.

Step 4: The watermark was extracted from the host image. The invisible watermark should be determined only through a watermark extraction or detection algorithm. Invisible watermarking, on the other hand, is a far more complex concept. It is most often used to identify copyrighted data, such as by the author, distributor, and the like. The extracting phase of the proposed method is a direct extraction from the chosen bit-plane which will give the watermark object.

Step 5: Next, the *LSB* was tested using the twelve original images.

Step 6: Similarly, the watermark was extracted from the host image.

Step 7: Results from Steps 2, 3, 4 and 6 were compared and recorded.

The output from this phase are 7 mathematical equations, and an enhanced *ISB* algorithm. The algorithm is named as *Robust_AGA*.

3.5 Phase 4 - Enhancement of ISB for Tradeoff

The purpose of this phase is to determine the best values for balancing image quality and robustness. The relationship between the quality of image and resilience (robustness) is contrary. In other words, the enhancement of image quality while degrading image robustness will lead to a distortion of the watermarked image. In this phase, an enhanced *ISB* algorithm to perform tradeoff was constructed. The steps involved are:

Step 1: 7 mathematical equations were incorporated in the *ISB* algorithm. The 7 mathematical equations are shown in Chapter 4, Section 4.5. These equations help to find out the best values for image quality and robustness. The procedure undertaken to produce the mathematical equations are:

a) Selecting two bits of the watermark sequentially (b_1, b_2) and comparing them with the original bits ($ykey_1$, $ykey_2$) from the pixel (p).

b) Another probability is that when the embedded bit b_1 is not equal to the corresponding original bit $ykey_1$ and the other embedded bit b_2 is equal to the corresponding original bit $ykey_2$.

c) Otherwise, if the embedded bit b_1 equals zero and the other bit b_2 is not equal to the corresponding original $ykey_2$.

d) Another probability is that when *b1* is equal to one and $ykey2 \neq b2$.

Step 2: The enhanced algorithm from Step 1 was tested on twelve original images.

Step 3: From the results, the *PSNR* value that is equal or greater than 30db were selected.

Step 4: based on step 3, the *NCC* values are calculated and the best value is chosen.

The output from this phase are 7 equations, and an enhanced *ISB* algorithm for performing tradeoff. The algorithm is named as *tradeoff _AGA*.

3.6 Phase 5 - Evaluation

This phase has two parts. The first part evaluates the enhanced ISB algorithm (*tradeoff_AGA*) in terms of image quality and robustness. The second part calculates the computational complexity of the enhanced algorithm.

Figure 3.6 shows the evaluation process.

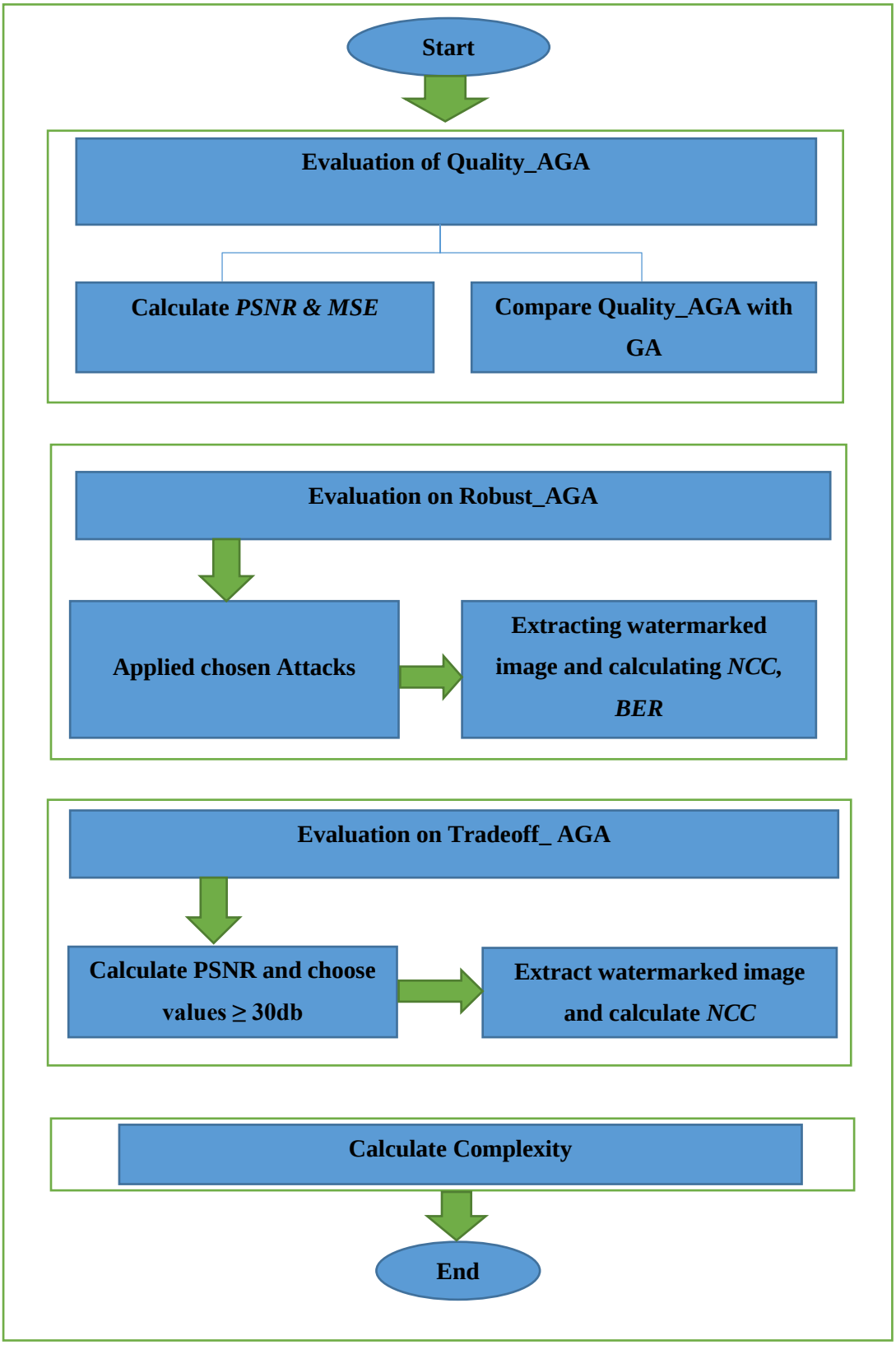


Figure 3.6. Evaluation process

The following paragraphs explain the parts respectively:

Part 1

For image quality, the metrics used are mean squared error (*MSE*), and Peak to Signal Noise Ratio (*PSNR*). For robustness, the metrics used are Normalized Cross Correlation (*NCC*), and Bit Error Rate (*BER*).

MSE is used to find the average term-by-term squared difference between the input signal (the original image, *P*) and the output signal (the watermarked image, *P`*). The equation used is shown below (3.1):

$$MSE = \frac{1}{N} \sum^{N} (p`_i - p_i)^2 \quad (3.1)$$

PSNR is to measure the image quality. Equation 3.2 shows the formula used. The formula is based on Zeki (2009).

$$PSNR\ (db) = 10\ log\ 10 \frac{p^2}{MSE} \quad (3.2)$$

where *p* represents the pixel.

NCC is to find the corresponding (correlated) pixel within a certain disparity range d (d E [0,….,dmax]) that minimizes the associated error and maximizes the similarity. The *NCC* value can be calculated using Equation 3.3 (Zeki and Manaf, 2009).

$$NCC = \frac{\sum X \sum Y W(X,Y)W`(X,Y)}{\sum X \sum Y [W(X,Y)]\wedge 2} \quad (3.3)$$

where W(x,y) is the original watermark image and W'(x,y) is the extracted watermark image.

BER is the rate at which errors occur between the extracted watermark and the original one and is calculated based on Equation 3.4.

$$BER = \frac{Number\ of\ errors}{Total\ number\ of\ bits\ sent} \quad (3.4)$$

Part 2

The steps to calculate complexity are:

Step 1: Embedding the bits of watermark image into the existing pixel of the original image.

Step 2: Calculating the time that needed for the embedding process which is called time out (toc) in seconds.

The output from this phase is the enhanced *ISB* algorithm for performing tradeoff in term of *MSE, PSNR, NCC,* and *BCR*. Besides that, calculating the time needed for the embedding process uses the Complexity algorithm.

The results for this phase (Phase 5) are presented in Chapter 5.

3.7 Summary

This chapter presents the methodology of the study. The study involved 5 phases: data preparation, enhancement of *ISB* for improving image quality, enhancement of *ISB* for improving image robustness, enhancement of *ISB* for tradeoff, and the last one is evaluation.

CHAPTER FOUR
FINDINGS

4.1 Introduction

This chapter presents the findings for the proposed algorithms. Section 4.2 presents the data after preparation for all types of original images and watermark images. Section 4.3 presents the enhanced *ISB* algorithm (*Quality_AGA*) with two embedded bits procedure, and an enhanced *GA* (*Quality_GA*). Section 4.4 presents the enhanced *ISB* algorithm (*Robustness_AGA*). Section 4.5 presents the enhanced *ISB* algorithm for performing tradeoff (*tradeoff _AGA*). Section 4.6 presents the enhanced *ISB* algorithm for performing tradeoff in term of *MSE*, *PSNR*, *NCC*, and *BCR*, and the time calculation needed for the embedding process. Finally, Section 4.7 presents the summary of this chapter.

4.2 Data After Preparation

The embedding process consists of choosing two bits from the watermark image and embedded into the existing pixel of original image based on *ISB*. Figure 4.1 shows the first three *BMP* grayscale original images after converting to the size of 256 × 256 pixels. In addition, Figure 4.2 shows the same images after converting to *TIFF*, *GIF*, and *PNG* format. Figure 4.3 shows the same image after converting to *JPEG* format. While Figure 4.4 shows the first grayscale watermark image after converting to the size of 128 × 128 pixels. Then, Figure 4.5 shows the same image after converting to *TIFF*, *GIF*, and *PNG* format. Finally, Figure 4.6 shows the same watermark image after converting to *JPEG* format.

Original 1 (Bridge)

Original 2 (Columbia)

Original 3 (Boats)

Figure 4.1. The first three BMP original images with size 256 × 256 pixels

Original 1 (TIFF)

Original 2 (TIFF)

Original 3 (TIFF)

Original 1 (GIF)

Original 2 (GIF)

Original 3 (GIF)

Original 1 (PNG)

Original 2 (PNG)

Original 3 (PNG)

Figure 4.2. TIFF, GIF and PNG original images with size 256 × 256 pixels

Original 1 (Bridge)

Original 2 (Columbia)

Original 3 (Boats)

Figure 4.3. The first three JPEG original images with size 256 × 256 pixels

Figure 4.4. The three BMP grayscale watermark images in 128 × 128 pixels

Watermark 1 (TIFF)

Watermark 2 (TIFF)

Watermark 3 (TIFF)

Watermark 1 (GIF)

Watermark 2 (GIF)

Watermark 3 (GIF)

Watermark 1 (PNG)

Watermark 2 (PNG)

Watermark 3 (PNG)

Figure 4.5. TIFF, GIF and PNG watermark images in size 128 × 128 pixels



Watermark 1 Watermark 2 Watermark 3

Figure 4.6. The first three JPEG watermark images in size 256 × 256 pixels

From the above figures it can be noticed that all the original images after converting the format and the size are very similar to original images before converting.

4.3 Enhanced ISB (Quality_AGA)

This section presents 3 results: (a) 10 mathematical equations, (b) *ISB* algorithm that was enhanced by embedding two bits of watermark image, and (c) an enhanced *GA* algorithm. Sections 4.3.1, 4.3.2, 4.3.3 show the respective results.

4.3.1 10 Mathematical Equations

This section presents the mathematical equations.

The length of each range can be found using the largest key (*key2*) according to Equation 4.1:

$$L\_range = 2^{Key2} \tag{4.1}$$

The length of each period can be obtained by dividing the length of the range with two, according to Equation 4.2:

$$L\_period = L\_range / 2 \quad (4.2)$$

Then, by using the Equation 4.3, the number of ranges (N) can be obtained by dividing 256 by the length of the range.

$$N = 256 / L\_range \quad (4.3)$$

The two embedded bits are b_1 and b_2, in which b_1 is embedded into key_1, while b_2 is embedded into key_2, respectively.

From this step, all of the values of key_2 in the first period are 0 while the second period that presents all values are 1 for key_2.

However, for key_1 at each period, there is zero value and one value at different positions, which means it is not enough for embedding two bits by using the standard *ISB* technique. Therefore, the proposed technique implicitly decomposes each period into logical regions by using the smallest key (key_1) according to Equation 4.4.

$$L\_sub\ period = 2^{key2-1} \quad (4.4)$$

Hence, that number of sub period can be found by dividing the length of period over the length of sub-period according to Equation 4.5:

$$No\_sub\text{-}period = L\_period \,/\, L\_sub\text{-}period \tag{4.5}$$

The original pixel value is p, as defined by Equation 4.6:

$$p = \sum_{i=1}^{8} yi\ 2^{i-1} \tag{4.6}$$

Where, y_i is the value of each bit-plane in the binary form (0 or 1), and i represent the ranges from 1 to 8, in particular i = 1 is the *LSB* and i = 8 is the *MSB*. Also, it is assumed that the selected two bits for embedding are key_1 and key_2.

In addition, it is assumed that the embedded two bits are b_1 and b_2, hence, the new watermarked pixels $p`$ can be defined as follows:

If the two embedded bits (b_1, b_2) are equal to the two original bits (key_1, key_2), then the watermarked pixel is then equal to the original pixel, as shown in Equation 4.7.

$$p` = p \tag{4.7}$$

Another probability is that when the embedded bit b_1 is not equal to the corresponding original bit $ykey_1$ and the other embedded bit *b2* is equal to the corresponding original bit $ykey_2$, $p`$ is found using Equation 4.8:

$$p` = MIN\ (p-(mod\ (p, (2^{(key1-1)} -1)-1), p-mod\ (p, (2^{(key1-1)}) +2^{(key1-1)}) \quad (4.8)$$

where $p`$ is in the same period of p.

Otherwise, if the embedded bit b_1 is equal to zero and the other bit b_2 is not equal to the corresponding original $ykey_2$, $p`$ is found using Equation 4.9:

$$P` = MIN\ (min\_\ period\ (p)-2^{(key1-1)}-1, min\_\ period\ (p) +L\_period) \quad (4.9)$$

where $p` >= 0$ and $p` <= 255$.

The last probability is that when $ykey_1$ is 1 and $ykey_2 \neq b2$, $p`$ is found using Equation 4.10:

$$p` = MIN\ (min\_\ period(p)-1, min\_period(p) +(2^{(key2-1)}/2)+2^{(key1-1)}) \quad (4.10)$$

where $0 => p` <= 255$.

The proposed image algorithm has found the best image quality based on the mathematical equations that cover all the probabilities after embedding the two bits to avoid image distortion. The best quality of the watermarked image can be found by choosing the nearest pixel to the original pixel, which has the two embedded bits

4.3.2 Enhanced ISB (Quality_AGA)

Figures 4.7 and 4.8 show the flowchart and pseudo code for the enhanced algorithm (*Quality_AGA*).

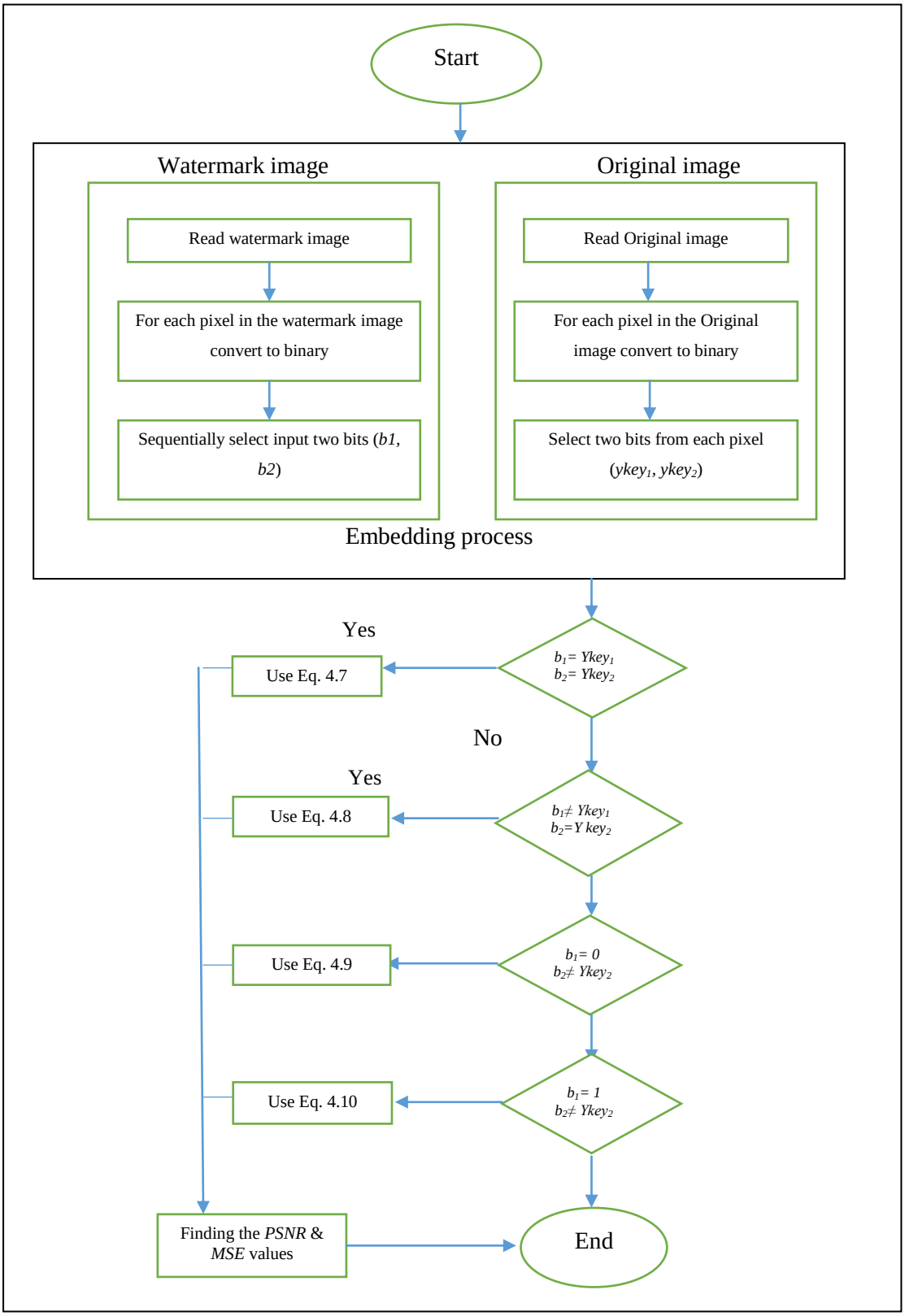


Figure 4.7. The flowchart of Quality_AGA

The Proposed Algorithm *Quality_AGA*
Input: original image, watermark image, key_1, key_2
Output: watermarked image, *PSNR*, *MSE*
Begin
Generate watermark _ array
for i= 1 to watermark _image size **do**
Select next pixel pix _ wat
Call convert – binary (pix _ wat)
Add watermark _array
end
Initialize image_ watermarked
for i=1 to original _ image size **do**
Select next pixel pix _ original
Call convert _ binary (pix _ original)
Select pixel (key_1), pix (key_2) to hos_1, hos_2
Select next two bits from watermark _ array wat_1, wat_2 sequentially
Compare (hos_1, wat_1), compare (hos_2, wat_2)
if hos_1=wat_1 and hos_2=wat_2
use Eq. (4.10)
end
if hos_1≠wat_1 and hos_2=wat_2
use Eq. (4.11)
end
if wat_1=0 and hos_2≠wat_2
use Eq. (4.12)
end
if wat_1=1 and hos_2≠wat_2
use Eq. (4.13)
end
end

Calculate *PSNR, MSE*

End

Figure 4.8. The pseudo code for Quality_AGA

4.3.3 Enhanced GA

This section presents a) the equation derived b) the pseudo code for the enhanced *GA*.

The explanation of the technique is done as follows:

Step 1: selecting any two bit-planes: "A bit-plane of digital images is a set of bits having the same position in the respective pixels of the digital images from 1 to 8", which are called (key_1, key_2) where ($key_2 > key_1$).

Step 2: the two embedded bits are b_1 and b_2, in which b_1 is embedded into key_1, and b_2 is embedded into key_2. However, $ykey_1$ & $ykey_2$ represents the binary value of the original bits. Two bits that have been selected are used for the watermarked object to be inserted.

Step 3: in case the two embedded bits are equal to the original bits, no change will be seen to the other remaining bits.

Step 4: *GA* is then brought in to solve this problem in case the original value is not equal to the embedded one. The first phase in this algorithm is generating the population (pop) with a size of 256. The representation of the chromosome is a one dimension array; each chromosome contains 8 bits from 0-255, then each chromosome into binary (*GA*_ chromosome) is converted in one dimension array.

Step 5: in the case of *GA*_ chromosome (key_1) = b_1 and *GA*_ chromosome (key_2) = b_2, the method will calculate the fitness for chromosome. It symbolizes the total value of the pixel minus that of the chromosome. This means that the procedure checks all possibilities by taking the first two embedded values and considering these values as the fitted values. This is also done for the second, third, and so forth. The fitness value has to be reached, according to Equation 4.11:

$$Fitness\ value = |pixel\text{-}chromosome| \tag{4.11}$$

Step 6: after embedding all values, the method will calculate the *PSNR* and *MSE* values and the time value. *GA* is used to find the best value by embedding two bits of watermarking data within each pixel of the original for all the bit-planes, starting from ($key_1=1$, $key_2=2$) to ($key_1=7$, $key_2=8$).

The *PSNR*, *MSE* and the time are presented for each embedding. The method clearly indicates the quality of the watermarked images of *PSNR* value using the proposed method showing gradual increase for all bit-planes. Figure 4.9 describes the proposed method and highlights the schedule steps.

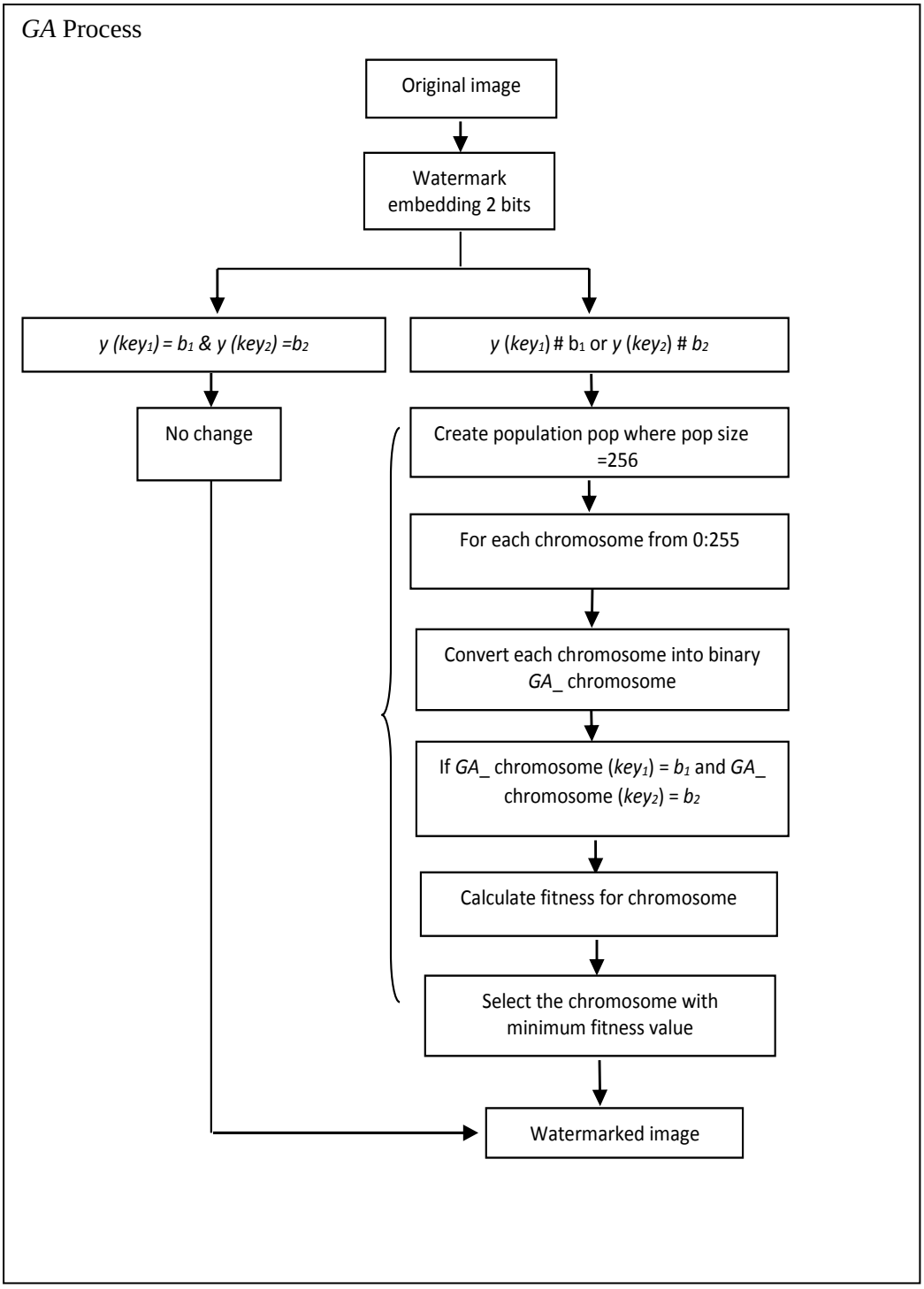


Figure 4.9. The flowchart of proposed GA

In addition, Figures 4.10 and 4.11 show the pseudo code of the proposed technique by using mathematical equations.

The Proposed Algorithm *Quality_GA*
Input: original image, watermark image, key_1, key_2
Output: watermarked image, *PSNR, MSE*
Begin
Generate watermark _ array
for i= 1 to watermark _image size **do**
Select next pixel pix _ wat
Call convert – binary (pix _ wat)
Add watermark _array
end
Initialize image_ watermarked
for i=1 to original _ image size **do**
Select next pixel pix _ original
Call convert _ binary (pix _ original)
Select pixel (key_1), pix (key_2) to hos_1, hos_2
Select next two bits from watermark _ array wat_1, wat_2 sequentially
Compare (hos_1, wat_1), compare (hos_2, wat_2)
if hos_1=wat_1 and hos_2=wat_2
use Eq. (4.10)
end
if $hos_1 \neq wat_1$ OR $hos_2 \neq wat_2$
Call *GA*_ function
end
End
Calculate *PSNR & MSE*
Calculate time (*T*)
End

Figure 4.10. The pseudo code of the proposed Quality_GA

GA_ Function
Create population of individuals
for each individual
Evaluate the fitness of the individuals using Eq. 4.11
Replace the worst individual of the population with the best new individual
End

Figure 4.11. The pseudo code of the proposed GA Function

4.4 Enhanced ISB (Robust_AGA)

This section presents 2 results: (a) 7 mathematical equations, (b) an enhanced *ISB.*

4.4.1 7 Mathematical Equations

This section discusses the mathematical analysis for the proposed algorithm according to the previous section.

In case the two embedded bits are equal ($b_{1=}0$, $b_{2=}0$), and equal to the two original bits where ($yk_{1=}0$, $yk_{2=}0$), then the watermarked pixel can be obtained using Equation 4.12.

$$p`=MAX\ (p-(mod\ (p,(2^{(key1-1)}-1)),\ p-mod(p,\ (2^{(key1-1)})+2^{(key1-1}-1^{)}) \quad (4.12)$$

In the case of the embedded bit b_1 being not equal to the corresponding original bit *ykey1* and the other embedded bit b_2 being equal to the corresponding original bit $ykey_2$, there are two possible ways to find $p`$. The two equations are shown below:

If $p < MIN\ (p-(mod\ (p,\ (2^{(key1-1)}-1)-1),\ p-mod\ (p,\ (2^{(key1-1)})+2^{(key1-1)})$, then the new pixel can be found according to the Equation 4.13:

$$p`=\ MIN\ (p-(mod\ (p,(2^{(key1-1)}-1)-1),\ p-mod\ (p,(2^{(key1-1)})+2^{(key1-1)}) \quad (4.13)$$

If $p > MIN\ (p-(mod\ (p, (2^{(key1-1)} -1)-1), p-mod\ (p, (2^{(key1-1)}) +2^{(key1-1)}))$, then the new pixel can be found according to Equation 4.14:

$$p` = MIN(p-(mod\ (p,(2^{(key1-1)} -1)-1), p-mod\ (p,(2^{(key1-1)})+2^{(key1-1)})-1 \quad (4.14)$$

where $p`$ is in the same period of p.

In case of the embedded bit b_1 is equal to zero and the other bit b_2 is not equal to the corresponding original $ykey_2$, therefore the two possible ways to find the new pixel are:

If $(p<MIN\ (min\_\ period\ (p)-1,\ min\_\ period\ (p) + (2^{(key2-1)} /2) +2^{(key1-1)}))$, then the new pixel can be found according to Equation 4.15:

$$P` = MIN\ (min\_\ period\ (p)-2^{(key1-1)}-1,\ min\_\ period\ (p) +l\_period) \quad (4.15)$$

If $(p>MIN\ (min\_\ period\ (p)-1,\ min\_period\ (p) + (2^{(key2-1)} /2) +2^{(key1-1)}))$, then the new pixel can be found according to Equation 4.16:

$$P` = MIN(min\_\ period(p)-2^{(key1-1)}-1, min\_\ period\ (p)+l\_period)-2^{key1} \quad (4.16)$$

where $p` > 0$ and $p <= 255$.

Another probability is that when b_1 is equal to one and $ykey_2 \neq b_2$, there are two ways to find the new pixel. These two probabilities are as shown below:

If $(p<p`=MIN\ (min\_\ period\ (p)-1,\ min\_period\ (p)\ +\ (2^{(key2-1)}/2)\ +2^{(key1-1)}))$, so the new pixel can be found according to Equation 4.17:

$$p`=MIN(min\_\ period\ (p)-1,\ min\_period\ (p)+(2^{(key2-1)}/2)+2^{(key1-1)}) \quad (4.17)$$

If $(p>p`=MIN\ (min\_\ period\ (p)-1,\ min\_period\ (p)\ +\ (2^{(key2-1)}/2)\ +2^{(key1-1)}))$ so the new pixel can be found according to Equation 4.18:

$$p`=MIN\ (min\_\ period(p)-1,\ min\_period\ (p)+(2^{(key2-1)}/2)+2^{(key1-1)}) \quad (4.18)$$

where $p`$ is in the same period of p.

Comparisons between the two embedded bits with the original bits have been done. The proposed image algorithm tries to find the best image robustness based on the mathematical equations that cover all the probabilities after embedding the two bits to get a strong watermarked image. Figure 4.12 highlights the proposed algorithm.

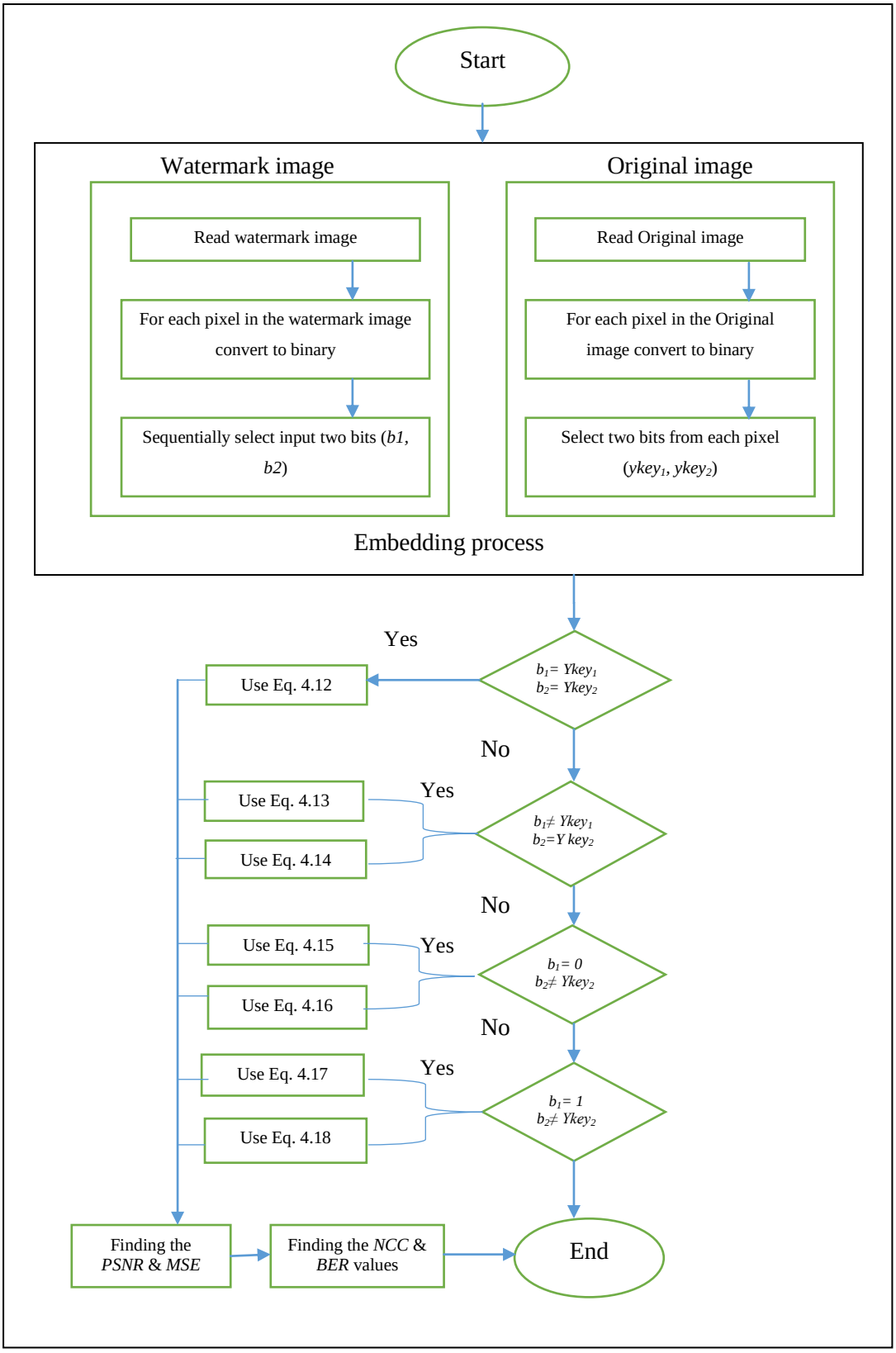


Figure 4.12. The flowchart for robust_AGA

4.4.2 Enhanced ISB (Robust_AGA)

Figure 4.13 below clarify the pseudo code for the proposed algorithm.

The Proposed Algorithm *Robust_ AGA*
Input: original image, watermark image, key_1, key_2
Output: watermarked image, *NCC, BCR, PSNR*
Begin
Generate watermark _ array
for i= 1 to watermark _image size **do**
Select next pixel pix _ wat
Call convert – binary (pix _ wat)
Add watermark _array
end
Initialize image_ watermarked
for i=1 to original _ image size **do**
Select next pixel pix _ original
Call convert _ binary (pix _ original)
Select pixel (key_1), pix (key_2) to hos_1, hos_2
Select next two bits from watermark _ array wat_1, wat_2 sequentially
Compare (hos_1, wat_1), compare (hos_2, wat_2)
if $hos_1=wat_1$ and $hos_2=wat_2$
use Eq. (4.12)
end
if $hos_1 \neq wat_1$ and $hos_2=wat_2$
use Eq. (4.13) or Eq.(4.14)
end
if $wat_1=0$ and $hos_2 \neq wat_2$
use Eq. (4.15) or Eq. (4.16)
end
if $wat_1=1$ and $hos_2 \neq wat_2$
use Eq. (4.27) or Eq. (4.18)
end
end

Calculate *NCC, BER, MSE, and PSNR*

End

Figure 4.13. The pseudo code for Robust_AGA

4.5 Enhancement of ISB for Tradeoff

This section presents 2 results: (a) 7 mathematical equations, (b enhanced *ISB* for performing tradeoff.

4.5.1 7 Mathematical Equations

There are many probabilities for performing tradeoff between quality and robustness.

Probability 1:

If the two original bits and two embedded bits are equal, this shows that b_1 equals $ykey_1$ and b_2 equals $ykey_2$. The watermarked pixel ($p`$) will be found according to Equation 4.19:

$$p`=MIN(p-(mod\ (p,(2^{key1-1}-1)),p-mod\ (p,(2^{key1-1})+2^{key1-1}-1)+DIST \quad (4.19)$$

Probability 2:

When the embedded bit b_1 is not equal to the corresponding original bit $ykey_1$ and the other embedded bit b_2 is equal to the corresponding original bit $ykey_2$, there are two probabilities to find the new pixel $p`$:

If $p< MIN\ (p-(mod\ (p,\ (2^{(key1-1)}-1)-1),\ p-mod\ (p,\ (2^{(key1-1)})+2^{(key1-1)}$, so the new pixel $p`$ will be found according to Equation 4.20 below:

$$p`= MIN(p-(mod(p,(2^{key1-1}-1)-1),\ p-mod(p,(2^{key1-1})+2^{key1-1})+DIST \quad (4.20)$$

If $p > MIN\ (p-(mod\ (p, (2^{(key1-1)} -1)-1), p-mod\ (p, (2^{(key1-1)}) +2^{(key1-1)})$, so the new pixel $p`$ will be found according to Equation 4.21 below:

$$p`=MIN(p-(mod(p,(2^{key1-1}-1)-1),p-mod(p, (2^{(key1-1)}+2^{key1-1})-DIST \quad (4.21)$$

where $p`$ in the same period of p.

Probability 3:

If the embedded bit b_1 equals zero and the other bit b_2 is not equal to the corresponding original $ykey_2$, there are two probabilities to find the new pixel $p`$:

If $(p<MIN\ (min\_\ period\ (p)-1, min\_period\ (p) + (2^{(key2-1)} /2)+2^{(key1-1)}))$, so the new pixel p` will be found according to Equation 4.22 below:

$$P`=MIN\ (min\_\ period\ (p)-2^{key1-1}-1, min\_\ period\ (p) +l\_period)\ DIST \quad (4.22)$$

If $(p>MIN\ (min\_\ period\ (p)-1, min\_period\ (p) + (2^{(key2-1)} /2) +2^{(key1-1)}))$, so the new pixel $p`$ will be found according to Equation 4.23 below:

$$p`=MIN\ (min\_\ period\ (p)-2^{key1-1}-1,\ min\_\ period\ (p)+l\_period) - DIST \quad (4.23)$$

where $p`> 0$ and $p <= 255$.

Probability 4:

When *b1* is equal to one and $ykey2 \neq b2$, there are two probabilities to find the new pixel $p`$:

If $(p<p`=MIN\ (min\_\ period\ (p)-1,\ min\_period\ (p) + (2^{(key2-1)}/2) + 2^{(key1-1)}))$, so the new pixel $p`$ will be found according to Equation 4.24 below:

$$p`=MIN(min\_\ period\ p-1,\ min\_period\ p+(2^{key2-1}/2)+2^{key1-1})+DIST \quad (4.24)$$

If $(p>p`=MIN\ (min\_\ period\ (p)-1,\ min\_period\ (p) + (2^{(key2-1)}/2) + 2^{(key1-1)}))$, so the new pixel $p`$ will be found according to Equation 4.25 below:

$$p`=MIN(min\_\ period\ p-1,min\_period\ p+2^{key2-1}/2)+2^{key1-1})-DIST \quad (4.25)$$

where $p`$ is in the same period of *p*.

The pseudo code of the proposed algorithm clarified all the steps as shown in Figure 4.14 below:

The Proposed Algorithm *Tradeoff_ AGA*
Input: original image, watermark image, key_1, key_2
Output: watermarked image, *NCC, PSNR, BER, MSE.*
Begin

Generate watermark _ array
for i= 1 to watermark _image size **do**
Select next pixel pix _ wat
Call convert – binary (pix _ wat)
Add watermark _array
end
Initialize image_ watermarked
for i=1 to original _ image size **do**
Select next pixel pix _ original
Call convert _ binary (pix _ original)
Select pixel (key_1), pix (key_2) to hos_1, hos_2
Select next two bits from watermark _ array wat_1, wat_2 sequentially
Compare (hos_1, wat_1), compare (hos_2, wat_2)
if $hos_1=wat_1$ and $hos_2=wat_2$
use Eq. (4.19)
end
if $hos_1 \neq wat_1$ and $hos_2=wat_2$
use Eq. (4.20) or Eq. (4.21)
end
if $hos_1=wat_1=0$ and $hos_2 \neq wat_2$
use Eq. (4.22) or Eq.(4.23)
end
if $hos_1=wat_1=1$ and $hos_2 \neq wat_2$
use Eq. (4.24) or Eq. (4.25)
end

end

Calculate *PSNR & MSE* (*PSNR* >=30)

Calculate *NCC* & *BER*
end

End

Figure 4.14. The pseudo code Tradeoff_ AGA

This research discusses watermark embedding in all bit-planes which were carried out with all the possible values of the *DIST* value, and every embedding for *PSNR, MSE, BER,* and *NCC* were also calculated. The optimum value was found by ignoring all the cases in which the *PSNR* are less than 30 (an acceptable image quality for the *PSNR* is considered to be equal or greater than 30 db). Meanwhile, the best value of the *NCC* was chosen as the best embedding status. Figure 4.15 presents the flowchart.

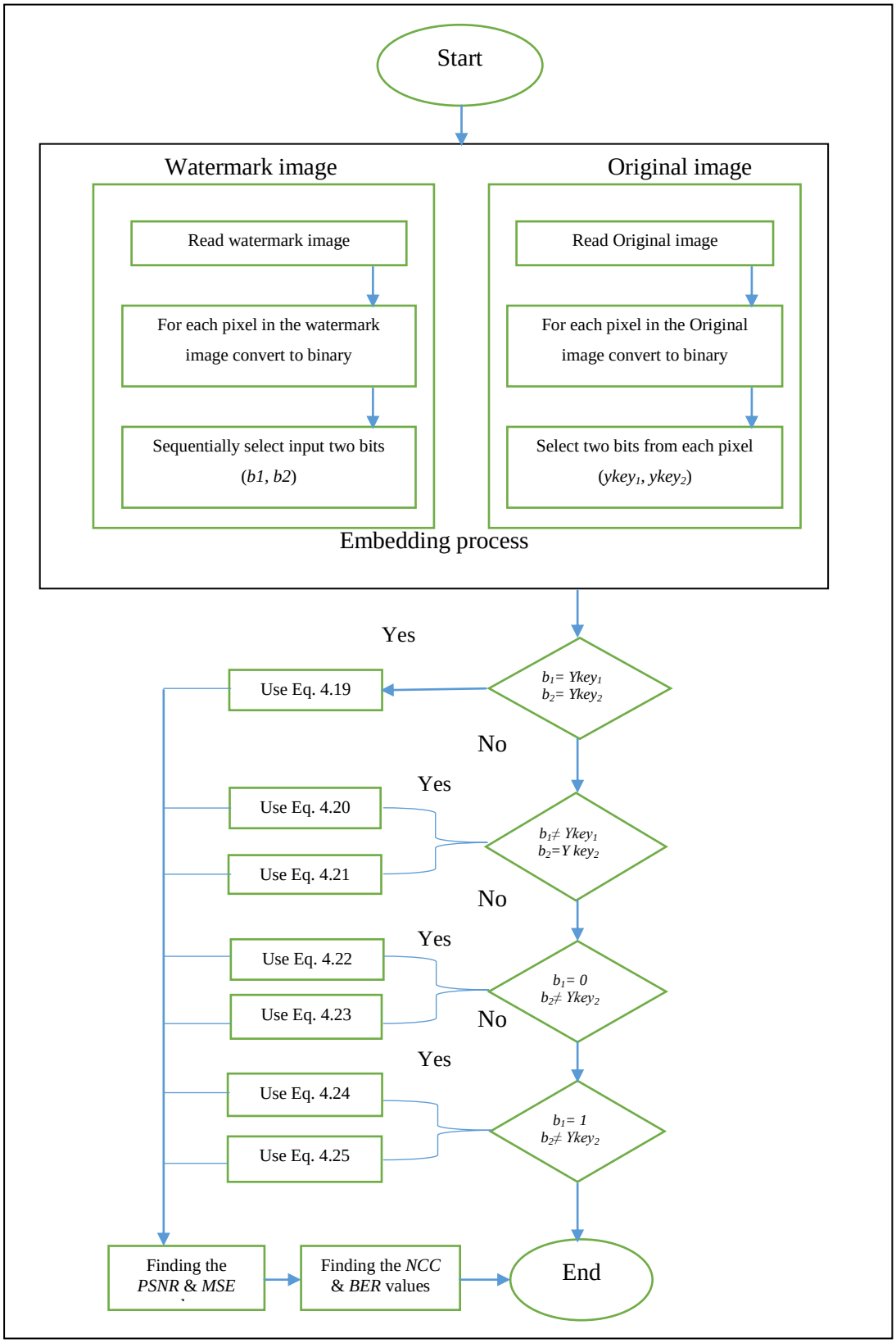


Figure 4.15. The flowchart of Tradeoff_ AGA

4.6 Summary

This chapter presents the techniques that are used for embedding the watermarked image into the original image in the spatial domain. The first technique is *LSB*, which is considered as the most common technique in the spatial domain presented briefly by clarifying the substitution process that is used in this technique. Apart from that, an example that clarifies the embedding process in this technique is also given. The technique has limitations in terms of image quality distortion and robustness against attacks. The other technique is *ISB*, which enhances the image quality and robustness as compared with the *LSB* method of embedding only one bit of the watermarked image that is focused with the mathematical equations. In addition, the Figure including the technique process and the Table of the technique division are also presented. The proposed *DISB* technique is focused on the new Equations; the Figures of the flowcharts, the pseudo codes, and embedding process are also presented. Later, the first algorithm of image quality with the equations and figures are clarified. This is followed by the second algorithm of image robustness and related equations with figures, which were also presented. The last algorithm of the tradeoff between image quality and robustness with the related figures and equations are also presented. The evaluation for the proposed *Tradeoff_AGA* algorithm have been done. Finally, the summary of the chapter is presented.

CHAPTER FIVE
EXPERIMENTAL RESULTS

5.1 Introduction

In this chapter the results are presented. Section 5.2 presents the data after embedding two bits. Section 5.3 presents the experimental results of the image quality by finding the *PSNR* and *MSE* values. The results of the robustness are presented in Section 5.4 by calculating the *NCC* and *BER* values for all bit planes. While Section 5.5 presents the results and analysis for tradeoff between image quality and robustness by choosing the *PSNR* values that are equal or greater than 30db and choosing the best *NCC* value. Then Section 5.6 presents the complexity results. Finally, Section 5.7 summarize the findings and results.

5.2 Results for Enhancement Image Quality Algorithm

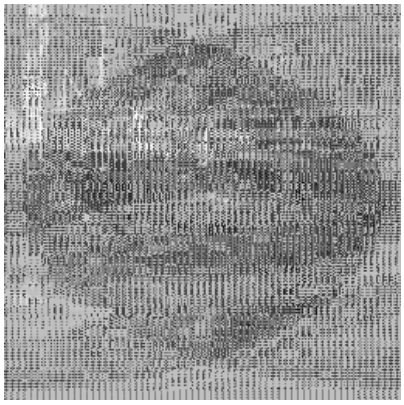
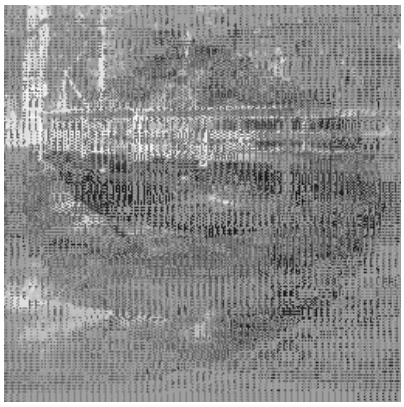
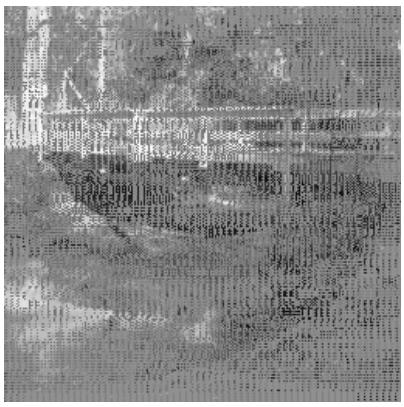
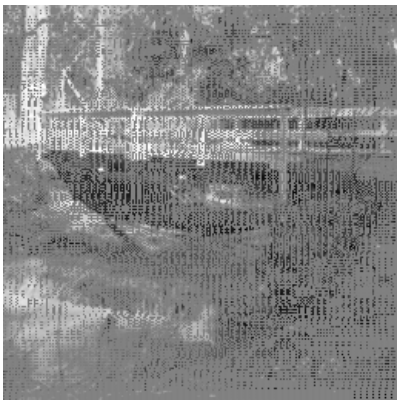
In this section, the results are compared with the *LSB* and *GA*, then the analysis for findings is also given. The *PSNR* and *MSE* were calculated to assess the quality of the watermarked images after embedding the watermark.

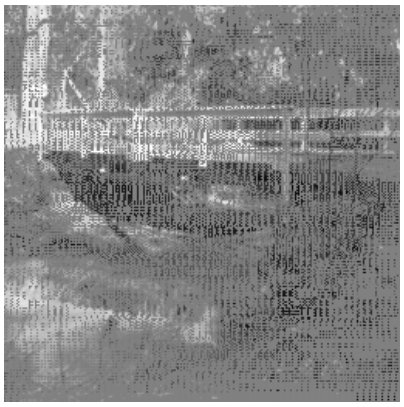
5.2.1 Comparison for Quality_AGA, LSB and GA (Uncompressed Image)

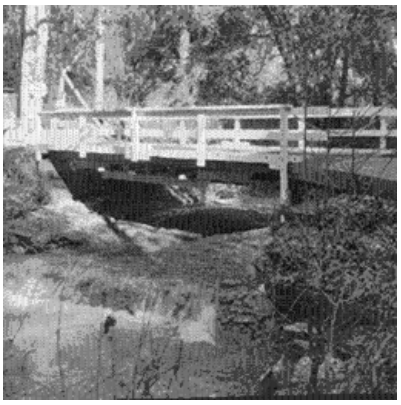
Table 5.1 shows the first watermarked image after embedding two bits on format *BMP* for *Quality_AGA* algorithm, Table 5.2 shows the same watermarked image for *LSB*, and Table 5.3 shows the same watermarked image for *GA*.

Table 5.1

BMP watermarked images for all bit-planes using Quality_AGA

Bit plane	Watermarked image	Bit plane	Watermarked image
k1=1 k2=2		k1=1 k2=5	
k1=1 k2=3		k1=1 k2=6	
k1=1 k2=4		k1=1 k2=7	

Bit plane	Watermarked image	Bit plane	Watermarked image
k1=1 k2=8		k1=2 k2=5	
k1=2 k2=3		k1=2 k2=6	
k1=2 k2=4		k1=2 k2=7	

Bit plane	Watermarked image	Bit plane	Watermarked image
k1=2 k2=8		k1=3 k2=6	
k1=3 k2=4		k1=3 k2=7	
k1=3 k2=5		k1=3 k2=8	

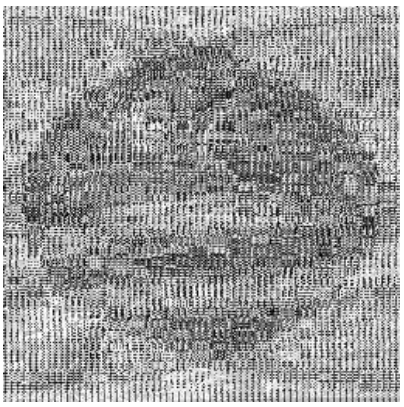
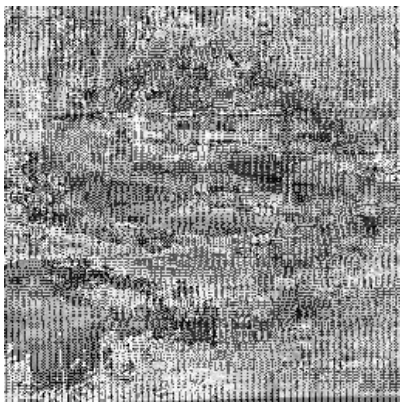
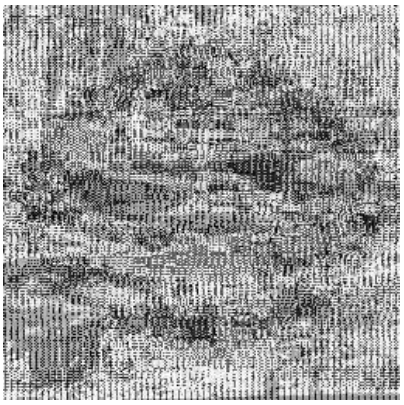
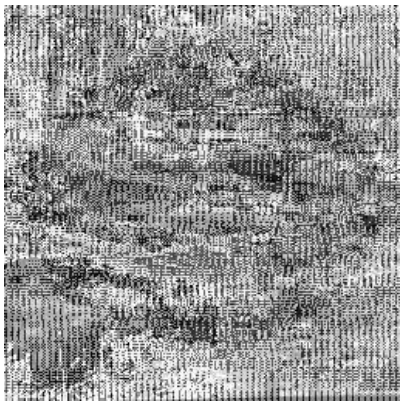
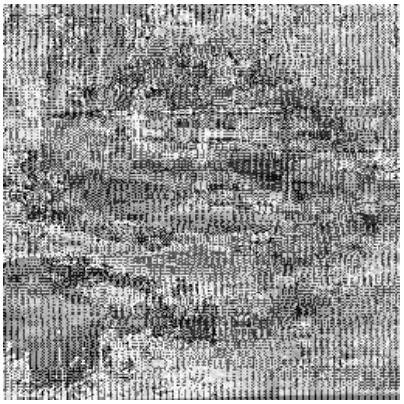
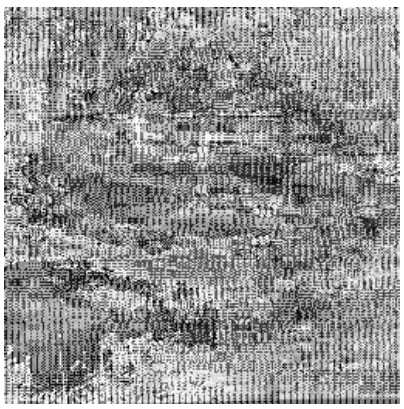
Bit plane	Watermarked image	Bit plane	Watermarked image
k1=4 k2=5		k1=4 k2=8	
k1=4 k2=6		k1=5 k2=6	
k1=4 k2=7		k1=5 k2=7	

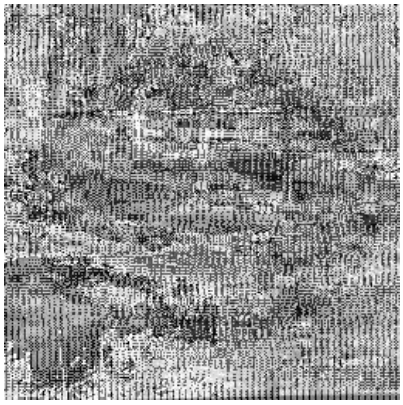
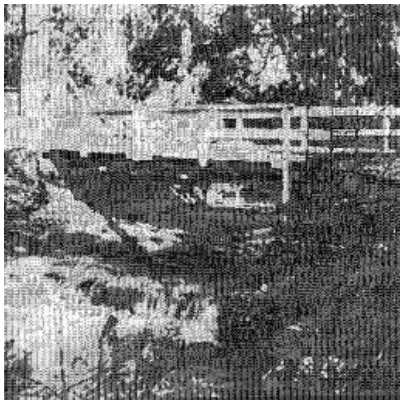
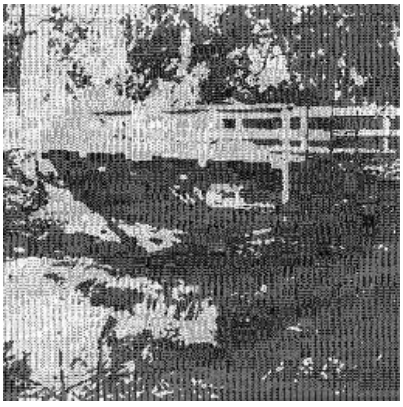
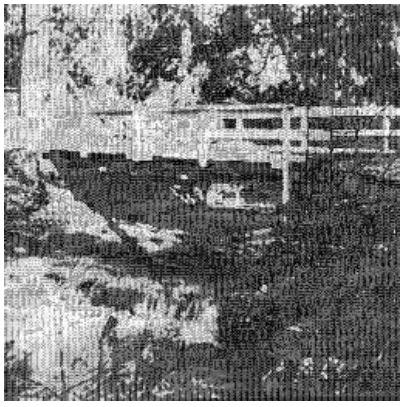
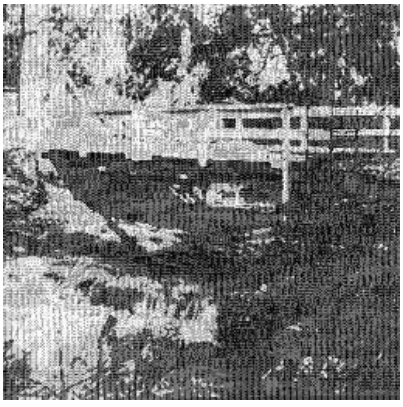
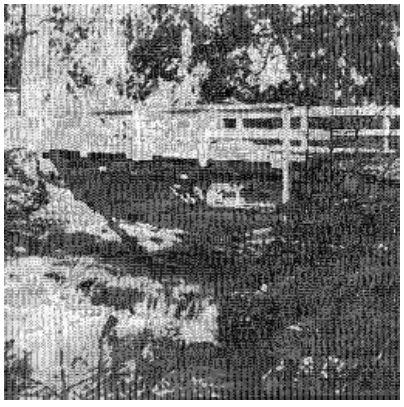
Bit plane	Watermarked image	Bit plane	Watermarked image
k1=5 k2=8		k1=6 k2=8	
k1=6 k2=7		k1=7 k2=8	

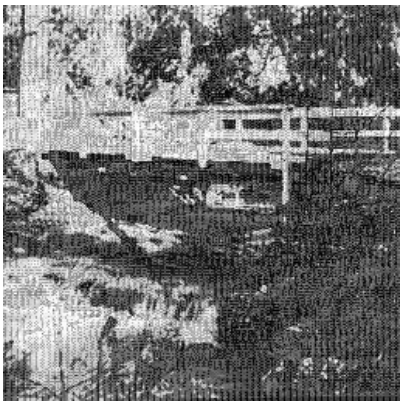
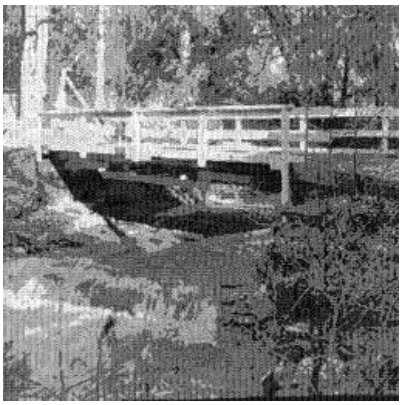
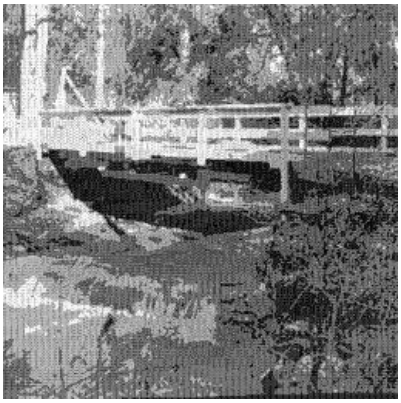
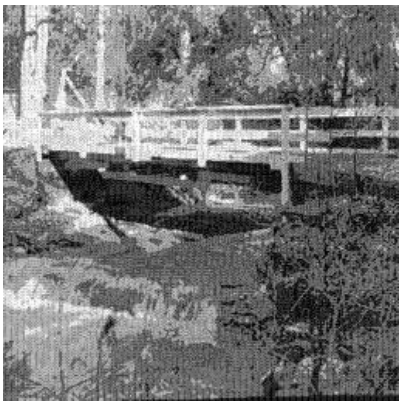
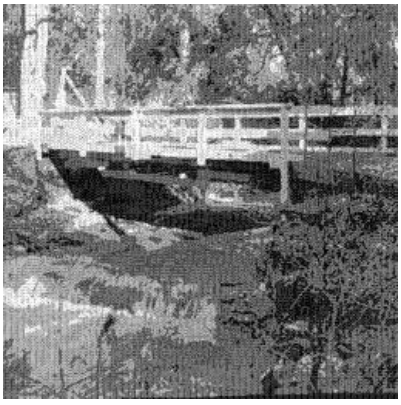
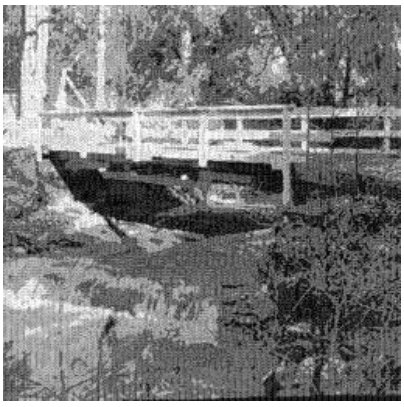
From Table 5.1, it can be seen that the watermarked image after embedding two bits of watermark starts with two keys (key1=1, key2=2) to (key1=7, key2=8) enhancing the image quality gradually which means the first embedded bits represents the worst case and at the same time the last embedded bits represents the best.

Table 5.2

BMP watermarked images for all bit-planes using LSB

Bit plane	Watermarked image	Bit plane	Watermarked image
key1=1 key2=2		key1=1 key2=5	
key1=1 key2=3		key1=1 key2=6	
key1=1 key2=4		key1=1 key2=7	

Bit plane	Watermarked image	Bit plane	Watermarked image
key1=1 key2=8		key1=2 key2=5	
key1=2 key2=3		key1=2 key2=6	
key1=2 key2=4		key1=2 key2=7	

Bit plane	Watermarked image	Bit plane	Watermarked image
key1=2 key2=8		key1=3 key2=6	
key1=3 key2=4		key1=3 key2=7	
key1=3 key2=5		key1=3 key2=8	

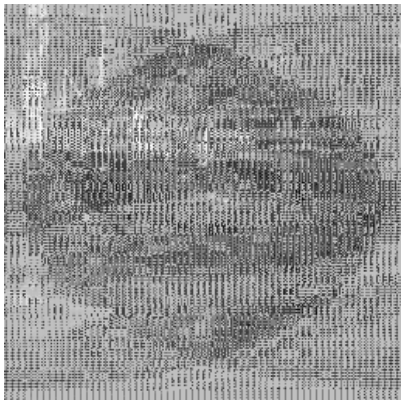
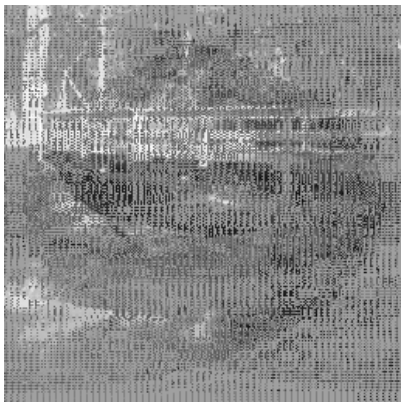
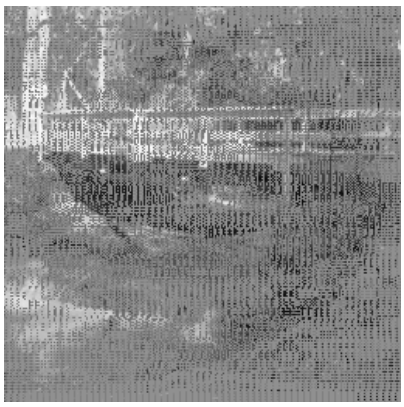
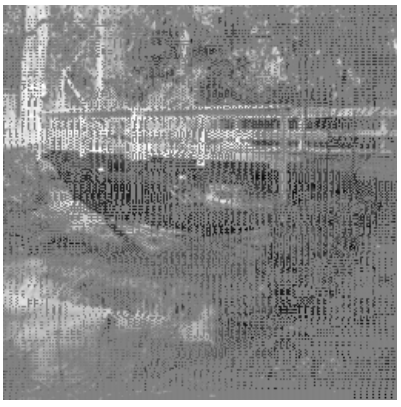
Bit plane	Watermarked image	Bit plane	Watermarked image
key1=4 key2=5		key1=4 key2=8	
key1=4 key2=6		key1=5 key2=6	
key1=4 key2=7		key1=5 key2=7	

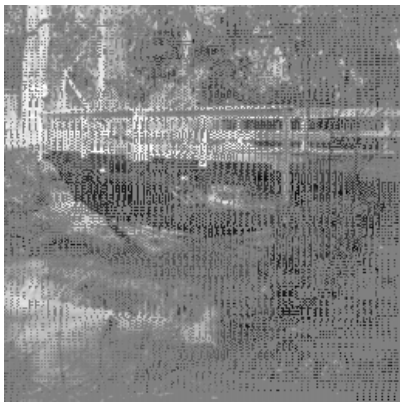
Bit plane	Watermarked image	Bit plane	Watermarked image
key1=5 key2=8		key1=6 key2=8	
key1=6 key2=7		key1=7 key2=8	

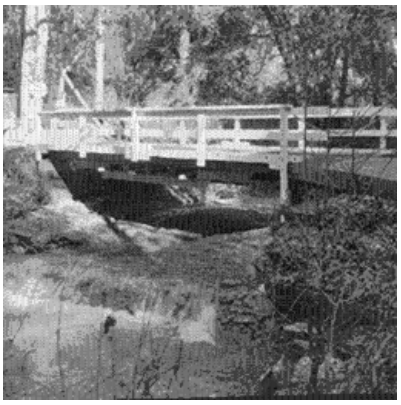
From the Table 5.2, it can be seen that the watermarked image after embedding two bits of watermark starts with the two keys (key1=1, key2=2) to (key1=7, key2=8,) which causes more image distortion as compared with *Quality_AGA*.

Table 5.3

BMP watermarked images for all bit-planes using GA

Bit plane	Watermarked image	Bit plane	Watermarked image
k1=1 k2=2		k1=1 k2=5	
k1=1 k2=3		k1=1 k2=6	
k1=1 k2=4		k1=1 k2=7	

Bit plane	Watermarked image	Bit plane	Watermarked image
k1=1 k2=8		k1=2 k2=5	
k1=2 k2=3		k1=2 k2=6	
k1=2 k2=4		k1=2 k2=7	

Bit plane	Watermarked image	Bit plane	Watermarked image
k1=2 k2=8		k1=3 k2=6	
k1=3 k2=4		k1=3 k2=7	
k1=3 k2=5		k1=3 k2=8	

Bit plane	Watermarked image	Bit plane	Watermarked image
k1=4 k2=5		k1=4 k2=8	
k1=4 k2=6		k1=5 k2=6	
k1=4 k2=7		k1=5 k2=7	

Bit plane	Watermarked image	Bit plane	Watermarked image
k1=5 k2=8		k1=6 k2=8	
k1=6 k2=7		k1=7 k2=8	

From Table 5.3, it can be seen that the watermarked image after embedding two bits enhances the image quality gradually. The algorithm tested with two measurements criteria to assess image quality in term of *PSNR* and *MSE*. Tables 5.4, 5.5, 5.6, and 5.7 show the results in term of *PSNR* and *MSE* values for the first original image on format *BMP*, *TIFF*, *GIF*, and *PNG* sequentially after embedding two bits of watermark1, besides the results for *LSB*, and *GA*.

Table 5.4

PSNR and MSE of the Quality_AGA, LSB and GA for original1 (BMP)

Bit-plane		**Quality_AGA**		**LSB**		**GA**	
key1	**key2**	**PSNR**	**MSE**	**PSNR**	**MSE**	**PSNR**	**MSE**
1	2	11.2002	976.2362	8.3935	968.6643	11.2002	976.2362
1	3	13.6643	945.0421	8.4372	943.8861	13.6643	945.0421
1	4	14.9819	927.9753	8.6639	926.8032	14.9819	927.9753
1	5	15.6461	912.7764	8.7372	911.6434	15.6461	912.7764
1	6	15.9750	893.6355	8.7726	892.6210	15.9750	893.6355
1	7	16.1379	854.4600	8.7882	852.3136	16.1379	854.4600
1	8	16.1379	786.2320	8.7965	783.6692	16.1379	786.2320
2	3	19.7150	715.5444	14.2759	715.3762	19.7150	715.5444
2	4	22.0819	417.1750	14.8630	415.5423	22.0819	417.1750
2	5	23.3990	310.4926	15.0798	310.7698	23.3990	310.4926
2	6	24.0867	266.4470	15.1419	264.3905	24.0867	266.4470
2	7	24.4355	246.6397	15.1597	246.6397	24.4355	246.6397
2	8	24.6066	237.4762	15.1676	235.5606	24.6066	237.4762
3	4	25.8624	168.9703	19.8391	169.8095	25.8624	168.9703
3	5	28.1060	100.9333	20.6418	101.1127	28.1060	100.9333
3	6	29.3894	74.8414	20.8947	75.9086	29.3894	74.8414
3	7	30.1206	63.7321	20.9760	63.9086	30.1206	63.7321
3	8	30.4291	58.9069	21.0105	57.9026	30.4291	58.9069
4	5	31.8069	42.8930	25.8218	41.9856	31.8069	42.8930
4	6	33.9811	26.0001	26.6346	25.8986	33.9811	26.0001
4	7	35.2521	19.4029	26.8932	19.5408	35.2521	19.4029
4	8	35.8758	16.8074	26.9811	15.9097	35.8758	16.8074
5	6	37.4098	11.8060	31.8779	11.4463	37.4098	11.8060
5	7	39.4823	7.3258	32.6770	7.2985	39.4823	7.3258
5	8	40.5140	5.7767	32.9390	5.9411	40.5140	5.7767
6	7	42.5753	3.5938	37.9163	3.4548	42.5753	3.5938
6	8	44.0495	2.5593	38.7077	2.7873	44.0495	2.5593
7	8	46.3119	1.5202	43.9233	1.4563	46.3119	1.5202

Table 5.5

PSNR and MSE of the Quality_AGA, LSB and GA for original1 (TIFF)

Bit-plane		**Quality_AGA**		**LSB**		**GA**	
key1	**key2**	**PSNR**	**MSE**	**PSNR**	**MSE**	**PSNR**	**MSE**
1	2	11.2002	976.2362	8.3935	968.6643	11.2002	976.2362
1	3	13.6643	945.0421	8.4372	943.8861	13.6643	945.0421
1	4	14.9819	927.9753	8.6639	926.8032	14.9819	927.9753
1	5	15.6461	912.7764	8.7372	911.6434	15.6461	912.7764
1	6	15.9750	893.6355	8.7726	892.6210	15.9750	893.6355
1	7	16.1379	854.4600	8.7882	852.3136	16.1379	854.4600
1	8	16.1379	786.2320	8.7965	783.6692	16.1379	786.2320
2	3	19.7150	715.5444	14.2759	715.3762	19.7150	715.5444
2	4	22.0819	417.1750	14.8630	415.5423	22.0819	417.1750
2	5	23.3990	310.4926	15.0798	310.7698	23.3990	310.4926
2	6	24.0867	266.4470	15.1419	264.3905	24.0867	266.4470
2	7	24.4355	246.6397	15.1597	246.6397	24.4355	246.6397
2	8	24.6066	237.4762	15.1676	235.5606	24.6066	237.4762
3	4	25.8624	168.9703	19.8391	169.8095	25.8624	168.9703
3	5	28.1060	100.9333	20.6418	101.1127	28.1060	100.9333
3	6	29.3894	74.8414	20.8947	75.9086	29.3894	74.8414
3	7	30.1206	63.7321	20.9760	63.9086	30.1206	63.7321
3	8	30.4291	58.9069	21.0105	57.9026	30.4291	58.9069
4	5	31.8069	42.8930	25.8218	41.9856	31.8069	42.8930
4	6	33.9811	26.0001	26.6346	25.8986	33.9811	26.0001
4	7	35.2521	19.4029	26.8932	19.5408	35.2521	19.4029
4	8	35.8758	16.8074	26.9811	15.9097	35.8758	16.8074
5	6	37.4098	11.8060	31.8779	11.4463	37.4098	11.8060
5	7	39.4823	7.3258	32.6770	7.2985	39.4823	7.3258
5	8	40.5140	5.7767	32.9390	5.9411	40.5140	5.7767
6	7	42.5753	3.5938	37.9163	3.4548	42.5753	3.5938
6	8	44.0495	2.5593	38.7077	2.7873	44.0495	2.5593
7	8	46.3119	1.5202	43.9233	1.4563	46.3119	1.5202

Table 5.6

PSNR and MSE of the Quality_AGA, LSB and GA for original1 (GIF)

Bit-plane		Quality_AGA		LSB		GA	
key1	**key2**	**PSNR**	**MSE**	**PSNR**	**MSE**	**PSNR**	**MSE**
1	2	11.2002	976.2362	8.3935	968.6643	11.2002	976.2362
1	3	13.6643	945.0421	8.4372	943.8861	13.6643	945.0421
1	4	14.9819	927.9753	8.6639	926.8032	14.9819	927.9753
1	5	15.6461	912.7764	8.7372	911.6434	15.6461	912.7764
1	6	15.9750	893.6355	8.7726	892.6210	15.9750	893.6355
1	7	16.1379	854.4600	8.7882	852.3136	16.1379	854.4600
1	8	16.1379	786.2320	8.7965	783.6692	16.1379	786.2320
2	3	19.7150	715.5444	14.2759	715.3762	19.7150	715.5444
2	4	22.0819	417.1750	14.8630	415.5423	22.0819	417.1750
2	5	23.3990	310.4926	15.0798	310.7698	23.3990	310.4926
2	6	24.0867	266.4470	15.1419	264.3905	24.0867	266.4470
2	7	24.4355	246.6397	15.1597	246.6397	24.4355	246.6397
2	8	24.6066	237.4762	15.1676	235.5606	24.6066	237.4762
3	4	25.8624	168.9703	19.8391	169.8095	25.8624	168.9703
3	5	28.1060	100.9333	20.6418	101.1127	28.1060	100.9333
3	6	29.3894	74.8414	20.8947	75.9086	29.3894	74.8414
3	7	30.1206	63.7321	20.9760	63.9086	30.1206	63.7321
3	8	30.4291	58.9069	21.0105	57.9026	30.4291	58.9069
4	5	31.8069	42.8930	25.8218	41.9856	31.8069	42.8930
4	6	33.9811	26.0001	26.6346	25.8986	33.9811	26.0001
4	7	35.2521	19.4029	26.8932	19.5408	35.2521	19.4029
4	8	35.8758	16.8074	26.9811	15.9097	35.8758	16.8074
5	6	37.4098	11.8060	31.8779	11.4463	37.4098	11.8060
5	7	39.4823	7.3258	32.6770	7.2985	39.4823	7.3258
5	8	40.5140	5.7767	32.9390	5.9411	40.5140	5.7767
6	7	42.5753	3.5938	37.9163	3.4548	42.5753	3.5938
6	8	44.0495	2.5593	38.7077	2.7873	44.0495	2.5593
7	8	46.3119	1.5202	43.9233	1.4563	46.3119	1.5202

Table 5.7

PSNR and MSE of the Quality_AGA, LSB and GA for original1 (PNG)

Bit-plane		**Quality_AGA**		**LSB**		**GA**	
key1	**key2**	**PSNR**	**MSE**	**PSNR**	**MSE**	**PSNR**	**MSE**
1	2	11.2002	976.2362	8.3935	968.6643	11.2002	976.2362
1	3	13.6643	945.0421	8.4372	943.8861	13.6643	945.0421
1	4	14.9819	927.9753	8.6639	926.8032	14.9819	927.9753
1	5	15.6461	912.7764	8.7372	911.6434	15.6461	912.7764
1	6	15.9750	893.6355	8.7726	892.6210	15.9750	893.6355
1	7	16.1379	854.4600	8.7882	852.3136	16.1379	854.4600
1	8	16.1379	786.2320	8.7965	783.6692	16.1379	786.2320
2	3	19.7150	715.5444	14.2759	715.3762	19.7150	715.5444
2	4	22.0819	417.1750	14.8630	415.5423	22.0819	417.1750
2	5	23.3990	310.4926	15.0798	310.7698	23.3990	310.4926
2	6	24.0867	266.4470	15.1419	264.3905	24.0867	266.4470
2	7	24.4355	246.6397	15.1597	246.6397	24.4355	246.6397
2	8	24.6066	237.4762	15.1676	235.5606	24.6066	237.4762
3	4	25.8624	168.9703	19.8391	169.8095	25.8624	168.9703
3	5	28.1060	100.9333	20.6418	101.1127	28.1060	100.9333
3	6	29.3894	74.8414	20.8947	75.9086	29.3894	74.8414
3	7	30.1206	63.7321	20.9760	63.9086	30.1206	63.7321
3	8	30.4291	58.9069	21.0105	57.9026	30.4291	58.9069
4	5	31.8069	42.8930	25.8218	41.9856	31.8069	42.8930
4	6	33.9811	26.0001	26.6346	25.8986	33.9811	26.0001
4	7	35.2521	19.4029	26.8932	19.5408	35.2521	19.4029
4	8	35.8758	16.8074	26.9811	15.9097	35.8758	16.8074
5	6	37.4098	11.8060	31.8779	11.4463	37.4098	11.8060
5	7	39.4823	7.3258	32.6770	7.2985	39.4823	7.3258
5	8	40.5140	5.7767	32.9390	5.9411	40.5140	5.7767
6	7	42.5753	3.5938	37.9163	3.4548	42.5753	3.5938
6	8	44.0495	2.5593	38.7077	2.7873	44.0495	2.5593
7	8	46.3119	1.5202	43.9233	1.4563	46.3119	1.5202

From Tables 5.4, 5.5, 5.6, and 5.7, it can be seen that the *MSE* value is the opposite of *PSNR* value, that is why *PSNR* increases gradually from the first two embedded bits to the last two while *MSE* decreases. The results from these tables after the comparison between *Quality_AGA*, *LSB*, and *GA*, show that the two algorithms *Quality_AGA* and *GA* investigated the better and same values for both measurements *PSNR* and *MSE*, while *LSB* investigated the worst values which means bad quality for the watermarked image.

5.2.2 Comparison for Quality_AGA, LSB and GA (Compressed Image)

Tables 5.8 shows the result in terms of *PSNR* and *MSE* values for the first original image on format *JPEG* after embedding two bits of watermark1, besides the results for *LSB*, and *GA*.

Table 5.8

PSNR and MSE of the Quality_AGA, LSB and GA for original1 (JPEG)

Bit-plane		**Quality_AGA**		**LSB**		**GA**	
key1	**key2**	**PSNR**	**MSE**	**PSNR**	**MSE**	**PSNR**	**MSE**
1	2	15.7535	976.2362	8.3935	968.6643	15.7535	976.2362
1	3	18.1122	945.0421	8.4372	943.8861	18.1122	945.0421
1	4	19.3626	927.9753	8.6639	926.8032	19.3626	927.9753
1	5	19.9884	912.7764	8.7372	911.6434	19.9884	912.7764
1	6	20.2972	893.6355	8.7726	892.6210	20.2972	893.6355
1	7	20.4498	854.4600	8.7882	852.3136	20.4498	854.4600
1	8	20.5254	786.2320	8.7965	783.6692	20.5254	786.2320
2	3	24.3532	715.5444	14.2759	715.3762	24.3532	715.5444
2	4	26.7048	417.1750	14.8630	415.5423	26.7048	417.1750
2	5	28.0023	310.4926	15.0798	310.7698	28.0023	310.4926
2	6	28.6757	266.4470	15.1419	264.3905	28.6757	266.4470
2	7	29.0164	246.6397	15.1597	246.6397	29.0164	246.6397
2	8	29.1832	237.4762	15.1676	235.5606	29.1832	237.4762
3	4	30.6177	168.9703	19.8391	169.8095	30.6177	168.9703
3	5	32.8548	100.9333	20.6418	101.1127	32.8548	100.9333
3	6	34.1605	74.8414	20.8947	75.9086	34.1605	74.8414
3	7	34.8618	63.7321	20.9760	63.9086	34.8618	63.7321
3	8	35.2058	58.9069	21.0105	57.9026	35.2058	58.9069
4	5	36.5842	42.8930	25.8218	41.9856	36.5842	42.8930
4	6	38.7539	26.0001	26.6346	25.8986	38.7539	26.0001
4	7	40.0266	19.4029	26.8932	19.5408	40.0266	19.4029
4	8	40.6526	16.8074	26.9811	15.9097	40.6526	16.8074
5	6	42.1895	11.8060	31.8779	11.4463	42.1895	11.8060
5	7	44.2611	7.3258	32.6770	7.2985	44.2611	7.3258
5	8	45.2941	5.7767	32.9390	5.9411	45.2941	5.7767
6	7	47.3596	3.5938	37.9163	3.4548	47.3596	3.5938
6	8	48.8137	2.5593	38.7077	2.7873	48.8137	2.5593
7	8	51.1105	1.5202	43.9233	1.4563	51.1105	1.5202

From Table 5.8, it can be seen that the *MSE* value is the opposite of *PSNR* value, that's why *PSNR* increases gradually from the first two embedded bits to the last two while *MSE* decreases. The results differ from uncompressed images and the image quality is better than other types of uncompressed image. Besides, from these tables after the comparison between *Quality_AGA*, *LSB*, and *GA*, it is shown that the two algorithms *Quality_AGA* and *GA* investigated the better and same values for both measurements *PSNR* and *MSE*, while *LSB* investigated the worst values which means bad quality for the watermarked image.

Furthermore, by comparing the proposed algorithm with the *LSB* method, it is also noticed that the quality of watermarked images has been improved using the proposed method. For example, the image of bits (3, 7) is observed to be better than those of bits (3, 7) and bits (4, 5) whereas the other images can show similar quality differences. While the *MSE* values for both methods decrease gradually from the first two embedded bits to the last two embedded bits.

Apart from that, Figure 5.1 shows the difference between the quality of watermarked images by using the proposed algorithm based on *ISB* and the *LSB* method, thus, the proposed technique is greatly better than the *LSB* by embedding two bits.

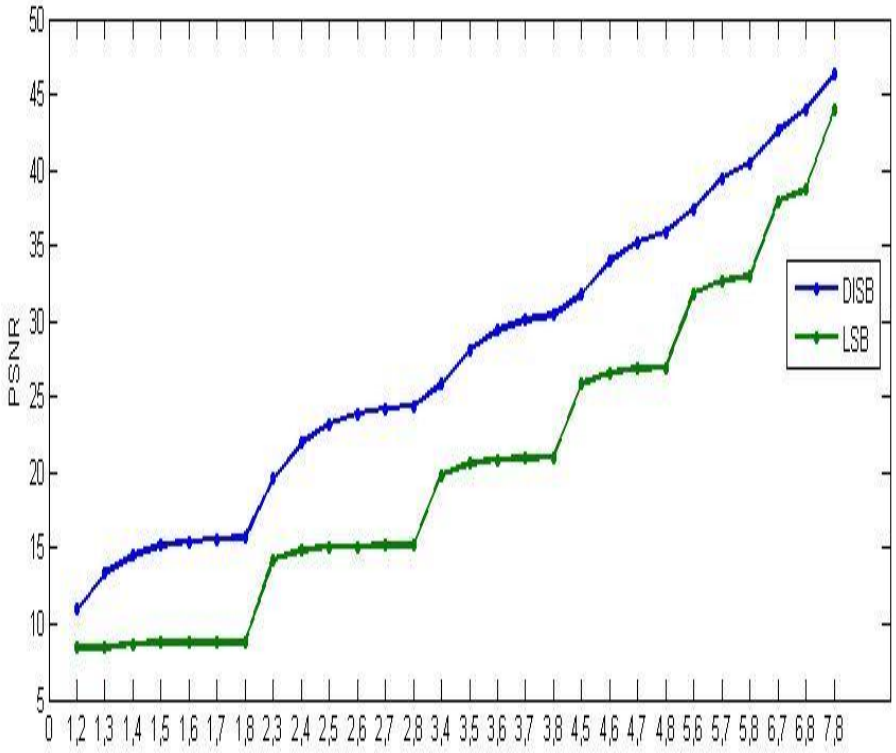


Figure 5.1. The PSNR values of the proposed algorithm and of the LSB method for the different bit-planes

From Figure 5.1, the difference between *Quality_AGA* and *LSB* can be seen. The proposed algorithm investigated better *PSNR* values than *LSB*; this is because the *LSB* method replaced the new pixels with the original ones directly even if the embedded bits were different, so the result will demonstrate worse quality and the watermarked image will be more distorted. The proposed algorithm takes over the new pixels closest to the original ones; hence, the quality is better.

5.2.3 Results of Quality_AGA and Computation Complexity

"Time complexity of an algorithm means the total time required by the program to run to completion. Time complexity is most commonly estimated by counting the number of elementary functions performed by the algorithm". Computational complexity can be easily established by measuring the time for embedding/extraction or by comparing the asymptotic expressions for complexity of the algorithms as a function of the image and message sizes (Fridrich and Goljan, 1999). In this study a comparison between *Quality_AGA* algorithm and *GA* has been conducted by calculating the time that needed for the two algorithms (second) for the embedding process which is clarified in Tables 5.9 and 5.10, respectively. The comparison between the two algorithms has been conducted by testing six of the twelve original images.

Table 5.9

The time (second) of the Quality_AGA for all bit planes

Bit- plane		Bridge	Boats	Camera	Milkdrop	Plane	Peppers
key1	key2						
1	2	24.072956	24.158659	24.326478	24.182818	24.176420	26.359278
1	3	24.028363	24.552305	24.213913	24.784743	24.342618	24.516936
1	4	24.069077	24.117336	24.297099	24.310352	24.314863	24.152103
1	5	24.031508	24.102940	24.332057	24.276632	24.250761	24.206052
1	6	24.122660	24.184117	24.442975	24.172006	24.349632	24.198835
1	7	24.131506	24.229291	24.245418	24.319664	24.328931	24.256518
1	8	24.373659	24.239144	24.334196	24.326571	24.344043	24.347229
2	3	24.017318	24.067735	24.103959	24.131253	24.132135	24.433370
2	4	24.244416	24.105408	24.220477	24.181623	24.207536	24.378236
2	5	24.226584	24.052312	24.246799	24.358380	24.219573	24.183067
2	6	24.293197	24.116909	24.340268	24.296714	24.162078	24.338308
2	7	24.090591	24.205585	24.231257	24.465374	24.240438	24.390419
2	8	24.179250	24.272626	24.304263	24.270194	24.171545	24.328321
3	4	24.023198	24.166605	24.357450	24.197657	24.214774	24.426009
3	5	24.099637	24.403260	24.250509	24.204865	24.140061	24.210264
3	6	24.065720	24.139410	24.301422	24.170181	24.372783	24.380663
3	7	24.155004	24.180062	24.343905	24.210993	24.414472	24.454599
3	8	24.253044	24.218694	24.236660	25.489612	24.244130	24.134379
4	5	24.353096	24.253922	24.425721	24.172493	24.141289	24.129428
4	6	24.254767	24.178023	24.420236	24.220038	24.383904	24.346539
4	7	24.133186	24.220247	24.301184	24.278162	24.251013	24.384200
4	8	24.198867	24.206845	24.220781	24.165735	24.207526	24.236719
5	6	24.319730	24.309608	24.367386	24.297263	24.142034	24.065566
5	7	24.231448	24.285174	24.294283	24.471295	24.258970	24.199370
5	8	24.159791	24.258373	24.154331	24.206877	24.175312	24.169725
6	7	24.146809	24.248790	24.125194	24.388843	24.153367	24.306317
6	8	24.814787	24.290160	24.198313	24.200084	24.221128	24.102909
7	8	24.106557	24.324736	24.265539	24.226687	24.258502	24.172980

Table 5.10

The time (second) of the GA for all bit planes

Bit-Key1	Plane Key2	Bridge	Boats	Camera	Milk drop	Plane	Peppers
1	2	1964	1968	1975	1971	1970	1968
1	3	1968	1972	1971	1966	1965	1966
1	4	1969	1969	1967	1965	1959	1965
1	5	1974	1977	1965	1968	1962	1961
1	6	1977	1968	1965	1963	1960	1965
1	7	1968	1965	1970	1975	1972	1972
1	8	1966	1970	1973	1971	1974	1959
2	3	1971	1975	1968	1962	1964	1966
2	4	1969	1972	1977	1967	1964	1974
2	5	1966	1962	1969	1963	1965	1975
2	6	1972	1963	1966	1967	1965	1961
2	7	1974	1978	1968	1973	1969	1966
2	8	1970	1972	1968	1963	1972	1961
3	4	1969	1966	1973	1967	1973	1978
3	5	1956	1965	1966	1963	1968	1977
3	6	1963	1968	1962	1971	1965	1961
3	7	1967	1966	1974	1955	1967	1976
3	8	1964	1972	1968	1969	1968	1971
4	5	1965	1967	1968	1967	1970	1976
4	6	1970	1969	1976	1966	1963	1969
4	7	1965	1967	1965	1963	1967	1972
4	8	1978	1967	1953	1961	1976	1962
5	6	1960	1963	1974	1965	1978	1966
5	7	1965	1968	1963	1969	1975	1967
5	8	1969	1961	1961	1967	1978	1971
6	7	1977	1973	1962	1965	1967	1969
6	8	1965	1970	1964	1971	1961	1960
7	8	1963	1962	1962	1966	1974	1961

It is seen from the tables (5.9 & 5.10) that the time is greatly better when using the *Quality_AGA* image algorithm than the time when using the *GA*. The main reason being the *GA* takes all the probabilities for all bit-planes. Hence, it takes longer for the appropriate pixel value to be reached. While the quality image algorithm replaces the new pixels which are the nearest to the original ones, the time taken is better. At the same time, the quality of both methods exactly matches and the results show the improvement for the two algorithms.

In addition, Figure 5.2 clarified the difference between the times of each algorithm needed for the embedding process. It is clear that the proposed algorithm is better than *GA*, which needed a long time for embedding.

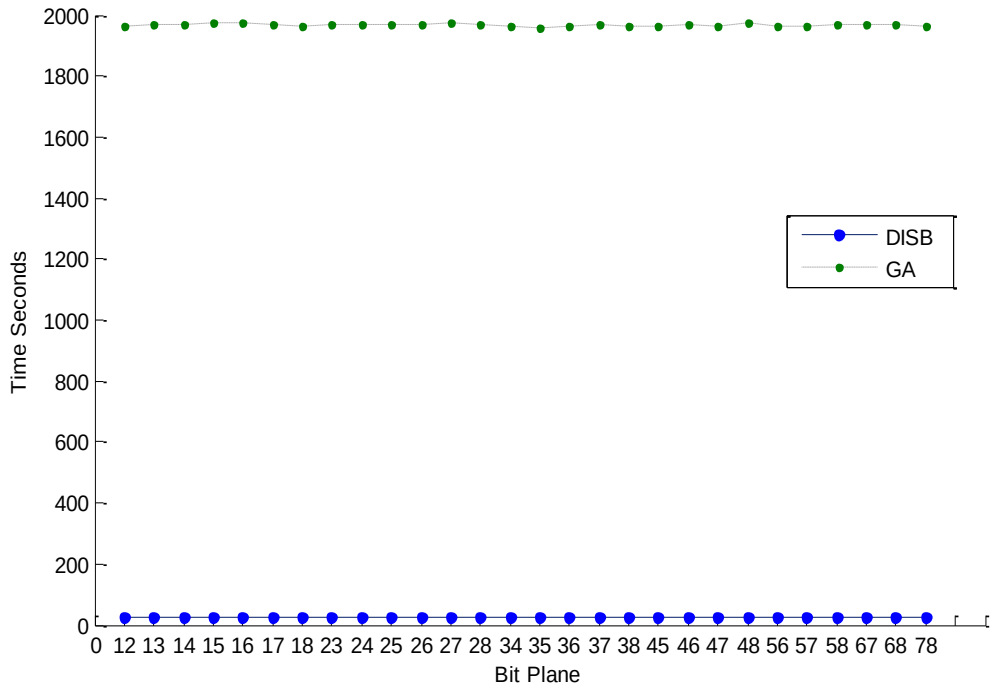


Figure 5.2. The time values of the proposed quality image algorithm and the GA for the different bit-planes

5.3 Results for Robustness_AGA Algorithm

In this section, the enhanced image robustness algorithm is applied based on *DISB* technique by embedding two bits of the watermarked image.

One watermark image from the six (as mentioned in the previous chapter) was embedded within twelve original images using the proposed technique explained. The results of one of these embedding are elaborated in detail in this section, while the other results are briefly presented.

The formulas and measurements of the robustness of image watermarking were given in Chapter Three. The *NCC* and *BER* were used to assess the robustness of the watermarked images after embedding the watermarked objects. In this section, the results compared to the *LSB* method and the analyses for findings are also given. The watermarking algorithm must embed the watermark, so that it will be robust against the chosen processing operations (attacks) that can destroy or distort the watermarked image. To consider the proposed algorithm under different image attacks, the following attacks were applied to the watermarked image: Blurring, Gaussian filter, Wiener filter, Speckle noise, and *JPEG* compression. The algorithm concentrates on the best robustness of the watermarked image, based on *ISB*. All the bit-planes were tested, starting from the 1st bit-plane (*MSB*) through the 8th bit-plane (*LSB*). Table 5.11 shows the *PSNR* with *NCC* for each embedding, while Table 5.12 shows the *PSNR* with *BER* for each embedding.

Table 5.11

PSNR and the NCC values of Robust_AGA

Bit-plane key1	Bit-plane key2	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
1	2	6.3269	1	1	1	1	1
1	3	10.1828	0.9244	1	1	1	0.9235
1	4	12.7696	0.9197	0.9672	0.9996	1	0.9192
1	5	14.2824	0.9047	0.9033	0.9844	0.9921	0.9087
1	6	15.0897	0.8536	0.8219	0.9361	0.9611	0.8779
1	7	15.5030	0.7856	0.7617	0.8524	0.8587	0.7816
1	8	15.7110	0.7392	0.7367	0.7750	0.6876	0.7332
2	3	13.9755	0.8169	0.9598	0.9910	0.9980	0.8233
2	4	18.1494	0.9001	0.9414	0.9895	0.9939	0.9085
2	5	21.1101	0.8864	0.8969	0.9726	0.9750	0.9015
2	6	22.9077	0.8546	0.8579	0.9368	0.9327	0.8651
2	7	23.8803	0.8194	0.8228	0.8850	0.8529	0.8362
2	8	24.3746	0.7935	0.8043	0.8373	0.7836	0.8003
3	4	20.1356	0.8071	0.8737	0.9819	0.9887	0.8223
3	5	24.3652	0.8590	0.8232	0.9718	0.9671	0.8856
3	6	27.4551	0.8252	0.7597	0.9212	0.8968	0.8560
3	7	29.3825	0.7721	0.7246	0.8364	0.7776	0.7964
3	8	30.4291	0.7382	0.6930	0.7531	0.7076	0.7549
4	5	26.3965	0.7412	0.7856	0.9537	0.9306	0.7795
4	6	30.7309	0.7750	0.7545	0.9311	0.8194	0.8227
4	7	33.9317	0.7285	0.7012	0.8466	0.7392	0.7746
4	8	35.8758	0.6936	0.6766	0.7623	0.6932	0.7297
5	6	32.7585	0.6623	0.6889	0.8963	0.7319	0.6916
5	7	37.2915	0.6652	0.6720	0.8481	0.6965	0.6949
5	8	40.5140	0.6498	0.6492	0.7685	0.6620	0.6671
6	7	39.4561	0.6043	0.6298	0.7830	0.6432	0.6108
6	8	44.0495	0.6092	0.6247	0.7420	0.6334	0.6140
7	8	46.3119	0.6007	0.6106	0.6802	0.6116	0.6154

Table 5.12

PSNR and the BER values of Robust_AGA

Bit-plane key1	Bit-plane key2	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
1	2	6.3269	0.4210	0.4185	0.3989	0.3890	0.4126
1	3	10.1828	0.4229	0.4329	0.4143	0.4068	0.4277
1	4	12.7696	0.4097	0.4372	0.4407	0.4322	0.4288
1	5	14.2824	0.4321	0.4392	0.4520	0.4541	0.4445
1	6	15.0897	0.4506	0.4528	0.4232	0.4377	0.4680
1	7	15.5030	0.4685	0.4755	0.4655	0.4705	0.4113
1	8	15.7110	0.4008	0.4091	0.4210	0.4121	0.4248
2	3	13.9755	0.4443	0.4626	0.4418	0.4339	0.4597
2	4	18.1494	0.4290	0.4240	0.4306	0.4316	0.4399
2	5	21.1101	0.4323	0.4146	0.4760	0.4105	0.4204
2	6	22.9077	0.4188	0.4267	0.4131	0.4244	0.4195
2	7	23.8803	0.4276	0.4373	0.4802	0.4506	0.4333
2	8	24.3746	0.4099	0.4143	0.4504	0.4262	0.4096
3	4	20.1356	0.4375	0.5022	0.4991	0.4883	0.4887
3	5	24.3652	0.4230	0.4447	0.4387	0.4630	0.4406
3	6	27.4551	0.4455	0.4481	0.4299	0.4092	0.4339
3	7	29.3825	0.4376	0.4460	0.4033	0.4559	0.4668
3	8	30.4291	0.4601	0.4594	0.4430	0.4600	0.4467
4	5	26.3965	0.4211	0.4426	0.4671	0.4387	0.4482
4	6	30.7309	0.4848	0.4848	0.9311	0.4848	0.4848
4	7	33.9317	0.4548	0.4548	0.8466	0.4548	0.4548
4	8	35.8758	0.4628	0.4628	0.7623	0.4628	0.4628
5	6	32.7585	0.4457	0.4457	0.8963	0.4457	0.4457
5	7	37.2915	0.4840	0.4840	0.8481	0.4840	0.4840
5	8	40.5140	0.4770	0.4770	0.7685	0.4770	0.4770
6	7	39.4561	0.4981	0.4981	0.7830	0.4981	0.4981
6	8	44.0495	0.4846	0.4846	0.7420	0.4846	0.4846
7	8	46.3119	0.4992	0.4992	0.6802	0.4992	0.4992

From Tables 5.11 and 5.12, it can be seen that by moving from the 8th bit-plane to the 1st bit-plane, the resilience in both techniques are developed since the attack modifies the small value (last bit-planes) much easier than the big value, such as in the first bit-planes. And at the same time the *BER* represents the error for the bits in the existing pixels that happened after embedding watermark, also after applying the chosen attacks the error happened in the existing pixels and the measurement *BER* is shown for all bit planes. The difference between LSB and the proposed algorithm can be shown clearly in Figure 5.3, which clarifies the watermarked image for both techniques after applying Gaussian filter and then extracting the watermarked image. Figure 5.4 shows the difference in *PSNR* values for both techniques.

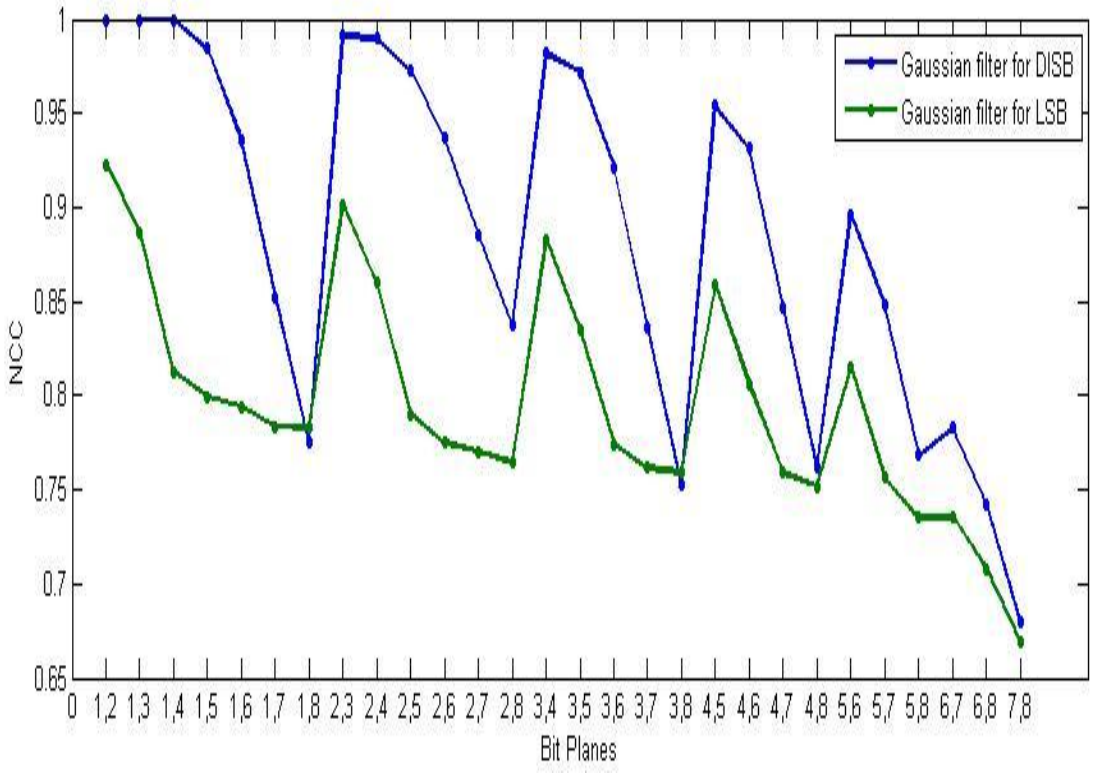


Figure 5.3. The NCC values of the proposed algorithm and of the LSB using Gaussian filter

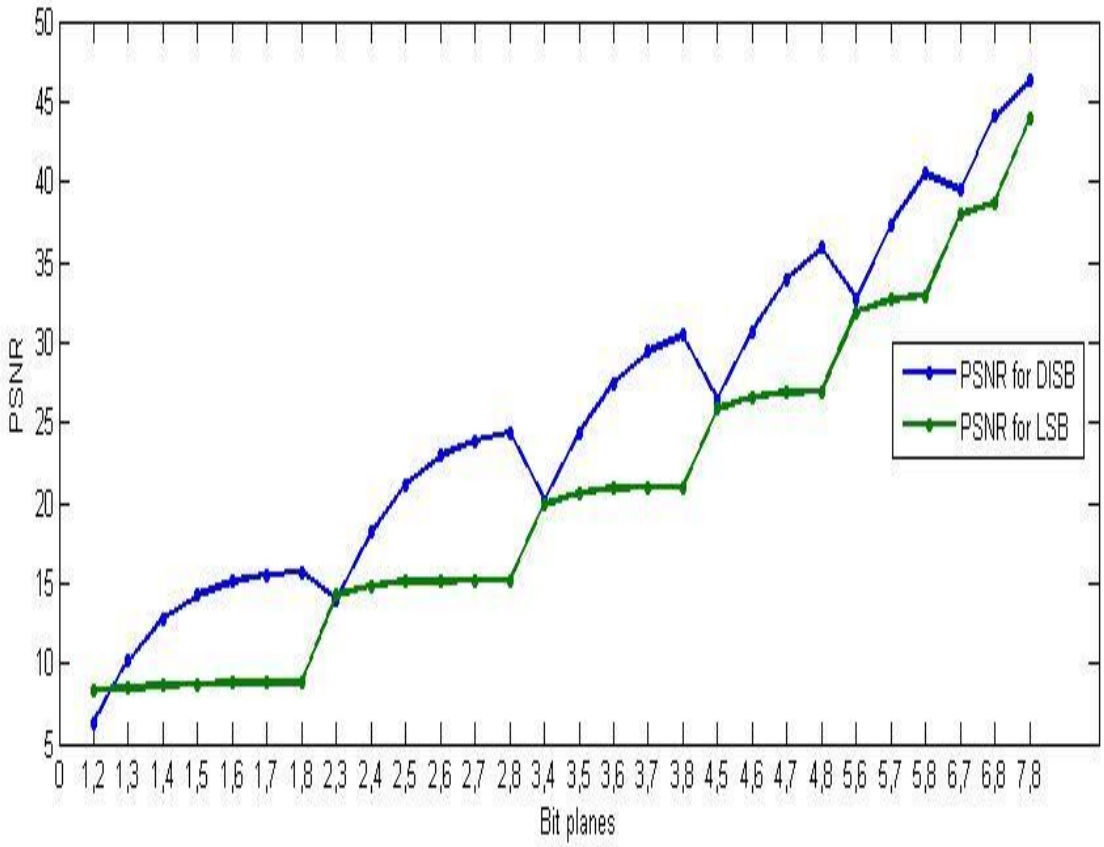


Figure 5.4. The PSNR values of the proposed algorithm and of the LSB using Gaussian filter

After applying the chosen attacks, the extracted watermarks (logos) for the proposed technique and the *LSB* method in all the bit-planes are illustrated in Tables 5.13 and 5.14, respectively.

Table 5.13

Extracted watermark after applying a Gaussian filter (ISB)

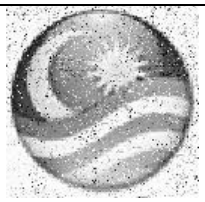
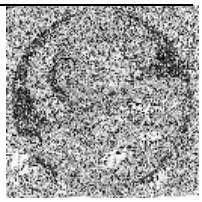
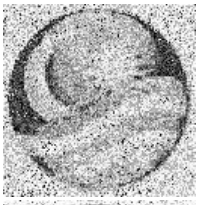
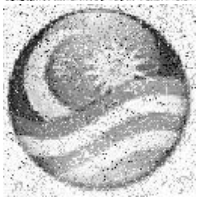
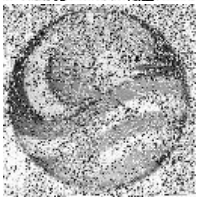
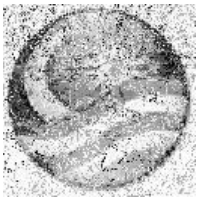
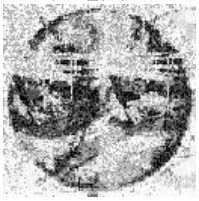
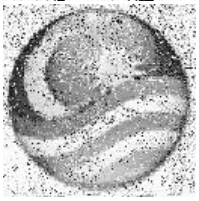
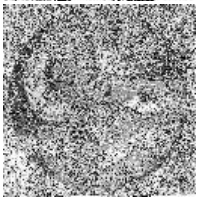
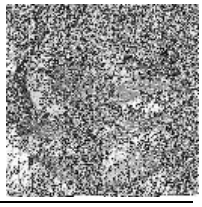
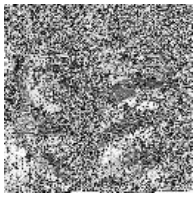
Bit plane k_1	Bit plane k_2	Watermarked image	Bit plane k_1	Bit plane k_2	Watermarked image	Bit plane k_1	Bit plane k_2	Watermarked image	Bit plane k_1	Bit plane k_2	Watermarked image
1	2		2	3		3	5		4	8	
1	3		2	4		3	6		5	6	
1	4		2	5		3	7		5	7	
1	5		2	6		3	8		5	8	
1	6		2	7		4	5		6	7	
1	7		2	8		4	6		6	8	
1	8		3	4		4	7		7	8	

Table 5.14

Extracted watermark after applying a Gaussian filter (LSB)

Bit plane k_1 k_2	Watermarked image	Bit plane k_1 k_2	Watermarked image	Bit plane k_1 k_2	Watermarked image	Bit plane k_1 k_2	Watermarked image
1 2		2 3		3 5		4 8	
1 3		2 4		3 6		5 6	
1 4		2 5		3 7		5 7	
1 5		2 6		3 8		5 8	
1 6		2 7		4 5		6 7	
1 7		2 8		4 6		6 8	
1 8		3 4		4 7		7 8	

From Tables 5.13 and 5.14, the *NCC* of the extracted logo is better than the *LSB* method using the proposed method, particularly in the first bit planes which have bigger values of the range. This improvement is gradually decreased from the (1, 2) to the (7, 8) bit-planes. That is to say that this technique is more resilient against image processing operations such as compression, filtering, blurring and noise, that changes the level of intensity of the pixels.

5.4 Results for Trading-off between Robustness and Image Quality

In the previous sections, the position of the watermarked pixel was tested based on the sub-period of each bit-plane. Thus, the value of the pixel was positioned on the edge of the sub- period, any kind of minor modification by the attacks was found to move the pixel from one range to another and the watermark could not be removed, as elaborated and shown in sub-section 5.2.1. On the other hand, if the watermarked pixel is according to the length of the sub-period (2^{k1-1}), any effect at the pixel of attacks would then make it difficult to move the selected two bits to another range and the bits could be extracted correctly. In this study, the balance between robustness and quality of watermarked image was achieved by moving the watermarked pixel away from the edge of the sub- period.

In addition, the threshold value considered as the value between the edges of the sub-period, was found to survive against different types of attacks, and at the same time kept the best image quality. It can be presumed that the threshold value (*DIST*) is the smallest distance from the location of the watermarked pixel $p`$ to the edge of the sub period, which is nearer to the initial pixel. In other words, if the distance from the

pixel to the edge of the sub period is larger than the threshold value, the pixel's location will not alter. However, if the distance from the pixel to the edge of the sub-period is lesser than the threshold value, the pixel's location will alter to be as far as the threshold value. The *PSNR* and the *NCC* for the proposed algorithm of threshold values (*DIST*) were calculated after applying the chosen attacks in which the *PSNR* was equal or greater than 30 db, as shown in Tables 5.15 through 5.26. The results of the next tables are for embedding *watermark1* within *original1*. Notice that the *PSNR* had been calculated before applying any attack. Although some attacks were found to improve the quality of the image (such as filtering and compression), some others were found to destroy the image (such as blurring and noise).

Table 5.15

PSNR and MSE of the Tradeoff_AGA where key1=3, key2=7

DIST	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	30.8057	0.7220	0.6712	0.6974	0.6880	0.7424
1	30.0872	0.7487	0.7100	0.7840	0.7335	0.7733

Table 5.16

PSNR and MSE of the Tradeoff_AGA where key1=3, key2=8

DIST	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	30.4291	0.7382	0.6930	0.7531	0.7076	0.7564

Table 5.17

PSNR and MSE of the Tradeoff_AGA where key1=4, key2=5

DIST	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	32.8518	0.7107	0.6670	0.6863	0.6848	0.7444
1	31.8069	0.7371	0.6933	0.7651	0.7238	0.7787
2	30.8418	0.7600	0.7107	0.8424	0.7641	0.8096
3	29.9523	0.7702	0.7301	0.9083	0.8041	0.8263
4	29.1314	0.7781	0.7569	0.9447	0.8487	0.8486
5	28.3719	0.7806	0.7662	0.9651	0.8928	0.8412
6	27.6665	0.7718	0.7739	0.9709	0.9224	0.8299
7	27.0092	0.7580	0.7817	0.9675	0.9351	0.8128

Table 5.18

PSNR and MSE of the Tradeoff_AGA where key1=4, key2=6

DIST	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	35.2633	0.6995	0.6729	0.7170	0.6905	0.7333
1	33.9811	0.7259	0.6995	0.7956	0.7305	0.7694
2	32.7970	0.7425	0.7194	0.8639	0.7666	0.7913
3	31.7160	0.7654	0.7388	0.9122	0.7952	0.8071

Table 5.19

PSNR and MSE of the Tradeoff_AGA where key1=4, key2=7

DIST	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	36.6660	0.6790	0.6576	0.7115	0.6746	0.7151
1	35.2521	0.7061	0.6815	0.7871	0.7115	0.7448

Table 5.20

PSNR and MSE of the Tradeoff_AGA where key1=4, key2=8

DIST	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	35.8758	0.6936	0.6766	0.7623	0.6932	0.7352

Table 5.21

PSNR and MSE of the Tradeoff_AGA where key1=5, key2=6

DIST	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	39.5278	0.6443	0.6359	0.6845	0.6506	0.6619
1	37.4098	0.6606	0.6524	0.7778	0.6821	0.6849
2	35.6119	0.6700	0.6676	0.8630	0.7100	0.6910
3	34.0803	0.6704	0.6854	0.9008	0.7287	0.6926

Table 5.22

PSNR and MSE of the Tradeoff_AGA where key1=5, key2=7

DIST	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	42.0862	0.6354	0.6339	0.6983	0.6467	0.6549
1	39.4823	0.6525	0.6518	0.7877	0.6772	0.6754

Table 5.23

PSNR and MSE of the Tradeoff_AGA where key1=5, key2=8

DIST	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	40.5140	0.6498	0.6492	0.7685	0.6620	0.6736

Table 5.24

PSNR and MSE of the Tradeoff_AGA where key1=6, key2=7

DIST	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	46.9316	0.6056	0.6110	0.6582	0.6147	0.6083
1	42.5753	0.6048	0.6241	0.7444	0.6384	0.6132
2	39.4561	0.6043	0.6298	0.7830	0.6432	0.6124
3	37.1114	0.6051	0.6333	0.7288	0.6320	0.6012

Table 5.25

PSNR and MSE of the Tradeoff_AGA where key1=6, key2=8

X	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	44.0495	0.6092	0.6247	0.7420	0.6334	0.6104

Table 5.26

PSNR and MSE of the Tradeoff_AGA where key1=7, key2=8

X	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	46.3119	0.6007	0.6106	0.6802	0.6116	0.6087

From Tables 5.15 to 5.26, the results prove what was presented in the previous Section 5.3, i.e. the top watermarked image quality (highest *PSNR*) was found when the *DIST* value was the minimum (*DIST* = 0, the nearest pixel in the original); whereas the worst was when the *DIST* value was the greatest. However, the greatest robustness (biggest *NCC*) was achieved the using the Equation 2^{k1-1}, so the best values can be obtained where for the *PSNR* equal or greater than 30 db. To select the best embedding status, an acceptable quality of the watermarked image is considered to occur if the *PSNR* is greater than 30db, as stated by Wu (2004), Bennour et al, (2007) and Zeki (2009).

The user can select any *PSNR* value since a watermarked image depends on the kind of original image; smooth or textural, and usually the deformation on the smooth

images becomes more visible by the human eyes as compared to the textured image areas (Jain and Uludag, 2002); (Macq and Quisquater, 1995); (Wu and Tsai, 2003), therefore, the PSNR value may be more than 30db in these types of images.

By simply comparing each embedding experiment with *PSNR* value larger than 30db, the greater *NCC* is chosen as the best embedding status. From the above tables, the best *NCC* was found in the position (key1= 4 and key2 = 6) when the DIST value was 3, as given in Table 5.18, where the *PSNR* was 31.7160 db.

In the position (key1 = 4 and key2 = 6) (which is considered as the best bit-plane for embedding), watermark1 has been embedded within all original images to prove the above results (the threshold value for the best robustness with the acceptable image quality for different type of images). The *PSNR* and *NCC* for all attacks of the 4th bit-plane with different bias values for the proposed method by embedding watermark 1 in (original 2-6) are shown in Tables 5.27 to 5.31.

Table 5.27

P*SNR and MSE of the Tradeoff_AGA where key1=4, key2=8 (original2)*

DIST	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	35.3653	0.7267	0.6740	0.6863	0.7025	0.7502
1	34.0467	0.7692	0.7615	0.8556	0.7429	0.8264
2	32.8373	0.7950	0.8050	0.9212	0.7848	0.8847
3	31.7385	0.8116	0.8323	0.9434	0.8206	0.9030

Table 5.28

PSNR and MSE of the Tradeoff_AGA where key1=4, key2=8 (original3)

DIST	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	35.6448	0.7386	0.7078	0.7184	0.7186	0.7307
1	34.2976	0.7726	0.7708	0.8594	0.7595	0.7602
2	33.0626	0.7930	0.8061	0.9074	0.7974	0.7866
3	31.9421	0.8035	0.8244	0.9315	0.8194	0.8035

Table 5.29

PSNR and MSE of the Tradeoff_AGA where key1=4, key2=8 (original4)

DIST	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	35.7989	0.7528	0.7156	0.7444	0.7562	0.7345
1	34.4435	0.7789	0.7479	0.8321	0.7797	0.7700
2	33.1999	0.7926	0.7651	0.8827	0.8180	0.8097
3	32.0718	0.8008	0.7775	0.9114	0.8385	0.8191

Table 5.30

PSNR and MSE of the Tradeoff_AGA where key1=4, key2=8 (original5)

DIST	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	35.6438	0.7095	0.6773	0.6658	0.6951	0.6863
1	34.2932	0.7560	0.7785	0.8607	0.7651	0.7122
2	33.0563	0.7841	0.8150	0.9116	0.8121	0.7264
3	31.9349	0.7957	0.8344	0.9407	0.8419	0.7477

Table 5.31

PSNR and MSE of the Tradeoff_AGA where key1=4, key2=8 (original6)

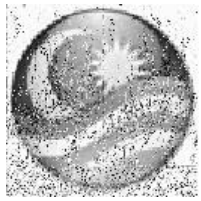
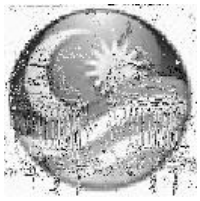
DIST	PSNR	JPEG	Blurring	Gaussian	Wiener	Speckle
0	35.3965	0.7285	0.6823	0.6913	0.6887	0.7107
1	34.0663	0.7690	0.7481	0.8400	0.7358	0.7604
2	32.8492	0.7955	0.7901	0.9100	0.7760	0.7948
3	31.7452	0.8086	0.8198	0.9383	0.8081	0.8107

The Tables 5.27 to 5.31 prove that the first result of the best embedding status in the position (key1 = 4, key2 = 6) at the *DIST* value = 3 and all the original images gave similar results. The extracted logo (watermark 1) from the different original images (when embedding in the position (key1 = 4, key2 = 6) at the *DIST* value = 3) is displayed in Table 5.30. Meanwhile, different *NCC* values for all the attacks and all the original images are illustrated in Table 5.31. In addition, Table 5.32 shows the

extracted watermark from different original images, while Figure 5.5 clarifies the difference between attacks.

Table 5.32

*Extracted watermark 1 from the different original images where key1=4, key2 =*6

Original	**Gaussian**	**Original**	**Gaussian**	**Original**	**Gaussian**
Original 1		Original 3		Original 5	
Original 2		Original 4		Original 6	

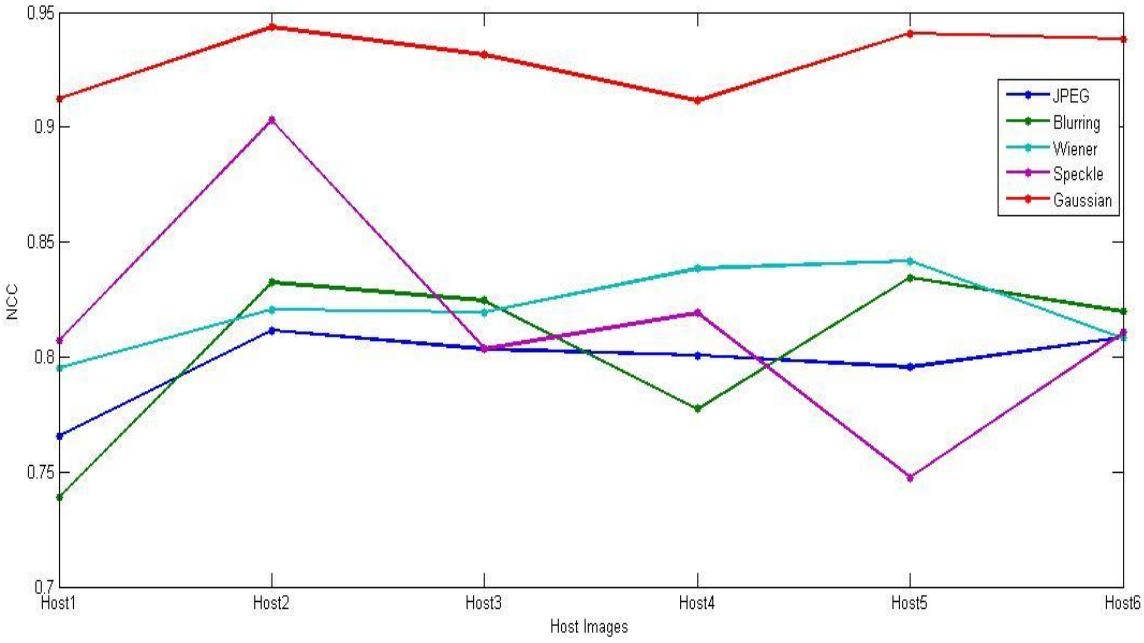


Figure 5.5. The NCC values for the extracted logo (watermark 1) from the different original images when embedding within (key1 = 4, key2 = 6) bit-planes at DIST = 3

The original images (watermarked images), after embedding the watermark1 in the position (key1 = 4, key2 = 6) bit-planes with the bias value (DIST) = 3, are shown in Figure 5.6. It is noticed that the *PSNR* values are greater than 30db.

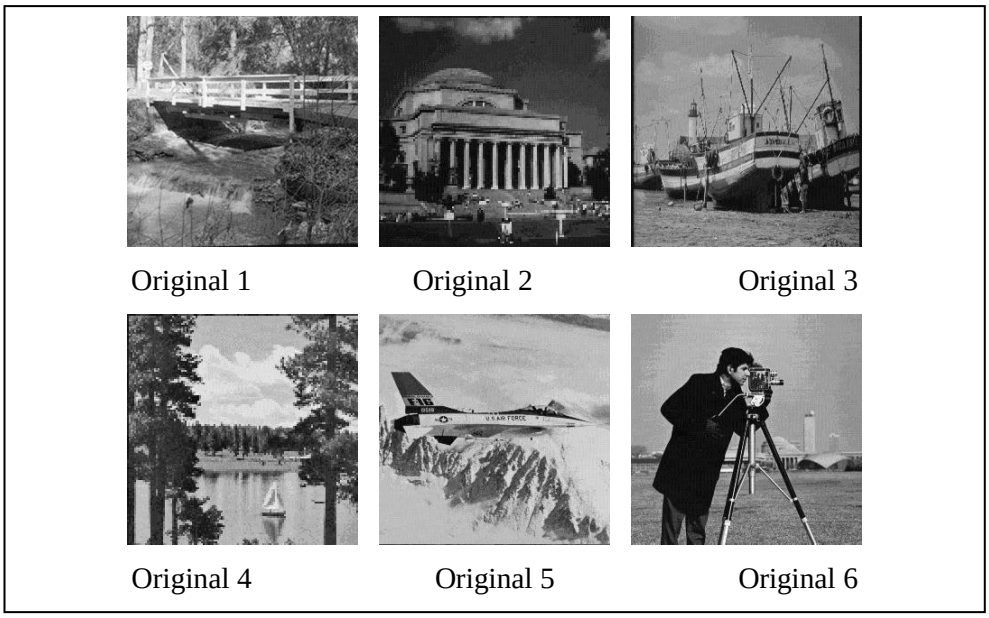


Figure 5.6. Different watermarked images after embedding watermark 1 in the (key1=4, key 2= 6) bit-planes at DIST = 3

To test other watermarked objects, two other images (Watermark 2 and Watermark 3) have been embedded in the chosen original images. These two watermarks were embedded in all the original images in the (key1=4, key2= 6) bit-planes at *DIST* = 3, and the result for the *PSNR* and *NCC* (after applying all attacks) are shown in Tables 5.33 and 5.34, respectively, and illustrated in Figures 5.7 and 5.8 respectively.

Table 5.33

PSNR and NCC of Tradeoff_AGA where key1=4, key2= 6 watermark 2 in different original images

Original	PSNR	NCC JPEG	NCC Blurring	NCC Gaussian	NCC Wiener	NCC Speckle
1	31.6828	0.7654	0.6775	0.8812	0.7419	0.7464
2	31.6613	0.8116	0.8049	0.9309	0.8054	0.8583
3	32.0140	0.8035	0.7794	0.9106	0.7940	0.7483
4	32.1994	0.8008	0.7349	0.8934	0.7845	0.7599
5	31.9970	0.7957	0.7836	0.9195	0.7899	0.6919
6	31.5992	0.8086	0.7840	0.9196	0.7736	0.7570

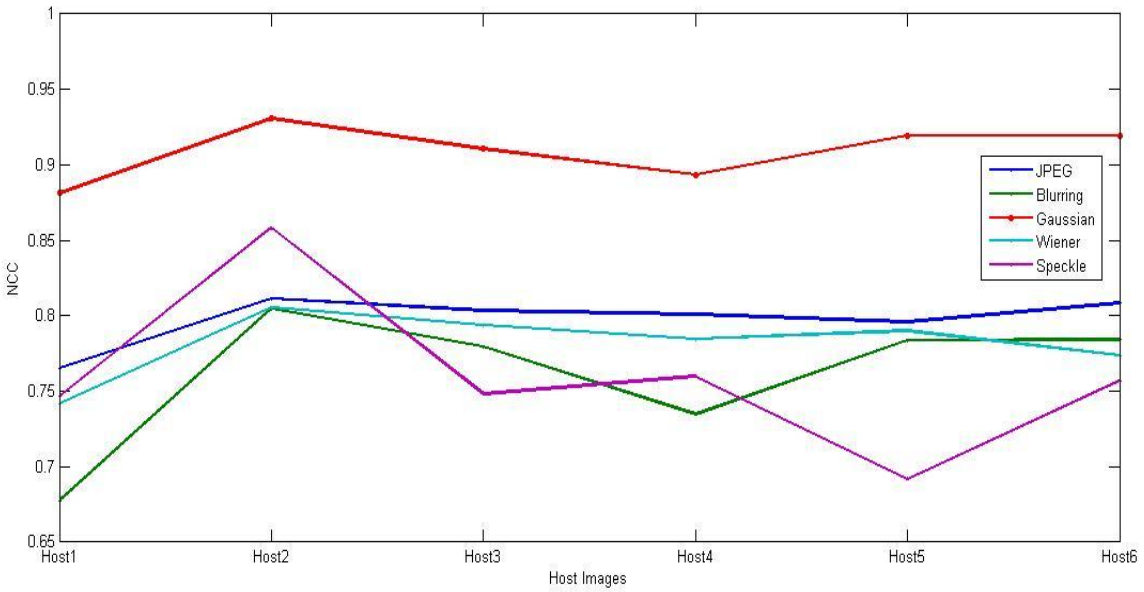


Figure 5.7. The NCC values of the extracted logo (watermark 2) from different original images at the embedding in (key1=4, key2= 6) bit-planes with DIST = 3

Table 5.34

PSNR and NCC of Tradeoff_AGA where key1=4, key2= 6 watermark 3 in different original images

Original	PSNR	NCC JPEG	NCC Blurring	NCC Gaussian	NCC Wiener	NCC Speckle
1	31.6895	0.7019	0.6894	0.8848	0.7501	0.7643
2	31.6873	0.7884	0.8216	0.9424	0.8215	0.8740
3	31.8573	0.7531	0.7933	0.9183	0.8065	0.7640
4	32.1723	0.7546	0.7384	0.8941	0.8000	0.7711
5	32.1328	0.7481	0.8011	0.9261	0.8144	0.6970
6	31.7454	0.7673	0.7852	0.9206	0.7779	0.7562

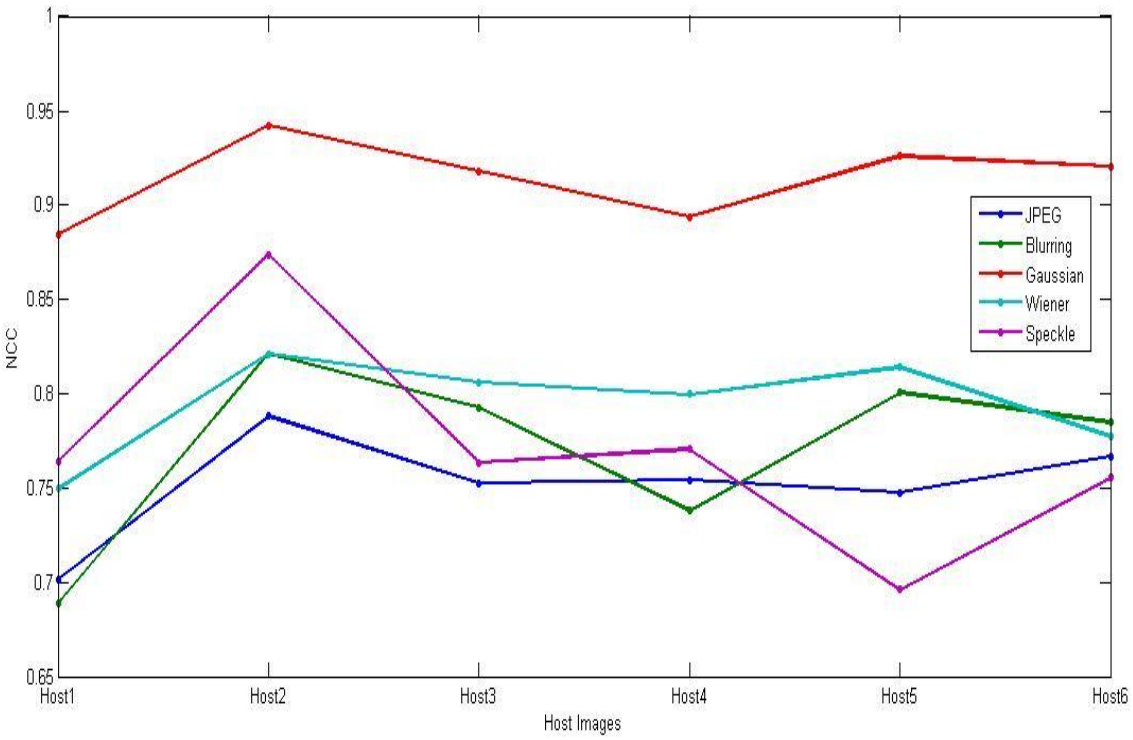


Figure 5.8. The NCC values of the extracted logo (watermark 3) from different original images at the embedding in (key1=4, key2= 6) bit-planes with DIST = 3

From the above results, embedding different watermarked objects within different original images, in the (key1=4, key2=6) bit-planes with *DIST* value = 3, gave the best embedding status with minimum distortion and acceptable image quality.

5.5 Summary

In this chapter, the quality of watermarked image has been found to improve by moving the pixel to the location on the edge of sub-period towards the original pixel, but at this location, the robustness has been found to decrease because when the pixel value is located on the edges of sub period, any small change by the attacks will move the pixel from one range to another, and the watermark cannot be extracted. The comparison between image quality algorithm and *LSB* method has been done and the results analyzed clarified all possibilities with each embedding two-bit position. The evaluation using *GA* guaranteed the image quality results and compared the time for each technique. Improving the robustness is achieved by moving every pixel used for embedding according to the Equation (2^{key1-1}). Therefore, any modification by attacks on the pixel will affect the selected bit modestly. In this chapter, the tradeoff between image quality and robustness has been done and all possible positions of pixel between the edge of the sub period and the value of Equation (2^{key1-1}) of the range were tested to find the best pixel value (threshold value), which was found to be in the position (k_1=4, k_2=6) bit-planes with a *DIST* value = 3 (the *DIST* value is the distance from the position of the watermarked pixel to the edge of the range).

This chapter proposed a new algorithm for the best image quality by embedding two bits from each pixel of the watermarked image into the original image. The proposed algorithm derived new equations based on the existing technique *ISB* to reach the best image quality. In addition, the chapter clarified the embedding process and the flowchart of the proposed algorithm in detail. The *PSNR* value was calculated and put in tables with the figures of the images after the embedding. In addition, *MSE* values for the watermarked images was calculated to measure the image quality. Meanwhile *NCC* and *BER* were used to measure the robustness after embedding two bits of watermark and study the effect of applying several kinds of image attacks. The comparison between the proposed algorithm and *LSB* was also discussed and clarified by figures and tables. Finally, *GA* did the evaluation of the proposed algorithm, and the time compared with the proposed algorithm.

CHAPTER SIX
CONCLUSION AND FUTURE WORK

6.1 Summary

This chapter is dedicated to summarize the thesis's achievements as well as to outline future guidelines in the *ISB* research field. The study is performed to solve the problems that have been found in *ISB*. Section 3.3 presents the developing algorithms that enhance *Quality_AGA* based on the *ISB* by adding another bit and handle image distortion, which is then compared with two existing methods *LSB* and *GA*. Section 3.4 presents the second enhanced algorithm for improving image robustness against attacks, which is named *Robust_AGA*. Section 3.5 presents the developed algorithm to make a balance between quality and robustness which is named *Tradeoff_AGA*.

Section 4.3 presents the results for the enhancing *Quality_AGA* in terms of two measurements *PSNR* and *MSE* when compared with the existing *LSB* and *GA*. This is done by finding the best quality of the watermarked image through choosing the nearest pixel to the original pixel that has the two embedded bits. The proposed algorithm enhanced image quality based on the mathematical equations, which cover all the probabilities after embedding the two bits to avoid image distortion. Another algorithm used in this study is *GA*, which evaluates the image quality and compare the results with the proposed algorithm. The algorithm calculated the *PSNR* value and *MSE* for the watermarked image and the time that was needed to do the embedding process. It has been found from the results of both algorithms that the

results of all embedded bits fully matched, guaranteeing the achievements of this study. Apart from that, the time results and the comparison with the time of *Quality_AGA* algorithm, showed that the proposed algorithm does the embedding process faster than the *GA*. The other proposed algorithm, *Robust_AGA* algorithm, is based on using the *DISB* technique to enhance the robustness of embedding two bits for watermarked image.

Section 4.4 presents the results of *Robust_AGA* that shows enhancing in term of two measurements *NCC* and *BCR* when comparing with the existing *LSB*. One watermark image from the six (as mentioned in the previous chapter) was embedded within twelve original images using the proposed technique explained. The results show enhancement of the watermarked images after applying five types of image attacks. The *NCC* and *BER* were used to assess the robustness of the watermarked images after embedding the watermarked objects, and the results were compared with the existing *LSB* method which were better than other methods.

Section 4.5 presents the results of *Tradeoff_AGA* that shows the performance of balancing between quality and robustness. The study used mathematical equations that were applied to test all probabilities and choose the image quality *PSNR* that was equal or greater than 30 db. At the same time, the *NCC* value was also calculated after applying the chosen attacks on the watermarked image. *Tradeoff* between image quality and robustness was done and all possible positions of pixel between the edge of the sub period and the value of Equation (2^{key1-1}) of the range were tested to find the best pixel value (threshold value), which was found to be in the position (key_1=4,

key_2=6) bit-planes with a *DIST* value = 3 (the *DIST* value is the distance from the position of the watermarked pixel to the edge of the range).

6.2 Contributions

This study made five contributions:

i. Enhanced the image quality of the watermarked image in accordance with the *ISB* method by embedding two bits of the watermarked image into the original image and compared the results with existing methods, *LSB* and *GA*, through using certain types of image format, in which the results show that the proposed algorithm is better than *LSB* and *GA* through investigating good *PSNR* values and short time for embedding process.

ii. Enhanced the image robustness of the watermarked image based on *ISB* technique by embedding two bits of the watermarked image into the original image, besides applying five types of image attacks on the watermarked image and comparing with *LSB* method. The results show that the proposed algorithm is better than *LSB* through investigating good *NCC* and lessened the error that happened after the embedding process by calculating *BER* values.

iii. Enhanced *Tradeoff* between image quality and robustness based on *ISB* technique by embedding two bits of the watermarked image into the original image, besides applying five types of image attacks on the watermarked image. The results show that the proposed algorithm investigated good *NCC* values after ignoring the *PSNR* values for watermarked images which were less than 30 db.

iv. The new derivative equations used in the algorithms were based on the existing *ISB* technique to enhance the image quality and robustness.

v. The proposed technique enhanced the time in terms of image quality when compared with existing *GA*.

6.3 Significance of the Research

The work in this research sets a new direction for *ISB* by enhancing it to *DISB* for embedding two bits that can handle many limitations by embedding two bits in the *LSB* method. This new direction is used to enhance the image quality using derivative mathematical equations, which study the effect of all bits in the embedding process. Apart from that, the study tries to obtain better robustness against attacks by using new sets of derivative equations. Because of the opposite relationship between image quality and robustness, the study makes a tradeoff between image quality and robustness using the *DISB* technique to get an acceptable quality of watermarked image and robust image against attacks. The outcome of this research is a new *DISB* technique that enhances the image quality and finds the best robustness against watermarking attacks by embedding two bits.

6.4 Future Work

This section concentrates on the future research recommendations based on this research. These recommendations can be outlined below:

i. In this research, the Dual Intermediate Significant Bits (*DISB*) technique is used to enhance the image quality and robustness by embedding two bits of watermarked image into the original image. The main algorithms were used in terms of image quality and robustness. The image robustness algorithm needs to be enhanced by applying other types of attacks, i.e. geometric attacks (rotation and scaling) to make sure that the proposed technique is effective against various types of attacks.

ii. Other methods can be used to enhance the image quality and robustness i.e. by repeating the embedding bits many times because the attacks try to move the pixel into another position and destroy the watermarked image.

iii. Though grayscale original images were used to cover the watermarked objects in the current study, this technique could also be applied to colored images (*RGB*).

iv. The proposed technique could also be extended for multimedia objects. For this purpose, the same theory could be applied to different environments.

v. Tradeoff between the two requirements - image quality and robustness - has been done depending on the *PSNR* value and *NCC* value, to make sure that it can be more accurate by choosing the best values through new methods for measurements.

References

Aarthi, R., Jaganya, V., & Poonkuntran, S. (2012). Modified LSB for Image Authentication. *International Journal of Computer & Communication Technology (IJCCT) Vol-3* (Iss-3), 62-65.

Abdullatif, M., Zeki, A. M., Chebil, J., & Gunawan, T. S. (2013). Properties of digital image watermarking. *paper presented at IEEE 9th International Colloquium on Signal Processing and its Applications, Kuala Lumpur, Malaysia*, 235-240.

Adrian, S. (2003). Enhanced Watermark Detection. *Master thesis*. University of Toronto, Canada.

Ahmad, K. A. A. a. H. A., & Gaydecki, P. (2009). A Blind Block Based DCT Watermarking Technique for Gray Level Images Using One Dimensional Walsh Coding. *IEEE International Conference on the Digital Object Identifier*, 1 - 6.

Al-Ataby, A., & Al-Naima, F. (2010). A Modified High Capacity Image Steganography Technique Based on Wavelet Transform. *The International Arab Journal of Information Technology*, Vol. 7, No. 4, 357-363.

Al-Jaber, A., and Aloqily, I. (2003). High Quality Steganography Model with Attacks Detection. *Pakistan Journal of Information and Technology*. Vol. 2 (No. 2), 116-127.

Aliwa, M. B., El-Tobely, T. E.-A., Fahmy, M. M., Nasr, M. E. S., & El-Aziz, M. H. A. (2013). A New Novel Fidelity Digital Watermarking Adaptively Pixel Based on Medial Pyramid of Embedding Error in Spatial Domain and Robust.

International Journal of Computer Theory and Engineering, Vol. 5, No. 4, 603-610.

Ansari, R., Devanalamath, M. M., Manikantan, K., & Ramachandran, S. (2012). Robust Digital Image Watermarking Algorithm in DWT-DFT-SVD Domain for Color Images. *IEEE International Conference on Communication, Information & Computing Technology (ICCICT),* 978-1-4577-2078-9/12, 1-6.

Anwar, M. J., Ishtiaq, M., Iqbal, M. A., & Jaffar, M. A. (2010). Block-based Digital Image Watermarking using Genetic Algorithm. *IEEE.6th International Conference on Emerging Technologies (ICET),* 204-209.

Asatryan, D., & Asatryan, N. (2010). Combined Spatial and Frequency Domain Watermarking. 1-4.

Bamatraf, A., Ibrahim, R., & Salleh, M. N. B. M. (2010). Digital Watermarking Algorithm Using LSB. *IEEE.International Conference on Computer Applications and Industrial Electronics (ICCAIE),December 5-7.*, 155-159.

Bamatraf, A., Ibrahim, R., & Salleh, M. N. M. (2011). A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit. *Journal of Computing Press, NY, USA, ISSN 2151-9617, Vol 3*(Iss 4), 1-8.

Bedi, S., Tomar, G. S. & Verma, A. S. (2009). Robust Watermarking of Image in the Transform Domain using Edge Detection. *11th International Conference on Computer Modelling and Simulation, 233-238.*

Bennour J., Dugelay J. L., and Matta, F. (2007). Watermarking Attack: *BOWS contest. Proceedings of SPIE.*

Bhatnagar, G., & Raman, B. (2008). A new robust reference watermarking scheme based on DWT-SVD. *Computer Standards & Interfaces*, doi:10.1016/j.csi.2008.09.031, 1-12.

Brabin, D., & Tamilselvi, J. J. (2013). Reversible Data Hiding: A Survey. *International Journal of Innovative Research in Computer and Communication Engineering ISSN : 2320 – 9798*, Vol. 1 (Issue 3), 695-700.

Chan, C. K., & Cheng, L. M. (2001). Improved hiding data in images by optimal moderately-significant-bit replacement. *Electronics Letters*, Vol 37, No 16, 1017-1018.

Chan, C. K., Cheng, L.M, Leung, K. C., and Li, S. L., (2004). Image Hiding Based on Block Difference, in the 8 th in International conference on control, Automation, Robotics, and Vision.

Changa, C. C., Hsiaob, J. Y., and Chana, C. S. (2003). Finding optimal least significant- bit substitution in image hiding by dynamic programming strategy. *Pattern Recognition.* 36: 1583–1595.

Chen, P. C. (1999). On the Study of Watermarking Application in WWW – Modelling, Performance Analysis, and Applications of Digital Image Watermarking Systems. *Ph.D. Thesis, Monash University*.

Chen, W. Y. (2003). A Comparative Study of Information Hiding Schemes Using Amplitude, Frequecy and Phase Embeddings. *Ph.D. dissertation. Department of Electrical Engineering, National Cheng Kung University*, Tainan, Taiwan, R.O.C.

Chen, & Lu. (2012). Robust Spatial LSB Watermarking Of Color Images Against JPEG Compression. *IEEE fifth International Conference on Advanced Computational Intelligence(ICACI)*, 872-875.

Chetouani, A., Nguyen, P. B., Luong, M., & Mostafaoui, G. (2010). Content-Based Watermarking Robust to Low Bit Rate JPEG Compression. *10th International Conference on Information Science, Signal Processing and their Applications (ISSPA 2010)*, 29-32.

Cheung, W. N. (2000). Digital image watermarking in spatial and transform domains. *TENCON Proceedings*. 3: 374-378.

Chin, C. C., Guei, M. C., and Lin, M. H. (2004). Information hiding based on searchorder coding for VQ indices. Pattern Recognition Letters.

Chung, K. L., Shen, C. H., and Chang, L. C., (2001). A Novel SVD- and VQ-based Image Hiding Scheme. *Pattern Recognition Letters. 22*: 1051-1058.

Cox, I. J., Kilian, J., Leighton, T., & Shamoon, T. (1995). Secure Spread Spectrum Watermarking for Multimedia. *Proceedings of the SPIE. San Jose, 2420*, 456-459.

Dadkhah, S., Manaf, A. A., and Sadeghi, S. (2012). Efficient Digital Image Authentication and tamper localization technique using 3 LSB bit. International journal of computer science issues.

Darmstaedter, V., Delaigle, J. F., Quisquater, J. J., and Macq, B. (1998). Low Cost Spatial Watermarking. *Comput. & Graphics*. 22(4): 417-424.

Dejun, Y., Rijing, Y., Yuhai, Y., & Huijie, X. (2009). Blind Digital Image Watermarking Technique Based On Intermediate Significant Bit and Discrete

Wavelet Transform. *paper presented at IEEE International Conference Computational Intelligence and Software Engineering (CiSE)*, 1-4.

Dubolia, R., Singh, R., Bhadoria, S. S., & Gupta, R. (2011). Digital Image Watermarking by Using Discrete Wavelet Transform and Discrete Cosine Transform and Comparison Based on PSNR. *IEEE.International Conference on Communication Systems and Network Technologies*, 593-596.

Eggers, J. J., Su J. K., and Girod, B. (2000). Robustness of a Blind Image Watermarking Scheme. I*nternational Conference on Image Processing (ICIP 2000)*, Canada.

Emami, M. S., Sulong, G. B., and Seliman, S. B. (2012). "A Novel Multiple Semi-Blind Enhanced ISB Watermarking Algorithm Using Watermark Bit-Pattern Histogram For Copyright Protection", *International Journal of Innovative Computing, Information and Control ICIC International, ISSN 1349-4198* , March, vol. 8, No 3(A), pp. 1665-1687.

Fazli, S., & Khodaverdi, G. (2009). Tradeoff between Quality and Robustness of LSB Watermarking using SSIM Quality Metrics. ICMV '09. Second International Conference on Issue Date: 28-30 Dec. 2009 101-104.

Fındık, O., Babaoğlu, İ., Ülker, E., (2009). " Watermarking schema using an arTIFFicial immune system in spatial domain ", Pr*oceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, ICIS* Seoul, Korea, November 24-26, 2, , 945-950,

Forrester, E. (2006). A Process Research Framework The International Process Research Consortium.

Fridrich, J., & Goljan, M. (1999) “Comparing Robustness of Watermarking Techniques,” SPIE Security and Watermarking of Multimedia Content, San Jose, CA, Jan 1999.

Fridrich, J., & Goljan, M. (2003). On Estimation of Secret Message Length in LSB Steganography in Spatial Domain.

Fung, A. G. C., & Junior, W. G. (2011). A Review Study on Image Digital Watermarking. *presented at the The Tenth International Conference on Networks, St. Maarten, The Netherlands Antilles.*

Ganesan, K., & Guptha, A. T. K. (2010). Multiple Binary Images Watermarking in Spatial and Frequency Domains. *An International Journal(SIPIJ) Vol.1, No.2,*,148-159.

Gao, X., Deng, C., Li, X., & Tao, D. (2010). Geometric Distortion Insensitive Image Watermarking in Affine Covariant Regions. IEEE Transections on Systems, Man, and Cybernetics Part C: Applications and Reviews, Vol. 40, No. 3, 278-286.

Geetha, Sindhu, S. S. S., Priya, B., Mubakiya, S., & Kamaraj, N. (2011). Geometric Attack Invariant Watermarking with Biometric Data - Applied on Offline Handwritten Signature. National Conference on, Computer Vision, Pattern Recognition, Image Processing and Graphics, 106-109.

Ghosh, S., Ray, P., Maity, S. P., & Rahaman, H. (2009). Spread Spectrum Image Watermarking with Digital Design. IEEE International Advance Computing Conference (IACC 2009), 868-873.

Greyscale Standard Images, http://www.dip.ee.uct.ac.za/imageproc/stdimages/greyscale/, last access 9 February 2008.

Gunjal, B. L., & Mali, S. N. (2013). Design and Implementation of Invisible and Visible Color Image Watermarking with Netbeans IDE International Journal of Computer Applications Vol 71 - NO.11 40-45.

Gong, H., Xie, S. J., Park, D. S., Yoon, S., & Shin, j. (2011). Novel robust blind image watermarking method based on correlation detector. *paper presented at IEEE International Conference on ICT Convergence (ICTC)*, 751-755.

Goyal, S., Gupta, R., & Bansal, A. (2009). Application of Genetic Algorithm to Optimize Robustness and Fidelity of Watermarked Images. International Journal on Computer Science and Engineering 239-242.

Gulati, K. (2003). Information Hiding Using Fractal Encoding. Master Thesis. Indian Institute of Technology Bombay, Mumbai.

Gunjal, B. L., & Mali, S. N. (2011). Secured Color Image Watermarking Technique in DWT-DCT Domain. *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT) Vol.1, No.3*, 36-44.

Gunjal, B. L., & Mali, S. N. (2013). Handling Various Attacks in Image Watermarking. *CSI Communications*, 30-32.

Gupta, S., & Jain, S. (2010). A Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform. *International Conference IJCCT Vol.1* (Issue 2, 3, 4), 222-227.

Hajisami, A., Rahmati, A., & Babaie-Zadeh, M. (2011). Watermarking Based on Independent Component Analysis In Spatial Domain. *IEEE UKSim 13th International Conference on Modelling and Simulation*, 299-303.

Hala, H., and Zayed, A. (2005). High-Hiding Capacity Technique for Hiding Data in Images Based on K-Bit LSB Substitution. *Proceedings of the 13th International Conference on Artificial Intelligence Applications*. February 23- 26. Cairo, Egypt.

Hemahlathaa, & Chellppan. (2012). A Feature-Based Robust Digital Image Watermarking Scheme. IEEE International Conference on Computing, Communication and Applications (ICCCA), 1-5.

Hsieh, C. T., Lu, Y. L., Luo, C. P., and Kuo, F. J. (2000). A Study of Enhancing the Robustness of Watermark. *ISMSE Conference*. 325-327.

http://decsai.ugr.es/cvg/CG/base.htm

Hongqin, S., & Fangliang, L. (2010). A Blind Digital Watermark Technique for Color Image Based on Integer Wavelet Transform *paper presented at IEEE International Conferen*ce for Biomedical Engineering and Computer Science (ICBECS), 1-4.

Hosinger, C., and Rabbani, M. (2000). Data embedding using phase dispersion. *presented at International Conference on Information Technology: Coding and Computing (ITCC2000).*

Ishtiaq, M., Sikandar, B., Jaffar, M. and Khan, A. (2010). Adaptive Watermark Strength selection using practice swarm optimization. *ICIC International conference, ISSN 1881-803X*, Vol 4 (No 5), 1-6.

Jadav, Y. (2013). Comparison of LSB and Subband DCT Technique for Image Watermarking. Conference on Advances in Communication and Control Systems (CAC2S), 398-401.

Jain, A. K., and Uludag, U. (2002). Hiding Fingerprint Minutiae in Images. *Workshop on Automatic IdenTIFFication Advanced Technologies.* March 14-15. Tarrytown, New York, USA: 97-102.

Jain, J., & Rai, V. (2012). Robust Multiple Image Watermarking Based on Spread Transform. *Book of Watermarking ISBN: 978-953-51-0619-7, Vol 2*, 43-64.

Jian, L., & Xiangjian, H. (2005). A Review Study on Digital Watermarking. *First International Conference on Information and Communication Technologie ICICT* 337-341.

Juergen, S. (2005). Digital Watermarking for Digital Media. University of Cooperative Education Heidenheim, Germany. ISBN:159140519X.

Jun, K. X., & Jun, D. L. (2009). Study of the Robustness of Watermarking Based on Image Segmentation and DFT. *IEEE International Conference on Digital Object IdenTIFFier ICIECS : 10.1109/ICIECS.2009.5362694* 1-4.

Kailasanathan, C. (2003). Fragile watermark based on polarity of pixel points. *Proceedings of the 3rd International Symposium on Image and Signal Processing and Analysis (ISPA 2003).*18-20 September. IEEE, 860-865.

Kao, C. H., & Hwang, R.-J. (2005). Information Hiding in Lossy Compression Gray Scale Image. *Tamkang Journal of Science and Engineering*, Vol. 8, No 2, 99 - 108.

Khodaei, M., & Faez, K. (2012). New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing. *IET Image Processing*, Vol 6, (Issue 6), 677 – 686.

Kumari, Kumar, Sumalatha, & Krishna. (2009). Secure and Robust Digital Watermarking on Grey Level Images. International Journal of Advanced Science and Technology.

Langelaar, G. C., Lagendijk, R. L., and Biemond J. (1998). Removing Spatial Spread Spectrum Watermarks by Non-linear Filtering. 9th European Signal Processing Conference (EUSIPCO'98). Island of Rhodes, Greece, 2281-2284.

Langelaar, G. Setyawan, I., and Lagendijk, R. L. (2000). Watermarking Digital Image and Video Data. IEEE Signal Processing Magazine. September. 17: 20-43.

Lee, G. J., Yoon, E. J., & Yoo, K. Y. (2008). A new LSB based Digital Watermarking Scheme with Random Mapping Function. *paper presented at IEEE International Symposium on Ubiquitous Multimedia Computing*, 130-134.

Li, C. T., and Yang, F. M. (2003). One-dimensional Neighbourhood Forming Strategy for Fragile Watermarking. Journal of Electronic Imaging. 12(2): 284-291.

Liu, J. C., and Chen, S. Y. (2001). Fast two-layer image watermarking without referring to the original image and watermark. *Image and Vision Computing*. 19(14): 1083-1097.

Lin, C. C. and Tsai, W. H. (2004). Secret image sharing with steganography and authentication. *Journal of Systems and Software*. November. 73: 405–414.

Lin, K. Y., Hong, W., Chen, J., Chen, T. S., & Chiang, W. C. (2010). Data Hiding by Exploiting Modification Direction Technique Using Optimal Pixel Grouping. IEEE 2nd international Conference on Education Technology and Computer (ICETC), 121-123.

Lu, C. S. (2005). Multimedia Security, Steganography and Digital watermarking Techniques for Protection of Intellectual Property. Idea Group Publishing.

Mabtoul, S., Elhaj, E. h. I., & Aboutajdine, D. (2007). Robust color image watermarking *based on s*ingular value decomposition and Dual tree complex wavelet transform. *paper presented at IEEE International Conference on Electronics Circuits and Systems*, 534-537.

Maity, S. P., & Kundu, M. K. (2002). Robust and Blind Spatial Watermarking In Digital Image. *Proceedings of 3rd Indian Conf. on Computer Vision, Graphics and Image Processing (ICVGIP '2002). 16-18th December. Ahmedabad, India: 388-393.*

Maity, Delpha, C., & Pha*dikar, A. (2009).* Spread-Spectrum Watermarking Security. *IEEE International Conference on Multimedia Information Networking and Security, 525-529.*

Macq, B. M., and Quisquater, J. J. (1995). Cryptology for Digital TV Broadcasting. *Proceedings of the IEEE. June. 83(6): 944-957*.

Massey, J. (1988). An introduction to contemporary cryptology. *Proceedings of the IEEE*. May. 76(5): 533– 549.

Mayer, J. o. (2011). Improved Spread Spectram Multibit Watermarking. *IEEE International Workshop on Information Forensics and Security (WIFS), 1-6.*

Megalingam, R. K., Nair, M. M., Srikumar, R., Balasubramanian, V. K., & Sarma, V. S. V. (2010). Performance Comparison of Novel, Robust Spatial Domain Digital Image Watermarking with the Conventional Frequency Domain Watermarking Techniques. IEEE International Conference on Signal Acquisition and Processing, 349-353.

Modaghegh, H, .H, K., & Akbarzadeh, M. (2009). A new adjustable blind Watermarking based on GA and SVD. IEEE,6th International Conference on Innovations in Information Technology, 6-10.

Mohamed, M., Afari, F., & Bamatraf, M. (2011). Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation. International Arab Journal of e-Technology, vol. 2, no. 1, 11-17.

Mohammad, A. M. F., & Asad, N. M. (2006). An Optimization Approach for Selecting Blocks of Embedding Process in Robust Watermarking System. *Journal of Computer Science 2 (1) ISSN 1549-3636 © 2006 Science Publications*, 114-117.

Mukherjee, D. P., Maitra, S., & Acton, S. T. (2004). Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication. *IEEE Transactionson multimedia*, vol. 6, No. 1, 1 - 15

Nasir, I., Weng, Y., & Jiang, J. (2007). A New Robust Watermarking Scheme for Color Image in Spatial Domain. *Third International IEEE Conference on Signal-Image Technologies and Internet-Based System SITIS '07*, 942-947.

Okagaki, K., Takahashi, K., & Ueda, H. (2010). Robustness Evaluation of Digital Watermarking Based on Discrete Wavelet Transform. *IEEE Sixth International*

Conference on Intelligent Information Hiding and Multimedia Signal Processing, 114-117.

Pal, G. Ghosh and M. Bhattacharya, (2012). Reversible Digital Image Watermarking Scheme Using Bit Replacement and Majority Algorithm Technique. *Journal of Intelligent Learning Systems and Applications,* Vol. 4 No. *3*, 199-206.

Pan, G., Wu, Z., and Pan, Y. (2002). A Data Hiding Method for Few-color Images. *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'02).* 13-17 May. Orlando, Florida: 3469-3472.

Pérez-Freire, L., & Pérez-González, F. (2009). Spread-Spectrum Watermarking Security. IEEE Transections on Information Forensics and Security, Vol. 4, No. 1, 2-24.

Parameswaran, L., and Anbumani, K. (2006). A Robust Image Watermarking Scheme using Image Moment Normalization. Transactions on Engineering, Computing and Technology. May. 13, ISSN 1305-5313.

Perumal, S. M., & Kumar, V. V. (2011). A Wavelet based Digital Watermarking Method using Thresholds on Intermediate Bit Values. International Journal of Computer Applications, Vol 15 No.3, 29-36.

Peungpanich, A., Areewan, Mettripun, N., & Amornraksa, T. (2010). Improved Image Watermarking Using Image Averaging Technique and Prediction of Tuned Watermarked Pixels. 2nd International Conference on Information Engineering and Computer Science.

Peungpanich, A., & Amornraksa, T. (2010). An Improving Method for Image Watermarking Using Image Averaging and Tuned Pixels Prediction. *IEEE,ISCIT, 755-760.*

Petitcolas, F. A. P., Anderson, R. J., and Kuhn, M. G. (1999). Information Hiding-A survey. *Proceedings of the IEEE. 87(7): 1062 -1078.*

Pieprzyk, J., Okamoto, E., and Seberry, J. (2000). Spatial-Domain Image Watermarking Robust against Compression, Filtering, Cropping, and Scaling. *ISW 2000, LNCS 1975, Berlin Heidelberg*. *Springer-Verlag*: 44–53.

Podilchuk, C. I., & Zeng, W. (1998). Image-Adaptive Watermarking Using Visual Models. IEEE Journal on selected Areas In Communacations Vol 16 No 4, 525-539.

Podilchuk, C. I., & Delp, E. J. (2001). Digital watermarking: algorithms and applications. IEEE Signal Processing Magazine, Vol 18(Iss 4), 33-46.

Qi, J. (2005). A rotation, scaling, and translation-resilient digital watermarking scheme based on image content. Master Thesis. Computer Science, UTAH State University.

Ramani, K., Prasad, E. V., Varadarajan, S., & Subramanyam, A. (2008). A Robust Watermarking Scheme for Information Hiding. *Advanced Computing and Communications, 16th International Conference,* 58-64.

Rohith, S. & Bhat, K. N. H. (2012). A Simple Robust Digital Image Watermarking against Salt and Pepper Noise using Repetition Codes. ACEEE Int. J. on Signal & Image Processing, Vol. 03, No. 01, 47-54.

Saxena, V. (2008). Digital Image Watermarking. *Phd thesis submitted to Jaypee Institute of Information Technology University, Inoida, India.*

Schneier, B. (1996). Applied Cryptography. (2nd ed.). New York, NY: John Wiley & Sons, Inc.

Schyndel, V. R. G., Tirkel, A. Z., & Osborne, C. F. (1994). A digital watermark. Proceedings of IEEE Int. *Conference on Image Processing. Austin, Texas, USA: 86–89.*

Seddik, H., Sayadi, M., Fnaiech, F., & Cheriet, M. (2003). A New Spatial Watermarking Method, based on a Logarithmic transformation of An Encrypted embeded Mark. 1-6.

Shelby, P. (2000). Robust Digital Image Watermarking. *Ph.D. Thesis. University of Geneve, Faculty of Science, Canada.*

Shih. (2010). Image Processing and Pattern Recognition:Fundamentals and Techniques *Wiley-IEEE Press eBook Chapters* 444-473.

Simmons, G. (1992). Contemporary Cryptology: The Science of Information Integrity. *Piscatoway, NJ: IEEE Pres*s.

Singh, R., & Gupta, R. (2011). Digital Watermarking with Visual Cryptography in Spatial Domain. *International Conference on Advanced Computing, Communication and Networks'11*, 948-951.

Song, C., Sudirman, S., & Merabti, M. (2010). Robust Digital Image Watermarking using Region Adaptive Embedding Technique. *paper presented at IEEE International Conference on Progress in Informatics and Computing (PIC), vol 1*, 378-382.

Song, C., Sudirman, S., Merabti, M., & Llewellyn-Jones, D. (2010). Analysis of Digital Image Watermark Attacks. *paper presented at 7th IEEE Computational Consumer Communications and Networking Conference (CCNC)* 1-5.

Swanson, M. D., Bin, Z., and Tewfik, A. H. (1996). Transparent Robust Image Watermarking. *Proceedings of the IEEE International Conference on Image Processing.* September. Lauzanne: 211-214.

Tao, P., & Eskicioglu, A. M. (2004). A Robust Multiple Watermarking Scheme in the Discrete Wavelet Transform Domain. *Optics East, Internet Multimedia Management Systems V Conference*.

Thanikaiselvan, Arulmozhivarman, Amirtharajan, R., & Balaguru, J. B. (2011). Wave(Let) Decide Choosy Pixel Embedding for Stego. *paper presented at IEEE International Conference on Computer, Communication and Electrical Technology – ICCCET*, 157-162.

Thapa, M., & Sood, S. (2011). On Secure Digital Image Watermarking Techniques. Journal of Information Security, volume 2 number 4, 169-184.

Tripathi, S., Ramesh, N., Bernito, & Neeraj. (2010). A DWT based Dual Image Watermarking Technique for Authenticity and Watermark Protection. Signal & Image Processing : An International Journal (SIPIJ), Vol.1, No.2, 33-45.

Tsai, Y., Y., Chen, J., T., and Chan C., S. (2014). Exploring LSB Substitution and Pixel-value Differencing for Block-based Adaptive Data Hiding. *International Journal of Network Security*, Vol.16, No.5, 363-368.

Voyatzis, G., and Pitas, I. (1998). Chaotic watermarks for embedding in the spatial digital image domain. *Proceedings of IEEE Int. Conf. Image Processing*. Chicago, IL, USA. 2: 432–436.

Wang, C. C., Tai, S. C., & Yu, C. S. (2000). Repeating Image Watermarking Technique by the Visual Cryptography. IEICE Trans. Fundamental. August. E83-A(8): 1589-1598.

Wang, R. Z., Lin, C. F. and Lin, J. C. (2001). Image hiding by optimal lsb substitution and genetic algorithm. Pattern Recognition. 34(3): 671–683.

Wang, Y., and Pearmain, A. (2004). Blind Image Data Hiding Based on Self Reference. *Pattern Recognition, 25: 1681-1689.*

Wu, C. F. (2001). The Research of Improving the Image Quality of Digital Watermarking Technique and Its Applications. *National Sun Yat-sen University, Kaohsiung*, 80424, Taiwan. etd-0612101-142904.

Wu, D. C. and Tsai, W. H. (2003). A steganographic method for images by pixelvalue differencing, Pattern Recognition Letters. 24(9-10): 1613–1626.

Wu, N. I., and Hwang, M. S. (2007). Data Hiding: Current Status and Key Issues. *International Journal of Network Security. January*. 4(1): 1–9.

Xiong, Z., Sun, X., & Wu, F. (2010). Robust Web Image/Video Super-Resolution. *paper presented at IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 19, Issue: 8*, 2017-2028.

Yang, S. L., & Zhang, Z.B. (2009). Digital Image Watermarking Using Iterative Blending Based on Wavelet Technique *paper presented at IEEE International Conference Multimedia Information Networking and Security (MINES), Vol 2*, 83-86.

Yin, C. Y., Wu, D. C., and Tsai, W. H. (2002). New data hiding methods for copyright protection, annotation, and authentication of BMP archive images in digital libraries and museums. *Proceedings of the 1st Workshop on Digital Archives Technologies.* Taipei, Taiwan, Republic of China: 168-183.

Yongqiang, C., Yanqing, Z., & Lihua, P. (2009). A DWT Domain Image Watermarking Scheme Using Genetic Algorithm and Synergetic Neural

Network. *International Symposium on Information Processing (ISIP'09), ISBN 978-952-5726-02-2*, 298-301.

Yusof, Y., & Khalifa, O. O. (2007). Digital watermarking for digital images using wavelet transform. *EEE International Conference on Telecommunications and Malaysia International Conference on Communications*, 665-669.

Zamani, M., Manaf, A. A., Ahmad, R., Zeki, A., & Abdullah, S. (2009). A Genetic-Algorithm-Based Approach for Audio Steganography. *International Conference on Communities and Communications World Academy of Science, Engineering and Technology 54, ISSN: 2070-3740.*, 359-363.

Zamani, M., Manaf, A. A., Ahmad, R., Zeki, A., & Abdullah, S. (2009). Genetic Algorithm as an Approach to Resolve the Problems of Substitution Techniques of Audio Steganography. *International Conference on Genetic and Evolutionary Methods SBN: 1-60132-106-6 and 1-60132-092-2. . Las Vegas, Nevada, USA*, 170-175.

Zamani, M., Taherdoost, H., Manaf, A. A., Ahmad, R., & Zeki, A. M. (2009). Robust Audio Steganography via Genetic Algorithm. *Third International Conference on Information & Communication Technologies ICICT*, 149 - 153.

Zeki, A. M., & Manaf, A. A. (2009). A Novel Digital Watermarking Technique Based on ISB (Intermediate Significant Bit. *World Academy of Science, Engineering and Technology 50*, 989-996.

Zeki, A. M., Manaf, A. A., & Mahmod, S. S. (2011). Improving the robustness of ISB watermarking techniques by repetition of the embedding. *In: Communications in C*omputer and Information Science. Springer-Verlag Berlin Heidelberg, 592-599.

Zeng, W., & Wu, Y. (2010). A Visible Watermarking Scheme in Spatial Domain Using HVS Model. Information Technology Journal 9 (8) ISSN 1812-5638, 1622-1628.

Zhang, F., & Zhang, H. (2004). Applications of neural network to watermarking capacity IEEE International Symposium on Communications and Information Technology ISCIT, Vol 1, 340-343.