A COMPARATIVE STUDY OF WATERMARKING TECHNIQUES IN SPATIAL
AND FREQUENCY DOMAINS

ABDULADHIM MOHAMAD ALI ALAMARI

A thesis submitted in partial
Fulfilment of the requirements for the award of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia

AUGUST 2014
ABSTRACT

The watermarking technique has served as a tool for the protection of Intellectual Property Rights (IPR) of multimedia contents. Due to the digital nature of multimedia documents, these documents can be duplicated, modified, transformed, and diffused very easily. As a result, a watermark that is embedded into the digital data cannot be distinguished from the data itself. Upon request, the watermark can be extracted to prove authorized ownership. In this research, an integration of two watermarking techniques; spatial Least Significant Bit (LSB), and frequency domains Discrete Wavelet Transform (DWT) in cover image, had been proposed. A simulation of the proposed method was done in order to determine the robustness and imperceptibility of the watermarked image when exposed to various attacks. The simulation of the proposed method was done in MATLAB, using the PSNR, MSE, and SSIM, as simulation parameters. The efficiency of the method that was based on the robustness and imperceptibility of the watermarked image was determined through the values of the PSNR, MSE, and SSIM. The PSNR of the LSB, the DWT, and the proposed method were 33.09%, 32.3%, and 34.6 respectively, and the MSE of the LSB, the DWT, and the proposed method were 34.4%, 44.9%, and 20.7% respectively. The findings showed that the proposed method was more efficient in terms of robustness and imperceptibility for the watermarked image, compared to LSB and DWT techniques.
ABSTRAK

Watermarking telah dijadikan sebagai satu alat untuk melindungi Hak Harta Intelek (IPR) yang berunsur multimedia. Dengan sifat digital watermark, dokumen multimedia boleh ditiru, diubah suai, dibina semula, dan disebarkan dengan mudah. Disebabkan oleh faktor ini, watermark yang tertanam ke dalam data digital tidak dapat dibezaan daripada data imej sendiri. Di atas permintaan, watermark boleh diekstrak supaya dapat membuktikan hak pemilikannya. Oleh itu, penyelidikan watermarking ini dijalankan untuk mengkaji imej digital yang disimpan di dalam kedua-dua spatial dan frequency domain. Dalam kajian ini, tumpuan diberikan kepada Least Significant Bit (LSB), dan Discrete Wavelet Transform (DWT). Keteguhan dan efisiensi teknik watermark telah dikaji kerana imej watermark mudah terdedah kepada pelbagai serangan. Kajian ini telah dijalankan dengan menggunakan MATLAB untuk mendapatkan nilai PSNR, MSE, dan SSIM. Hasilnya, teknik watermarking yang menggunakan algoritma LSB+DWT adalah terbukti terbaik, kerana ia memberikan nilai PSNR yang paling tinggi, iaitu sekitar 6%, lebih baik daripada watermarking yang menggunakan spatial domain LSB, dan 8% lebih baik daripada watermarking yang menggunakan frequency domain DWT, serta menunjukkan nilai yang paling rendah dalam MSE.
CONTENTS

TITLE i
DECLARATION ii
DEDICATION iii
ACKNOWLEDGEMENT iv
ABSTRACT v
ABSTRAK vi
CONTENTS vii
LIST OF TABLES x
LIST OF FIGURES xi
ABBREVIATIONS xiv

CHAPTER 1 INTRODUCTION
  1.1 Background of the Study 1
  1.2 Problem Statement 2
  1.3 Objectives 3
  1.4 Scope 3
  1.5 Significance of Research 4
  1.6 Organization of Thesis 4

CHAPTER 2 LITERATURE REVIEW
  2.1 Introduction 5
  2.2 Host Signals 4
  2.3 Digital Image Watermarking 7
  2.4 Watermarking algorithm 8
  2.5 Characteristics of Watermark 9
  2.6 Watermark embedding technique 10
  2.7 Watermark detection techniques 10
  2.8 Watermarking Applications 10
2.9 Techniques for Digital Image Watermarking

2.9.1 Spatial Domain Technique

2.9.2 Frequency Domain Technique

2.10 Removal attacks

2.10.1 Compression

2.10.2 Additive noise

2.10.3 Denoising

2.10.4 Filtering attacks

2.10.5 Statistical averaging

2.11 Evaluation

2.12 Watermarking Using Least Significant Bit (LSB)

2.12.1 Working Mechanism of Least Significant Bit (LSB)

2.13 Watermarking Using Discrete Wavelet Transform (DWT)

2.13.1 Working Mechanism of Discrete Wavelet Transform (DWT)

2.14 Advantages of using Wavelet Transformed as watermark technique

2.15 Summary

CHAPTER 3 METHODOLOGY

3.1 Introduction

3.2 General Watermarking approach

3.3 Research Watermarking Scheme

3.4 Spatial Domain Watermarking

3.4.1 Watermark Embedding

3.4.2 Watermark Extraction

3.5 Frequency Domain Watermarking

3.5.1 Watermark Embedding

3.5.2 Watermark Extraction

3.6 The Proposed Method

3.6.1 Watermark Embedding

3.6.2 Watermark Extraction
3.7 Summary

CHAPTER 4 IMPLEMENTATION 38

4.1 Introduction 38

4.2 Implementation Equipment 38

4.3 Watermarking in spatial domain 40
   4.3.1 The Embedding Process 40
   4.3.2 The Extracting Process 41

4.4 Watermarking in frequency domain 42
   4.4.1 The Embedding Process 42
   4.4.2 The Extracting Process 43

4.5 Watermarking in proposed method 45
   4.5.1 The Embedding Process 45
   4.5.2 The Extracting Process 46

4.6 Attacks on the Watermarked Images 46
   4.6.1 Compression attack 46
   4.6.2 Noise attack 47

4.7 Summary 47

CHAPTER 5 RESULTS AND DISCUSSION 49

5.1 Introduction 49

5.2 Experimental Results 49
   5.2.1 Evaluation of watermarked images 50
   5.2.2 Evaluation of recovered watermarks 54
      5.2.2.1 Recovered watermarks before the attack 54
      5.2.2.2 Recovered watermarks after the attack 56

5.3 Summary of experimental result 64

5.4 Summary 66

CHAPTER 6 CONCLUSION AND FUTURE WORK 67

6.1 Introduction 67

6.2 Future work 68

REFERENCES 69

VITA 76
LIST OF TABLES

2.1 Illustration of LSB (Tilley, 2003; Lee et al., 2008) 20
5.1 Comparison of the MSE of the watermarked images between LSB, DWT 52
      and LSB+DWT
5.2 Comparison of the PSNR of the watermarked images between LSB, DWT 53
      and LSB+DWT
5.3 Comparison of the SSIM of the recovered watermark images between LSB, 56
      DWT and LSB+DWT
5.4 Comparison of the SSIM of the recovered watermark images after JPEG 60
      Compression between LSB, DWT and LSB+DWT
5.5 Comparison of the SSIM of the recovered watermark images after adding 64
      Noise between LSB, DWT and LSB+DWT
5.6 Summary of the results based on the fidelity 65
5.7 Summary of the results based on the robustness 66
LIST OF FIGURES

2.1 Example of traditional LSB and Lee et al.,’s algorithm 17
2.2 An example of one black and white pixel 19
2.3 One level wavelet domains 22
2.4 Two levels wavelet domains 22
2.5 Illustrating implementation of watermark using DWT (Asaad, 2005) 23
3.1 Flowchart illustrating embedding process in spatial domain 29
3.2 Flowchart illustrating extraction process in spatial domain 30
3.3 Flowchart illustrating embedding process in frequency domain 32
3.4 Flowchart illustrating extraction process in frequency domain 34
3.5 Division of the watermark 35
3.6 Flowchart illustrating embedding process in proposed method 36
3.7 Flowchart illustrating extraction process in proposed method 37
4.1 The cover images: (a) Peppers, (b) Girl, (c) Lena and (d) Jet 39
4.2 The watermark image 40
4.3 Code segment for reading the cover image and the watermark 40
4.4 Code segment for embedding the length of the watermark 41
4.5 Code segment for reading the watermarked image and the watermark 41
4.6 Code segment for extracting the length of the watermark 42
4.7 Code segment for reading the cover image and the watermark 43
4.8 Code segment for embedding the watermark at HL and LH
4.9 Code segment for (IDWT) & Writing the watermark image in file
4.10 Code segment for reading the watermarked image and the watermark
4.11 Code segment for Decomposing, Initializing, Comparing and Reverting Watermark
4.12 Code segment for reading the cover image and the watermark
4.13 Code segment for reading the watermarked image and the watermark
4.14 Code segment for writing the watermarked image in file
4.15 Code segment for reading the watermarked image and the second watermark
4.16 Code segment for reading the watermarked image and the first watermark
4.17 Code segment for JPEG compression in MATLAB
4.18 Code segment for adding noise in MATLAB
4.19 Watermarked image after noise
5.1 Watermarked image using LSB in Peppers image
5.2 Watermarked image using DWT in Peppers image
5.3 Watermarked image using LSB+DWT in Peppers image
5.4 Comparison chart of the MSE for watermarked images between LSB, DWT and LSB+DWT
5.5 Comparison chart of the PSNR for watermarked images between LSB, DWT and LSB+DWT
5.6 Recovered watermark from watermarked-LSB
5.7 Recovered watermark from watermarked-DWT
5.8 Recovered parts of watermarks from watermarked-LSB+DWT
5.9 Recovered watermark from compressed watermarked-LSB with quality (55)
5.10 Recovered watermark from compressed watermarked-DWT with quality (55)
5.11 Recovered parts of watermarks from compressed watermarked-LSB+DWT with quality (55)
5.12 Recovered watermark from compressed watermarked-LSB with quality (75)
5.13 Recovered watermark from compressed watermarked-DWT with quality (75)
5.14 Recovered watermarks parts from compressed watermarked- LSB+DWT with quality (75) 58
5.15 Recovered watermark from compressed watermarked-LSB with quality (95) 59
5.16 Recovered watermark from compressed watermarked-DWT with quality (95) 59
5.17 Recovered parts of watermarks from compressed watermarked- LSB+DWT with quality (95) 59
5.18 Recovered watermark from watermarked-LSB after noise attack with quality (0.02) 61
5.19 Recovered watermark from watermarked-DWT after noise attack with quality (0.02) 61
5.20 Recovered parts of watermark from watermarked- LSB+DWT after noise attack with quality (0.02) 61
5.21 Recovered watermark from watermarked-LSB after noise attack with quality (0.05) 62
5.22 Recovered watermark from watermarked-DWT after noise attack with quality (0.05) 62
5.23 Recovered parts of watermark from watermarked- LSB+DWT after noise attack with quality (0.05) 62
5.24 Recovered watermark from watermarked-LSB after noise attack with quality (0.08) 63
5.25 Recovered watermark from watermarked-DWT after noise attack with quality (0.08) 63
5.26 Recovered parts of watermark from watermarked- LSB+DWT after noise attack with quality (0.08) 63
ABBREVIATIONS

LSB  Least Significant Bit
DWT  Discrete Wavelet Transform
DCT  Discrete Cosine Transform
FFT  Fast Fourier Transform
PSNR Peak Signal-to-Noise Ratio
MSE  Mean Squared Error
SSIM Structural similarity
HVS  Human Visibility System
CHAPTER 1

INTRODUCTION

1.1 Background of the Study

Modern technological tools have served as time and energy saving mechanisms in assisting people to complete their jobs easily and successfully. Nevertheless, similar mechanisms are used by those who are fraudulent to commit crimes, such as illegal copying, modifying, and tampering of information contained in documents, thus, violating the integrity of the document (Pindar, 2014). In fact, the rapid usage of the internet has increased the rate of fraudulent activities (Bamatraf et al., 2010).

Besides, Albrecht (2013) asserts that in this current ICT age, there are several ways to proof the authenticity of information contained in a document, for example, initial discovery, interviews, search, and legal prosecution. According to Chapter XVIII of the laws of Malaysia Penal Code Act 574 2006, falsification of information is considered as a crime, and individuals caught in the act are punished under the law of the state (Malaysia, 2006).

Integrity is one of the three branches of information security, which deals with mechanisms and tools in protecting the integrity of information. Integrity protection mechanisms can be grouped into two: prevention and detection mechanisms. Prevention mechanism prevents unauthorised individuals from modifying the information. On the other hand, detection mechanism detects unauthorised modification when preventive mechanism fails (Pindar, 2014). Amongst the most prominent prevention mechanisms
that prevent unauthorised information modification and alteration include steganography and watermarking.

Bamatraf et al., (2010) describe steganography is the process of hiding information or embedding an imperceptible signal or signature into a given document. Bamatraf et al., (2010) further argue that the strength of steganography is measured based on its capacity to withstand malevolent alterations and attacks caused by fraudulent individuals. According to Bilal et al., (2013), the procedure for embedding data is done by manipulating and altering image pixels to hide the data.

In addition, watermarking is another mechanism that is used in protecting the integrity of intellectual property rights of digital media, such as texts, audios, videos, and images. A watermarking algorithm is made up of two main basic algorithms: the embedding and the extraction algorithms. The embedding algorithm embeds the signature or data on the document, while the extraction algorithm detects the signature and decodes its content (Zhang, 2009). There are two basic types of digital watermarking: visible watermarking, and invisible watermarking. Visible Watermarks are illustrated using visible descriptions, such as logo or stamp, to identify the owner. The watermark signal is visible in the image, video, or text. Some well-known examples of visible watermark are the logos of CNN and Cartoon Network, which are found on the television set (Gopal, 2013). On the other hand, the invisible watermark is not visible to the naked eye, and through this method, images, and other documents, such as PDF files, are protected from being copied, modified, or printed (Gopal, 2013).

1.2 Problem Statement

In addition, there has been recent development of watermarking algorithms using spatial and transform domains. The techniques in the spatial domain have relatively low-bit capacity and are not resistant to lossy image compression and other image processing procedures, as a simple noise in the watermarked image may damage the watermark data. However, frequency domain-based techniques have the capacity to embed more bits of data for watermark and are relatively more robust to attack. Discrete Cosine
Transform (DCT) and Discrete Wavelet Transform (DWT) are some of the transforms used for watermarking in the frequency domain.

Several watermarking algorithms have been proposed using DCT and DWT. The robust nature of a watermarking algorithm is a very important aspect when attacks on watermarks are considered. With much regards to this, a watermarking algorithm is regarded as robust if the watermark data embedded by that algorithm in an image or document cannot be damaged or removed without destroying or damaging the data itself. Hence, an attack is regarded successful if it can eliminate the watermark without distorting the image.

Hence, this research combined the two techniques of LSB and DWT to improve the digital watermarked image in terms of fidelity and resistance.

1.3 Objectives

The research aims were:

1. To investigate the existing watermarking techniques.
2. To compare these techniques by using PSNR and MSE; a good technique should have high PSNR value and low MSE value.
3. To test the recovered watermarks for these domains with several attacks, such as compression and noise attacks via SSIM.

1.4. Scope

This research used an image saved in BMP format as the watermark. This watermark was turned into a grayscale image and was saved in BMP format. There were two techniques used, LSB and DWT techniques, to hide the watermark. The experiment was carried out using a simulation in MATLAB.
1.5 Significance of Research

The main significances of this research are:

1. To identify the quality of the watermarked image retrieved from different domains by using MSE and PSNR and to determine the better technique.
2. To look at the robustness of these watermarked images and to identify the one that could hold up against attacks. Besides, SSIM was used to measure the recovered watermarks.

1.6 Organisation of Thesis

The organisation of this research is as follows: Chapter 2 describes the fundamental concept of digital watermarking and reviews the existing researches related to this study. Chapter 3 describes the research techniques that embedded the watermarks into the images and extracted the watermarks from the watermarked images. Next, Chapter 4 describes the implementation of the research techniques. The experimental results of the research techniques and a comparison between the techniques are discussed and are analysed in detail in Chapter 5. Finally, the conclusion of the study and future work are suggested in Chapter 6.
CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Watermarking can be described as the process of embedding data (logo or text) in a signal, such as video, image or audio, that identifies the copyright information of the file, such as author and rights (Cramer, 2005). Thus, watermarking is an approach to make sure that the data are protected. Besides, watermarking is designed to be completely invisible. The actual bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated.

According to Katzenbeisser and Petitcolas (2000), there are certain types of mechanisms in digital watermarking that are used to undetectably embed or transmit information by embedding the watermark into the cover data. However, certain issues arise in establishing the identity of the genuine owner of an object. Hence, in order to deal with this situation, a unique identity is created by stamping the name or logo of the owner on the item (image, audio, video, etc.). Thus, in the present technological age, where items are patented or copyrighted, sophisticated mechanisms are developed to establish the identity and leave the object unconstrained (Mandhani, 2004).

According to Mandhani (2004), in regards to printed watermarks, digital watermarking is a mechanism whereby information is embedded in an item in a way that it is completely invisible to the naked eye. However, the issue in concern is related to the traditional way of stamping logos or names on items, whereby the logos or names may
be easily altered or duplicated. Katzenbeisser, and Petitcolas (2000) argue that in digital 
watermarking, the actual bits are disseminated in the image in a way that demonstrate 
resistance against attempts to remove or damage the hidden information and the hidden 
itself can hardly be identified.

In addition, Al-Dharrab (2005) mentions that the use of watermarking has begun 
since a long time ago when it was used to stamp items with unique identities. In the 
present day, the watermarking technology has found its application in computing as it is 
used for embedding watermark into digital images, audio, video files, etc. Besides, 
Nagra et al., (2002) have outlined that in the late 80s, researchers focused on media 
research and digital image watermarking as an important protection mechanism, as 
researchers have implemented this mechanism for many security purposes and 
applications. Furthermore, Zheng et al., (2007) outline that watermarking can be used 
for copyright protection, content authentication, copy and usage control, and content 
description.

2.2 Host Signals

Host signal is the item or object that carries the watermark inside it. The host signals are 
used to transfer data from sender to receiver. Zheng et al., (2007) claim that there are 
different categories in digital watermarking based on the host signal. The major types 
are discussed below:

a) Digital Image

Currently, the researches on digital watermarking are concentrated on image 
watermarking. This is because images are most frequently used freely without 
any copyright protection.

b) Digital Video

A video is made up of a sequence of images. Hence, the watermarking method 
used in image is applicable on video. However, video watermarking comes with 
other problems. For instance, Zhao et al., (2000) assert that it is unsuitable to use 
the same watermarking key for the entire video. If the same key is used for all the
frames in a video sequence, the watermarking algorithm will become defenceless against collusion attacks. If a singular key is used for every frame or shot in the video sequence, it would be very difficult to manage the key management and key distribution. Besides, a video watermark should be able to resist different types of attacks, such as frame averaging, frame dropping, and frame swapping.

c) **Digital Sound**

In sound signals, watermarking is used to inaudibly transmit additional data. This mechanism is based on the psycho-acoustical approach of perceptual audio coding techniques. It examines the properties of the human ear by embedding one or more key-dependent watermark signals below the hearing threshold.

d) **3D Virtual Objects**

3D polygonal mesh is the most important component for embedding watermarking into VRML (Virtual Reality Modelling Language) and MPEG4. The outline of 3D polygonal mesh is described by two components: vertex coordinate and vertex topology. When a vertex coordinate is combined with vertex topology, it defines a more complex geometrical primitive, such as lines and polygons. Thus, the mentioned components are the most important targets for embedding in 3D mesh polygonal meshes.

### 2.3 Digital Image Watermarking

Zheng et al., (2007) describes digital image watermarking as a means of embedding a watermark into the host images in an imperceptible or perceptible way. Digital image watermarking is applied in many applications with different requirements, including copyright protection, content authentication, and content description. This form of watermarking is said to be an effective solution to the arising issues of copyright infringement since the embedded watermark can be used as a proof of the genuine ownership.

Digital watermarking can be categorized into three classes: fragile, semi fragile, and robust. A digital image watermark is said to be fragile if it cannot be detected after the slightest modification. Semi fragility occurs if it resists benign transformations, but
cannot be detected after malignant transformations. On the other hand, a digital watermark is said to be robust if it resists a designated class of transformations.

Among the most important requirement of a watermark is that it should be robust against alterations or intentional/unintentional attacks based on the design requirement. Besides, Hartung, and Kutter (1999) state that an attempt to remove or destroy a watermark downgrades the quality of the host image. Watermarking can also be used to address the issue of tampering. For instance, if an image is used as evidence, it must be proven reliable beyond the benefit of doubt. Watermarking with such property is referred to as “fragile watermarking” or “semi fragile watermarking”, which can indicate if the original image data has been damaged, or provide to more information about the attacks and the degradation of the host image (Zkeng et al., 2003).

Moreover, watermarking can be divided to be either invisible or visible. Visible is when the watermark is visible to the naked eyes and it occurs in visual patterns like signatures or names, which are embedded into or over images. This is good for identification purpose. The visible watermarking is the earliest form and the most traditional way of watermarking. Invisible watermark, unlike the visible watermark, is not visible to the naked eyes. Invisible watermarks occur in different patterns, like signatures or names, which are inserted in images without seeing the watermark on the image (Mandhani, 2004; Lee, & Jung, 2001). The watermarked image has to be similar with the original image and the human eyes should fail to identify any differences between them.

2.4 Watermarking algorithm

Every watermarking algorithm consists of two basic parts. One part embeds the watermark, and the other one detects and decodes the watermark. In embedment, the watermark is embedded along with a chosen optional key within the cover image through selected embedding algorithm. The embedding part can be designed using spatial or frequency domain. Once the watermark is embedded, then it can be identified as visible or invisible. On the other hand, the detection procedure is the reverse process of embedding. It is further described as the process of authenticating the watermarked
image. For comparison purpose, the original watermark is compared with the extracted watermark. Some algorithms may or may not require the use of original image, which is found in the comparison procedure. This is referred to as either blind or non blind watermarking.

2.5 Characteristics of Watermark

According to Cox et al., (2008), Wang et al., (2009), and Luo, and Tian (2008), a watermark can be characterised as fidelity, payload, robustness, and security.

a) Fidelity or Imperceptibility
Fidelity refers to the perceptual similarity between the cover image and the watermarked image. The embedded watermark should not reduce the quality of the cover image. This means that the cover image and the watermarked version should appear similar to the naked eye.

b) Data Payload
This refers to as the number of watermark bits that can be encoded in a cover image. The amount of data payload to be encoded relatively depends on the size of the cover image. It is said that the higher the data payload, the lesser the fidelity and robustness of the watermark. The volume of information that can be stored in the watermark is relatively dependent on the application and the quality of the embedding algorithm.

c) Robustness
The robustness of a watermarking algorithm is measured based on its capability of extracting watermark from a watermarked image, even after it has gone through attacks. The higher the robustness of a watermarking algorithm, the more valuable is the watermarked image.

d) Security
A watermarked image is considered as secured if it is able to defeat hostile attacks. A hostile attack refers to any process specifically designed to the purpose of the watermark, such as unauthorized removal, embedding, and detection.
2.6 Watermark embedding techniques

The methodologies for inserting a watermark can be categorised into visible or invisible. Visible watermarking is a visible and a transparent image is overlaid on the cover image, for example, company name, copyright, website address, logo, or text. This allows the watermark to be visible, but it is still displayed as the property of the owning organization with the motive of copyrights authentication purpose. Besides, visible watermarks discourage the illegal copying of documents, but perpetrators can remove or alter them (Hu, Kwong, & Huang, 2004). On the other hand, the invisible watermark is described as the imperceptibly embedment of watermark information into a cover image. This method is mostly preferred by researchers, as it is invisible to the naked eye.

2.7 Watermark detection techniques

Watermark detection techniques can be classified into blind and non-blind techniques. Blind techniques are deployed with watermarked image for watermark detection and do not require the application of an original image (Jun et al., 2007; Wang et al., 2009; Dorairangaswamy, 2009). On the other hand, non-blind techniques require the original image (Liu et al., 2005; Nasir et al., 2007; El-Taweel et al., 2005).

2.8 Watermarking Applications

Watermarking has found its application in different fields. Below are some specific examples where watermarking is applied (Wang et al., 2008; Cox et al., 2008; Woo, 2007).

a) Copyright Protection

Watermark helps the legitimate owners of a certain item or property to verify the illegitimate copies of their works by inserting watermark signature into their digital works. Hence, the detected watermark signature can be used as an evidence to prove ownership of the property.
b) **Fingerprinting**
When a customer purchases a digital material, a unique identity, such as a serial number, is secretly embedded within the digital material. This method discourages customers from redistributing the content. The fingerprinting signature enables the intellectual property owner to identify which customer broke their license agreement.

c) **Copy Control**
Owners of a legitimate property can control the terms of use of their work with watermarking, either copying once, copying many or no copying at all.

d) **Broadcast Monitoring**
Media broadcast channels, such as TV and radio stations, are monitored through active monitoring techniques. This monitoring techniques investigate what content is transmitted and when. This assists in verifying advertising broadcasts and royalty payments, and also to catch instances of piracy.

e) **Data Authentication**
Watermark signatures are used to identify any illegal alteration applied on a cover work, for instance, checking for fake international passport used by fraudulent individuals.

### 2.9 Techniques for Digital Image Watermarking

According to Kamble et al., (2012), digital image watermarking techniques can be classified into spatial domain technique and transform domain technique.

#### 2.9.1 Spatial Domain Technique

One of the first image watermarking techniques was implemented by Tirkel et al., (1993). His method was based on the pixel value of Least Significant Bit (LSB) modifications. The watermark algorithm was proposed by Kurah, and McHughes (1992), which involves embedding information into the LSB, and it has been known to reduce the quality of the image. This problem affects the efficiency of the algorithm.
The LSB technique works by taking the most significant bits of the watermark image and embedding it into the least significant bits of the cover image. Hence, a rough estimate of the watermarked image can be identified by simply eliminating the LSB of the watermark image. Another algorithm was proposed by Bruyndonckx et al., (1995), which is based on pixel region classification technique. Zheng et al., (2007) state that pixels with grey levels follow a certain rule when embedding a signature into a watermark.

### 2.9.2 Frequency Domain Technique

Two techniques were introduced by Cox et al., (1997) and they are spread spectrum and transform domain watermarkings. The new approach that uses spread spectrum communication technique inserts a single bit into the image. Pickholtz et al., (1982) define spread spectrum communications as “a means of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information; and the band spread is accomplished by a code which is independent of the data, and a synchronized reception with the code at the receiver is used for disspreading and subsequent data recovery.”

Another approach based on spread spectrum watermarking was proposed by O’Ruanaidh, and Pun (1998). The approach uses a pseudo-random sequence to embed watermark. A key is used as a seed to generate the pseudo-random sequence. The generated sequence is used to embed and detect the watermark. A most preferred spread spectrum is one with a combination of statistical properties and cryptographic security. Watermarking based on spatial domain is not difficult to implement, however, the consequences of this is that it is does not provide strong resistance against attacks. The transform spectral domain based watermarking, on the other hand, is more preferable because it is robust in nature.

Attacks on watermark image can be said to be intentional or unintentional. Hostility and malevolence can be identified as intentional attacks on watermark images, whereby perpetrators attempt to damage, remove or modify the watermark. On the other hand,
coincidental attacks can be said to be unintentional. This occurs during common image processing and it is not an attempt to damage the watermark image. Besides, the most common form of attack is lossy image compression (Samˇcovic, & Turan, 2008). Some categories of attacks, which can be invoked to penetrate a watermarking system, include; removal attacks, geometrical attacks, cryptographic attacks, and protocol attacks.

2.10 Removal attacks

An attack is known as a “removal attack” if a perpetrator attempts to separate and remove the watermark. The method that is mostly deployed for this type of attack is filter models taken from statistical signal theory. Eliminating noise from a watermarked image can be done through the means of median or high pass filtering, as well as nonlinear truncation or spatial watermark prediction, has proven to be successful and efficient. According to Roma et al., (2008), the main purpose of the attack is to distort the host image in order to render the watermark undetectable or unreadable. However, the image is still good in shape and it can be used for other purposes. Below are some of the attack operations that have been proposed:

a) Lossy image compression (JPEG, and JPEG 2000)
b) Addition of Gaussian noise
c) Denoising
d) Filtering
e) Median filtering and blurring
f) Signal enhancement (sharpening, and contrast enhancement)

2.10.1 Compression

This mode of attack is generally unintentional and appears quite often in multimedia applications. In a practical sense, all images currently being used on the Internet have been compressed. A watermarking algorithm is expected to resist several levels of compression, however, it is advised that the watermark insertion should be done in the same domain where the compression has taken place. For example, Roma et al., (2008)
argue that the Discrete Cosine Transform (DCT) domain image watermarking is more robust towards Joint Photograph Expert Group (JPEG) compression than the spatial domain watermarking. Meanwhile, the Discrete Wavelet Domain (DWT) domain watermarking is robust towards JPEG 2000 compression.

2.10.2 Additive noise

This occurs when a random signal with a given distribution is added to the image unintentionally. In some applications, the additive noise is a result of conversion from Digital-to-Analog (D/A) and Analog-to-Digital (A/D) signals, or it is a result of transmission errors. According to Roma et al., (2008), a perceptually shaped noise with maximum unidentified strength can be introduced by a perpetuator, and this increases the threshold at which the correlation detector operates.

2.10.3 Denoising

According to Roma et al., (2008), this type of attack explores the idea that a watermark is an additive noise, which is relative to the original image, and thus, can be modelled statistically. Some of the attacks comprise of local median, midpoint, trimmed mean filtering, Wiener filtering, and hard and soft thresholds.

2.10.4 Filtering attacks

These types of attacks are also known as linear filtering. They degrade the quality of the image. Other types of attacks, such as low pass filtering, for example, do not degrade the quality of the watermarked images, but drastically affect the performance since spread-spectrum-like watermarks have no negligible high frequency spectral contents. Therefore, in order to design a watermark robust, one should identify the group of filters that might be applied to the watermarked image. Besides, the watermark message should be designed in such a way to have most of its energy in the frequencies which filters change the least (Roma et al., 2008).
2.10.5 Statistical averaging

The main aim of these attacks is based on the attempt to retrieve the host image or watermark by statistical analysis of multiple marked data sets. The perpetuator makes an attempt to estimate the watermark, and then, “unwatermarks” the object by subtracting the estimation (Abdullah, 2013). However, the application of this method is not advisable if the watermark is not substantiated on the data. This stands as a purpose for using perceptual masks to create a watermark. This sort of attack belongs to the group of averaging and collusion attacks. Averaging attack consists of averaging many instances of a given data set when marked with a different watermark. Roma et al., (2008) claim that through this process, an estimate of the host data is computed, and each watermark is weakened. The resulting signal can potentially serve as an estimate of the watermark, which can further be used to remove it from the watermarked data.

2.11 Evaluation

The most reliable form of evaluation is through observation of the original host image and the watermark. The host images with an embedded watermark and an extracted watermark, under certain conditions, such as good lighting, quiet, and non distraction environment, would be presented to the observers for them to make judgements. Furthermore, Johnson et al., (2006) state that the results of the observation would de-test the trade-off concerning the robustness of the watermark, and if the watermark is apparent in the image. Besides, the two prominent error metrics used for comparing the techniques used in image watermarking are Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR).

The MSE is defined as the cumulative squared error between the compressed and the original image. It achieves this by measuring the average of the square of the “error”. On the other hand, the PSNR is a measure of the peak error. The result of the MSE produces an estimate of the differences between the original and the watermarked images. This also involves corrupted image. The result of an MSE comparison that is “0” indicates that the images are “the same”. Individual MSE results cannot be used,
except in comparison with each other. Given an image I (i, j) and an image K (i, j) of equal dimension. The mathematical equation (1) for calculating an MSE is defined as shown below:

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [(I(i, j) - K(i, j))^2]$$  \hspace{1cm} (1)$$

where “M” and “N” are denoted as the dimensions of the image, and the multiple energy difference between the images is the reason why MSE is often used.

The MSE of the square is as an average measurement of the “error”. The error is the amount by which the estimator differs from the quantity to be estimated. Another performance measurement for watermarking efficacy is PSNR. In order to measure the results in this study, the PSNR was used. The quality of an N × M host image (I (i, j)) is compared to the N × M image containing the watermark (K (i, j)) using the formula below.

$$PSNR = 10 \times \log_{10} \left( \frac{MAX I^2}{MSE} \right)$$  \hspace{1cm} (2)$$

As illustrated in the equation above, the MSE is embedded in the equation for PSNR beneath the square root symbol. The PSNR indicates a closer approximation between I (i, j) and K (i, j). A lower value for MSE means less error, and as seen from the inverse relationship between MSE and PSNR, this translates to a high value of PSNR. A higher value of PSNR is preferable due to the fact that the ratio of Signal to Noise is higher. Hence, understanding how the human visual system (HVS) works and how to emulate this programmatically has been some of the major research areas. Presently, the HVS seems to be too complex to be understood completely, but if even a simplified version can be modelled into objective measures, perhaps superior methods can be formulated that more closely simulate responses from human observers (Eskicioglu et al., 1995).

The main problem about the previous two criteria is that they are not similar to what similarity means to HVS. Thus, Structural Similarity (SSIM) is a function, as defined in equation (3) by Wang et al., (2004), that can be used to overcome this problem to a great extent.

$$SSIM = \frac{(2\mu_x \mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$  \hspace{1cm} (3)$$
Where $\mu$, $\sigma$, and $\sigma_{xy}$ are mean, variance, and covariance of the images, and $C1$ and $C2$ are the stabilizing constants. SSIM has a value between 0 - 1. Similar images have SSIM near to 1.

### 2.12 Watermarking Using Least Significant Bit (LSB)

A self-embedding watermarking algorithm for digital images was proposed by Luo et al., (2008). In their algorithm, the cover image is used as the watermark. The watermark is generated by half toning the host image into a half-toned image. Thus, the watermark is then permuted and inserted into the LSB of the host image. The watermark can be retrieved from the LSB of the image and then be permuted inversely.

Another watermarking testing and verification technique using Public Key Infrastructure (PKI) was introduced by Yang et al., (2008). Their algorithm combines the strength of Public Key Cryptography and watermark techniques to achieve a novel testing and verifying method.

In addition, Lee et al., (2008) proposed a new LSB digital watermarking algorithm that uses the concept of Random Mapping Function. The concept of the algorithm is to insert random watermarks in the coordinates of the image using random mapping function. This technique has been proven more robust than the traditional LSB technique. Figure 2.1 illustrates the traditional LSB technique and the algorithm mechanism proposed by Lee et al., (2008).

![Figure 2.1 Example of traditional LSB and Lee’s et al., (2008) algorithm](image_url)
Besides, Low et al., (2008) proposed a novel watermarking scheme known as “biometric watermarking”. It has been designed to embed handwritten signature invisibly in the host as an indication of legitimate ownership. Their proposed algorithm integrates the LSB and DWT techniques into a unison framework, which is known as a LSB-DWT scheme. The performance of LSB-DWT scheme is validated against simulated frequency and geometric attacks, specifically JPG compression, low pass filtering, median filtering, noise addition, scaling rotation and cropping through visual inspection, PSNR, and watermark distortion rate.

2.12.1 Working Mechanism of Least Significant Bit (LSB)

According to Tilley (2003), and Lee et al., (2008), information can be inserted directly into every bit of image information into less perceptible parts of an image. The LSB provides a better and a less perceptible location to insert information. The section elaborates the working mechanism of a 24-bit colour image and the possible effects of altering the image. A 24-bit true colour bitmap image is used in this instance. The file is first read, and then, the information is inserted into the LSB of each colour component.

Every true colour (RGB) image is made up of a basic component called “PIXEL”. Pixels are represented by 3 bytes. Each byte in a pixel is 8-bit long, and thus, explains the reason it is called a 24-bit image.

Every 3 bytes in a pixel represents a value of the three primary colours: red, green, or blue colour component. However, each byte can represent 256 different values. According to Tilley (2003), each pixel can have approximately 17 million of different colour values. Figure 2.2 shows an example for the bit-data of black and white pixels:
The principle of encoding for each of this byte, i.e. the bit on the far right hand side, uses the LSB. As the LSB is used as the mechanism for encoding information, it is possible to apply more bits to encode the data. However, actions lead to trade off, as with more bits used, more colours are added, and the image becomes altered in a way that it becomes perceptible to the human eye. Tilley (2003), and Lee et al., (2008) argue that the perceptibility of the watermark depends on the image itself. However, they mention that the last four LSBs of a colour component are the largest number of bits that can be used to insert information before the created noise becomes evident to the observer. However, information inserted into at the least two significant bits of each colour component is unlikely to be noticed. This is because the retina of the human eye has a limiting factor of viewing 24-bit pictures. Two pixels that slightly differ in the 24-bit palette are not visible to the human eye, hence named true colour.

Furthermore, Table 2.1 illustrates the procedure of embedding a watermark into the LSB. In the illustration given, the LSB of each colour component is used to insert the information. The information, which might be in the form of text and image, is first converted into a binary format. Then, each byte is spread over 3 pixels. Thus, the last byte is used to encode the start of the next byte of the hidden file.

The three basic steps of embedding information into LSB are given in Table 2.1. The first step is to assemble the pixels of the image, which are represented in binary format. Second, the values of the first LSB are changed to “0”. Lastly, the watermark, which is represented in bytes, is used to replace the first LSB. In the final byte, the blue component of pixel 3 is used at the start of the next byte of the hidden information.

<table>
<thead>
<tr>
<th>red byte</th>
<th>green byte</th>
<th>blue byte</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000000</td>
<td>00000000</td>
<td>00000000</td>
</tr>
<tr>
<td>Black</td>
<td></td>
<td></td>
</tr>
<tr>
<td>red byte</td>
<td>green byte</td>
<td>blue byte</td>
</tr>
<tr>
<td>11111111</td>
<td>11111111</td>
<td>11111111</td>
</tr>
<tr>
<td>White</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 2.2 An example of black and white pixels
Table 2.1: Illustration of LSB (Tilley, 2003; Lee et al., 2008)

<table>
<thead>
<tr>
<th>The step</th>
<th>The pixel</th>
<th>The pixel value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td><strong>The first Step</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Showing the pixels</td>
<td>Pixel 1</td>
<td>1 0 1 0 1 0 0</td>
</tr>
<tr>
<td></td>
<td>Pixel 2</td>
<td>0 1 0 1 0 1 0</td>
</tr>
<tr>
<td></td>
<td>Pixel 3</td>
<td>1 1 0 1 1 1 0</td>
</tr>
<tr>
<td><strong>The second step</strong></td>
<td>Pixel 1</td>
<td>1 0 1 0 1 0 0</td>
</tr>
<tr>
<td>Change the first LSB to 0</td>
<td>Pixel 2</td>
<td>0 1 0 1 0 1 0</td>
</tr>
<tr>
<td></td>
<td>Pixel 3</td>
<td>1 1 0 1 1 1 0</td>
</tr>
<tr>
<td><strong>The third step</strong></td>
<td>Pixel 1</td>
<td>1 0 1 0 1 0 0</td>
</tr>
<tr>
<td>Embed the byte 0 1 0 0 1 0 0 0 in the first LSB</td>
<td>Pixel 2</td>
<td>0 1 0 1 0 1 0</td>
</tr>
<tr>
<td></td>
<td>Pixel 3</td>
<td>1 1 0 1 1 1 0</td>
</tr>
</tbody>
</table>

Table 2.1 above gives an illustration of how a watermark is embedded using the LSB. However, the method used has certain limitations. Manipulation of the image, which certainly alters the pixel values of the image, results in irretrievable loss of hidden information. However, lossy compression techniques, such as JPEG, cannot be used on the image. This would result in an approximation of the image rather than a full reconstruction of the information hidden within. This also applies to cropping or scaling of the image. Thus, operations, such as rotations, reflections, or negative images can be done; however, reversing the process will restore the original bit values (Tilley, 2003).

Another limitation of the LSB technique was identified by Tilley (2003), as the observations were specifically on bitmap images, which is the file size. For example, 24-bit bitmaps can increase in size, which would make them appear suspicious during transmission over internet. Although the LSB method of concealing information is said to have a high storage capacity, 12.5% of the storage covers the size of the image. However, professional photographers and artists are known to transmit these sizes of
image in an uncompressed format, such as BMP. This is in an attempt to retain the quality of images in their high resolution.

2.13 Watermarking Using Discrete Wavelet Transform (DWT)

He et al., (2006) proposed a new approach, which uses wavelet-based fragile watermarking scheme to secure image authentication. In their mechanism, the watermark is generated and embedded using DWT, and then, a security framework is integrated into their proposed technique that scrambles the encryption embedded into the LSB of the host image. Besides, another algorithm was proposed by Bhatnagar, and Raman (2008), which uses a semi blind reference watermarking scheme based on DWT and Singular Value Decomposition (SVD). Their proposed mechanism is intended for copyright protection and authenticity, and the watermark contains a grey scale logo image.

Their proposed mechanism embeds a watermark by transforming the original image into wavelet domain. Through this procedure, a reference sub image is formed using directive contrast and wavelet coefficients. Thus, the watermark is embedded into reference image by modifying the singular values of reference image using the singular values of the watermark.

2.13.1 Working Mechanism of Discrete Wavelet Transform (DWT)

Wavelet transform is described as a time domain localized analysis method with the window’s size fixed and forms convertible. The working mechanism of the DWT in image processing is to multi differentiate and to disintegrate the image into sub-images of different spatial domain and independent frequency district. Then, it transforms the coefficient of the sub image. It further disintegrates into 4 frequency districts (i.e. one low frequency district: LL, and three high frequency districts: LH, HL, and HH), once the original image has been DWT transformed. Gunjal et al., (2010) outline that at this instance, the sub level frequency district information is obtained once the information of
low frequency district is DWT transformed. Figure 2.3 illustrates how DWT is decompressed in a single level.

<table>
<thead>
<tr>
<th>LL</th>
<th>HL</th>
</tr>
</thead>
<tbody>
<tr>
<td>LH</td>
<td>HH</td>
</tr>
</tbody>
</table>

Figure 2.3 One level wavelet domains

1. LL: Approximation coefficients matrix
2. HL: Horizontal details coefficients matrix
3. LH: Vertical details coefficients matrix
4. HH: Diagonal details coefficients matrix

Approximation coefficients LL can be further transformed to obtain two-layer approximation coefficients: LL2, and horizontal, vertical, and diagonal details coefficients: HL2, LH2, and HH2 respectively. Figure 2.4 illustrates the disintegration of DWT into two levels.

<table>
<thead>
<tr>
<th>LL2</th>
<th>HL2</th>
<th>HL1</th>
</tr>
</thead>
<tbody>
<tr>
<td>LH2</td>
<td>HH2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LH1</td>
<td>HH1</td>
</tr>
</tbody>
</table>

Figure 2.4 Two levels wavelet domains

In a two-dimensional separable dyadic DWT, every level of disintegration produces four bands of data. One of the bands corresponds to the low pass band LL, and the other three correspond to horizontal HL, vertical LH, and diagonal HH high pass bands. The disintegrated image illustrates an abrasive approximation of the image in the lowest possible resolution of the low pass band, and the three-detailed information of the image
in the higher bands. The low pass band can further be disintegrated to obtain another level of lower pass band. Thus, the procedure can be continued until the number of wanted levels is obtained (Wu, & Liu, 1998).

Among the many advantages of the DWT is that it has been understood to possess more accurate model image LL, as well as horizontal HL, vertical LH, and diagonal HH detail components. Figure 2.5 illustrates the mechanism of 2 scales DWT.

![Figure 2.5 Implementation of watermark using DWT (Asaad, 2005)](image)

According to Asaad (2005), the aspects of HVS, compared to FFT or DCT, allow the use of higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands LH, HL, and HH. By embedding watermarks into these regions, it can certainly allow the increase of the robustness of the watermark, at little to no additional impact on the quality of the image.

**Besides,** the image is decomposed into four sub images through sub sampling, and then, they are transformed via DWT to obtain the sets of coefficients Vi [n1, n2]. One pair of coefficients from two different sub images situated in the same DWT domain location is used to insert one watermark sample. The watermark insertion order sequence is that four consecutive numbers in the sequence must be different. When the pair of coefficients is Vi and Vj, the following operations are performed.

\[ V = \frac{(V_i + V_j)}{2} \]
If \(\text{abs} [(V_i-V_j)/V] < 6a\),

Then \(V_i' = V (1 +aW)\), \(V_j' = V (1-aW)\); where positive constant \((a)\) is alpha and it has a value between 0 and 1.

At the decoder stage, a similar process is followed. If the recovered watermark is \(W' [n]\), and each selected pair of coefficients is \(U_i\) and \(U_j\), \(U = (U_i+U_j)/2\);

\[
\text{If } (U_i-U_j)/U < 6a, \text{ then } W' = (U_i-U_j)/(a*(U_i+U_j)).
\]

Tsun et al., also proposed a watermarking algorithm using DWT. The proposed idea consists of the following steps:

a) Perform \(n\) level at the 2D DWT decomposition level, on the input image, and generate the output image \(X\).

b) Generate a binary matrix \(A\) with the same dimension and the structure of the matrix \(X\) using a secret key. The secret key is shared between the embedder and the authenticator.

c) Generate a binary matrix \(B\) with the same dimension as matrix \(X\), so that all its pixels that correspond to the non-zero-valued coefficients in \(X\) are set to 1 and the rest are set to 0, while \(BHH1\) is modified by projection operation on all bands at every level to this band. This projection is performed in the following manner. An OR operation is performed on all of the three sub bands, \(LLi\), \(LHi\), and \(HLi\), at each level of \(B\) to generate a sequence of binary sequences as \(C = \{C_n, C_{n-1}, ..., C_1\}\).

d) The binary watermark sequence is calculated by XOR of matrix \(A\) and matrix \(B\), which is called matrix \(W\), \(W = A \ XOR \ B\). In other words, a binary watermark \(W\) is generated by performing XOR on matrix \(A\) and matrix \(B\).

e) The wavelet coefficients in sub band \(XHH1\) are watermarked that their counterparts in sub band \(BHH1\) have a value of 1.

f) The watermark bit is embedded into the watermarkable wavelet coefficient, \(XHH1(i,j)\).
REFERENCES:


Cramer C. (2005), About Digital Watermarking. From the following website “http://www.willamette.edu/wits/idc/mmcamp/watermarking.htm”


Mandhani, N. K. (2004). Watermarking Using Decimal Sequences. Thesis submitted to the Graduate Faculty of the Louisiana State University, USA.


