DIGITAL IMAGE WATERMARKING BY USING INTERMEDIATE SIGNIFICANT BITS IN GRAY SCALE IMAGES

ALI SHARIFARA

A dissertation submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Science (Computer Science)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

AUGUST 2012

To my lovely father, AliAkbar Sharifara to support and encourage me in the whole of my life specially for being my source of inspiration…

Thanks for being there & no words could describe your support & encouragement

I love you…

ACKNOWLEDGEMENT

My appreciation first of all goes to my supervisor, Prof. Ghazali Bin Sulong, I would like to take this opportunity to thank him who gives me a lot of encouragement and guidance during the dissertation. His guidance has been a valuable asset for me during this dissertation.

I also would like to thank all my friends who are given appreciated opinion and idea of this dissertation. They are also willing to share their knowledge with me. All the discussion and recommended opinion of my course mare and friends were appreciated by me.

Finally, I would like to send my appreciation to my lovely family for their support and encouragement throughout my whole life.

ABSTRACT

The rapid growths of the computer technologies have been increased over the last half century in terms of amount and complexity of data. Also, access to the data has become much easier due to rapid growth of the networks such as Internet. Furthermore, most of the people use image to represent information and it is transferred throughout the internet. Digital watermarking techniques are used to protect the copyrights of multimedia data by embedding secret information inside them, for example, embedding in images, audios, or videos. Digital Image watermarking also has been used to detect original images against forged images by embedding an evidence of the owner of image. Digital Image watermarking can be categorized into two domains namely; spatial, and frequency domains. The former has been chosen for the current research and some remaining problems have been studied such as imperceptibility, security, and robustness of watermarked image. A repeated method is proposed to solve the problem of robustness, and a Zig-zag algorithm is also recommended to change the order of embedding in watermarked image. Furthermore, the proposed method aims to embed watermark in different bit planes of host image which can improve both the visual quality and robustness. To evaluate the proposed technique, some attacks have been applied for the approach and the experimental results have shown that the proposed technique successfully withstood against most of the attacks, and at the same time preserved the watermarked image quality.

ABSTRAK

Kadar tumbesaran teknologi komputer telah melonjak naik sejak dari separuh abad yang lalu dari segi aspek perubahan jumlah dan kerumitan data. Juga, capaian data menjadi lebih mudah dengan kemajuan pesat jaringan seperti internet. Selanjutnya, kebanyakkan orang lebih cenderung menggunakan imej sebagai medium utama untuk menyampaikan maklumat melalui internet. Teknik Tera Air digunakan untuk menlindungi hak milik data multimedia dengan membenamkan maklumat rahsia ke dalamnya, sebagai contoh, pembenaman dalam gambar, audio dan video. Tera Air digital juga digunakan dalam mengesan keaslian imej daripada yang palsu dengan membenamkan bukti pemilik asal imej tersebut. Tera Air digital boleh di kategorikan dalam 2 domain iaitu spatial dan frekuansi. Domain spatial dipilih dalam kajian ini dan masalah yang masih wujud ini dikaji seperti ketampakan, keselamatan dan kekukuhan imej tera air . Kaedah pengulangan dicadangkan untuk menyelesaikan masalah ketampakan dan algoritma zig-zag dicadangkan untuk mengubah susunan pembenaman imej tera air. Seterusnya kaedah yang dicadangkan ini mensasarkan untuk membenamkan tera air dalam satuan 'bit' yang berlainan pada imej luas supaya dapat meningkatkan kualiti visual dan kekukuhan pada tera air tersebut. Untuk menilai kaedah yang dicadangkan ini, beberapa serangan telah dilakukan dan keputusan kajian telah menunjukan bahawa kaedah tersebut berjaya mempertahankan hampir keseluruhan serangan dan pada masa mengekalkan kualiti imej tera air.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

LSB	-	Least significant Bit
MSB	-	Most significant Bit
ISB	-	Intermediate Significant Bit
CWT	-	Continues Wavelet Transform
DFT	-	Discrete Fourier Transform
DCT	-	Discrete Cosine Transform
HVS	-	Human Visual System
PSNR	-	Peak Signal to Noise Ratio
MSE	-	Mean Squared Error
NCC	-	Normalized Cross Correlation

CHAPETR 1

INTRODUCTION

1.1 Introduction

Over the last half century the pace of change in the digital technologies has been widely increased. Digital images as one of the digital technologies also have been replaced with the analog images. Moreover, Internet also became as one of the most important tools to transfer digital images from one part to other parts of the world. For this reason, the security of digital documents became a challenging concern and digital image watermarking as a solution is use to decrease the number of digital forged documents (Langelaar, 2000; Kumar N.M. , 2011).

Information hiding methods have been using since the presence of paper and after that used to many application areas such as digital image, audio, video which put an evidence of the owner of documents such as a logo, serial numbers and etc (Moulin, 2003). This might be helpful to decrease the number of unauthorized copy of them. In addition, information hiding must be imperceptible and the signals of embedded data must be low enough when projected into the human eyes.

Digital watermarking as a solution has been presented to be very practical for identifying the owner of documents (Yongjian Hu, 2004). It has been presented for some purposes like: copyright protection, data authentication, fingerprint, medical

applications, and broadcast monitoring. Furthermore, documents can be divided into two main groups, analog and digital.

Image watermarking is the process of embedding an image into a host image. For Instance, watermarks are embedded in bank cheque for preventing forgery. Consequently, unauthorized modification of data is the concern of researchers about copyright of documents and numerous image watermarking methods have been proposed with different complexity levels so far, and all of them try to set up the balance between quality and robustness of images.

Moreover, for extracting watermark there are two general approaches. The first one is blind watermarking and the second one is non-blind watermarking (Hyeong-In Choi, 2010). In blind watermarking there is no need to have the original document, while in the non-blind extraction we need to have the original document to detect the watermark (Song-Hwa Kwon, 2011). In addition, watermark can be visible or invisible in both digital and analog documents. As an example, a visible watermark can be a signature in an image that is used to point out the ownership of image; meanwhile an invisible watermark is not apparent easily. The embedded watermark can extract by using an extraction algorithms for identifying the copyright owner.

Existing digital watermarking techniques can be categorized into one of the two domains including spatial and frequency, according to the embedding domain of the host image. There are lots of researches that have been proposed base on frequency and spatial domains. For example, digital image watermarking by applying LSB (Least Significant Bit) and MSB (Most Significant Bit) are two common techniques that try to achieve robustness and quality at the same time in spatial domain(Ibrahim Nasir, 2007).

1.2 Background of the Problem

There are lots of images on the internet without having watermark, and everybody can download and modify them illegally. Furthermore, the owner of the image can be missed without watermarking (Nour El-Houda Golea, 2010). Consequently, watermarking is used to protect this behavior by adding an image as a watermark into the host image. Regardless of images we also can use it for other important documents such as video, audio, and text. Generally, there are some concerns about this area of research that still need to be solve, such as imperceptibility, robustness, security (Jiang Nan, 2006).

The first concern about the digital image watermarking is imperceptibility. It means a watermark can be inserted in the cover image without making any kind of degradation. It means, after embedding the watermark, the watermarked image and host image must be identical. In other words, the watermarked image must be the same as original image and nobody can realize the differences between them by the naked eye. In fact, the embedded watermark is really imperceptible if human eyes cannot distinguish between watermarked image and the original image.

The second one is robustness; it means the watermarking scheme must be able to protect a watermark against geometric distortion attacks like rotation, JPEG compression, and also signal processing attack like sharpening, blurring, adding noise and so on. Robustness related to ability of recovering the watermark after performing various processing attacks on watermarked image. The robustness must be sufficient if any kind of attacks occurs. The watermarking scheme should be able to protect watermark against possible signal processing operations, in addition for evaluating the quality of the watermark after applying attacks.

Security is another important issue in watermarking, which means protecting the watermark from unauthorized users and a digital watermark must be completely invisible. Due to use algorithms for embedding the watermark into the cover image

and extract it as well, presence of a secret key is needed for keeping those algorithms safe; otherwise unauthorized users can detect, remove, or modify the watermark form the host image easily.

Moreover, the human eyes have different sensitivity for different image regions and a watermark should embed in the highest priority part of the host image. In the processing of watermarking, it is important to detect the best parts of the image and embed the watermark within these areas of images.

Robustness and imperceptibility are two main parameters in the watermarking that tries to adjust beside the capacity of information which can be embedded into the host image (Ching-Tang Hsieh 2001).

1.3 Statement of the Problem

Illegal copying, modifying and copyright protection have become very significant issues with the quick use of internet and no one can deny the importance of Internet in our lives. Moreover, everyone can access to the vast of information on the Internet that includes image, video, audio and text formats and also use them for personal or commercial goals. Hence, malicious users can abuse of these digital documents. So, digital watermarking can protect them from forgery. Therefore, the digital watermarking methods have been identified as a possible solution to the copyright protection, and have become an area of increased research activity over the last decade (Gang Liu 2010).

Digital watermarking should be satisfied the below questions:

1- How we can embed an image as a watermark into the host image without causing visible degradation?

2- How we can achieve quality of watermarked image without losing robustness?
3- How much information we can put into the host image?
4- How we can extract watermark from the watermarked image?

1.4 Aim of dissertation

The main aim of this research is to propose a technique based on ISB (Intermediate Significant Bit) to achieve high robustness and imperceptibility of gray scale watermarked image. Applying ISB in watermarking is robustness enough to protect image from attacks and also preserve quality of watermarked image in spatial domain.

1.5 Objectives of the Study

To answer the problem statement, following objectives of this project are:

1- To study and apply watermarking in gray scale image by using ISB (Intermediate Significant Bits).
2- To improve the robustness of gray scale image watermarking.
3- To apply image attacks and evaluate the quality and robustness of proposed watermarking method by using PSNR (Peak Signal to Noise Ratio) and NCC (Normalized Cross Correlation).
4- To compare proposed method to LSB and MSB methods after and before applying attacks.

1.6 Scope of the Study

In this paper we deal with gray scale images as host image that we want to add and extract watermark, and the approach is using non-blind watermarking in spatial domain by applying ISB. The applied attacks are Gaussian filter, salt and pepper, speckle, and Blurring attacks. Host image and watermark images are a grey scale image with 256 × 256 pixels and a gray scale logo with 50 × 50 pixels, respectively and both of the images are in TIF format.

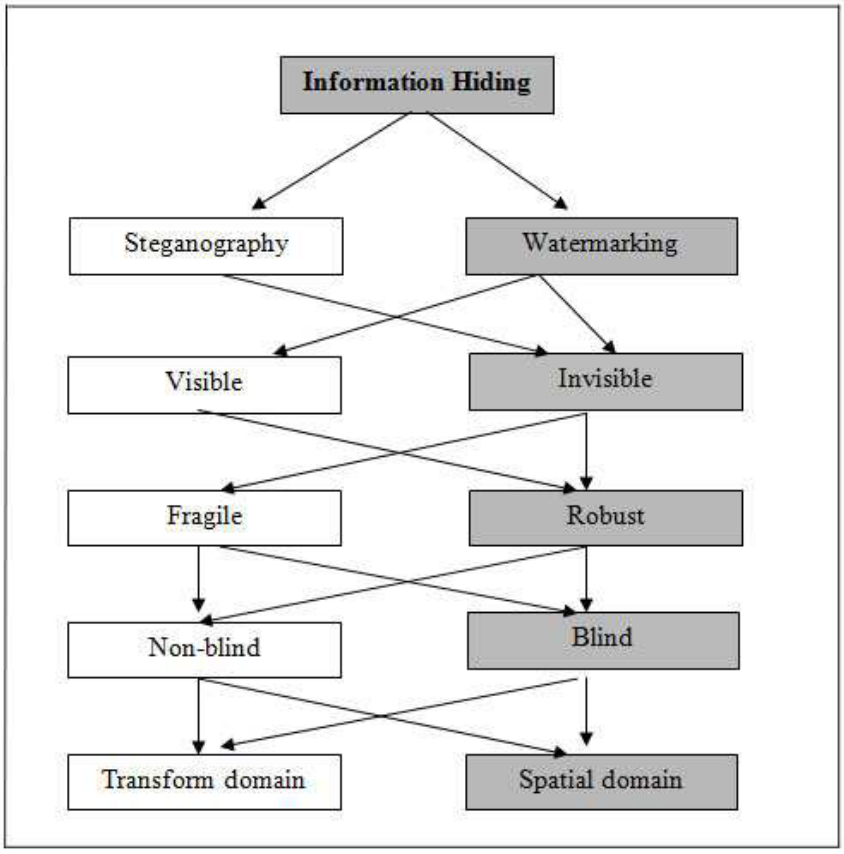

Figure 1.1 The approach of study

1.7 Significance of the study

Over the past few years digital watermarking has became more popular due to its significance in content authentication and legal ownership for digital multimedia data. Furthermore, digital watermarking and data hiding has become an important tool for protecting digital images from theft, illegal copying and unlawful reproduction.

1.8 Dissertation organization

This research consists of five chapters. The first chapter presents introduction to the project which includes the problem background, problem statements, aim of project, the main objectives and scope of the project. In the chapter two covers information about literature review on watermarking, which focused on current algorithms that have been using for protecting image against attacks. The project methodology is discussed in Chapter three where comparative study and pre-lab testing have been used as the research strategy. In Chapter 4, the implementation of the methodology where the findings of comparative study and pre-lab testing take place and eventually, in Chapter five the result and findings of the lab testing is explained and the overall project will concluded as well.