BLIND COLOUR IMAGE WATERMARKING TECHNIQUES IN HYBRID DOMAIN USING LEAST SIGNIFICANT BIT AND SLANTLET TRANSFORM

HARITH RAAD HASAN

A thesis submitted in fulfilment of the
requirements for the award of degree of
Doctor of Philosophy (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

MAY 2014

Dedicated to:

My lovely Father, Mother, Fariaa, Sara, and Taha.

My dearest brothers.

ACKNOWLEDGEMENT

Thanks to Allah SWT for everything, I was able to achieve and for everything I tried but I was not able to achieve.

First of all, I would like to take this opportunity to gratefully acknowledge the wholehearted supervision of Professor Dr. Ghazali bin Sulong during this work. His dedication, skillful guidance, helpful suggestions and constant encouragement made it possible for me to deliver a dissertation of appreciable quality and standard.

I would also like to say special thanks to:

My co-supervisor Professor Dr. Ali Selamat, for his guidance during this study.

My friends who support me to finish this study, especially (M. Rostam, Dr. Soran, Dr. Alaa, M Haval and M.Gulala).

I am forever indebted to my parents for their patience and understanding, alleviating my family responsibilities and encouraging me to concentrate on my study.

Finally and most importantly, I would like to express special thanks to Fariaa and for her support when it was most required. Without her help and encouragement, this study would not have been completed.

ABSTRACT

Colour image watermarking has attracted a lot of interests since the last decade in tandem with the rapid growth of internet and its applications. This is due to increased awareness especially amongst netizens to protect digital assets from fraudulent activities. Many research efforts focused on improving the imperceptibility or robustness of both semi-blind and non-blind watermarking in spatial or transform domain. The results so far have been encouraging. Nonetheless, the requirements of the watermarking applications are varied in terms of imperceptibility, robustness and capacity. Ironically, limited studies concern on the authenticity and blind watermarking. Hence, this study presents two new blind RGB image watermarking techniques called Model1 and Model2 in hybrid domain using Least Significant Bit (LSB) insertion and Slantlet Transform (SLT). The models share similar pre-processing and LSB insertion stages but differ in SLT approach. In addition, two interrelated watermarks known as main watermark (MW) and sub-watermark (SW) are also utilized. Firstly, the RGB cover image is converted into YCbCr colour space and then split up into three components namely, Y, Cb and Cr. Secondly, the Cb component is selected as a cover for the MW embedding using the LSB substitution to attain a Cb-watermarked image (CbW). Thirdly, the Cr component is chosen and converted into the transform domain using SLT, and is subsequently decomposed into two paths: three-level sub-bands for Model1 and two-level sub-bands for Model2. For each model, the sub-bands are then used as a cover for sub-watermark embedding to generate a Cr-watermarked image (CrW). Following that, the Y component, CbW and CrW are combined to obtain a YCbCr-watermarked image. Finally, the image is reverted to RGB colour space to attain the actual watermarked image (WI). Upon embedding, the MW and SW are extracted from WI. The extraction process is similar to the above embedding except it is accomplished in a reverse order. Experimental results which utilized the standard dataset with fifteen well-known attacks revealed that, among others: Model1 has produced high imperceptibility, moderate robustness and good capacity, with Peak Signal-to-Noise Ratio (PSNR) rose to 65dB, Normalized Cross Correlation (NCC) moderated at 0.80, and capacity was 15%. Meanwhile, Model2, as per designed, performed positively in all aspects, with NCC strengthened to 1.00, capacity jumped to 25% and PSNR softened at 55dB but still on the high side. Interestingly, in terms of authenticity, Model2 performed impressively albeit the extracted MW has been completely altered. Overall, the models have successfully fulfilled all the research objectives and also markedly outperformed benchmark watermarking techniques.

ABSTRAK

Penandaan air imej warna telah menarik banyak minat sejak dekad yang lalu seiring dengan pertumbuhan pesat internet dan aplikasinya ekoran peningkatan kesedaran terutama di kalangan netizen untuk melindungi aset digital daripada aktiviti penipuan. Banyak usaha penyelidikan memberi tumpuan kepada peningkatan ketidaktampakan atau keteguhan bagi kedua-dua jenis penandaan air semi-petunjuk dan berpetunjuk dalam domain spatial atau transformasi. Walau bagaimanapun, keperluan terhadap penandaan air adalah pelbagai dari sudut ketidaktampakan, keteguhan dan kapasiti. Ironinya, kajian mengenai kesahihan dan penandaan air tanpa-petunjuk adalah terhad. Oleh itu, kajian ini membentangkan dua teknik baru penandaan air tanpa-petunjuk imej *RGB* yang digelar Model1 dan Model2 dalam domain hibrid menggunakan kemasukan bit signifikan terkecil (*LSB*) dan transformasi *Slantlet* (*SLT*). Model-model tersebut berkongsi peringkat pra-pemprosesan dan sisipan *LSB* yang sama tetapi berbeza dalam pendekatan *SLT*. Di samping itu, dua tera air saling berkaitan yang dikenali sebagai tera air utama (MW) dan sub-tera air (SW) turut digunakan. Pertama, imej pelindung *RGB* ditukar kepada ruang warna *YCbCr* dan kemudiannya dipecahkan kepada tiga komponen iaitu, *Y*, *Cb* dan *Cr*. Kedua, komponen *Cb* dipilih sebagai pelindung untuk pembenaman MW menggunakan pendekatan penggantian *LSB* untuk memperolehi imej tera air *Cb* (CbW). Ketiga, komponen *Cr* dipilih dan ditukar kepada domain tranformasi menggunakan *SLT*, dan kemudiannya dihuraikan kepada dua laluan: tiga peringkat sub-jalur untuk Model1 dan dua peringkat sub-jalur untuk Model2. Bagi setiap model, sub-jalur tersebut digunakan sebagai pelindung untuk pembenaman sub-tera air bagi menjana imej tera air *Cr* (CrW). Seterusnya, komponen *Y*, CbW dan CrW digabungkan untuk mendapatkan imej tera air *YCbCr*. Akhirnya, imej tersebut dikembalikan kepada ruang warna *RGB* untuk mencapai imej tera air sebenar (WI). Setelah pembenaman, MW dan SW diekstrak daripada WI. Proses pengekstrakan adalah sama seperti pembenaman di atas melainkan ianya dilaksanakan dalam susunan songsang. Keputusan eksperimen yang menggunakan set data piawai dengan lima belas serangan tersohor mendedahkan bahawa, antara lain: Model1 telah menghasilkan ketidaktampakan yang tinggi, keteguhan sederhana dan kapasiti yang baik, dengan Nisbah Puncak Isyarat-terhadap-Hingar (*PSNR*) meningkat kepada 65dB, Korelasi Silang Ternormal (*NCC*) sederhana pada 0.80, dan kapasiti 15%. Manakala Model2, seperti yang direka, prestasinya adalah positif dalam semua aspek, dengan *NCC* mengukuh kepada 1.00, kapasiti melonjak kepada 25% dan *PSNR* mengendur kepada 55dB tetapi masih pada tahap tinggi. Menariknya, dari segi kesahihan, prestasi Model2 begitu terserlah walaupun MW yang diekstrak telah benar-benar berubah. Keseluruhannya, model-model tersebut berjaya memenuhi kesemua objektif kajian dan juga dengan ketara mengatasi prestasi teknik tanda aras penandaan air.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

dB	-	Decibel
DCT	-	Discrete Cosine Transform
DFT	-	Discrete Fourier Transform
DWT	-	Discrete Wavelet Transform
EISB	-	Enhanced Intermediate Significant Bit
FFT	-	Fast Fourier Transform
HH	-	High-High frequency band
HL	-	High-Low frequency band
HVS	-	Human Visual System
IDCT	-	Invert Discrete Cosine Transform
IDFT	-	Invert Discrete Fourier Transform
IDWT	-	Invert Discrete Wavelet Transform
IP	-	Inverted Pattern
ISB	-	Intermediate Significant Bit
ISLT	-	Invert Slanlet Transform
JPEG	-	Joint Photographic Expert Groups
LH	-	Low-High frequency band
LL	-	Low-Low frequency band
LPAP	-	Local Pixel Adjustment Process
LSB	-	Least Significant Bit
MSB	-	Most Significant Bit
MSE	-	Mean Square Error
NCC	-	Normalized Cross Correlation
OPAP	-	Optimal Pixel Adjustment Process
OSR	-	Optimal Similarity Rate
PSNR	-	Peak Signal to Noise Ratio

PVD	-	Pixel Value Differencing
SLT	-	Slantlet Transform
SSIM	-	Structural Similarity Index Measurement
TIBV	-	Thresholds based on Intermediate Bit Values

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Since the early 1990 resources in the form of text, images, audio and video are easily accessible from the internet. As businesses are built on the use of such resources, it has become increasingly important to have some form of references which confirms ownership of the digital media. Digital watermarking has been proposed as a way to accomplish this protection.

It is possible to accomplish digital watermarking by embedding a digital signal or pattern onto a digital image. A digital watermark is considered a digital signature when it is present in each unaltered copy of the original image. A given watermark may be unique to each copy (e.g. to identify the intended recipient), or be common to multiple copies (e.g. to identify the document source). In either case, the watermarking of the document involves the transformation of the original into another form which is a persistent, yet imperceptible digital identifier added to the original images to communicate copyright ownership and help locate where they are used online.

Digital watermarking is different from public key encryption. In public key encryption, the image is changed to a form that is unrecognizable. It will be necessary to use a description key to view the image in its original form. After decryption, there is no trace of the public encryption process on the digital image. In watermarking the original image is basically intact and unrecognizable. Decrypted documents are free of any residual effects of encryption, whereas digital watermarks are designed to be persistent in viewing, printing, or subsequent re-transmission or dissemination (El-Gayyar and Gathen, 2006).

1.2 Problem Background

The rapid growth of the internet makes it easy to access multimedia resources easily and quickly. The use of internet sourced multimedia materials for different purposes has proliferated, resulting in the increase of diversified copyright problems. In the beginning, the developers were using analog technology to build the multimedia applications but, multimedia applications were difficult to manipulate using analog technology due to limited performance (Friedmanet, 1993). Therefore digital technology appeared with more flexibility and reliability, which lead to easier manipulation (Friedmanet, 1993).

The watermarking Technique is essentially a process of embedding security information within other information. The technique of watermarking involves modifying a host content to include a representation of some specific authentication information, i.e. password, identification, ownership, etc. Once the host is watermarked, it can be distributed by the owner as the “original” content. Since the protection is permanently embedded within the original data, watermarking serves as a complement to data encryption (Hoan & Roland, 2007). A generic watermarking system consists of an encoder, which performs the embedding of the watermark into the host data and a decoder, which performs the extraction and verification of authenticity of the watermarked content in order to provide or deny access to the data (Hartung and Kutter, 1999).

Watermarking schemes can be classified as “blind”, “semi-blind” or “non-blind” based on the method of the detection used. In non-blind watermark detection, both the original host information and watermark key are needed to estimate the embedded watermark data. In semi-blind watermark detection only the watermark key is needed (Cox & Miller, 1997). In blind watermark, detection does not require any information about the original host. This Digital watermarking techniques were using to protect the copyrights of multimedia data by embedding secret information in the host media.

Many techniques fail to satisfy all the requirements for imperceptibility and robustness because of the multifarious multimedia applications, multimedia communications and multimedia networking applications. In the search for a technique which will satisfy all requirements of imperceptibility and robustness, watermark is embedded in spatial domain or in transform domain.

When watermark is embedded in spatial domain, the quality of its extracted image tends to be high in imperceptibility and low in robustness. When it is embedded in transform domain, the quality of its extracted image gives low imperceptibility but high in robustness. This pro and contra between spatial domain and transform domain is the limit cycle for the process of embedding watermark. Robustness, Imperceptibility, Capacity and Authenticity (El-Gayyar and Gathen, 2006) is defined it as follows:

i. Robustness

Robustness of watermark is a characteristic property which will determine how this watermark survive signal manipulations. It is important to design a watermark which can survive common signal processing operations and possibly certain malicious attacks (Wu and Hwang, 2007; Song et al., 2010). Embedding a watermark into the perceptually significant parts of the image is a good strategy for robustness. This watermarking strategy is likely to survive lossy Compression because the embedding process is on to the perceptually significant data while lossy compression discard the perceptually non-significant data. Unfortunately, the perceptually significant parts of the image is sensitive to the human vision. If the watermark is embedded on to this part of the image, it will degrade the quality of the host. Applications scenarios determine the degree of robustness of watermarking. Some applications need high degree of robustness but do not worry about the quality of the image. On the other hand, other applications will require high quality of the image even the robustness is low. Indeed, a watermark needs only to survive the attacks and those signal processing operations that are likely to occur during the period when the watermarked signal is in communication channel (Emami et al., 2012; Su et al., 2013).

ii. Imperceptibility

This concept is based on the properties of the Human Visual System (HVS). The embedded information is imperceptible if an average human person is unable to distinguish the hidden information from the background information. High imperceptibility is achieved when the human eye cannot determine the difference between the watermarked image and the original host image. If the watermarking used embedding algorithm which embed the watermark onto the perceptually non-significant part of the host image, the distortion is reduced. However, this algorithm is prone to attacks which alter the watermark information without being noticed. (Podilchuk and Zeng, 1998; Podilchuk and Delp, 2001).

iii. Capacity

The capacity of watermarking depends on it size. The bigger the watermark the lower would be the value of imperceptibility and robustness (refer to Fig. 1.1). In some applications, high capacity is important. For example, when transmitting medical images where the personal data, and the diagnosis are embedded into the same picture.

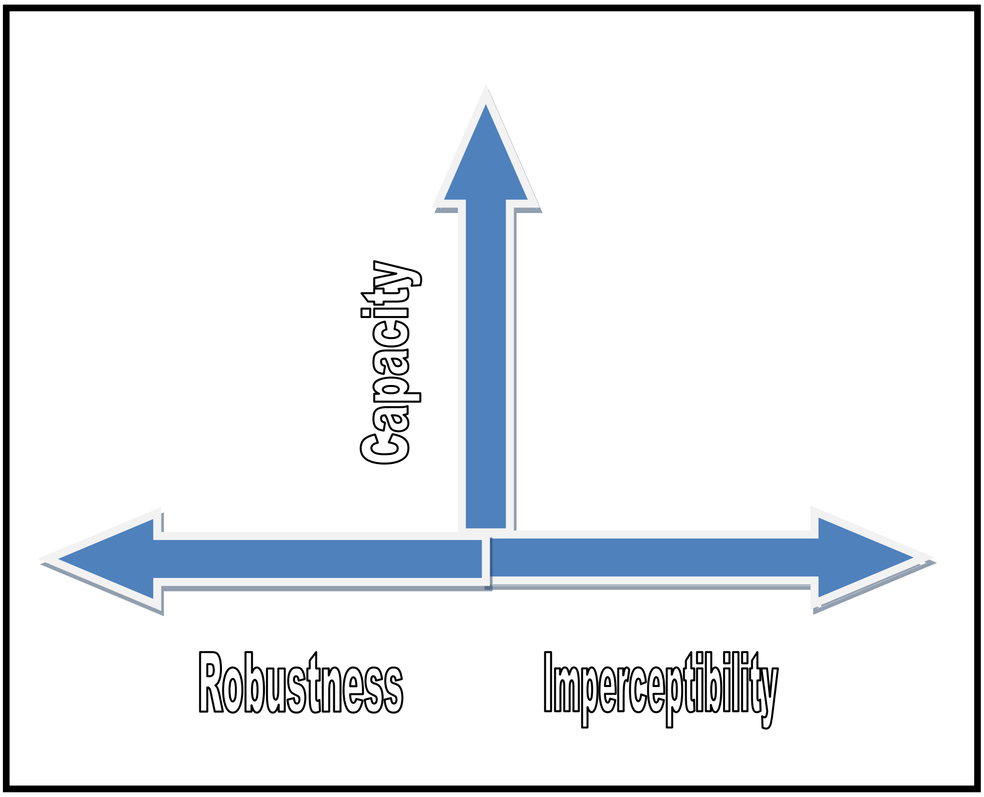

Figure 1.1 Diagram of the trade-off between imperceptibility, Robustness, and Capacity

iv. Authenticity (Security)

The purpose of watermarking is to protect the original host image. For this reason, high security is important. Security of watermarking will ensure that the location of embedded watermark is indeterminate and that the information of the extracted watermark is not corrupted or completely changed. Malicious attacks can completely alter the watermark. For this reason the security of watermarking must ensure the secrecy and Authenticity of the watermark information (Li and Yang, 2003).

The above mentioned requirements (factors) are such that one will increase at the expense of the others. Clearly, optimization will entail some kind of trading off between these requirements entities. If a large watermark is to be hidden inside an image, absolute imperceptibility and large robustness would not be achieved. A reasonable compromise is always a necessity. On the other hand, if robustness to large distortion is an issue, the watermark that can be reliably hidden cannot be too big. There are related basic issues which have to be sorted out if both the desirable robustness and imperceptibility requirements need to be met. The reliability of some of the techniques used to embed the watermark may be ascertained by looking at the extent of degradation after applying various attacks on the watermarked image. Ultimately, the winning technique is that which can achieve and improve the imperceptibility, robustness, capacity and authenticity of watermarked images which have been exposed to various attacks.

Researchers have been focusing on human visual system (HVS) in order to improve the watermarking systems and fulfill the basic requirements of watermarking (Barni et al., 2001; Reddy and Chatterji, 2005; Chanet and Chang, 2004). By making reference to HVS, a maximum hiding level can be obtained for the watermark embedding process while keeping the visible image distortions to a minimum (Temi et al., 2005; Zhang, 2009).

Each part of an image has different properties which may affect watermarking imperceptibility and robustness. The human visual system is sensitive to some parts of the image and may not be sensitive to another part of the host image. For this reason the best embedding region is in the less sensitive part of the host image (Liu and Wang, 2008).

HVS will be less sensitive to alteration in the parts of the host image where there are edges and textures (Ramos et al, 1997; Helsingius et al, 2000; Lixionget and Yunde, 2007). These areas can accommodate embedded watermark image without degradation of the watermark information. Embedding in areas where there are textures and edges increases the robustness of watermarking (Reddy and Varadarajan, 2009).

Currently, applications of watermarking serve the following purposes (Podilchuk and Zeng, 1998):

a. Copyright protection: the objective is to embed information about the source/owner of the digital media in order to prevent other parties from claiming the ownership of the media.

b. Fingerprinting: the objective of fingerprinting is to convey information about the recipient of the digital media (rather than the owner) in order to identify every single distributed copy of the media. This concept is very similar to serial numbers of software products.

c. Copy protection: watermarking can be used to control data copying devices and prevent them from copying the digital media when the watermark embedded in the media indicates that the media is copy-protected.

d. Image authentication: the objective is to check the authenticity of the digital media. This requires the detection of modifications to the data.

The three processes of steganography, watermarking and cryptography are interlinked. Drawing a boundary separating these can be both arbitrary and confusing. Therefore, it is necessary to discuss briefly these processes before a thorough review can be provided. Figure 1.2 may facilitate understanding which can allow distinguishing one from the other. The work presented here concerns steganography of digital images and does not include other types of steganography, such as linguistic or audio. Table 1.1 summarizes the differences and similarities between steganography, watermarking and cryptography.

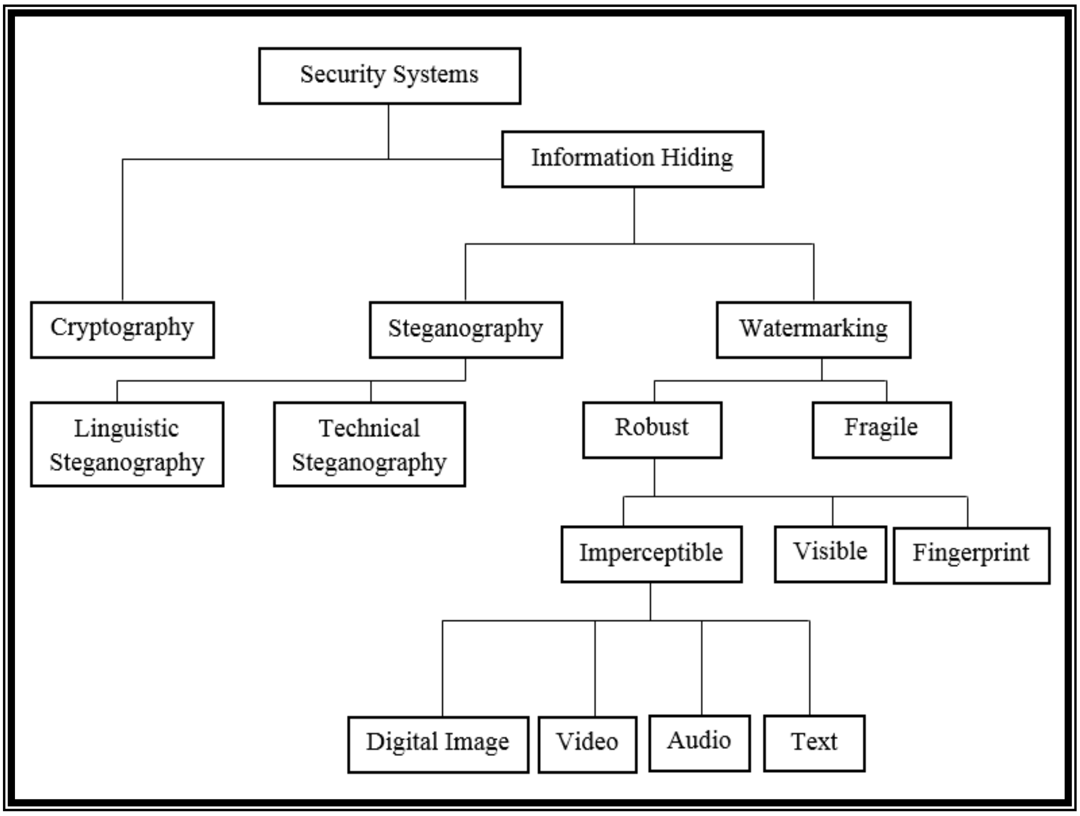

Figure 1.2 The different embodiment disciplines of security system (Abbas Cheddad, 2009).

Table 1.1: Comparison of steganography, watermarking and cryptography (Abbas Cheddad, 2009).

Criterion/Method	Steganography	Robust Watermarking	Cryptography
Carrier	any digital media	mostly image/audio files	usually text based, with some extensions to image files
Secret data	payload	watermark	plain text
Structure	no changes to the structure		changes the structure
Key	optional		necessary
Input files	at least two unless in self-embedding		one
Detection	blind	usually informative, i.e., original cover or watermark is needed for recovery	blind
Authentication	full retrieval of data	usually achieved by cross correlation	full retrieval of data
Objective	secrete communication	copyright preserving	data protection
Result	stego-file	watermarked-file	cipher-text
Concern	detectability/ capacity	robustness	robustness
Type of attacks	steganalysis	signal processing and Geometric	cryptanalysis
Visibility	never	sometimes	always
Fails when	it is detected	it is removed/replaced	de-ciphered
Relation to cover	not necessarily related to the cover. The message is more important than the cover.	usually becomes an attribute of the cover image. The cover is more important than the message.	N/A
Flexibility	free to choose any suitable cover	cover choice is restricted	N/A
History	very ancient except its digital version	modern era	modern era

1.3 Problem Statement

Internet and digital multimedia content have significant effect on present day business. Open access of digital media content makes them prone to privacy intrusion and forgery which results in many kinds of intellectual property abuses. To protect the millions of innocent users of the internet from these abuses, it will be necessary to come up with some techniques which can protect ownership of intellectual properties such as watermarking. However, watermarking techniques have some problems. The four measures associated with watermarking that is considered very important; viz: Imperceptibility, Robustness, Capacity and Authenticity, works against one another. For example, increase of imperceptibility results in the decrease of robustness and vice versa.

Many previous research efforts were focused to improve and increase the imperceptibility or robustness of watermarking. The results so far have been significant. Nevertheless, the techniques have good imperceptibility or good robustness and limited capacity. The requirements of the watermarking applications are varied- some require high imperceptibility and reasonable robustness and capacity, on the other hand, some prefer high robustness and capacity and acceptable imperceptibility. Ironically, very limited studies concerns on the Authenticity - most of them rely 100% on the values of NCC (El-Gayyar and Gathen, 2006; Emami et al., 2012; Su et al., 2013).

Most previous studies proposed non-blind and semi-blind watermarking techniques: these techniques require all or part of the host image information to extract the watermark image; however, most applications do not provide the information of the host image to the second party for watermark image extraction (Lin et al., 2010).

Normalized Cross Correlation (NCC) has been used to measure the robustness by evaluating the difference between original watermark and the extracted watermark which has gone through the different types of attacks such as noise, geometric and filtering assaults. A value of NCC greater than 0.70 indicates that the extracted watermark is recognizable (Al-Otum & Samara, 2010; Song et al., 2010) However, the value of NCC is high but, HVS unable to recognize the extracted watermark images especially in spatial domain. It is therefore necessary to find a way to improve the Authenticity of the extracted watermark in spatial domain.

1.4 Research Questions

i. How to design a new blind watermarking scheme that can fulfil two different requirements:
   a) High imperceptibility.
   b) High robustness.

ii. How to design a new blind watermarking technique that can ensure the Authenticity of the watermark is intact in the event of the extracted watermark has been partially or completely altered?

1.5 Research Aim

Most previous works on watermarking use one domain process and test results for watermarked image were against one or two types of attacks. This thesis was to propose a new blind colour image watermarking scheme where two domains are used continuously. The embedding process starts in the spatial domain and ends in the transform domain. The purpose of using two domains which are spatial and transform (hybrid domain) is essential to improve the performance result for Imperceptibility, Robustness, Capacity and Authenticity.

1.6 Research Objectives

The objectives of this thesis are:

1. To propose a new blind color image watermarking scheme with two models to serve two different needs.
2. To propose a new blind color image watermarking technique by using hybrid domain in order to obtain high imperceptibility and good robustness, capacity and Authenticity.
3. To propose a new blind color image watermarking technique by using hybrid domain in order to obtain high robustness, capacity and Authenticity.as well as good imperceptibility.
4. To authenticate the owner identification of the attacked watermarked image (Authenticity) by using two interrelated watermarks.

1.7 Research Scope

The objectives of this study are attained by recognizing the problem scope which covers the following aspects:

a. Host/ Cover image: standard RGB image (512 X 512 pixels) take from SIPI http://sipi.usc.edu.

b. Watermark image: Gray scale image (128 X 256).
c. Domain: Hybrid domain.
d. Attacks: two groups of common attack Signal processing attacks and Geometric attacks.

1.8 The Importance of the Study

Owners of digital media have lost considerable business due to copy-write piracy. Watermarking techniques are currently considered an effective way to combat this problem. Research work done on watermarking so far have been unable to come up with good robustness, good imperceptibility, high capacity as well as good Authenticity. The watermarking technique proposed in this thesis satisfies all the required aspect for high robustness, high imperceptibility, high capacity and Authenticity.

1.9 Organization of the Thesis.

This thesis is organized as follow: Chapter 1 presents an overview of the study and the background of research. Recent research contributions in this area as well as the problem statements are discussed. The aim, objectives, scope, and significance of the research work are declared. Chapter 2 presents an overview of significant contributions in the area of watermarking techniques. Slantlet Transform (SLT) is explained in Chapter3. Different techniques of using hybrid domain (spatial domain and transform domain) to embed the two watermark images within two components of YCbCr as cover image are explained in Chapter 4. Results are given and discussed in Chapter 5. Finally, the conclusion, contributions and suggestions for future work are illustrated in Chapter 6.

REFERENCES

Abbas Cheddad. (2009). *A New Image Steganography Algorithm*. M.Sc.thesis, School of Computing & Intelligent Systems Faculty of Computing & Engineering University of Ulster.

Adelson, E. H. (1990). *Digital signal encoding and decoding apparatus*. U.S. Patent 4939515.

Al-Asmari, A. K. and Al-Enizi, F. A. (2009). A Pyramid-Based Watermarking Technique for Digital Color Images Copyright Protection. *International Conference on Computing, Engineering and Information*. 978-0-7695-3538.

Alattar, A.M. (2004). Reversible watermark using the difference expansion of a generalized integer transform. *IEEE Transactions on Image Processing*, 13 (8), 1147–1156.

Aliwa, M. B., El-Tobely, T. E. and Fahmy, M. M . (2010). A New Novel Fidelity Digital Watermarking Based on Adaptively Pixel- Most-Significant-Bit-6 in Spatial Domain Gray Scale Images and Robust. *American Journal of Applied Sciences*, vol.7, no.7, pp.987-1022.

Al-Otum, H. M. and Samara, N. A. (2010). A robust blind color image watermarking based on wavelet-tree bit host difference selection. *Signal Processing, Elsevier*, vol :90, pp. 2498-2512.

Atawneh S, Almomani A and Sumari P. (2013). Steganography in digital images: Common approaches and tools. *IETE Tech Rev*, volume 30, issue 4.

Baisa L Gunjal and Dr. Suresh N Mali. (2013). Handling Various Attacks in Image Watermarking. *CSI Communications*, 30.

Baisa L.Gunjal and R.R. Manthalkar. (2010). An Overview Of Transform Domain Robust Digital Image Watermarking Algorithms. *Journal of Emerging Trends in Computing and Information Sciences*, Volume 2 No.1.

Barni, M. bartolini, f. and piva, a. (2001). Improved Wavelet Based Watermarking Through Pixel-wise Masking. *IEEE transactions on image processing*, 10(5), 783- 791.

Bas, P. and Chassery, J. M. (2004). Tatouage couleur adaptatif fondé sur l'utilisation d'espaces perceptifs uniformes. *Traitement du Signal*, 21, 517- 531.

Belkacem, S., Batna Dibi, Z. and Bouridane, A. (2007). Colour Image Watermarking based on Chaotic Map. *Electronics, Circuits and Systems, 2007. ICECS 2007. 14th IEEE International Conference*. pp. 343 – 346.

Bender, D. Gruhl, and N. Morimoto. (1995). Techniques for Data Hiding Proceedings of the SPIE. *Storage and Retrieval for Image and Video Databases III*, vol. 2420, pp. 164-173.

Bennour, J., Dugelay, and Matta. (2007). Watermarking Attack (BOWS contest). *Security, Steganography, and Watermarking of Multimedia Contents, Proceedings of SPIE-IS&T Electronic Imaging,* vol. 6505, pp. 650518-1 - 650518-6, SPIE-IS&T.

Cachin C. (2004). An Information-Theoretic Model for Steganography. *Information and Computation*, vol. 192, no. 1, pp. 41-56.

Chai, D. and Bouzerdoum. A. (2000). A Bayesian Approach to Skin Classification in YCbCr Color Space. *IEEE*. School of Engineering and Mathematics Edith Cowan University Joondalup 6027, Perth, AUSTRALIA.

Chan, C. and Cheng, L. M. (2001). Improved Hiding Data in Images by Optimal Moderate Significant Bit Replacement. *IEE Electronics Letters*, vol.37, no.16, pp.1017-1018.

Chanet , M. and Chang, L. W. (2004). A Novel Public Watermarking System based on Advanced Encryption System. *IEEE International Conference on Advanced Information Networking and Application*. 0-7695-2051-0/04.

Chang, C., and Tseng, H. (2004). A Stenganographic Method for Digital Images using Side Match. *Pattern Recognition Letters*, vol. 25, pp. 1431–1437.

Chang, C., Lin, C., and Hu, Y. (2007). An SVD Oriented Watermark Embedding Scheme with High Qualities for the Restored Images. *International Journal of Innovative Computing, Information and Control*, vol. 3, no. 3.

Chang, K., Huang, P. Tu, S., T., and Chang, C. (2007). Adaptive image steganographic scheme based on Tri-way Pixel-Value Differencing. *IEEE International Conference on Systems, Man and Cybernetics,* pp. 1165 - 1170, IEEE Computer Society.

Chaumont, M. and Puech, W. (2006). A Color Image Hidden in a Grey-Level Image. *In proceedings of IS&T, Conference on Color in Graphics, Imaging, and Vision*, 226-231.

Chaumont, M. and Puech, W. (2007). A Fast and Efficient Method To Protect Color Images. *In proceedings of The International Society for Optical Engineering, Visual Communications and Image Processing*, vol. 65089.

Chen and G. Wornell. (1999). Dither Modulation: a New Approach to Digital Watermarking and Information Embedding. *Proceeding of SPIE on Security and Watermarking of Multimedia Contents*, vol. 3657, pp. 342.

Cheung, W. N. (2000). Digital Image Watermarking in Spatial and Transform Domains. *Proceedings TENCON 2000*,pp. III-374 – III-378, IEEE Computer Society.

Chiou-Ting Hsu and Ja-Ling Wu. (1996). Multiresolution Watermarking for Digital Images. *IEEE Trans. Circuits and Systems II*, vol. 45, no. 8 pp. 1097-1101.

Chitwongd S., Seksan Phonsrib, and Punya Thitimajshimab. (2000). Reference Line Extraction for Automated Data-Entry System Using Wavelet Transform. *IS&T/SPIE Conference on Document Recognition and Retrieval VII*, 110 San Jose, California.

Chu, S., Jain, L. C., Huang, H. and Pan, J. (2010). Error-Resilient Triple-Watermarking with Multiple Description Coding. *Journal of Networks*, vol. 5, no. 3, pp. 267-274, IEEE Computer Society.

Cox and M. Miller. (1997). A Review of Watermarking and the Importance of Perceptual Modeling. *Proceedings of Proc. SPIE*, vol. 3016, pp. 92.

Cox, I. J. Miller, M. L. Bloom, J. A. Fridrich, J. and Kalker, T. (2008). *Digital Watermarking and Steganography*, 2nd. Ed. morgan kaufmann publishers.

Cox, J. Kilian and F. Leighton. (1997). Secure Spread Spectrum Watermarking for Multimedia. *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687.

Cox, L. Miller and A. Bloom. (2002). *Digital Watermarking*. Morgan Kanfman Publisher, ISBN: 1-55860-714-5.

Daubechies, I. (1992). Ten lectures on wavelets. *CBMS-NSF conference series in applied mathematics*, SIAM Ed.

Dejun, Y., Rijing, Y., Yuhai, Y. and Huijie, X. (2009). Blind Digital Image Watermarking Technique Based On Intermediate Significant Bit and Discrete Wavelet Transform. Proc, *International Conference on Computational Intelligence and Software Engineering*, CISE.

Depovere, T. Kalker, and J. Linnartz. (1998). Improved Watermark Detection Using Filtering Before Correlation. *International Conference on Image Processing*, vol. 1, pp. 430.

Dharwadkar, N. V. and amberker, b. b. (2010). Watermarking Scheme for Color Images using Wavelet Transform Based Texture Properties and Secret Sharing. *International Journal of Information and Communication Engineering*, 6(2), 93-100.

Dong P., G. Jovan. (2005). Digital Watermarking Robust to Geometric Distortions. *IEEE Transaction on Image Processing,* vol. 14, no. 12, pp. 2140-2150.

Eggers, J. J., Su, J. K. and Girod, B. (2000). Robustness of a Blind Image Watermarking Scheme. *International Conference on Image Processing*, pp. 17-20, IEEE Computer Society.

El-Gayyar. Mohameed. (1998). Resolving Rightful Ownerships with Invisible Water- marking Techniques. *IEEE Journals*, vol. 16, no. 4, pp.573-586.

El-Gayyar.Mohamed, Joachim von zur Gathen. (2006). Watermarking Techniques Spatial Domain. *Digital Rights Seminar, Media Informatics University of Bonn Conference,* Germany.

Emami Mir Shahriar, Ghazali Bin Sulong and Salbiah Binti Seliman. (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*, vol. 8, no. 3(A).

Frank Y. Shih, Scott Y. T. Wu. (2003). Combinational image watermarking in the spatial and frequency domains. *Pattern Recognition*, 36(4): 969-975.

Friedman. g. l. (1993). The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image. *IEEE Transactions on Consumer Electronics*, 39(4), 905 -910.

Ghazali Bin Sulong, Harith Hasan**,** Ali Selamat**,** Mohammed Ibrahim and Saparudin (2012). A New Color Image Watermarking Technique Using Hybrid Domain. *IJCSI International Journal of Computer Science Issues*, vol. 9, Issue 6, no 1.

Gonzales, R. C. and Woods, R. E. (2002). *Digital Image Processing Reading*. MA, Addison-Wesley.

Gunjal B. L. and Manthalkar R.R. (2010). An Overview of Transform Domain Robust Digital Image Watermarking Algorithms. *Journal of Emerging Trends in Computing and Information Sciences.* vol. 2, no. 1.

Guo H. and Nicolas G. D. (2002). Digital Image Watermarking for Joint Ownership. *ACM Multimedia, ACM,* pp. 362-371 .

Habes, A. (2006). Information Hiding in BMP image Implementation Analysis and Evaluation. *Information Transmissions In Computer Networks*, vol. 6, no. 1.

Hanaa A. , M. hadhoud, and A. Shaalan. (2009). A Blind Spread Spectrum Wavelet Based Image Watermarking Algorithm, *International Conference on Computer Engineering & Systems*. pp. 251-256.

Hartung and M. Kutter. (1999). Multimedia Watermarking Techniques. *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1079-1107.

Hartung, K. Su, and B. Girod. (1999). Spread Spectrum Watermarking Malicious Attacks and Counter-Attacks. *Proceeding of SPIE on Security and Watermarking of Multimedia Contents*, vol. 3657, pp. 147-158.

Hassanien A. (2006). A Copyright Protection Using Watermarking Algorithm. *Informatica Journal* , vol. 17, no. 2, pp. 187–198.

Haval Muhammed Sidqi. (2010). *Robust Frequency Image Watermarking Scheme Resilient to Malicious Attacks*. M.Sc. thesis at University of Sulimanyah, Iraq.

Helsingius m, Kuosmanen p, and Astola j. (2000). Image Compression using Multiple Transforms. *Image Communication,* 15(6):513-529.

Hikmat N. Abdullah, Safa'a A. Ali. (2010). Implementation of 8-Point Slantlet Transform Based Polynomial Cancellation Coding-OFDM System Using FPGA. *7th International Multi-Conference on Systems*, Signals and Devices.

Hoan N. and P. Roland. (2007). Multiresolution Quantization- Based Image Watermarking. *IEEE International Conference on Electro/Information Technology*, pp. 401-407.

Honsinger, C. (2000). Data Embedding using Phase Dispersion. *IEE Seminar on Secure Images and Image Authentication* , pp. 5/1 - 5/7, IEEE Computer Society.

Hore Alain and Ziou Djemel. (2010). Image qualitymetric: PSNR vs. SSIM. *International Conference on Pattern Recognition*, IEEE Computer Society.

Jayant N., J. Johnston, and R. Safranek. (1993). Signal Compression Based on Models of Human Perception. *Proceedings of the IEEE*, vol. 81, no. 10, pp. 1383-1422.

Juneja, M. and Sandhu P. S. (2009). Performance Evaluation of Edge Detection Techniques for Images in Spatial Domain. *International Journal of Computer Theory and Engineering*, vol. 1, no. 5, pp. 1793-8201.

Kattoush. Abbas Hasan. (2012). A Radon Slantlet Transforms Based OFDM System Design and Performance Simulation under Different Channel Conditions. *International Scholarly Research Network ISRN Communications and Networking*, vol. 2012, Article ID 318921, 8 pages.

Khalili, M. (2003). A Comparison between Digital Images Watermarking in Tow Different Color Spaces Using DWT2. *National Academy of Science of Armenia Yerevan*, Armenia.

Koduvayur P. Subbalakshmi, Palak K. Amin. (2009). Robust hidden data extraction method for scaling attacks. *The Trustees Of Stevens Institute Of Technology*, US 7529384 B2, Patent.

Kong, F. and Peng Y. (2010). Color Image Watermarking Algorithm Based On HSI Color Space. *2nd International Conference on Industrial and Information Systems IEEE*, 978-1-4244-8217-7110.

Kumer A. (2006). *Improved Content Based Image Watermarking* . M.Sc. thesis, University of Louisiana State.

L. Yu and S. Sun. (2006). Slantlet Transform based image fingerprints. *Proceedings of the Third IASTED International Conference on Communication Network and Information Security*, Cambridge, MA,USA, pp.41-43, 9-11 October.

Li and F.M. Yang. (2003). One-dimensional Neighborhood Forming Strategy for Fragile Watermarking. *In Journal of Electronic Imaging*, vol. 12, no. 2, pp. 284-291.

Li C. and S. Wang. (2000). Digital Watermarking Using Fractal Image Coding. *IEICE Trans Fundam Electron Commun Comput Sci*, vol. E83-A, no. 6, pp. 1286-1288.

Lie, W. and Chang, L. C. (1999). Data Hiding in Images with Adaptive Numbers of Least Significant Bits Based on the Human Visual System. *International Conference on Image Processing*, vol. 1, pp. 286 – 290.

Lin C.-H., Chao M.-W., Liang C.-Y. and Lee T.-Y. (2010). A Novel Semi-Blind-and-Semi-Reversible Robust Watermarking Scheme for 3D Polygonal Models. *Springer-Verlag. Vis Comput,* 26: 1101–1111, DOI 10.1007/ s00371- 010-0461-y.

Lin C.-H. D.-Y.Chan H. Su W.-S. Hsieh. (2006). Histogram-Oriented Watermarking Algorithm: Colour Image Watermarking Scheme Robust Against Geometric Attacks and Signal Processing. *IEE Proceedings - Vision, Image and Signal Processing*, vol. 153, Issue 4, August, pp. 483 – 492.

Liu P. and Ding Z. (2009). A Blind Image Watermarking Scheme Based on Wavelet Tree Quantization. *Proceeding ISECS '09 Proceedings of the 2009 Second International Symposium on Electronic Commerce and Security*, vol. 01, pp. 218- 222.

Liu, L. X. and Wang, W. W. (2008). A Wavelet Image Coding Algorithm Based on Human Visual System Characteristics. *Proceedings of the 2008 International Conference on Wavelet Analysis and Pattern Recognition*, hong kong, 30-31.

Lixiong, L. and Yunde J. (2007). Bits Allocation of Matching Pursuit Video Coder Based on Visual Properties. *The Iasted International Conference on Computer Graphics and Imaging, Innsbruck*, Austria, 156-160.

Lu, w. Lu, H. and chung F. L. (2006). Feature-Based Watermarking using Watermark Template Match. *Applied Mathematics and Computation*, 177(1), 377- 386.

Luo and G. Heileman. (2004). A Fast and Robust Watermarking Method for JPEG Images. *Computer Modeling & New Technologies*, vol. 8, no. 1, pp. 39-47.

Maini R. and Dr. Aggarwal H. (2009). Study and Comparison of Various Image Edge Detection Techniques. *International Journal of Image Processing,* vol. (3): Issue (1).

Maity S. P. and Kundu, M. K. (2002). Robust and Blind Spatial Watermarking in Digital Image. Proc, *3rd Indian Conference on Computer Vision, Graphics and Image Processing (ICVGIP 2002)*, pp. 388 -393.

Mallat, S. (1989). A Theory for Multiresolution Signal Decomposition: The Wavelet Representation. *IEEE Pattern Anal. and Machine Intell.*, vol. 11, no. 7, pp. 674-693.

Mehemed, B.A., El-Tobely, T.E.A., Fahmy, M.M., Naser, M.E.L.S. and El-Aziz, M.H.A. (2009). Robust Digital Watermarking Based Falling-off Boundary in Corners Board-MSB-6 Gray Scale Images. *International Journal of Computer Science and Network Security*, vol. 9, no. 8, PP. 227-240.

Min-Jet1 Tsai, Kuang-Yao YU and Chen Yi-Zhang. (2000). Joint Wavelet and Spatial Transformation for Digital Watermarking. *Consumer Electronics, IEEE Transactions*, vol. 46 Issue1.

Mohammed, A. A. , Haval Sidqi (2011). Robust Image Watermarking Scheme Based on Wavelet Technique. *International Journal of Computer Science and Security* (IJCSS), 5.

Mutt S.K. and Kumar Sushil. (2009). Secure Image Steganography Based on Slantlet Transform. *International Conference on Methods and Models in Computer Science.*

Nadernejad, E. (2008). Edge Detection Techniques: Evaluations and Comparisons. *Applied Mathematical Sciences*. vol. 2. no. 31, pp.1507 – 1520.

Nagaraj B. Patil, V. M. Viswanatha , Dr. Sanjay Pande M. B. (2011). Slant Transformation As Atool for Pre-Processing in Image Processing. *International Journal of Scientific & Engineering Research*, vol. 2, Issue 4.

Nikolaidis N. and Pitas I. (1998). Robust Image Watermarking in the Spatial Domain. *Signal processing*, vol. 66 Issue 3, pp. 385-403: Elsevier.

Panda G., Dash P. K., Pradhan A. K., and Meher S. K., A. (2002). Data Compression of Power Quality Events Using the Slantlet Transform. *IEEE Transactions on Power Delivery*, vol. 17, no. 2.

Paunwala, M. C. and Patnaik, S. (2011). Biometric Template Protection with Robust Semi-Blind Watermarking Using Image Intrinsic Local Property. *International Journal of Biometrics and Bioinformatics (IJBB),* vol. 5, Issue 2.

Perumal S. M. and 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, pp. 29-36.

Podilchuk and W. Zeng. (1998). Image-adaptive Watermarking Using Visual Models. *In IEEE Journal Selected*. Areas of Communications, vol. 16, pp. 525-539.

Podilchuk C. and E. Delp. (2001). Digital Watermarking Algorithms and Applications. *In IEEE Signal Processing Magazine*, vol. 18, No. 4.

Q. Cheng and T. Huang. (2000). Blind Digital Watermarking for Images and Videos and Performance Analysis. *IEEE International Conference on Multimedia and Expo*, vol. 1, pp. 389–392.

Ramos, m. g. hemami, s. s. and tamburro, m. a. (1997). Psychovisually-Based Multiresolution Image Segmentation. *Proceedings IEEE International Conference on Image Processing*, Santa Barbara, ca, 3, 66-73.

Reddy, A. A. and Chatterji, B. N. (2005). A New Wavelet Based Logo-Watermarking Scheme. *Pattern Recognition Letters*. 26(7), 1019-1027.

Reddy, v. p. and varadarajan, d. s. (2009). Human Visual System Sentient Imperceptible and Efficient Wavelet-Based Watermarking Scheme for Copyright Protection of Digital Images. *International Journal of Computer Science and Network Security*, 9(4).

Ren-Junn, H., Chuan-Ho K. and Rong-Chi C. (2002). Watermark in Color Image. *Proceedings of the first International Symposium on Cyber Worlds*, pp. 225-229.

Riaz. Saba, M. Javed, and M. Anjum. (2008). Invisible Watermarking Schemes in Spatial and Frequency Domains. *4th International Conference on Emerging Technologies, pp. 211-216.*

Rohith.S, Dr. K.N.hari bhat. (2012). A Simple Robust Digital Image Watermarking against Salt and Pepper Noise using Repetition Codes. *Signal & Image Processing*, vol. 03, no. 01.

Samcovic A. and Jan Turan. (2008). Attacks on Digitalwavelet Imagewatermarks. *Journal of ELECTRICAL ENGINEERING*, vol. 59, no. 3, pp.131–138.

Schyndel, R. G. V., Trike, A. Z. and Osborne, C. F. (1994). A Digital Watermark. *proc, 1st International IEEE Image Processing Conference*. :RMIT, Houston, USA.

Selesnick I. W. (1999). The Slantlet Transform. *IEEE Transactions on Signal Processing*, vol. 47, no. 5, pp. 1304-1313.

Shieh, J., Lou, D., and Chang, M. (2006). A Semi-Blind Digital Watermarking Scheme Based on Singular Value Decomposition. *Computer Standards & Interfaces*, vol. 28, pp. 428– 440, Elsevier.

Solachidis V. and Pitas L. (2001). Circularly Symmetric Watermark Embedding in 2-D DFT Domain. *IEEE Transactions on Image Processing archive.* vol. 10, Issue: 11, pp. 1741-1753.

Solachidis, A. Tefas, N. Nikolaidis, S. Tsekeridou, A. Nikolaidis, and I.Pitas. (2001). A Benchmarking Protocol for Watermarking Methods. *IEEE International Conference on Image Processing*, pp. 1023-1026.

Song, C., Sudirman, S., Merabti, M. and Jones, D. L. (2010). Analysis of Digital Image Watermark Attacks. *Proc, Consumer Communications and Networking Conference (CCNC)*, 2010 7th IEEE , IEEE Computer Society.

Su. Qingtang, Yugang Niu, Xianxi Liu and Tao Yao. (2013). A Novel Blind Digital Watermarking Algorithm for Embedding Colour Images into Colour Image. *Optik*, 124 (2013) 3254– 3259.

Sun Q. and Zhang, Z. (2006). A Standardized JPEG2000 Image Authentication Solution based on Digital Signature and Watermarking. *China Communications*, pp. 71-80.

Swanson M., M. Kobayashi, and A. Tewfik. (1998). Multimedia Data- Embedding and Watermarking Technologies. *Proceedings of the IEEE*, vol. 86, no. 6, pp. 1064-1087.

Temi, C. Choomchuay, S. and Lasakul, A. (2005). A Robust Image Watermarking Using Multiresolution Analysis of Wavelet. *Mongkut's Institute of Technology Ladkrabang*, Bangkok, Thailand, 0-7803-9538-7/05.

Tudor Barbu. (2013). Variational Image Denoising Approach with Diffusion Porous Media Flow. *Abstract and Applied Analysis*, vol. 2013, Article ID 856876, 8 pages.

Tzovaras D., Nikitas Karagiannis and Michael G. Strintzis. (1998). Robust Image Watermarking in the Subband or DCT Domain. *EUSIPCO'98*, vol. IV, pp. 2285–2288, 8–11 September, Rhodes, Greece.

Vahedi Ehsan, Reza Aghaeizadeh Zoroofi, and Mohsen Shiva. (2012). Toward a New Wavelet-Based Watermarking Approach for Color Images using Bio-Inspired Optimization Principles. *Digital Signal Processing*, pp. 153–162.

Voyatzis G., Pitas I. (1999). The Use of Watermarks in the Protection of Digital Multimedia Products. *Proceedings of the IEEE*, vol. 87, Issue: 7, pp. 1197-1207: IEEE.

Wang, S., Zheng, D., Zhao , J., Tam, W. J., and Speranza, F. (2005). An Accurate Method for Image Quality Evaluation using Digital Watermarking. *IEICE Electronics Express*, vol. 2, no. 20, pp. 523-529.

Woo Chaw Seng, Jiang Du and Binh Pham. (2009). Semi Fragile Watermark With Self Authentication and Self Recovery. *Malaysian Journal of Computer Science*, vol. 22(1).

Wu, D.C. and Tsai, W.H. (2000). Spatial-Domain Image Hiding using Image Differencing. *IEE Proc.-Vcs. hncige Signal Process,* vol. 147, no. 1, pp. 29-37.

Wu, H.-C., Wu, N., Tsai. (2003). A Stegnographic Method for Images by Pixel-value Differencing. *Pattern Recognition Letters*, vol. 24, pp. 1613-1626.

Wu, N. (2004). *A Study on Data Hiding for Gray-Level and Binary Image*. Master Thesis, Chaoyang University of Technology, Taiwan.

Wu, N. I., and Hwang, M. (2007). Data Hiding: Current Status and Key Issues. *International Journal of Network Security*. vol. 4 No.1 PP.1–9.

Wu, X. and Guan, Z. (2007). A Novel Digital Watermark Algorithm based on Chaotic Maps. *Physics Letters A*, vol. 365, pp. 403– 406.

Xuan, M., and Jiang, J. (2009). A Novel Watermarking Algorithm in Entropy Coding Based on Image Complexity Analysis. *Proc, International Conference on Multimedia Information Networking and Security*, MINES'09, pp. 128-129.

Y. Zhang. (2009). Digital Watermarking Technology: A Review. *International Conference on Future Computer and Communication*, pp. 250-252.

Yang, C. (2008). Inverted Pattern Approach to Improve Image Quality of Information Hiding by LSB. *Pattern Recognition 41*, pp. 2674 – 2683, Elsevier.

Yin, L. H. (2009). *Study of Digital Image Watermarking in Curvelet Domain*. Master. Thesis. Department of Electronic Engineering City University of Hong Kong.

Yoo, J., Choi, B. and Choi, H. (2010). 1-D Fast Normalized Cross-Correlation using Additions. *Digital Signal Processing*, vol. 20, pp. 1482–1493, Elsevier.

Yoshida, M., Fujita, T. and Fujiwara, T. (2006). A New Optimum Detection Scheme for Additive Watermarks Embedded in Spatial Domain. *Proc, International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, IEEE Computer Society.

Yusof, Y. and Khalifa, O. O. (2007). Digital Watermarking For Digital Images Using Wavelet Transform. *Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications*, pp. 14-17.

Zeki A. M., and Manaf A. A. (2009). A Novel Digital Watermarking Technique Based on ISB (Intermediate Significant Bit). *International Journal of Information Technology*, vol. 5:3, 2009.

Zeki, A. M. and Manaf, A. A. (2011). ISB Watermarking Embedding: A Block Based Model. *Information Technology Journal*, vol. 10, no. 4, pp.841-848.

Zhang. Y. (2009). Blind Watermark Algorithm Based on Hvs and Rbf Neural Network in Dwt Domain. *Wseas Transactions on Computers*, 8(1).