

RGB COLOR IMAGE WATERMARKING USING DISCRETE WAVELET  
TRANSFORM DWT TECHNIQUE AND 4-BITS PLAN BY HISTOGRAM  
STRETCHING

KARRAR ABDUL AMEER KADHIM

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

Faculty of Computing  
Universiti Teknologi Malaysia

JULY 2013

This dissertation is dedicated to my beloved parents, fiancée, brothers, sister and my friends.

## ACKNOWLEDGEMENTS

All praise is to Allah and my peace and blessing of Allah be upon our prophet, Muhammad and upon all his family and companions. In particular, I wish to express my sincere appreciation to my thesis supervisor, **PROF. DR. DZULKIFLI MOHAMAD**, and to all my friends for encouragement, guidance, critics, advices and supports to complete this research. I really appreciate his ethics and great deal of respect with his students, which is similar to brothers in the same family.

In addition, I am extremely grateful to my father for unlimited support and encouragement during this research. I would like to thanks my beloved family: mother, fiancée, brother, and sisters who I am always beholden to them for their everlasting patience, support, encouragement, sacrifice, and love which have been devoted to me sincerely. I could endure for being away and eventually my master program came to fruition. For that, I ask Allah to bless all of them.

Besides, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) and Faculty of Computing (FK) for providing me with a good environment and facilities such as computer laboratory to complete this project with software which I need during process.

## ABSTRACT

Recently, access to multimedia data has become much easier due to rapid growth of the internet; everyone could access these data, and use them for personal or commercial purposes, for these reason copy right problems appeared. Digital watermarking techniques are used to protect the copyrights of multimedia data by embedding secret information in the host media, for example, embedding in images, audios, or videos. Many watermarking techniques have been proposed in the literature to solve the copyright violation problems, but most of these techniques failed to satisfy both imperceptibility and robustness requirements. In this thesis, adaptive color image watermarking technique is proposed. The proposed technique involves two main stages, which are, embedding, and extraction. Before embedding stage, a host image is converted from RGB to YCbCr color space to preserve imperceptibility and robustness, then, Cb component is extracted and partitioned into four quadrants. In the embedding stage select Cb component to apply DWT to decompose the cover image to four frequencies which are LL, HL, LH and HH, then selected the LH2 band to embedding the watermark image, while watermark image will convert to 4-bits plane to compress the image to ensure the capacity. In the extracting stage, DWT is used again to decompose the selected quadrant of watermarked image, and finally the watermark image is extracted. To prove the efficiency of proposed technique, six types of attacks are applied on watermarked image namely, Gaussian noise, Salt & Pepper Noise, Sharpening filter, Median filter, Rotation, and JPEG Compression. The experiments results have shown that the proposed technique successfully withstood against all the mentioned attacks, and at the same time preserved the watermarked image quality.

## ABSTRAK

Baru-baru ini, capaian kepada data multimedia telah menjadi lebih mudah disebabkan oleh pertumbuhan pesat internet. Semua orang boleh mendapatkan data-data ini, dan menggunakannya untuk tujuan peribadi atau komersial, atas sebab inilah masalah hak cipta muncul. Teknik “*Watermarking*” digunakan untuk melindungi hak cipta data multimedia dengan memasukkan maklumat rahsia dalam media hos. Sebagai contoh, memasukkan maklumat rahsia dalam imej, audio, atau video. Pelbagai teknik penandaan air yang telah dicadangkan dalam literasi untuk menyelesaikan masalah pelanggaran hak cipta tetapi kebanyakan teknik ini gagal memenuhi keperluan ketidak boleh nampak dan kekukuhan. Dalam tesis ini, teknik penyesuaian imej warna tera air telah dicadangkan. Teknik melibatkan dua peringkat utama iaitu pembenaman dan pengekstrakan. Sebelum peringkat pembenaman, imej hos ditukar dari RGB ke ruang warna YCbCr untuk mengekalkan ketidak boleh nampak dan kekukuhan. Kemudian, komponen Cb diekstrak dan dibahagikan kepada empat kuadran. Pada peringkat pembenaman, komponen Cb dipilih untuk digunakan DWT bagi menguraikan imej penutup kepada empat frekuensi iaitu LL, HL, LH dan HH. Seterusnya, jalur HH dipilih untuk membenamkan imej tera air, sementara imej tera air akan menukarkan/ditukarkan ke 4-bit satah untuk memampatkan imej bagi memastikan kapasiti. Pada peringkat pengekstrakan, DWT digunakan semula untuk menguraikan kuadran imej tera air terpilih. Akhirnya, imej tera air diekstrak. Untuk membuktikan keberkesanan teknik yang dicadangkan, enam jenis serangan digunakan pada imej tera air iaitu gangguan Gaussian, gangguan Salt & Pepper, penajaman penapis, penapis Median, Putaran, dan mampatan JPEG. Keputusan eksperimen menunjukkan teknik yang dicadangkan berjaya bertahan dengan semua gangguan, dan pada masa yang sama mengekalkan kualiti imej tera air. Hasil eksperimen membuktikan bahawa teknik yang dicadangkan berjaya mengatasi semua gangguan tersebut dan pada masa yang sama mengekalkan kualiti imej yang di “*watermark*”.

## TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xi
	LIST OF FIGURES	xiii
	LIST OF ABBREVIATIONS	xvi
<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
	1.1 Introduction	1
	1.2 Background of the Study	3
	1.3 Statement of the Problem	5
	1.4 Research Question	7
	1.5 Aim of the study	7
	1.6 The Objectives of the study	8
	1.7 Scope of the study	8
	1.8 Purpose of the study	8
	1.9 Thesis Organization	9
<b>2</b>	<b>LITERATURE REVIEW</b>	<b>11</b>
	2.1 Introduction	11
	2.2 Data Protection	12

2.2.1	Data Hiding	13
2.2.2	Cryptography	14
2.3	History of Watermarking	15
2.4	Digital Watermarking Overview	16
2.5	Type of Watermarking	16
2.5.1	Visible Watermarking	17
2.5.2	Invisible Watermarking	18
2.6	Embedding and Extracting	20
2.6.1	Watermarking Embedding	20
2.6.2	Watermarking Extracting	20
2.7	Color Image Watermarking	22
2.8	Watermarking Application	22
2.8.1	Protection of Copyright	23
2.8.2	Fingerprinting	23
2.8.3	Protection of Copy	23
2.9	Basic Requirement	24
2.9.1	Imperceptibility	24
2.9.2	Robustness	24
2.9.3	Security	24
2.9.4	Capacity	25
2.9.5	Complexity	25
2.10	Watermarking Technique	26
2.10.1	Spatial Domain	26
2.10.2	Frequency Domain	26
2.11	Watermarking and Steganography	27
2.12	Watermarking and Cryptography	28
2.13	Watermarking Attack	30
2.14	Related Work	30

3.1	Introduction	39
3.2	Embedding Stage	37
3.2.1	Requantization Image	39
3.2.2	Compression Image	40
3.2.3	Convert RGB color to YCbCr color space	42
3.2.4	Extract Cb component	43
3.2.5	Apply DWT on Cb Component	44
3.2.6	Embedding Watermarking in cover image	45
3.2.7	Wavelet Reconstruction (IDWT)	46
3.2.8	Reconstruction YCbCr	47
3.3	Extract Stage	47
3.3.1	Apply DWT for Cb component	48
3.3.2	Extract Watermarking pieces	49
3.3.3	Inverse Convert Image	49
3.3.4	Wavelet Reconstruction (IDWT)	50
3.4	Imperceptibility Measuring	51
3.5	Robustness Measuring	51
<b>4</b>	<b>RESULTS AND DISCUSSION</b>	<b>53</b>
4.1	Introduction	53
4.2	Implementation of Result	56
4.3	Watermarked image before attacks	54
4.3.1	Converting RGB channel to YCbCr color space	54
4.3.2	Applying DWT on Cb component	55
4.3.3	Requantization and compress watermark image	56
4.3.4	Embedding watermark image on Cb component	57
4.3.5	Inverse DWT and merge new Cb to YCbCr	58
4.3.6	Converting YCbCr to RGB color space	59



4.4	Testing and evaluation before attack	60
4.5	Watermarked Image after Attacks	62
4.5.1	Gaussian Noise Attack	63
4.5.2	Salt & Peppers Attack	64
4.5.3	Sharpening Attack	66
4.5.4	Median Filter Attack	67
4.5.5	Rotation Attack	69
4.5.6	JPEG Compression Attack	71
4.6	Result of Comparison	73
4.6.1	First Comparison	73
4.6.2	Second Comparison	75
<b>5</b>	<b>CONCLUSION</b>	<b>76</b>
5.1	Introduction	76
5.2	work Summary	77
5.3	Contribution	78
5.4	Future work	78
	<b>REFERENCES</b>	<b>80</b>

## LIST OF TABLES

<b>No.</b>	<b>TITLE</b>	<b>PAGE</b>
2.1	Comparisons between Digital Watermarking and Steganography	28
2.2	Comparisons between Digital Watermarking and Cryptography	29
2.3	Summary of related work	33
4.1	Explain the PSNR ratio for watermarked image	62
4.2	Gaussian noise attack results	64
4.3	Salt & Pepper noise attack results	66
4.4	Sharpening attack results	67
4.5	Median Filter attack results	69
4.6	Rotation attack results	71
4.7	JPEG Compression attack results	72
4.8	Explain summary of results	73
4.9	Illustrate the compression of results with Kong and Peng, (2010)	74
4.10	Illustrate the compression of results with Ibrahim, M.(2011)	75

## LIST OF FIGURES

<b>FIGURE NO.</b>	<b>TITLE</b>	<b>PAGE</b>
2.1	Data protection	12
2.2	Visible Watermarking	18
2.3	Invisible Watermarking	19
2.4	Watermarking Techniques	27
3.1	The propsed method	38
3.2	Requantization Lena image, a: 0-255range, b: 0-15 range	40
3.3	Compress image by change to one dimensional array	42
3.4	The conversion of RGB to YCbCr color image	43
3.5	Extracting Y, Cb, and Cr components	44
3.6	The application of DWT on the host image	45
3.7	Reconstruction YCbCr	47
3.8	Extracting Stage	50
4.1	RGB cover image afrter convert it to YCbCr color space	55
4.2	Apply DWT on Cb component	56
4.3	Requantization watermark image	57
4.4	Watermark image in one dimensional array	57
4.5	Embedding Watermark image on Cb components	58
4.6	The YCbCr components with new Cb including watermark image	59
4.7	Watermarked image, (a): Lena image; (b): Baboon image	60

4.8	The watermarked images, (a) Lena, (b) Baboon, (c) Pepper, (d) Tiffany, (e) Airplane	61
4.9	Benchmark with previous results	62
4.10	Lena image with 0.01% Gaussian Noise Attack	63
4.11	Baboon image with 0.01% Gaussian Noise Attack	63
4.12	Extract Watermark image after Gaussian Noise Attack	64
4.13	Lena image with 0.01% of Salt & Peppers noise	65
4.14	Baboon image with 0.01% of Salt & Peppers noise	65
4.15	Extracted watermark image after attack	65
4.16	Lena image after applying sharpening attack	66
4.17	Baboon image after applying sharpening attack	67
4.18	Extracted watermark image after attack	67
4.19	Lena image after applying Median filter attack	68
4.20	Baboon image after applying Median filter attack	68
4.21	Extracted watermark image after attack	69
4.22	Lena image with 1° of rotation	70
4.23	Baboon image with 1° of rotation	70
4.24	Extracted watermark image after attack	70
4.25	Lena image with 10% of JPEG compression	71
4.26	Baboon image with 10% of JPEG compression	72
4.27	Extract watermark image after attack	72

**LIST OF ABBREVIATIONS**

<b>DWT</b>	Discrete Wavelet Transform
<b>DCT</b>	Discrete Cosine Transform
<b>ECC</b>	Error Correction Codes
<b>LSB</b>	Last Significant Bit
<b>RGB</b>	Red Green Blue
<b>PSNR</b>	Peak Signal Noise Ratio
<b>MSE</b>	Mean Square Error
<b>DFT</b>	Discrete Fourier Transform
<b>SRLE</b>	Sliding Run Length Encoding
<b>CF</b>	Compression Factor
<b>HVS</b>	Human Visual System
<b>NCC</b>	Normalized Cross-Correlation

## **CHAPTER 1**

### **INTRODUCTION**

#### **1.1 Introduction**

There is no doubt that using the Internet has become ubiquitous in the 21<sup>st</sup> century and it is quite true that everyone feels it is an indispensable part for the future of business communication. Going by the systematic digital data attainment and the way it can be easily transmitted, duplicated and modified. The copyright protection of the intellectual property of the sensitive or critical digital information is an important legal issue globally. According to Tsai et. al., (2000) and Wu, C. W. (2002) recently highlighted that, through analyzing the trend of studies in digital watermark for audio, image or video data; it can be seen that watermark techniques provide the essential mechanism for ownership authentication.

Using the Internet as a global communication or data tool, different multimedia data classes have grown to be easily attacked. This is because everybody can download these data from different sources and modify them without been authorized to do so legally. The many copyright problems have lately become so common (Dharwadkar, N. V. & Amberker, B.B., 2010). The digital watermarking which was produced like a tool is essentially to safeguard multimedia data from copyright violations or just being incorrectly used again (Cox, et al., 2008). Digital watermarking techniques are utilized to safeguard the copyrights of multimedia data by embedding secret information within the host media, for instance, text images, video and audio. There are two watermarking methods which are suggested. The first

thing is as simple as adding an obvious watermark which may be clearly seen in the cover image. The second thing is by embedding a concealed watermark inside the host image.

Watermarking algorithms can be classified based on the domain used for watermark embedding. Studies have shown that two popular techniques; spatial and transform watermarking techniques exist. Spatial domain watermarking techniques are useful for higher data embedding applications. Transform domain watermarking techniques are suitable in applications where robustness is of prime concern. These techniques as proposed include, Discrete Cosine Transform (Chandramouli et al., 2001); Discrete Fourier Transform (Premaratne, P., 1999); Discrete Wavelet Transform (Kundur, D. and Hatzinakos, D., 1998); Discrete Hadamard Transform (Anthony, T.S.; Shen, J.; Tan, S.H. and Kot, A.C., 2002); Contourlet Transform (Jayalakshmi, M. ; Merchant, S.N. and Desai, U.B., 2006); and Singular Value Decomposition (Mohan , B.C. and Kumar, S.S., 2008) are some of the useful transformations for image processing applications.

With the introduction of the JPEG2000 standard digital image, watermarking schemes that are derived from Discrete Wavelet Transform (DWT) are becoming a robust area attracting lots of attention. Nearly all watermarking schemes consider Discrete Cosine Transform known as DCT method of preference. A summary is available in (Cox et.al. 2008). Though, study result shows that DWT has the potentials of enhancing the strength of watermark against intentional and unintended attacks. The primary reason would be that the former JPEG standard depended on DCT and today using the creation of JPEG 2000, schemes according to DWT are widely attaining interest. Though, watermark robustness varies using the underlying changed algorithms', provisions must automatically get to harden a watermark against attacks. The methods are, e.g. multiple embedding, Nasir, I. Weng, Y. and Jiang, J. (2008) and the use of error correction codes (ECC) (Friedman, G. L., 1993) are being used to restore the embedded watermark.

DWT is basically a recent method used in place of an image but in a new time and frequency scale. The basic function of DWT is decomposing the input signal to multi-resolutions. DWT can be used to decompose input signal that poses as image into low frequency (LL) and high frequency (HL, LH and HH). HL here means the horizontal detail, while LH stands for the vertical detail and HH for the diagonal part. The lowest frequency band which serves as the optimal approximation of the original image, is influenced using the DWT decomposition progressions technique which represent the maximum scale and distinguishing degree (Qun, C. et.al 2007 ; Yusof, Y. & Khalifa, O. O., 2007).

## **1.2 Background of the Study**

It is generally believed that, many studies centers on the development of watermarking schemes for grayscale images than color images (Liu, K.C. and Chou, C.H., 2007). Consequently, available records show that, information hiding has been an important research area in recent years. However, the techniques to help address the issue of unauthorized copying, tampering and multimedia data delivery through the internet require urgent attention. Information hiding techniques currently involves merely the steganography and digital watermarking. In recent times, many watermarking schemes have been developed using DWT and DCT. This implies that where watermark is embedded perceptually with the most significant components, then the scheme has to be robust to attacks but, the watermark may be difficult to hide. Similarly, if the watermark is embedded in perceptually insignificant components, then it is bound to hide the watermark while interestingly the scheme may be less resilient to attacks (Navas, et al., 2008).

The piracy of digital assets like software, images, video, audio and text or data extended has been a bother for entrepreneurs of individual's characteristics. Placing digital watermarks directly into these assets could be a major approach to safeguarding these data possession. Most of the watermarking information provides a few errors for the object being watermarked. These deliberate errors are known as



marks. These marks must have a minor contact over the effectiveness inside the data and can be handled in manners the malicious attacker cannot destroy marks without making the data useless. It ought to be observed that watermarking action does not prevent copying of digital objects; nevertheless it might prevent unofficial copying by showing systems for verifying the initial getting digital objects.

Generally, the quality in the digital image following a watermark embedding process is degraded. Thus, the degradation amount of a watermarking formula needs to be given serious attention inside the evaluation from the watermarking plan performance. A couple of from the recommended watermarking information may be robust enough nonetheless they may drastically degrade the conventional in the digital media. Actually, there is a trade-off among watermarking performance needs including visual imperceptibility, robustness and embedding capacity but to cope with this trade-off, a technique is needed to determine it. Although, we will find several metrics to evaluate watermarking performance needs, none of individuals watermarking metrics gave concrete on measure this trade-off.

Furthermore, digital watermarking schemes concerning the data taken into account through getting rid of might be categorized as blind and non-blind approaches. In non-blind watermarking approaches, both data for actual host image and understanding statistics about watermarked image are known inside the amount of watermark recognition and extraction (Tao and Eskicioglu, 2004). In contrast, in blind approach finding the watermark and not mention for the original image is preferred (Al-Otum and Samara, 2010). We find several difficulties regarding the blind watermarking approaches. On one hand, high effectiveness of blind watermarking may also be proven. Therefore, a completely new technique referred to as semi-blind watermarking was introduced. Within this kind of watermarking approach, only the original watermark or perhaps the watermarked multimedia statistics are known (Tao and Eskicioglu, 2004; Shieh, and Athaudage, 2006).

Similarly, Paunwala, and Patnaik, (2011), applied semi-blind strategy in their approach by which principal direction within the subject watermarked image as record particulars are available throughout duration of watermark extraction to

prevent while using the initial host image. Consequently, within the non-blind approaches within the original host particulars are essential carrying out a extraction time to uncover the rightful owner. However, in blind approaches finding and eliminating the watermark information will finish off very hard when the watermarked image is extremely assaulted either deliberately or inadvertently. Therefore, the semi-blind approach as being a key choice is greater quality compared to blind approach and even more effective compared to non-blind approach.

To summarize, within the watermarking approaches, the possession in the attacked image cannot be recognized against a myriad of intentional and unintentional attacks and preserve the conventional in the watermarked image concurrently. In addition, several intentional attacks with the aim of eliminating or altering in the embedded watermarks may appear soon. Furthermore, an over-all purposed attack modeling is complicated as some severe attacks cannot be simply modeled or perhaps the behavior of other watermarking attacks may be unknown. In this case, acquiring a correctly-balanced trade-off one of the robustness, the visual imperceptibility along with the embedding capacity has changed into challenging within the digital watermarking research area.

An issue surrounding using the internet today is users "stealing" other individual's images and taking advantage of them on the web site without permission. It's impossible to prevent someone from installing images out of the web pages. If we are an artist, we will most likely wish to safeguard your images by watermarking them.

### **1.3 Statement of the Problem**

Immediate digital image watermarking is certainly an urgent requirement for several today's programs such as digital cameras and smart phone cameras. Evaluating watermarking technique, transform domain watermarking approaches require greater computational complexity over spatial domain techniques (Wolfgang

et al., 1999; Lan, H. et al., 2008 & Tsui, T. 2006 Kougianos et al., 2011). This could further be as a result of forward and inverse changes in the transform-domain watermarking approaches. However, it is common to understand that, there are difficulties with spatial-domain techniques. For instance, high embedding errors in LSB bit-planes result in many researchers employing low-order bit-planes for instance LSB for data hiding (Maity & Kundu, 2007). However, the lower-order bit-planes techniques does not contain visually significant information so, the embedded watermark may be simply corrupted or transformed by unauthorized clients without affecting on visual effects. Abolghasemi et al. (2010) for instance recommended a technique using co-occurrence matrix and bit-plane clipping that could find out the hidden data in LSB.

Studies have revealed the existence of several diversities of attacks against watermarking methods. For example Basu, S. et al. (2010), experimental investigations showed that watermarking approaches in the past were prone to several kinds of malicious attacks. Consequently, in order to identify the ownership of the digital media, they had to be made unavailable to extract the embedded watermark. Additionally, several attacks against watermarking schemes may be too complex to model (Cox et al., 1997). Consequently, a universal watermarking approach that could withstand several kinds of attacks and, concurrently, satisfies the conventional as well as the embedding capacity needs getting a minimal complexity isn't discovered yet. In this case, approximation approaches may be used to have the ability to discover the possession in the attacked watermarked image with low computational complexity. The best way to develop a solution that could withstand against various kinds of attacks is lacking the knowledge of their exact actions.

Ibrahim (2011), use watermarking technique using DWT and encryption canny edges, so as to include an watermark image include the cover image. Through the use of this method researcher was able to get acceptable results for PSNR and NCC after shedding a number of potential attacks. The main requirements for watermarking are: Imperceptibility, Robustness and capacity. Managed researcher attention imperceptibility and robustness, but neglected capacity, so were some of the extracted watermark pictures after the attack prone to damage because the size of

watermark image .Therefore, it is necessary to attention imperceptibility and robustness and capacity simultaneously to get the best results extracted after a number of potential attacks.

#### **1.4 Research Question**

An urgent need rises for improving the algorithms that are used to maintain the security and confidentiality of data. This need is because of the weakness of some encryption algorithms, watermarks, and the large number of internet piracy, as well as using without permission from the rightful owner. In order to solve these problems, there are some primary issues discussed hereunder:

- How to include a watermark image in the cover image without causing an obvious deterioration and what will be the storage capacity required?
- How to use DWT to decompose the original image to band of four frequencies.
- How to achieve transparency without loss of durability, strength and vice versa?
- How to compress the Watermark image and the ability to extract it without any effect on image features.
- How to make (extract) watermark image using cover image without having an influence on both images, which are watermark image and the cover image?

#### **1.5 Aim of the study**

The main aim of this study work is to come up with a proposed method of scheming color image by using watermarking through discrete wavelet transform (DWT) and Histogram Stretching methods. This study aims further at achieving and developing robustness, imperceptibility and available capacity of cover image for the watermarked image, which can withstand against various attacks.

## **1.6 The Objectives of the Study**

This research work was set out to achieve the following objectives, to:

1. To improve watermarking technique on RGB color image through the use of discrete wavelet transform technique (DWT) for cover image.
2. To apply histogram stretching for watermark image to do 4 bit plan to ensure the robustness and compress watermark image.
3. To evaluate the performance of the proposed technique against potential Attacks as well Robustness (NCC) and Imperceptibility (PSNR).

## **1.7 Scope of the Study**

The scope of this research contains two types of images. First one is the cover image, standard images which are Lena and pepper RGB color, which is of (512 x 512) bytes as a size, the source for those standard images from USC-SIPI dataset. Second one is Watermark image, which is UTM logo grayscale image of (128 x 128) bytes as a size. RGB color scheme will be used for cover images. DWT transform will be applied for cover image in order to decompose it into four frequencies. Histogram stretching will be used for watermark image compression. Compressed watermark image will be embedded in the "HH" band of the transformed cover image to insure the robustness and enhance the watermark image after extract it.

## **1.8 Purpose of the Study**

This study is essentially carried out introduce an approach which was based on statistical data in terms of embedding watermark and the extracting watermark. This is to establish an equilibrium which provides a balanced trade-off among robustness, visual imperceptibility and embedding capacity. This is achievable

through proposing a new robust image watermarking technique using histogram equalization and the remnant information of the embedded watermarks so as to identify the ownership of the watermarked image even after severe attacks. The proposed approach is realizable in order to achieve a reliable balanced trade-off between visual imperceptibility, robustness and embedding capacity. Watermarking scheme can resist different kinds of attacks while preserving the host image quality with a high embedding capacity as well. According to Golshan, F. et al.,(2011) watermarking approaches encounter restrictions. For this reason therefore, several techniques must be employed simultaneously to attain the acceptable degree of trade-off among robustness, imperceptibility and capacity.

## **1.9 Thesis Organization**

Chapter one contents the main aim for proposed technique, in this chapter we talking about the introduction of the image watermarking and the background of the watermarking study and what the problem statement for watermarking. Then we explain the important question to solve those problems. In objective we discuss the research work to achieve the solution for problem statement. The last one is the purpose of study.

Chapter two talking about the literature review for data protection and data hiding, and the types of data protection and talking about some of previous researcher works. The watermarking types details and what the basic requirement of digital watermarking, also the summary of related works.

Chapter three contents simple introduction about the research methodology for research objective study to execution the proposed objectives. The embedding and extracting watermark image and apply some of a potential attack such as Gaussian noise, Salt & Pepper, Sharpening, rotation and JPEG compression.

Chapter four is the results and discussion contents introduction and implementation of results explain the execution stapes to illustrate the embedding, extracting, attack of the watermarking image and then evolution of results to combine with the previous watermarking results.

Chapter five the conclusion contents simple introduction and the contribution to illustrate the new technique we used it with the digital watermarking. The future work to explain the more studies in watermarking issue depend on how to improve the main requirement for watermarking.

## REFERENCES

- Ahire, V. K. and Kshirsagar, V. (2011). Robust Watermarking Scheme Based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) for Copyright Protection of Digital Images. *IJCSNS International Journal of Computer Science and Network Security*. 11 (8), 208-213.
- Al-Haj, A. (2007). Combined DWT-DCT Digital Image Watermarking. *Journal of Computer Science* 3 (9), 740-746.
- Aliwa, M. B., Fahmy, M., Nasr, M. S. and 3 El-Aziz, M. H. (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* (7), 987-1022.
- Al-Otum, H. M., Samara, N. A.(2010). A robust blind color image watermarking based on wavelet-tree bit host difference selection. *Signal Processing* 90 (8), 2498-2512.
- Anthony, T.S.H., Shen, J., Tan, S.H. and Kot, A.C.(2002). Digital image-in-image watermarking for copyright protection of satellite images using the fast hadamard transform. *IEEE International Geoscience and Remote Sensing Symposium*, 6 (25), 3311-3313.
- Baithoon, N. Y. (2011). Combined DWT and DCT Image Compression Using Sliding RLE Technique. *Baghdad Science Journal*. 8 (3), 238-238.
- Bas, P. Chassery, J. M. and Macq, B.(2004). Image watermarking : An evolution to content based approaches . Neuve: Belgium.
- Basheer, N. M. and Abdulsalam, S. S. (2011). Digital Image Watermarking Algorithm in Discrete Wavelet Transform Domain Using HVS Characteristics. 'The Fourth Scientific Conference of the College of Computer Science & Mathematics'. Iraqi Journal of Statistical Science (20), 351-368.



- Basu, D., Sinharay, A. and Barat, S. (2010). Bit Plane Index Based Fragile Watermarking Scheme for Authenticating Color Image. *ICIIC '10 Proceedings of the First International Conference on Integrated Intelligent Computing*, 136-139.
- Bauschke, H. H. (2003). Recompression of JPEG images by requantization. *Image Processing, IEEE Transactions on image processing*. 12 (7), 843- 849.
- Bender, W., D. Gruhl, M., N. and Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal*, 35, 3-4.
- Berghel, H. (1998). Digital watermarking makes it mark Networker: The craft of network computing, 2 (4), 30-39.
- Bloom, J. M. (1999). Revolution by the Ream: A History of Paper. Saudi Aramco World. 26-39.
- Chaelynne M. W. (2001). Digital Watermarking. School of Computer and Information Sciences : Nova Southeastern University.
- 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 Perth, Australia*.
- Chandramouli, R.R., Benjamin, G. and Collin, R. (2001). A multiple description framework for oblivious watermarking. *Proceedings of Security, Watermarking and Multimedia*, 4314 ,585-593.
- Chin, C. C., Yung. C. C. and Tzu, C. L. (2007). A Semi-blind Watermarking Based on Discrete Wavelet Transform. *Proceddings of 9th International Conference Information and Communications Security*, Zheng zhou, China, 164-176.
- Clark, T.(2008). *Strategies for Data Protection*. (First Edition). USA. eBook, June.
- Cox, I. J. and kalker, T.(2004). Digital Watermarking. Third *international workshop, IWDW*, UK.
- Cox, I.J., Miller, Bloom, M.L.A., Fridrich, J. and Kalker, T.(2008). Digital watermarking and steganography, second edition, Morgan Kaufmann publishers.
- 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*.

- Dunbar B.,(2002). A detailed look at Steganographic Techniques and their use in an *Open-Systems Environment*.
- El-Gayyar, M.(2006). Watermarking Techniques Spatial Domain Digital Rights Seminar. *Ph.D. Thesis*. Media Informatics University of Bonn Germany.
- Emami, M. S. (2012). A New Robust Image Watermarking Approach Using Two-Level Intermediate Significant Bits Coupled With Histogram Intersection Technique. Doctor of Philosophy. Universiti Teknologi Malaysia.
- Friedman. G. I., (1993). The trustworthy digital camera: restoring credibility to the photographic image. *IEEE transactions on consumer electronics*, 39 ( 4), 905 -910.
- Ganesan, K. and Guptha, T. K. (2010). Multiple Binary Images Watermarking in Spatial and Frequency Domains. *Signal & Image Processing : An International Journal(SIPIJ)* 1, (2).
- Golshan, F. and Mohammadi, K.(2011). A Hybrid Intelligent SVD-Based Digital Image Watermarking. *ICSENG '11 Proceedings of the 21st International Conference on Systems Engineering*. 137-141 .
- González, R. C. and Woods, R. E. (2008). Digital Image Processing. *Prentice Hall*.
- Gritzalis, S.(2004). Enhancing Privacy and Data Protection in Electronic Medical Environments. *Journal of Medical Systems*, 6 (28), 535-547.
- Hajisami, A., Rahmati, A. and Zadeh, M. B. (2011). Watermarking Based on Independent Component Analysis In Spatial Domain. *UKSim 13th International Conference on Modelling and Simulation. IEEE*, 299-303.
- Hartung, F. and Kutter M. (1999). Multimedia Watermarking Techniques. *Proceedings of IEEE*. 87 (7).
- Hong, W. and Hang, M.(2006). Robust Digital Watermarking Scheme for Copy Right Protection, *IEEE Trans. Signal Process*, 12, 1- 8.
- Ibrahim, M. (2011). Adaptive Color Image Watermarking Using Wavelet Transform. Universiti Teknologi Malaysia. Malaysia.
- Jayalakshmi, M., Merchant, S.N. and Desai, U.B. (2006). Digital watermarking in contourlet domain. *18th International conference on Pattern Recognition*. 3, 861-864.
- Johnson, N.F., Duricn Z., and Jajodia, S.(2001). Information Hiding: Steganography and Watermarking Attack and Countermeasurments. *Kluwer Academic Publishers*, USA.

- Kashyap, N. and Sinha, G. R. (2012). Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT). *I.J.Modern Education and Computer Science*.(3), 50-56.
- Katzenbeisser, S. (2003). On the Integration of Cryptography and Watermarks. International Workshop on Digital Watermarking, Springer Lecture Notes in Computer Science. 50-60.
- Khalili, M. (2003). A Comparison between Digital Images Watermarking in Tow Different Color Spaces Using DWT2. *National Academy of Science of Armenia Yerevan, Armenia*.
- Kong, F. and Peng Y. (2010). Color Image Watermarking Algorithm Based On HSI Color Space. *2nd International Conference on Industrial and Information Systems*.
- Kougianos , E. and Mohanty, S. P. (2011). Real-time perceptual watermarking architectures for video broadcasting. *Journal of Systems and Software* , 84 (5), 724-738.
- Kumar, A. and Pooja, K. (2010). Steganography- A Data Hiding Technique. *International Journal of Computer Applications*. 9 (7). 19-23.
- Kumar, P. M. and Shunmuganathan, K. L. (2010). A reversible high embedding capacity data hiding technique for hiding secret data in images. *International Journal of Computer Science and Information Security*. 7 (3). 109-115.
- Kundur, D. and Hatzinakos, D.(1998). Digital watermarking using multiresolution wavelet decomposition. *Proceedings of IEEE International conference on Acoustics, Speech and Signal Processing, Seattle, Washington*,5. 2969-2972.
- Lan, H., Chen, S., Li, T. and Hu, A. (2008).A Digital Watermarking Algorithm Based on Dual-tree Complex Wavelet Transform. *ICYCS '08 Proceedings the 9th International Conference for Young Computer Scientists*, 1488-1492.2008. IEEE Computer Society Washington.
- Le, T. H., Nguyen, K. H. and Le, H. B. (2010). Literature Survey on Image Watermarking Tools, Watermark Attacks, and Benchmarking Tools. *Second International Conferences on Advances in Multimedia*. 978-0-7695-4068-9.
- Lee, Y. and Kim, J. (2012). Imperceptibility Metric for DWT Domain Digital Image Watermarking. *Communications in Computer and Information Science*. Korea, 342. 102-109.

- Lin, Y. L., Deal, R. L. And Kulie, M. S. (1998). Mechanisms of Cell Regeneration, Development, and Propagation within a Two-Dimensional Multicell Storm. University at Raleigh, Raleigh, North Carolina. USA.
- Liu, A. C. and Chou, C.H. (2007). Robustness comparison of color image watermarking schemes in uniform and non-uniform color spaces. *IJCSNS International Journal of Computer Science and Network Security*,.7.
- Liu, T. Y. and Tsai, W. H. (2010). Generic Lossless Visible Watermarking - A New Approach. *IEEE Transactions On Image Processing*. 19 (5). 1224-1235.
- Maity, S. P., Kundu, M. K., and Das, T. S. (2007). Robust SS watermarking with improved capacity. *Pattern Recognition Letters*.
- Megalingam, R. K., Nair, M. M. Srikumar, R. B. V. K. and Sarma V. S. V. A. (2010). Comparative Study on Performance of Novel, Robust Spatial Domain Digital Image Watermarking with DCT Based Watermarking. *International Journal of Computer Theory and Engineering*. 2(4). 8201.
- Ministry of Justice. ( 2006). *Personal Data Protection*. Additional copies can be ordered from the Ministry of Justice, SE-103 33 Stockholm. [www.sweden.gov.se](http://www.sweden.gov.se).
- Mohan, B.C. and Kumar, S.S.(2008). A robust image watermarking scheme using singular value decomposition. *Journal of Multimedia*.3.(1).7-15.
- Nasir, I. Weng, Y. and Jiang, J. (2007). A New Robust Watermarking Scheme for Color Image in Spatial Domain. School of Informatics, University of Bradford, UK.
- Nasir, I.,Weng, Y. and Jiang, J.(2008). Novel multiple spatial watermarking technique in color images. *Fifth international conference on information technology: new generations*. 777-782.
- Navas K. A., Cheriyan, A.M., Lekshmi, M., Archana Tamy, S. and Sasikumar, M.(2008). DWT-DCT-SVD Based Watermarking. *3rd International Conference on Communication Systems Software and Middleware and Workshops*.
- Paunwala, C. N. and Patnaik, S. (2011). Scene-Retrieved Attributes for Automatic License Plate Localization. *Cybernetics and Systems* 42(8), p567-584 .
- Premaratne, P.(1999). A novel watermark embedding and detection scheme for images in DFT domain. *Proceedings of IEE 7th International Conference on Image Processing & Applications*.2.780- 783.

- Provos, N. and Honeyman, P.( 2001). Detecting steganographic content on the internet. *Ann Arbor*. (1001) . 48103-4943.
- Qun, C. L. L., Qiang, A. L. and Qu, L.(2007). “Color Image Watermarking Algorithm Based on DWT-SVD”, *International conference on Automation and Logistics*, August 18-2.
- Ryoichi, S. and Hiroshi, Y. (2001). Consideration on Copyright and Illegal Copy Countermeasures under IT Revolution. *Joho Shori Gakkai Kenkyu Hokoku*, 37-42.
- Salah, I. S.(2003). *Steganography for embedding data in digital image*. Degree of Master of Science. Universiti Putra Malaysia.
- Sathik, M. M. and Sujatha, S. S. (2010). An Improved Invisible Watermarking Technique for Image Authentication. *International Journal of Advanced Science and Technology*. . 24. 61-74.
- Shieh, W. and Athaudage, C. (2006).Coherent Optical Orthogonal Frequency Division Multiplexing. *Electronic Letters*. 42. 587-589.
- Singh, J., Garg, P. and De, A. N. (2009). Audio Watermarking Using Spectral Modifications. *International Journal of Information and Communication Engineering*, 5(4). 297-301.
- Sullivan, S.(2002). Office of Naval Research. Issue in Information Hiding Transform Techniques.
- Sulong, G. B., Hasan, H., Selamat, A., Ibrahim, M. and Saparudin(2012). A New Color Image Watermarking Technique Using Hybrid Domain. *IJCSI International Journal of Computer Science Issues*. 9(1), 109-114.
- Tao, P., Eskicioglu, A. M.(2004). A robust multiple watermarking scheme in the discrete wavelet transform domain. *Internet Multimedia Management Systems V*, John R. Smith; Tong Zhang; Sethuraman Panchanathan, Editors, *Proceedings of SPIE Vol. 5601* (SPIE, Bellingham, WA 2004), .133-144.
- Tsai, M. J., Yu, K.Y. and Chen, Y.Z.(2000) .Joint wavelet and spatial transformation for digital watermarking. *IEEE Trans. on Consumer Electronics*. 46 (1). 241-245.
- Tsui, T. K. and Zhang, X. P. (2006).Quaternion image watermarking using the spatio-chromatic fourier coefficients analysis. *MULTIMEDIA '06 Proceedings of the 14th annual ACM international conference on Multimedia*, 149-152.

- Tzeng, W. G. and Hu, C. M. (2002). A New Approach for Visual Cryptography. 27 (3).
- Wolfgang (1999). Video Watermarking Technique using Visual Sensibility and Motion Vector. *National Polytechnic Institute of Mexico*.
- Wu, C. W. (2002). One the design of content-based multimedia authentication systems. *IEEE Trans. on Multimedia*. 4. (1). 385-393, Sep.
- Yin, L. H. (2009). Study of Digital Image Watermarking in Curvelet Domain. *Master. Thesis Department of Electronic Engineering University of Hong Kong*.
- Yusof, Y. and Khalifa, 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, 14-17 May, Penang, Malaysia.
- Zhong, J. (2006). Watermark Embedding and Detection. Doctor of Philosophy. Shanghai Jiaotong University.