A COMPARATIVE STUDY OF WATERMARKING TECHNIQUES IN SPATIAL AND FREQUENCY DOMAINS

ABDULADHIM MOHAMAD ALI ALAMARI

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

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

AUGUST 2014

DEDICATION

TO MY BELOVED MOTHER AND FATHER

For the love and support I have received throughout my studies.

To my mother, for all her sacrifices in bringing happiness to my life.

To my father, for all his motivation and inspiration.

ACKNOWLEDGEMENT

My gratitude goes to Allah for giving me the strength, patience, courage, and determination to complete this work.

I would like to express my sincere appreciation to my supervisor, Dr Kamaruddin Malik Mohamad. He has been extremely helpful and has offered me all the necessary support needed to succeed in every stage of my research, and as such, I owe him much appreciation.

My heartfelt gratitude goes to my parents for bearing with my weaknesses upon weaknesses from cradle to date. I am also grateful to my wife for her continuous support during my study. I am indeed grateful to all my family members.

Besides, I would like express my personal appreciation to my friend, Mr Ali Elrowayati, for his guidance and time. His effort really meant a lot to me. I would like to thank him for his comments and ideas that helped me to achieve the objectives of this research.

Lastly, I would like to thank all my friends, all postgraduate members, all staff from the Faculty of Computer Science and Information Technology and Postgraduate Center for their support, cooperation, and endless contributions along the journey.

Thank you very much.

ABSTRACT

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

ABSTRAK

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

CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

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

CHAPTER 1

INTRODUCTION

1.1 Background of the Study

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

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

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

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

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

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

According to Mandhani (2004), in regards to printed watermarks, digital watermarking is a mechanism whereby information is embedded in an item in a way that it is completely invisible to the naked eye. However, the issue in concern is related to the traditional way of stamping logos or names on items, whereby the logos or names may

be easily altered or duplicated. Katzenbeisser, and Petitcolas (2000) argue that in digital watermarking, the actual bits are disseminated in the image in a way that demonstrate resistance against attempts to remove or damage the hidden information and the hidden itself can hardly be identified.

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

2.2 Host Signals

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

a) Digital Image

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

b) Digital Video

A video is made up of a sequence of images. Hence, the watermarking method used in image is applicable on video. However, video watermarking comes with other problems. For instance, Zhao et al., (2000) assert that it is unsuitable to use the same watermarking key for the entire video. If the same key is used for all the

frames in a video sequence, the watermarking algorithm will become defenceless against collusion attacks. If a singular key is used for every frame or shot in the video sequence, it would be very difficult to manage the key management and key distribution. Besides, a video watermark should be able to resist different types of attacks, such as frame averaging, frame dropping, and frame swapping.

c) Digital Sound

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

d) 3D Virtual Objects

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

2.3 Digital Image Watermarking

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

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

cannot be detected after malignant transformations. On the other hand, a digital watermark is said to be robust if it resists a designated class of transformations.

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

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

2.4 Watermarking algorithm

Every watermarking algorithm consists of two basic parts. One part embeds the watermark, and the other one detects and decodes the watermark. In embedment, the watermark is embedded along with a chosen optional key within the cover image through selected embedding algorithm. The embedding part can be designed using spatial or frequency domain. Once the watermark is embedded, then it can be identified as visible or invisible. On the other hand, the detection procedure is the reverse process of embedding. It is further described as the process of authenticating the watermarked

image. For comparison purpose, the original watermark is compared with the extracted watermark. Some algorithms may or may not require the use of original image, which is found in the comparison procedure. This is referred to as either blind or non blind watermarking.

2.5 Characteristics of Watermark

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

a) Fidelity or Imperceptibility

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

b) Data Payload

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

c) Robustness

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

d) Security

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

2.6 Watermark embedding techniques

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

2.7 Watermark detection techniques

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

2.8 Watermarking Applications

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

a) **Copyright Protection**

   Watermark helps the legitimate owners of a certain item or property to verify the illegitimate copies of their works by inserting watermark signature into their digital works. Hence, the detected watermark signature can be used as an evidence to prove ownership of the property.

b) Fingerprinting

When a customer purchases a digital material**,** a unique identity, such as a serial number, is secretly embedded within the digital material. This method discourages customers from redistributing the content. The fingerprinting signature enables the intellectual property owner to identify which customer broke their license agreement.

c) Copy Control

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

d) Broadcast Monitoring

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

e) Data Authentication

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

2.9 Techniques for Digital Image Watermarking

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

2.9.1 Spatial Domain Technique

One of the first image watermarking techniques was implemented by Tirkel et al., (1993). His method was based on the pixel value of Least Significant Bit (LSB) modifications. The watermark algorithm was proposed by Kurah, and McHughes (1992), which involves embedding information into the LSB, and it has been known to reduce the quality of the image. This problem affects the efficiency of the algorithm.

The LSB technique works by taking the most significant bits of the watermark image and embedding it into the least significant bits of the cover image. Hence, a rough estimate of the watermarked image can be identified by simply eliminating the LSB of the watermark image. Another algorithm was proposed by Bruyndonckx et al., (1995), which is based on pixel region classification technique. Zheng et al., (2007) state that pixels with grey levels follow a certain rule when embedding a signature into a watermark.

2.9.2 Frequency Domain Technique

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

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

Attacks on watermark image can be said to be intentional or unintentional. Hostility and malevolence can be identified as intentional attacks on watermark images, whereby perpetrators attempt to damage, remove or modify the watermark. On the other hand,

coincidental attacks can be said to be unintentional. This occurs during common image processing and it is not an attempt to damage the watermark image. Besides, the most common form of attack is lossy image compression (Samˇcovic, & Turan, 2008). Some categories of attacks, which can be invoked to penetrate a watermarking system, include; removal attacks, geometrical attacks, cryptographic attacks, and protocol attacks.

2.10 Removal attacks

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

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

2.10.1 Compression

This mode of attack is generally unintentional and appears quite often in multimedia applications. In a practical sense, all images currently being used on the Internet have been compressed. A watermarking algorithm is expected to resist several levels of compression, however, it is advised that the watermark insertion should be done in the same domain where the compression has taken place. For example, Roma et al., (2008)

REFERENCES:

Abdullah O. A. B. (2012) An Improved Digital Watermarking Algorithm Using Combination Of Least Significant Bit (LSB) And Inverse Bit. Universiti Tun Hussein Onn Malaysia: Master's Thesis.

Albrecht, C. C, (2013). Prevention, F. Fraud and Forensic Accounting in a Digital Environment. (http://www.theifp.org/research-grants/IFP-Whitepaper-4.pdf).

Al-Dharrab, M. A. A. (2005). Benchmarking Framework for Software Watermarking . A master thesis presented to the deanship of the graduate studies in King Fahad University of Petroleum & Minerals.

Asaad Ibrahim, M .A (2005). Image Watermarking. ECE 618 – Fall 2005.

Bamatraf, A., Ibrahim, R., & Salleh, M. N. B. M. (2010, December). Digital watermarking algorithm using lsb. In Computer Applications and Industrial Electronics (ICCAIE), 2010 International Conference on (pp. 155-159). IEEE.

Basheer, N. M., & Abdulsalam, S. S. (2011, March). Digital Image Watermarking Algorithm in Discrete Wavelet Transform Domain Using HVS Characteristics. In Proceedings of the IEEE International Conference on Information Technology: Coding and Computing (pp. 122-127).

Bhatnagar, G. and Raman, B. (2008). A new robust reference watermarking scheme based on DWT-SVD, Elsevier B.V. All rights reserved

Bilal, M., Imtiaz, S., Abdul, W., & Ghouzali, S. (2013, May). Zero-steganography using DCT and spatial domain. In Computer Systems and Applications (AICCSA), 2013 ACS International Conference on (pp. 1-7). IEEE.

Bruyndonckx, O., Quisquater, J. J., and Macq, B. (1995). Spatial method for copyright labeling of digital images. In Proceedings of the IEEE Workshop Nonlinear Signal and Image Processing. IEEE Computer Society Press, Los Alamitos, CA, 456–459.

Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J. and Kalker, T. (2008). Digital Watermarking and Steganography. 2nd edition. Morgan Kaufmann Puplishers.

Cox, I., Kilian, J., Leighton, T., and Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process. 6, 12, 1673–1687.

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

Dorairangaswamy, M.A. (2009), 'A Novel Invisible and Blind Watermarking Scheme For Copyright Protection of Digital Images', International Journal of Computer Science and Network Security, vol. 9, no. 4. Retrieved January 3, 2010, from http://paper.ijcsns.org/07_book/200904/20090411.pdf.

El-Taweel, G.S., Onsi, H.M., Samy, M., & Darwish M.G.(2005), 'Secure and Non-Blind Watermarking Scheme for Color Images', ICGST International Journal on Graphics, Vision and Image Processing, vol. SI1. Retrieved January 3, 2010, from http://www.icgst.com/gvip/v4/P1150442004.pdf.

Eskicioglu, A. M., & Fisher, P. S. (1995). Image quality measures and their performance. Communications, IEEE Transactions on, 43(12), 2959-2965.

Fouad, M., El Saddik, A., & Petriu, E. (2010, May). Combining DWT and LSB watermarking to secure revocable iris templates. In Information ciences Signal Processing and their Applications (ISSPA), 2010 10th International Conference on (pp. 25-28). IEEE.

Gopal, N. V., & Koteswaramma, A. (2013). International Journal of Advanced Research in Computer Science and Software Engineering. International Journal, 3(3).

Gunjal, B. L., & Manthalkar, R. R. (2010). An overview of transform domain robust digital image watermarking algorithms. Journal of Emerging Trends in Computing and Information Sciences, 2(1), 2010-2011.

Hameed, K., Mumtaz, A., & Gilani, S.A.M. (2006), 'Digital Image Watermarking in the Wavelet Transform Domain', World Academy of Science, Engineering and Technology.RetrievedJanuary1,2010,from http://www.waset.org/journals/waset/v13/v13-16.pdf.

Hartung, F. and Kutter, M., (1999). Multimedia Watermarking Techniques. Proceedings of the IEEE, VOL. 87, NO. 7, JULY 1999.

He, H. J., Zhang, J. S. and Tai, H. M., (2006). A Wavelet-Based Fragile Watermarking Scheme for Secure Image Authentication. Springer-Verlag Berlin Heidelberg 2006.

Hu, Y., Kwong, S., Huang, J. (2004), 'Using invisible watermarks to protect visibly watermarked images', Proceedings of International Symposium Circuits and Systems, vol. 5, pp. V-584 - V-587. Retrieved January 3, 2010, from IEEEXplore database.

Johnson, N. F., Duric, Z., & Jajodia, S. (2006). Information Hiding: Steganography and Watermarking-Attacks and Countermeasures (Advances in Information Security, Volume 1)(Advances in Information Security).

Jun, Y., Chi, J.R. & Zhuang, X.D. (2007), 'A New Wavelet-based Robust Watermarking for Digital Image', IEEE International Conference on Networking, Sensing and Control, pp.1391-1394. Retrieved February 4, 2009, from IEEEXplore database.

Kamble, S., Maheshkar, V., Agarwal, S and Srivastava, V. K (2012). DWT-SVD Based Robust Image Watermarking Using Arnold Map. International Journal of Information Technology and Knowledge Management.

Katzenbeisser, S. and Petitcolas, F.A.P., (2000). Information hiding techniques for steganography and digital watermarking. Artech House Publishers.

Kundur, D. and Hatzinakos, D. (1997). A robust digital image watermarking method using wavelet based fusion. In Proceedings of the IEEE International Conference on Image Processing. Vol. 1. IEEE Computer Society Press, Los Alamitos, CA, 544–547.

Kurah, C. and Mchughes, J. (1992). A cautionary note on image downgrading. In Proceedings of the IEEE Computer Security Applications Conference. Vol. 2. IEEE Computer Society Press, Los Alamitos, CA, 153–159.

Lee, G. J., Yoon, E. J. and Yoo, K. Y. (2008). A new LSB based Digital Watermarking Scheme with Random Mapping Function. In 2008 IEEE DOI 10.1109/UMC.2008.33.

Lee, S. J. and Jung, S. H., (2001). A Survey of Watermarking Techniques applied to Multimedia. 2001 IEEE, ISIE 2001, Pusan, KOREA.

Li, C. T., & Si, H. (2007). Wavelet-based fragile watermarking scheme for image authentication. Journal of Electronic Imaging, 16(1), 013009-013009.

Liu, J.L., Lou, D.C., Chang, M.C. & Tso, H.K. (2005), 'A robust watermarking scheme using self-reference image', Computer Standards & Interfaces, vol. 28, no. 3, pp. 356-367. Retrieved February 4, 2009, from ScienceDirect database.

Low, C. Y., Teoh, A. B. J., & Tee, C. (2008, May). Fusion of lsb and dwt biometric watermarking for offline handwritten signature. In Image and Signal Processing, 2008. CISP'08. Congress on (Vol. 5, pp. 702-708). IEEE.

Lu, W., Lu, H., & Chung, F. (2006), 'Feature based watermarking using watermark template match', Applied Mathematics and Computations, vol. 177, no. 1, pp.377-386. Retrieved March 27, 2009, from ScienceDirect database.

Luo, H, Chu, S. H. and Lu, Z. M. (2008). Self Embedding Watermarking Using Halftoning Technique. Circuits Syst Signal Process (2008) 27: 155–170.

Luo, K. & Tian, X. (2008), 'A New Robust Watermarking Scheme based on Wavelet Transform', Congress on Image and Signal Processing, vol. 1, pp. 312-316. Retrieved February 4, 2009, from IEEEXplore database.

Malaysia (2006), Laws of Malaysia: Offences Relating To Documents and To Currency Notes and Bank: Forgery 46, Penal Act 574, 2006.

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

Nagra, J., Thomborson, C. and Collberg, C. (2002). a functional taxonomy for software watermarking.In M. Oudshoorn, ed., `Proc. 25th Australasian Computer Science Conference 2002', ACS, pp. 177-186.

Nasir, I., Weng, Y. & Jiang, J. (2007), 'A New Robust Watermarking Scheme for Color Image in Spatial Domain', Third International IEEE Conference on Signal-Image Technologies and Internet-Based System, pp.942-947. Retrieved May 10,2009, from IEEEXplore database.

O'Ruanaidh, J. and Pun, T. (1998). Rotation, scale, and translation invariant digital image watermarking. Signal Process. 66, 3, 303–317.

Pickholtz, R., Schilling, D., and Milstein, L. (1982). Theory of spread spectrum communications—a tutorial. IEEE Trans. Commun. 30, 5, 855–884.

Pindar, Z. A. (2014). UTHM Certificate Verification Using Microtext Double Check Digit. Universiti Tun Hussein Onn Malaysia: Master's Thesis.

Roma Rewani, Mahendra Kumar and Aditya Kumar Singh Pundir. (2008). Digital Image Watermarking: A Survey. International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.1750-1753.

Salama, A., Atta, R., Rizk, R., & Wanes, F. (2011, June). A robust digital image watermarking technique based on Wavelet transform. In System Engineering and Technology (ICSET), 2011 IEEE International Conference on(pp. 100-105). IEEE.

Samˇcovic, A., & Turan, J. (2008). Attacks on digital wavelet image watermarks. JOURNAL OF ELECTRICAL ENGINEERING-BRATISLAVA-, 59(3), 131.

Tilley, A. (2003). Steganography: Reversible Data Hiding Methods for Digital Media Bachelor project.

Tirkel, A., Rankin, G., Schyndel, R. V., Ho, W., Mee, N., and Osborne, C. (1993). Electronic watermark. In Proceedings of DICTA. 666–672.

Wang, X.Y., Hou, L.M. & Yang, H.Y. (2009), 'A feature-based image watermarking scheme robust to local geometrical distortions', Journal of Optics : Pure and Applied Optics. Retrieved March 27, 2009, from Institute of Physics (IOP) Journals database.

Wang, X.Y., Yang, H.Y. & Cui, C.Y. (2008), 'An SVM-based robust digital image watermarking against de synchronization attacks', Signal Processing, vol. 88,no. 9, pp. 2193-2205. Retrieved March 26, 2009, from ScienceDirect database.

Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. Image Processing, IEEE Transactions on, 13(4), 600-612.

Woo, C.S. (2007), 'Digital image watermarking methods for copyright protection and authentication', Doctor of Philosophy Thesis, Queensland University of Technology. Retrieved April 5, 2009, from http://eprints.qut.edu.au/16457/1/Chaw-Seng_Woo_Thesis.pdf.

Wu, M., & Liu, B. (1998, October). Watermarking for Image Authentication. InICIP (2) (pp. 437-441).

Yang, W. C., Wen, C. Y. and Chen, C. H.,(2008). Applying Public-Key Watermarking Techniques in Forensic Imaging to Preserve the Authenticity of the Evidence. Springer-Verlag Berlin Heidelberg 2008.

Zhang, Y. (2009, June). Digital Watermarking Technology: A Review. In Future Computer and Communication, 2009. FCC'09. International Conference on (pp. 250-252). IEEE.

Zhao, J., Hayasaka, R., Muranoi, R., Ito, M., and Matsushita, Y. (2000). A video copyright protection based on contented. IEICE Trans. Inf. Syst. E83-D, 12, 2131–2141.

Zheng, D., Liu, Y., Zhao, J. and El Saddik, A., (2007). A Survey of RST Invariant Image Watermarking Algorithms, ACM 0360-0300/2007/06. DOI 10.1145/1242471.1242473.

Zkeng, D., Zhao, J., Tam, W., and Speranza, F. (2003). Image quality measurement by using digital watermarking. In Proceedings of the IEEE International Workshop on Haptic, Audio and Visual Environments and their Applications. IEEE Computer Society Press, Los Alamitos, CA, 65–70.