DIGITAL IMAGE WATERMARKING BASED ON THREE LEVELS DISCRETE WAVELET TRANSFORM TO ACHIEVE ROBUSTNESS AGAINST GEOMETRICAL ATTACKS

ZAHRA SADAT SHAMS DOLATABADI

A thesis submitted in partial fulfillment of

the requirements for the award of the degree of

Master of Computer Science (Information Security)

Advanced Informatics School

Universiti Teknologi Malaysia

January 2013

ACKNOWLEDGMENT

My first and foremost thanks are to God almighty for giving me the blessings to complete this study.

Also I would like to thank my supervisor Prof. Dr. Azizah Abd Manaf for her support and guidance. I am grateful to her for sharing many precious experiences with me during this project.

In addition I would like to express my gratitude and many thanks to my dear father and mother whom inspired, encouraged and kindly supported me through this way. Without their kindness and patience I would not be able to finish this project. Finally, many thanks to my kind sister for her encouragement and understanding when it was most required.

ABSTRACT

The availability of the Internet and the growth in using its services has simplified and highly affected the transmission, exchange and acquisition of multimedia information. As a disadvantage of this event, the chances of piracy have increased and became easier. In order to overcome this problem, techniques for identification, authentication and protection of multimedia information are required. Digital image watermarking as a method that provides ownership authentication and copyright protection can be used to protect against piracy. One of the important issues that different image watermarking methods are facing is to have the robustness against different categories of image distortions especially those in geometrical or transform category. Also, since achieving robustness is in contrast with capacity and quality, it is more difficult to offer a method that satisfies all the three requirements. So this project is aimed to propose a method that can offer high resistance against some image distortions in the geometrical attack category while maintaining capacity and quality. The method which is proposed uses discrete wavelet transform (DWT) in combination with singular value decomposition (SVD) in order to achieve high robustness against geometrical attacks. The DWT is performed in three levels on both cover and watermark images and mid and high frequency subbands are selected for hiding the watermark data. Also in order to have a reliable method against the false positive problem, the principal components of the watermark are calculated to be embedded in cover image. The proposed method robustness is tested against scaling, rotation and crop attacks. The experimental results demonstrate that the proposed method has a high robustness against scale attack which is almost 99.9%. Also, robustness against crop and rotation attacks has increased by 14 and 50 percent, respectively, compared to two recent methods. In addition, the capacity for watermark embedding is increased compared to recent proposed methods while the quality of watermarked image is maintained.

ABSTRAK

Peningkatan dalam teknologi dan aplikasi internet telah secara tidak langsung menjejaskan penghantaran, pertukaran dan pemerolehan maklumat multimedia. Antara kelemahan utama proses ini adalah wujudnya banyak peluang untuk melakukan kesalahan cetak rompak. Dalam usaha untuk mengatasi masalah ini, teknik bagi pengenalan, pengesahan dan perlindungan maklumat multimedia diperlukan. Peneraan air kepada imej digital sebagai kaedah yang menyediakan pengesahan pemilikan dan perlindungan hakcipta boleh digunakan bagi melindungi daripada cetak rompak. Antara isu utama bagi kaedah peneraan air imej adalah bagi memastikan keteguhan terhadap kategori herotan imej yang berlainan, terutamanya dalam kategori geometri atau pengubahan. Proses mencapai keteguhan imej adalah bertentangan dengan kapasiti dan kualiti imej, oleh itu, lebih sukar untuk mendapatkan satu kaedah yang dapat memenuhi kesemua tiga keperluan. Oleh itu, projek ini bertujuan untuk mencadangkan satu kaedah yang boleh mencapai rintangan yang tinggi terhadap beberapa herotan imej (kategori serangan geometri) dan pada masa yang sama mengekalkan kapasiti dan kualiti imej tersebut. Kaedah yang dicadangkan merupakan kombinasi Discrete Wavelet Transform (DWT) dan Singular Value Decomposition (SVD) bagi mencapai keteguhan yang tinggi terhadap serangan geometri. DWT dilakukan dalam ketiga-tiga peringkat yang dicadangkan di dalam kajian ini. Keteguhan kaedah yang dicadangkan diuji keatas serangan berskala, putaran dan pangkas. Keputusannya menunjukkan, selain kualiti imej dapat dikekalkan, kaedah yang dicadangkan mempunyai keteguhan yang sangat tinggi terhadap serangan berskala, iaitu hampir 99.9%. Pada masa yang sama, keteguhan terhadap serangan pangkas dan putaran telah meningkat sebanyak 14% dan 50%, berbanding dengan kaedah yang dicadangkan baru-baru ini. Di samping itu, keupayaan untuk menanamkan tera air meningkat berbanding dengan kaedah yang dicadangkan baru-baru ini manakala kualiti imej tera air dikekalkan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Overview

Availability and growth of high speed computer networks and the internet, together with inexpensive digital recording and storage peripherals has made duplication, unauthorized use and distribution of digital content easier. So the need for secure identification, authentication and protection of information have achieved a broad attention during recent years. (Chen and Yin, 2012)

One way of providing this security is through Steganography that is the art of concealed communication where communication is carried out in secret. The other newer way is through watermarking (Woo, 2007).

Watermarking as a way of information hiding seems to have been created near the end of the 19th century but the idea of digital watermarking is not that old and refers back to 1979 when Szepanski described a machine detectable pattern to be placed on documents for anti-counterfeiting purposes, but it was in 1988 that the term digital watermarking was firstly used and in the 1990s it started to develop (Cox *et al.*, 2008).

Digital watermarking is the technique for embedding hidden information (copyright information, time stamp, movie subtitles, etc.) into multimedia data. This technique is an alternative or complement to cryptography that can protect content from distribution or manipulation even after it is decrypted (Woo, 2007).

Watermarking has two categories, visible and invisible. Visible watermarking has been around for centuries in the form of stamps, signatures or classical watermarks. Nevertheless, the hidden digital watermarks (invisible watermarks) are essential for known data manipulation technologies in most of the applications (Terzija, 2006). Some of the known watermarking applications considered in the literature are as follows: copyright protection, owner identification, finger printing, authentication, broadcast monitoring, transaction tracking, copy control, device control, and legacy enhancements. In each of these applications, the characteristics of the problem make watermarking a suitable solution (Saxena, 2008; Woo, 2007).

During recent years, many researches have been conducted on watermarking and industrial interest in digital watermarking schemes keeps growing. Three main characteristics for recognizing these effective watermarking schemes are: imperceptibility, robustness and security (Lu *et al.*, 2011). Imperceptibility means hiding a watermark should not significantly degrade the quality of the protected data. Robustness refers to the ability of resisting against non-malicious distortions such as compression. And security is the ability of watermark to withstand malicious attacks including intentional operations of removal or modification with the aim of defeating the purpose of watermarking (Lu *et al.*, 2011; Nyeem *et al.*, 2012; Woo, 2007).

Also these watermarking schemes can be classified under two main categories of spatial and transform (frequency) domain. In Spatial Domain, the watermarking system directly alters the main data elements (like pixels in an image) to hide the watermark data while Transformed Domain techniques alter the frequency transforms of data elements to hide the watermark data (Terzija, 2006).

Generally, several forms of multimedia data are digital audio, image, video, and text. Among these, image watermarking receives more attention as it is the basis of video watermarking and some other watermarking applications (Lu *et al.*, 2011; Saxena, 2008). Therefore the focus of this study is on invisible digital image watermarking.

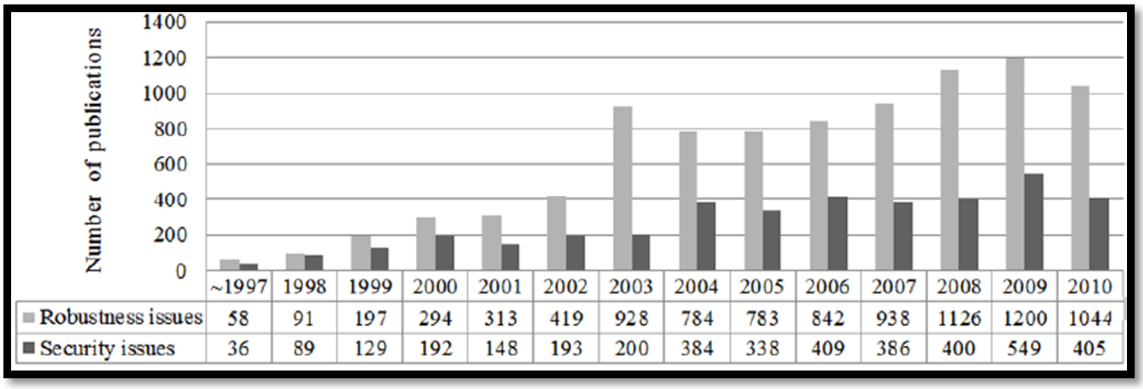
1.2 Background of the Problem

Since digital multimedia can be easily distributed with the help of World Wide Web, intellectual property right (IPR) has been facing threats of unlimited copying and determining the owner of a property has become difficult. Despite several laws with the purpose to protect the authors from unauthorized use of their intellectual products, the digital piracy phenomenon is constantly growing. Therefore it becomes strategic and very important to be able to create and develop methods and numerical algorithms to resolve copyright problems and owner identification (Agreste and Puccio, 2011).

The solution to this problem is of great interest to big media organizations and also to other vendors of digital information, such as news and photo agencies. Some amount of information that is watermarked to the original data, coupled with an acceptable degree of resistance to signal modifications, can be a solution to existing problems (Saxena, 2008). The embedded watermark can be used as a proof, e.g. in a court if someone intentionally infringed the copyright (Terzija, 2006).

Although researchers during the past years have worked on digital image watermarking techniques, there are still needs for it in various areas (Saxena, 2008). As already mentioned, some of the most important characteristics of effective watermarking schemes are imperceptibility, robustness and security.

Many researchers have worked on these characteristics and tried to suggest effective schemes for image watermarking (Agreste *et al.*, 2007; Kang *et al.*, 2003; Tao and Eskicioglu, 2004). But as long as attacks on watermarked images are concerned, robustness against a reasonable (image quality after such manipulation should be high enough) amount of manipulation is very important and still an open and challenging issue (Dietze, 2005; Saxena, 2008). In a work done by Nyeem *et al.* (2012) on the Robustness and Security of Digital Image Watermarking, shown on figure 1-1, the amount of work done on these areas shows the importance and interest of researchers toward this topic during recent years.



	~1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Robustness issues	58	91	197	294	313	419	928	784	783	842	938	1126	1200	1044
Security issues	36	89	129	192	148	193	200	384	338	409	386	400	549	405

Figure 1-1: Yearly published articles in digital watermarking regarding robustness and security problems

According to an attack classification by Woo (2007), there are different attacks against watermark robustness: image degradation, image enhancement (contrast enhancement), image compression (lossy and lossless) and image transformation (RST). During recent years some schemes and algorithms have been suggested focusing on each of the above mentioned attacks on watermark robustness such as Kang *et al.* (2003). But still works need to be done in some of these areas as there are weaknesses, especially on image transformation attacks.

According to Terzija (2006) and Saxena (2008) findings, resistance of watermarking schemes against geometrical distortions is still an open problem. Furthermore, Wang *et al.* (2011) state that, it is well known that resisting affine attacks is still a challenging issue for image watermarking. Also in previous suggested algorithms more improvements in robustness against other watermark distortions and attacks can be done, in order to have more robust algorithms against existing attacks. Regarding this, it is necessary to mention that, since there is a trade-off between different effective watermarking characteristics, researchers have focused or preferred one characteristic against the other according to the application area of suggested algorithm.

Therefore it seems that there are interests in the robustness of watermark images against transformation attacks and also improvements and enhancements on robustness against other attacks in the existing algorithms.

1.3 Problem Statement

As far as there are various important applications of digital image watermarking and because of their financial implications, this is an important area of research (Saxena, 2008).

One of the main differences between steganography and watermarking is that, watermarking requires the hidden data to be robust to attempts aimed at removing it. This is exactly the area of many problems in watermarking as there are many intentional and unintentional attacks toward robustness of watermarked images (Saxena, 2008; Terzija, 2006).

Some of the issues or problems are as follows:

- Watermarking requires the hidden data to be robust to attempts aimed at removing it. This is a vital issue for watermarking (Cox *et al.*, 2008).
- Despite the robustness of watermarked image against attacks is a vital requirement, increasing robustness, decreases imperceptibility and the amount of watermarked information. So maintaining the proper balance (based on the application) between these requirements is an important issue (Lin and Lin, 2009; Terzija, 2006; Woo, 2007).
- The resistance of watermarking techniques against the category of transformation attacks that includes geometrical distortions (like RST) and affine attacks is still an open and challenging problem. This is due to their ease of implementation and de-synchronization effects (Saxena, 2008; Terzija, 2006; Wang *et al.*, 2011).

So the focus of the proposed project is on invisible digital image watermarking and using wavelet transform domain which is included in frequency (transform) domain (since frequency domain techniques have better robustness quality rather than spatial domain techniques). A technique which is based on wavelet transform domain would be selected in order to achieve better robustness against some of the attacks in the category of transform attacks that includes geometrical transforms (RST). Also it is important to maintain a balance between robustness and quality of the image.

1.4 Project Objectives

The objectives of the proposed project are:

- To identify some of the existing techniques based on wavelet transform which offer robustness against image distortions or attacks.
- To enhance the robustness of a wavelet based method against some existing geometrical attacks, such as scaling, rotation and cropping.
- To evaluate the behavior of the proposed method and measure its performance against specified attacks.

1.5 Project Aim

The aim of this study is to have an enhanced method which is based on wavelet transform domain that offers better robustness against some unintentional or intentional existing attacks. Therefore, first is, identifying the properties and behavior of some of the existing wavelet transform domain techniques and determining the properties of wavelet transform domain which are effective in increasing robustness of watermarked images. Then, to propose a wavelet transform domain technique to have the robustness and resistance against some attacks in the Transform attacks category that includes geometrical transforms. And finally, testing and evaluating the performance of the improved technique with respect to its robustness.

1.6 Project Scope

- The study is focused on invisible digital image watermarking.
- Among the important factors in image watermarking, the focus of this study is on robustness.
- The proposed method will be tested with one image format and against some geometrical attacks which are cropping, rotation and scaling attacks.
- The experiments will be conducted on gray scale images.
- MATLAB software will be used for generating the prototype.
- The experiments will be conducted on windows environment.

1.7 Summary

In past years, digital watermarking is proposed as a solution for solving problems in various application fields such as copyright protection and authentication. So during recent years, interests in digital watermarking have grown significantly and research efforts have been devoted to study this area. Several aspects of watermarking have been developed or improved but there are still works to be done as there are lots of financial implications in this area.

Therefore the focus of this study is to propose a method in the wavelet transform domain in the area of invisible digital image watermarking with respect to owner identification and copyright protection. The enhancement is with the aim of achieving a better robustness against some of the image manipulations in the category of transformation attacks including rotation, scaling and cropping.

REFERENCES

Agreste, S., Andaloro, G., Prestipino, D., and Puccio, L. (2007). An image adaptive, wavelet-based watermarking of digital images. *Journal of Computational and Applied Mathematics.* 210(1-2), 13-21.

Agreste, S., and Puccio, L. (2011). Wavelet-based watermarking algorithms: theory, applications and critical aspects. *International Journal of Computer Mathematics.* 88(9), 1885-1895.

Amiri, S. H., and Jamzad, M. (2009). A Robust Image Watermarking Method in Wavelet Domain Using Genetic Algorithm. *International Conference on Availability, Reliability and Security*. 612-617.

Bhatnagar, G., and Raman, B. (2009). A new robust reference watermarking scheme based on DWT-SVD. *Computer Standards & Interfaces.* 31(5), 1002-1013.

Chen, Y. F., and Yin, G. (2012). A Wavelet-Based Watermarking Algorithm Using the Human Visual System. *Advanced Materials Research.* 424, 304-308.

Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., and Kalker, T. (2008). *Digital Watermarking and Steganography*. USA: Morgan Kaufmann Publishers.

Davoine, F. (2000). Comparison of two wavelet based image watermarking schemes. *International Conference on Image Processing*. 682-685.

Dietze, M. (2005). *Second Generation Image Watermarking in the Wavelet Domain.* University of Buckingham.

Ganic, E., and Eskicioglu, A. M. (2004). Robust DWT-SVD domain image watermarking: embedding data in all frequencies. *International Multimedia Conference*. 166-174.

Gunjal, B. L., and Manthalkar, R. R. (2010). Discrete Wavelet Transform Based Strongly Robust Watermarking Scheme for Information Hiding in Digital Images. *Third International Conference on Emerging Trends in Engineering and Technology*. 124-129.

Jain, C., Arora, S., and Panigrahi, P. K. (2008). A Reliable SVD based Watermarking Schem. *arXiv preprint arXiv:0808.0309*.

Kang, X., Huang, J., Shi, Y. Q., and Lin, Y. (2003). A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression. *IEEE Transactions on Circuits and Systems for Video Technology* 13(8), 776-786.

Kapre Bhagyashri, S., and Joshi, M. (2010). Robust image watermarking based on singular value decomposition and discrete wavelet transform. *3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT)* 337-341.

Kejgir, S. G., and Kokare, M. (2012). Lifting Wavelet Transform with Singular Value Decomposition for Robust Digital Image Watermarking. *International Journal of Computer Applications.* 39(18), 10-18.

Kumsawat, P., Attakitmongcol, K., and Srikaew, A. (2005). A new approach for optimization in image watermarking by using genetic algorithms. *IEEE Transactions on Signal Processing.* 53(12), 4707-4719.

Kumsawat, P., Attakitmongcol, K., and Srikaew, A. (2009). An optimal robust digital image watermarking based on genetic algorithms in multiwavelet domain. *WSEAS Transactions on Signal Processing.* 5(1), 42-51.

Lai, C. C., and Tsai, C. C. (2010). Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transactions on Instrumentation and Measurement.* 59(11), 3060-3063.

Li, N., Zheng, X., Zhao, Y., Wu, H., and Li, S. (2008). Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform. *International Symposium on Electronic Commerce and Security*, 942-945.

Lin, T.-C., and Lin, C.-M. (2009). Wavelet-based copyright-protection scheme for digital images based on local features. *Information Sciences.* 179(19), 3349-3358.

Lu, W., Sun, W., and Lu, H. (2011). Novel robust image watermarking based on subsampling and DWT. *Multimedia Tools and Applications*.

Mohanty, S. P. (1999). Digital watermarking: A tutorial review.

Nyeem, H., Boles, W., and Boyd, C. (2012). On the robustness and security of digital image watermarking. *International Conference on Informatics, Electronics & Vision*. Dhaka, Bangladesh.

Okagaki, K., Takahashi, K., and Ueda, H. (2010). Robustness Evaluation of Digital Watermarking Based on Discrete Wavelet Transform. *Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. 114-117.

Potdar, V. M., Han, S., and Chang, E. (2005). A survey of digital image watermarking techniques. *3rd IEEE International Conference on Industrial Informatics (INDIN)*. 709-716.

Prasad, R., and Koliwad, S. (2010). A robust wavelet-based watermarking scheme for copyright protection of digital images. *Second International conference on Computing, Communication and Networking Technologies*. 1-9.

Raval, M., and Rege, P. (2003). Discrete wavelet transform based multiple watermarking scheme. *Conference on Convergent Technologies for Asia-Pacific Region*. Bangalore, India: 935-938.

Run, R. S., Horng, S. J., Lai, J. L., Kao, T. W., and Chen, R. J. (2012). An improved SVD-based watermarking technique for copyright protection. *Expert Systems with Applications.* 39(1), 673-689.

Saxena, V. (2008). *Digital image watermarking.* Jaypee Institute of Information Technology, India.

Tao, P., and Eskicioglu, A. M. (2004). A robust multiple watermarking scheme in the discrete wavelet transform domain 133-144.

Terzija, N. (2006). *Robust digital image watermarking algorithms for copyright protection.* University Duisburg-Essen.

Wang, J., Peng, H., and Shi, P. (2011). An optimal image watermarking approach based on a multi-objective genetic algorithm. *Information Sciences.* 181(24), 5501-5514.

Wang, Z., Wang, N., and Shi, B. (2006). A novel blind watermarking scheme based on neural network in wavelet domain. *6th World Congress on Intelligent Control and Automation*. Dalian, China: 3024-3027.

Wen, X.-B., Zhang, H., Xu, X.-Q., and Quan, J.-J. (2008). A new watermarking approach based on probabilistic neural network in wavelet domain. *Soft Computing*. 13(4), 355-360.

Woo, C. S. (2007). *Digital image watermarking methods for copyright protection and authentication.* Queensland University ot Technology.

Yang, Q., Gao, T., and Fan, L. (2010). A novel robust watermarking scheme based on neural network. *Intelligent Computing and Integrated Systems (ICISS)*. 71-75.

Zhang, D., Wu, B., Sun, J., and Huang, H. (2009). A new robust watermarking algorithm based on DWT 1-6.

Zhang, L., and Li, A. (2009). Robust watermarking scheme based on singular value of decomposition in DWT domain 19-22.

Zhong, N., He, Z., Kuang, J., and Zhuo, Z. (2007). An optimal wavelet-based image watermarking via genetic algorithm. *Third International Conference on Natural Computation*. 103-107.