A STUDY OF WATERMARKING METHODS IN MEDICAL APPLICATION

by

NG LEE PING

A report submitted for partial fulfillment of the
requirement for the degree of
Master of Science

June 2004

ACKNOWLEDGEMENTS

The report you hold in your hands would not have been completed without the generous contributions and support from numerous individuals. I gratefully acknowledge my project supervisor, Dr. Khoo Bee Ee, who has provided all the essential and important guidance towards achieving the objectives of this project. This useful and helpful information has assisted me extensively in this research.

Special thanks are owed to Masters Research students Lim Say Yarn and Muhammedali Bharmal for their time and effort spent in helping me on how to use Matlab and information in Image Processing. Finally, my sincerest gratitude goes to my parents, friends and my sponsor, Kolej Universiti Teknologi Tun Hussein Onn (KUiTTHO), for without their endless support, my efforts would have been meaningless.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Nowadays, watermarking technology is playing an important role in medical image watermarking as it can hide the patient information and then get back the information by the owner itself using certain private key. The objective of this project is to address the specific requirements needs for watermarking of medical images and compare three appropriate schemes for watermarking of medical images. Four important requirements in medical image watermarking are imperceptible watermarking, integrity control, authentication and capacity hiding. The three methods of medical image watermarking that have been studied are Least Significant Bit (LSB), Rivest, Shamir and Adleman (RSA) encryption and decryption with LSB, RSA encryption and decryption with feature-based. These three methods of image watermarking are categorized in spatial domain. Performance for watermarking scheme is carried out and comparisons are made. There are three quality metrics used in this project which are Peak-to-Noise Ratio (PSNR), Mean Square Error (MSE) and Signal-to-Noise Ratio (SNR). Among these three methods, LSB method has the most capacity of watermark and fastest rate in embedding process. These three algorithms implemented in this project are shown to be sensitive for the attack. Attacks applied in this project are salt & pepper noise with 0.0001 noise density, median filtering, JPEG compression with index 100 and index 75, cropping and rotation. These three methods that being studied are better for integrity control. Meanwhile, a Graphic User Interface (GUI) is developed for embedding and extracting purpose. User can embed a watermark into their host image and extract the watermark from the watermarked image.

ABSTRAK

Pada masa terkini, teknologi tera air memainkan peranan penting dalam tera air imej perubatan, memandangkan ia boleh menyembunyikan maklumat pesakit dan kemudian pemilik tersebut boleh mengeluarkan maklumatnya dengan kunci rahsia tertentu. Objektif projek ini adalah untuk mempelajari keperluan khusus yang diperlukan oleh imej perubatan dalam tera air dan membandingkan tiga jenis skim yang sesuai bagi tera air imej perubatan. Empat keperluan yang penting dalam tera air imej perubatan adalah tera air tanpa disedari, kawalan keutuhan, keboleharapan dan penyembunyian kapasiti. Tiga jenis kaedah bagi tera air imej perubatan yang dipelajari adalah Bit Bererti Terkecil (LSB), Rivest, Shamir dan Adleman (RSA) "encryption" dan "decryption" dengan LSB, RSA "encryption" dan "decryption" dengan berdasarkan ciri-ciri imej. Ketiga-tiga kaedah ini adalah dikategorikan dalam domain ruang (spatial domain). Perlaksanaan bagi skim tera air telah dikaji dan perbezaannya telah dianalisis. Tiga jenis matrik kualiti yang digunakan dalam projek ini adalah nisbah puncak hingar (PSNR), ralat min kuasa dua (MSE) dan nisbah isyarat hingar (SNR). Daripada tiga jenis kaedah yang dipelajari, kaedah LSB menunjukkan keputusan yang paling banyak dalam penyembunyian kapasiti bagi "watermark" dan cepat dalam process pembenaman dengan huruf "watermark" yang maksimum. "Algorithm" yang dilaksanakan dalam projek ini telah menunjukkan ia adalah sensitif terhadap serangan. Serangan yang digunakan dalam projek ini adalah hingar "salt & pepper" dengan kelebatan hingar 0.0001, penurasan median, kemampatan JPEG dengan indeks

100 dan indeks 75, "cropping" dan putaran. Maka, tiga jenis kaedah ini adalah baik dari segi kawalan keutuhan. Di samping itu, pengantaran grafik pengguna (GUI) telah dibangunkan bagi tujuan proses pembenaman dan pengeluaran data. Pengguna boleh membenam "watermark" ke dalam imej mereka dan mengeluarkan "watermark" daripada imej yang telah terbenam dengan "watermark".

CHAPTER I

INTRODUCTION

Watermarking describes techniques that are used to imperceptibly convey information by embedding it into the host image. Information that needed to be conveyed was inserted into the host image through the embedding process. The information can be extracted at anytime by the user. A popular application of watermarking is to give proof of ownership of digital data by embedding copyright statements. It is obvious that for this application the embedded information should be robust against manipulations that may attempt to remove it.

1.1 History

The idea of communicating secretly has begun since ancient time and is as old as communication itself. There are several ways introduced for communicating secretly in the past. Paper watermarks were one of the methods that were introduced and it has appeared in the art of handmade papermaking at the end of the 13th century to differentiate paper makers of that time. The oldest watermarked paper found in archives dates back to 1292 and has its origin in Fabriano, Italy, which is considered the birthplace of watermarks [Hartung & Kutter, 1999].

At the end of the thirteenth century, about 40 paper mills were sharing the paper marked in Fabriano and producing paper with different format, quality and price. Raw, coarse paper which was smoothed and postprocessed was produce by artisans and sold by merchants. There were competition among paper mills, artisans and merchants and it was difficult to keep track of paper provenance and thus the format and quality identification. The introduction of watermarks helped avoiding any possibility of confusion.

In the 17th century, Claude Lorrain introduced a method for protecting his intellectual property nearly hundred years before any relevant law was introduced [Hartung & Kutter, 1999]. The first 'copyright' law was the 'Statute of Anne' introduced by the English Parliament in 1710. A good example illustrating the legal power of watermarks is a case in 1887 in France called "Des Decorations". The idea of digital image watermarking arose independently in 1990 [Hartung & Kutter, 1999].

The use of watermarks is almost as old as paper manufacturing. Watermark is a technique of impressing into the paper a form of image or text derived from the negative in the mold. Paper Watermarks have been in wide use since the late Middle Ages. Today most developed countries watermark their paper, currencies and postage stamps to make forgery more difficult [Hartung & Kutter, 1999].

1.2 Basic On Digital Watermarking

Watermarking is a process that embeds data called a watermark or digital signature or tag or label into a multimedia object such that the watermark is secure in the signal mixture but can be detected or extracted later to make an assertion about the object [Mohanty, 1999]. The multimedia object may be an image or audio or video. A simple example of a digital watermark would be a visible "seal" placed over an image to identify the copyright. However the watermark might contain additional information including the identification of the purchaser of that particular copy of the material.

Every owner has a unique watermark. They can also put different watermarks in different objects. The embedding algorithm incorporates the watermark into the object or image. The extraction algorithm authenticates the object or image determining both the owner and the integrity of the object or image.

In general, any watermarking scheme (algorithm) consists of three parts.

- The watermark
- The embedding algorithm
- The extraction algorithm

1.2.1 Fundamental of Digital Watermarking Scheme

Figure 1.1 and Figure 1.2 illustrate the fundamental concept of digital watermarking scheme. Figure 1.1 shows the watermarking embedding process. The input to the scheme is the watermark, the host image and an optional public or private key. Private key has higher security level compared to public key. Private key is only accessible by authorized personnel in order to perform any watermark. On the other hand, public key is the key that anyone is authorized to detect the watermark. The watermark can be of any nature such as a number, text or an image. The output of the watermarking embedding is the watermarked image [Hartung & Kutter, 1999; Katzenbeisser & Petitcolas, 2000].

Figure 1.2 shows the watermarking extracting process. Inputs to the scheme are the watermarked data, the private or public key and the original watermark. The output of watermarking extracting process is either the watermark or some kind of confidence measure indicating how likely it is for the given watermark at the input to be present in the data under inspection [Hartung & Kutter, 1999; Katzenbeisser & Petitcolas, 2000].

1.2.1.1 Watermark Generation

The design of the watermark signal W is added to the host signal. Typically, the watermark signal depends on key K and watermark information I [Hartung & Kutter, 1999],

$$W = f_0(I,K)$$

Possibly, it may also depend on the host image X into which it is embedded.

$$W = f_0(I,K,X)$$

1.2.1.2 Watermark Embedding

The design of the embedding method itself that incorporates the watermark signal W into the host image X yielding watermarked data Y [Hartung & Kutter, 1999] is shown in Figure 1.1.

$$Y = f_1(X,W)$$

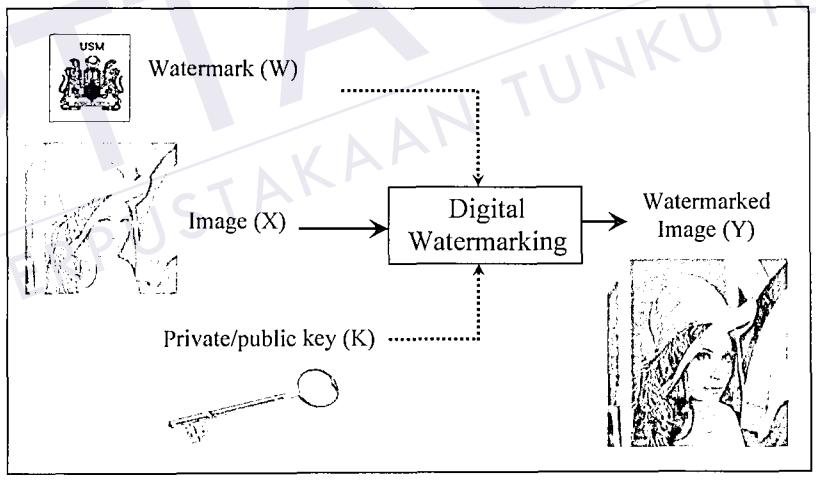

Figure 1.1 : Watermark Embedding

1.2.1.3 Watermark Extraction

Design of the corresponding extraction method [Hartung & Kutter, 1999] that recovers the watermark information from the signal mixture using the key and with the help of the original is shown in Figure 1.2.

$$I' = g(X, Y, K)$$

or without the original $I' = g(Y, K)$

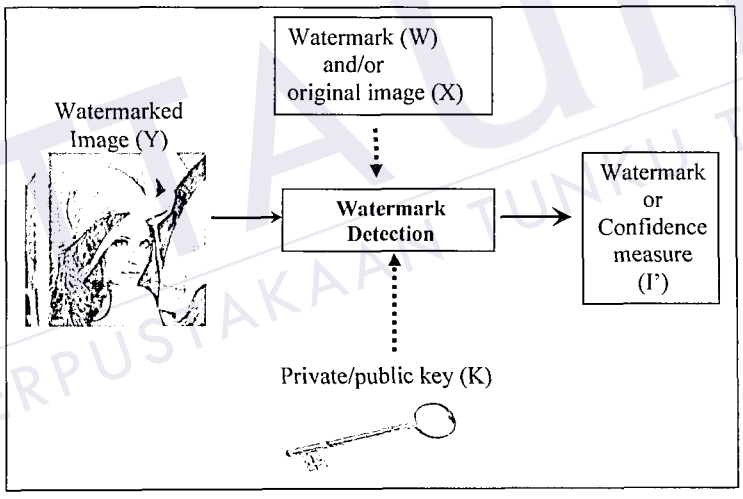

Figure 1.2 : Watermark Extraction

1.3 Type of Digital Watermarks

Watermarks and watermarking techniques can be divided into various categories in various ways. Different types of watermarks are shown in the Figure 1.3 [Mohanty, 1999].

The watermarks can be applied in spatial domain. The first watermarking scheme that was introduced works directly in the spatial domain. By some image analysis operations (e.g. edge detection), it is possible to get perceptual information about the image, which is then used to embed a watermark, directly in the intensity values of predetermined regions of the image. Those pretty simple techniques provide a simple and effective way for embedding an invisible watermark into an original image but do not show robustness to common image alterations [Wolfgang, Podilchuk & Delp, 1999].

An alternative to spatial domain watermarking is frequency domain watermarking. The another way to produce high quality watermarked image is by first transforming the original image into the frequency domain by the use of Fourier, Discrete Cosine or Wavelet transforms for example. With the frequency technique, the marks are not added to the intensities of the image but to the values of its transform coefficients. Then inverse-transforming the marked coefficient forms the watermarked image [Paquet, 2001]. It has been pointed out that the frequency domain methods are more robust than the spatial domain techniques [Wolfgang, Podilchuk & Delp, 1999].

Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows:

- Image Watermarking
- Video Watermarking
- Audio Watermarking
- Text Watermarking

According to the human perception, the digital watermarks can be divided into three types as follows [Mohanty, 1999]:

i. Visible watermark - the watermark appears visible to a casual viewer on a careful inspection.

ii. Invisible-Robust watermark - embedded in such a way that alternations made to the pixel value is perceptually not noticed and it can be recovered only with appropriate decoding mechanism.

iii. Invisible-Fragile watermark - embed in such a way that any modification of the image would destroy the watermark.

From application point of view digital watermark could be as follows [Mohanty, 1999]:

i. Source based - watermark are desirable for ownership identification or authentication where a unique watermark identifying the owner is introduced to all the copies of a particular image being distributed.

ii. Destination based - where each distributed copy gets a unique watermark identifying the particular buyer.

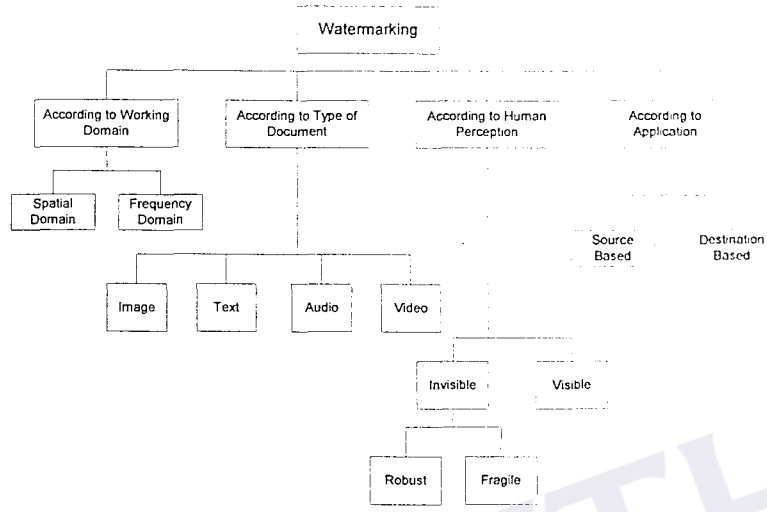

Figure 1.3 : Classification of Watermarking Techniques

1.4 Watermarking of Medical Image

Nowadays, digital watermarking of medical images is important due to integrity control therefore the patient information such as patient details or medical history can be used as watermark. Medical images are stored for the following purposes [Wakatani, 2002]:

- Diagnosis
- Database
- Long-term storage

However, anybody with privilege can access to images which are contained in database and can modify them maliciously therefore the integrity of the images must be protected by using watermarking, which is called integrity watermark [Dittman & Nack, 2000]. The copyright and intellectual property of the database should be also protected by a watermark, which is called copyright watermark [Dittman & Nack, 2000]. For long-term storage, the protection of the integrity and copyright of image is also a critical issue [Wakatani, 2002]. It contributes to two major roles in the medical image watermarking. Firstly, when a person stores an image in the long-term storage system long ago, if a viewer refers to the image, the viewer can confirm the integrity of the image only through a watermark embedded in the image. Secondly, when a patient does not want his/her medical images open to the public; the copyright of the image is thought to belong to the patient. Therefore the patient can protect the copyright of the image by using watermarking.

1.5 Objective And Scope Of Project

The main objective of this project is to study and determine the important requirements in medical images. The second objective is to evaluate the three identified medical image watermarking methods based on the determined requirements.

The scope of this project is to study three methods of the digital watermarking of medical images and present a Graphic User Interface (GUI). The

three identified methods for watermarking of medical images are Least Significant Bit (LSB) [Derbel et al., 2002], RSA encryption and decryption with LSB [Anand & Niranjan, 1998] and RSA encryption and decryption with feature-based.

LSB method is chosen because it is a simple and standard watermarking technique. While RSA encryption and decryption with LSB and RSA encryption and decryption with feature-based methods are chosen because RSA method has private key and it is secure and difficult to be cracked by attacker.

Fifteen medical images in four groups of sizes (400x400, 455x431, 640x480 and 827x827) were selected to be used as host images in this project.

1.7 Report Organization

This report contains six chapters. The reader is first oriented with motivation of this project and some watermarking knowledge in Chapter I.

Chapter II is generally about the requirements for medical image watermarking, common attack for digital image watermarking and a survey of medical digital image watermarking techniques.

Chapter III describes the three identified methods of the digital watermarking of medical imaging that have been studied in this project. Chapter

REFERENCES

Anand, D. & Niranjan, U.C. (1998). *Watermarking Medical Images with Patient Information.* in Proceeding IEEE/EMBS Conference, Hong Kong, China, pp. 703 – 706

Chen, P.C. (1999). *On the Study of Watermarking Application in WWW.* Department of Electrical Engineering National Tsing Hua University. Available from: http://Amp.ece.cmu.edu/publication/Trista/ms_thesis_trista.pdf [20 March 2004]

Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y. & Collorec, R. (2000) *Relevance of Watermarking in Medical Imaging.* In Proceedings of 3rd Conference Information Technology Application in Biomedicine, ITAB, Airlington, USA, pp. 250-255

Coatrieux, G., Sankur, B. & Maitre, H. (1999). *Strict Integrity Control of Biomedical Images.* Available from: http://www.busim.ee.boun.edu.tr/~sankur/SankurFolder/SPIE_GC.pdf [13 February 2004]

Cox, I.J., Miller, M.L. & Bloom, J.A. (2002). *Digital Watermarking.* A Harcourt Science and Technology Company, USA: Academic Press

Delp, E.J. & Lin, E.T. (2000). *A Review of Data Hiding in Digital Images.* Available from: http://citeseer.nj.nec.com/cache/papers/cs/1313/ftp:zSzzSzskynet.ecn.purdue.eduzSzpubzSzdistzSzdelpzSzpics99-stegozSzpaper.pdf/lin99review.pdf [3 December 2003]

Derbel, N., Bouhlel, M.S., Kamoun, L. & Trichili, H. (2002). *A New Medical Image Watermarking Scheme for a Better Telediagnosis.* IEEE International Conference on Volume 1, pp. 556 – 559

Dittman, J. & Nack , F. (2000). *Copyright – copy wrong.* IEEE multimedia, vol. 7, No. 4, pp. 14-17

Flinn, P.J. & Jordan, J.M. (1997). *Using the RSA Algorithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?* Available from: http://www.cyberlaw.com/rsa.html [12 April 2004]

Fridrich, J. (1998). *Methods for Tamper Detection in Digital Images.* Available from: http://citeseer.nj.nec.com/405800.html [2 April 2004]

Giakoumaki, A., Pavlopoulos, S. & Koutsouris, D. (2003). *A Medical Image Watermarking Scheme Based on Wavelet Transform.* Proceeding of the 25th Annual International Conference of the IEEE EMBS, pp. 856-859

Hartung, F. & Kutter, M. (1999). *Multimedia Watermarking Techniques.* Available from: http://www.cosy.sbg.ac.at/~pmeerw/watermarking/ [12 October 2003]

Katzenbeisser, S. & Petitcolas, F.A.P. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking.* Norwood: Artech House, INC. MA 02062, pp. 97 – 99

Kong, X. & Feng, R. (2001). *Watermarking Medical Signals for Telemedicine.* IEEE Transactions on information technology in biomedicine, Vol. 5, No.3, pp. 195-201

Kutter, M., Bhattacharjee , S.K. & Ebrahimi, T. (1999). *Towards Second Generation Watermarking Schemes.* Int. Conf. on Image Processing, Vol.1, pp. 320-323

Kutter, M. & Petitcolas, F.A.P. (1999). *A Fair Benchmark for Image Watermarking Systems.* Available from: www.petitcolas.net/fabien/publications/ei99-benchmark.pdf [4 March 2004]

Lin, E.T. & Delp, E.J. (1999). *A Review of Fragile Image Watermarks.* Available from: http://citeseer.nj.nec.com/cache/papers/cs/14065/ftp:zSzzSzskynet.ecn.purdue.eduzSzpubzSzdistzSzdelpzSzacm99zSzpaper.pdf/lin99review.pdf [20 March 2004]

Liu, T., & Qiu, Z.D. (2002). *The Survey of Digital Watermarking-based Image Authentication Techniques*, Signal Processing, 2002 IEEE International Conference on, vol. 2, pp. 1556-1559

Macq, B. & Deweyand, F. (1999). *Trusted Headers for Medical Images.* Available from: http://www.lnt.de/~watermarking/speakers/macq/macqpaper.ps.gz [14 December 2003]

Miaou, S.G., Hsu, C.M., Tsai, Y.S. & Chao, H.M. (2000). *A Secure Data Hiding Technique with Heterogeneous Data-Combining Capability for Electronic Patient Records*. In Proceedings of the World Congress on Medical Physics and Biomedical Engineering, Session Electronic Healthcare Records, IEEE-EMB, Ed.,Chicago, USA, vol. 1, pp. 280-283

Mohanty, S.P. (1999). *Digital Watermarking: A Tutorial Review*. Available from: http://www.csee.usf.edu/~smohanty/research/Reports/WMSurvey1999Mohanty.pdf [10 October 2003]

NEMA (1993). *Standards Publication Digital Imaging and Communications in Medicine (DICOM)*. Available from: http://medical.nema.org [2 May 2004]

Paquet, A. (2001). *Multiresolution Watermark Based on Wavelet Transform for Digital Images*. Project report, University of British Columbia, Department of Electrical Engineering

Rajatasereekul, T. & Kiettrisalpipop, V. (2002). *RSA Encryption and Descryption using Matlab*. ECE575 Project, Oregon State University. Available from: http://islab.oregonstate.edu/koc/ece575/02Project/Kie+Raj/ [15 March 2004]

Salomaa, A. (1996). *Public-Key Cryptography*. Germany: Springer-Verlag Berlin Heidelberg, pp. 125-126

Skraparlis, D. (2003). *Design of an Efficient Authentication Method for Modern Image and Video*. Consumer Electronics, IEEE Transactions on, vol. 49, pp. 417-426

The Mathworks (2002). Matlab 6.5.1

Trichili, H., Bouhlel, M., Derbel, S.N. & Kamoun, L. (2002). *A Survey and Evaluation of Edge Detection Operators Application to Medical Images*. 2002 IEEE International Conference on vol. 4, pp. 4

Van Der Lubbe, J.C.A. (1998). *Basic Methods of Cryptography*. Cambridge: Cambridge University Press. pp. 131-133

Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J.J. & Su, J.K. (1999). *Attacks on Digital Watermarks: Classification, Estimation- Based Attacks and Benchmarks*. Available from: http://www.Int.de/~eggers/texte/IEEEcom2.pdf [12 April 2004]

VSOFTS Digital Video (1998). *PSNR Computation*. Available from: http://www.vsofts.com/codec/codec-psnr.html [12 April 2004]

Wakatani, A. (2002). *Digital Watermarking for ROI Medical Images by Using Compressed Signature Image*. Proceedings of the 35th Hawaii International Conference on System Sciences, pp. 2043-2048

Wolfgang, R.B., Podilchuk, C.I. & Delp, E.J. (1999). *Perceptual Watermarking for Digital Images and Video*. Proceedings of the IEEE, vol. 87, pp. 1108-1126