

Abstract of thesis presented to Senate of Universiti Putra Malaysia in fulfillment  
of the requirement for the degree of Master of Science

**FINGERPRINT IMAGE WATERMARKING USING ENCRYPTED  
IDENTIFICATION NUMBER**

By

**INTAN SHAFINAZ MUSTAFA**

**August 2006**

**Chairman: Associate Professor Abd Rahman Ramli, PhD**

**Faculty: Engineering**

Watermarking biometric data is growing importance and relatively new issue that used in authentication system. Watermarking is a technique of hiding specific data for copyright authentication. This data can be used to verify the ownership. Today, with the rapid growth of the Internet, the increased of functionality of computers and recent developments in fingerprint sensing technology for acquiring a fingerprint without using the traditional ink and paper make these image of biometric data (fingerprints) open to the potential attacks during transmission. Recipients required a mechanism which can prove the accuracy of their image. If the images are watermarked, it is easy for the owner to verify the images.

This thesis focuses on the study of watermarking on fingerprint images. A watermarking technique together with an encryption method to increase the security of the biometric data especially fingerprints is proposed. Digital watermark is used to embed information of the owner of the fingerprint image to protect the intellectual property rights of the fingerprint data. While encryption technique can be applied to the embedded information for increasing security.

Encryption is the commonest and easiest way to guarantee secure information. AES (Advance Encryption Standard) has been used in this project. AES is more reliable not only because its key size is variable over 128 bits but also enhanced transformation scheme is unpredictable at all.

This thesis provides a comprehensive discussion on the comparison of the digital watermarking techniques and their desirable features, common method of attacks such as translation, rotation, scaling, resizing, cropping, JPEG compression, noise addition, median filter, histogram equalization and gamma correction. Experimental results demonstrate that the frequency domain scheme is robust to most of the attacks.

Finally, with the application of watermarking method, in which a user's biometric data is hidden in the fingerprint image, combining the advantage of encryption system, the security of the biometric data should be thought of as the means to eliminate at least some of the attacks.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

**'WATERMARKING' IMEJ CAP JARI MENGGUNAKAN ENKRIPSI**

**NOMBOR PENGENALAN**

Oleh

**INTAN SHAFINAZ MUSTAFA**

**Ogos 2006**

**Pengerusi: Profesor Madya Abd Rahman Ramli, PhD**

**Fakulti: Kejuruteraan**

Data biometrik 'watermarking'(tanda air) sedang berkembang dan secara relatifnya produk baru yang boleh digunakan di dalam sistem pengenalan. Data ini boleh digunakan untuk mengesahkan kepunyaan (ownership). Hari ini, dengan pertumbuhan pesat internet, peningkatan fungsi komputer dan pembangunan terkini teknologi cap jari untuk meminta cap jari tanpa penggunaan dakwat tradisional dan kertas membuatkan imej data biometrik mempunyai peluang untuk serangan penghantaran. Penerima mengkehendaki satu mekanisma di mana dapat membuktikan secara tepat imej tersebut. Jika imej tersebut adalah ber'watermarked', ia adalah mudah bagi tuan punya untuk mengesahkan imej tersebut dengan bantuan mesin pengolah digital seperti komputer.

Justeru itu, tesis ini memfokuskan kajian terhadap imej cap jari yang di'watermarking'kan. Teknik 'watermarking' bersama dengan cara enkripsi untuk

meningkatkan keselamatan terutamanya biometrik data cap jari adalah yang dicadangkan. 'Watermark' merupakan suatu cara untuk menyembunyikan data atau informasi tertentu ke dalam suatu data digital lainnya. Tesis ini menumpukan kepada penggunaan teknik 'watermarking' ke atas imej cap jari dengan menyembunyikan informasi tuan punya imej cap jari bagi melindungi hak harta intelektual (Intellectual Property) dan juga demi keselamatan data tersebut.. Sementara itu, teknik enkripsi boleh diaplikasikan ke atas data tersebut sebelum proses 'watermarking' dilakukan bagi meningkatkan keselamatan.

Enkripsi adalah cara yang biasa dan mudah bagi memastikan keselamatan informasi. AES (Advance Encryption Standard) telah digunapakai dalam projek ini. AES adalah lebih relevan bukan kerana saiz kunci (key) adalah melebihi 128 bit tetapi juga skema transformasinya yang telah dikembangkan dan keputusannya adalah di luar jangkaan.

Perbandingan ke atas dua domain teknik 'watermarking' telah dikupas dan diperbincangkan dengan lebih terperinci. Kelebihan ciri-ciri teknik dan juga ketahanan 'watermarked' imej terhadap beberapa siri serangan juga dipersembahkan. Keputusan eksperimen menunjukkan domain frekuensi lebih tegar terhadap kebanyakan serangan yang diuji.

Akhirnya, dengan penggunaan cara 'watermarking' di mana data biometric pengguna adalah disembunyikan dalam imej cap jari, kelebihan system enkripsi

digabungkan, keselamatan data biometric dapat menghapuskan sekurang-kurangnya beberapa serangan ke atas imej cap jari.

## **DECLARATION**

I hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UPM or other institutions.

---

**INTAN SHAFINAZ MUSTAFA**

Date :

## **TABLE OF CONTENTS**

### **Page**

**ABSTRACT** ii

**ABSTRAK** iv

**ACKNOWLEDGEMENTS** vii

**APPROVAL** viii

**DECLARATION** x

**LIST OF TABLES** xiv

**LIST OF FIGURES** xv

**LIST OF ABBREVIATIONS** xx

## **CHAPTER**

### **1 INTRODUCTION**

1.0 General Overview 1.1

1.1 Motivation for Studying this Problem 1.2

1.2 Objectives 1.4

1.3 Scope of the Thesis 1.5

1.4 Contribution 1.7

1.5 Thesis Organization 1.8

### **2 LITERATURE REVIEW**

2.0 Overview 2.1

2.1 Watermarking 2.3

2.1.1 Definition of Digital Watermarking 2.4

2.1.2 History of Digital Watermarking 2.4

2.1.3	Types of Watermarking	2.6
2.1.4	Classes of Watermarking	2.9
2.1.5	Requirement of Digital Watermarking	2.11
2.1.6	Techniques of Digital Watermarking	2.13
2.1.7	Application of Digital Watermarking	2.23
2.2	Cryptography System	2.29
2.2.1	History of Cryptography	2.29
2.2.2	Properties of Cryptography	2.30
2.2.3	Symmetrical Key Cryptography	2.32
2.2.4	Public Key Cryptography	2.36
2.2.5	Introduction of AES Algorithm	2.39
2.3	Biometrics	2.45
2.3.1	Biometric System	2.45
2.3.2	Requirement of Biometric Identifiers	2.47
2.3.3	Biometrics System Performance	2.48
2.4	Fingerprint Biometrics	2.49
2.4.1	Fingerprint Image Capture	2.50
2.4.2	Fingerprint Representation	2.51
2.5	Digital Watermarking for Fingerprint Image Processing and Recognition	2.52
2.6	Review on Fingerprint Watermarking Techniques	2.53
2.7	Summary	2.59



## **3 METHODOLOGY**

3.0 Overview 3.1

3.1 Research Approach 3.1

3.1.1 Process Flow of the System 3.3

3.1.2 Selection of Programming Environment 3.4

3.2 Encryption of Text Message File 3.4

3.2.1 AES Implementation 3.6

3.3 Watermarking System 3.9

3.4 Implementation of Watermarking on Different Domain 3.10

3.5 Spatial Domain 3.11

3.5.1 Procedure for Embedding the Text Message 3.13

3.5.2 Procedure for Extracting the Text Message 3.16

3.6 Frequency Domain 3.18

3.6.1 The Discrete Fourier Transform 3.19

3.6.2 The Discrete Cosine Transform 3.25

3.6.3 The Discrete Wavelet Transform 3.29

3.7 Test Images 3.35

3.8 Visual Quality Metrics 3.43

3.9 Possible Attacks 3.45

3.9.1 Translation 3.46

3.9.2 Rotation 3.47

3.9.3 Scaling 3.47

3.9.4 Resizing of Resample 3.48

3.9.5 Cropping	3.48
3.9.6 JPEG Compression	3.49
3.9.7 Noise Addition	3.49
3.9.8 Median Filter	3.50
3.9.9 Histogram Equalization	3.51
3.9.10 Gamma Correction	3.51
3.10 Summary	3.52

## **4 RESULTS AND DISCUSSION**

4.0 Overview	4.1
4.1 Spatial Domain Watermarking Technique	4.1
4.2 Frequency Domain Watermarking Technique	4.6
4.2.1 Discrete Fourier Transform (DFT) Technique	4.7
4.2.2 Discrete Cosine Transform (DCT) Technique	4.13
4.2.2 Discrete Wavelet Transform (DWT) Technique	4.15
4.3 Visual Quality Metrics (Perceptual Quality)	4.26
4.4 Attacks	4.31
4.4.1 Translation	4.31
4.4.2 Rotation	4.34
4.4.3 Scaling	4.35
4.4.4 Resizing or Resample	4.37
4.4.5 Cropping	4.39
4.4.6 JPEG Compression	4.41
4.4.7 Noise Addition	4.43

4.4.8 Median Filter 4.50

4.4.9 Histogram Equalization 4.51

4.4.10 Gamma Correction 4.53

4.5 Summary 4.54

## **5 CONCLUSION AND FURTHER RESEARCH**

5.1 Conclusion 5.1

5.2 Further Research 5.3

**REFERENCES R1**

**APPENDICES A1**

**BIODATA OF THE AUTHOR B1**

## LIST OF TABLES

### Table Page

2.1 Quantization Values Used in JPEG Compression Scheme	2.19
2.2 AES Key Size	2.40
2.3 Look-up Table ( <i>S-box</i> )	2.44
2.4 Comparison of Performance of Various Biometric Technologies	2.49
4.1 PSNR, SNR and MSE Value for Varying $\alpha$	4.21
4.2 PSNR, SNR and MSE Value for Varying $\alpha$ (cont)	4.22
4.3 MSE of Watermarked Images Vs Original Images	4.27
4.4 SNR of Watermarked Images Vs Original Images (dB)	4.29
4.5 PSNR of Watermarked Images Vs Original Images (dB)	4.30
4.6 Resizing Impact on Bit Error Rate	4.38
4.7 Impact of Median Filter Attack Impact on Bit Error Rate	4.51
4.8 Impact of Median Filter Attack Impact on Bit Error Rate (cont)	4.51
4.9 Bit Error Rate (%) due to Histogram Equalization	4.52
4.10 Bit Error Rate (%) due to Gamma Correction Attack	4.53
4.11 Attack Performance Rating on a Scale from 1 to 5	4.55
4.12 Rating for Series Attacks	4.56
4.13 Rating for Watermarking Requirements	4.57

## **LIST OF FIGURES**

### **Figure Page**

- 1.1 Scope of Work 1.7
- 2.1 Example of Visible Watermark 2.7
- 2.2 Example of Invisible Watermark 2.8
- 2.3 Definition of DCT Region 2.18
- 2.4 2-Scale 2-Dimensional Discrete Wavelet Transform 2.20
- 2.5 Symmetrical Cryptography Analogy 2.33
- 2.6 Asymmetrical Cryptography Analogy 2.37
- 2.7 The Rijndael Algorithm Flowchart 2.41
- 2.8 The Enrolment Module and the Verification Module of a Biometric System 2.46
- 2.9 Fingerprint Image 2.50
- 2.10 Summary of Sonia's Proposal 2.54
- 2.11 WSQ Algorithm 2.56
- 2.12 Summary of Jain's Proposal 2.57
- 2.13 Steganography-based Minutiae Hiding 2.58
- 3.1 Proposed Fingerprint Watermarking System 3.2
- 3.2 The Flow of AES Text Encryption 3.5
- 3.3 Original Text to Plaintext 3.7
- 3.4 AES Demonstration 3.7
- 3.5 Main Program aes\_demo 3.8
- 3.6 Model of Implemented Watermarking System 3.9

3.7	Illustration of the Techniques Trees	3.10
3.8	The Scheme of the Embedding Process of the LSB Techniques	3.11
3.9	The Flow Chart of the LSB Embedding Techniques	3.15
3.10	The Flow Chart of the LSB Extracting Techniques	3.17
3.11	General Schematic Representation of Frequency Domain Watermarking Scheme	3.18
3.12	Original Image and 2D FFT of the Image	3.20
3.13	Mask of Ring with Encoded Data	3.21
3.14	The Flowchart of the DFT Embedding Techniques	3.22
3.15	The Flowchart of the DFT Extracting Techniques	3.34
3.16	The Flowchart of the DCT Embedding Techniques	3.28
3.17	Symlet (Sym8) Wavelet	3.29
3.18	DWT Transformed Image	3.30
3.19	The Flowchart of the DWT Embedding Techniques	3.32
3.20	The Flowchart of the DWT Extracting Techniques	3.34
3.21	Test Image JEN	3.36
3.22	Test Image HAN	3.38
3.23	Test Image NANI	3.39
3.24	Test Image SITI	3.40
3.25	Test Image FELIX	3.41
3.26	Test image IJA	3.42
3.27	Model of Watermarking Process	3.45
4.1	Original and Watermarked Image (LSB Techniques)	4.3

4.2 Original and Watermarked Image (LSB Techniques) - cont 4.4

4.3 Histogram Difference of JEN Image (Original and Watermarked Image – LSB 4.5

4.4 (a) DFT Magnitude of Original JEN; (b) Ring-Mask Created to Embed Watermark; (c) DFT Magnitude of Watermarked JEN 4.7

4.5 Distorted Image When Radius,R is Set Too Low 4.8

4.6 Impact on Bit Error Rate Sensitivity on Watermark Radius 4.9

4.7 Radius Impact on Image Quality 4.11

4.8 Radius Impact on MSE 4.11

4.9 Histogram Difference of The Original Image and Watermarked Image Using DFT Technique 4.12

4.10 DCT Implementation of Test Image JEN 4.13

4.11 Histogram Difference of The Original Image and Watermarked Image Using DCT Technique 4.14

4.12 One-Dimensional of The Wavelet Transform 4.15

4.13 Original and DWT Transformed Image 4.16

4.14 DWT Watermarking Technique by Taking One Coordinate of a Circle 4.17

4.15 (a) DWT Magnitude of Original JEN; (b) Ring-Mask Created to Embed Watermark; (c) DWT Magnitude of Watermarked JEN 4.18

4.16 DWT Watermarking Result 4.19

4.17 Effect on Test Image NANI on Varying Scaling Parameter,  $\alpha$  4.20

4.18 Impact on Varying Scaling Parameter on PSNR 4.23

- 4.19 Impact on Varying Scaling Parameter on SNR 4.23
- 4.20 Impact on Varying Scaling Parameter on MSE 4.24
- 4.21 Impact on Varying Scaling Parameter on Bit Error Rate 4.24
- 4.22 Histogram Difference of the Original Image and Watermarked Image using DWT Technique 4.25
- 4.23 MSE of Watermarked Images Versus Original Images 4.27
- 4.24 Simplified SNR of Watermarked Images Versus Original Images 4.29
- 4.25 Simplified PSNR of Watermarked Images Versus Original Images 4.30
- 4.26 Translation Attacks 4.31
- 4.27 Translation Impact on Watermarked Image 4.33
- 4.28 Rotation Attacks 4.34
- 4.29 Scaling Attacks 4.35
- 4.30 Scaling Attacks on Bit Error Rate 4.37
- 4.31 Resizing or Resampling Attacks 4.38
- 4.32 Cropping Attack Images 4.39
- 4.33 Cropping Attack on Bit Error Rate 4.40
- 4.34 JPEG Compression Attack on Image JEN 4.41
- 4.35 JPEG Compression Attack on Image NANI 4.41
- 4.36 Gaussian Noise 4.43
- 4.37 Salt and Pepper Noise 4.44
- 4.38 Speckle Noise 4.45
- 4.39 Gaussian Noise Addition Attack on Bit Error Rate 4.47
- 4.40 Salt and Pepper Noise Addition Attack on Bit Error Rate 4.48



4.41 Speckle Noise Addition Attack on Bit Error Rate 4.49

4.42 Median Filtering Attacks 4.50

4.43 Histogram Equalization Image Attacks 4.52

4.44 Gamma Correction Attacks 4.53

## **LIST OF ABBREVIATIONS**

3DES Triple Data Encryption Standard

AES Advance Encryption Standard

AFIS Automatic Fingerprint Identification System

AFRS Automatic Fingerprint Recognition System

ASCII American Standard Code for Information Interchange

ATM Automatic Teller Machine

BMP Bit Mapped Format Image

DCT Discrete Cosine Transform

DEA Data Encryption Algorithm

DES Data Encryption Standard

DFT Discrete Fourier Transform

DWT Discrete Wavelet Transform

FFT Fast Fourier Transform

FBI Federal Bureau of Investigation

GIF Graphics Interchange Format of Image

HVS Human Visual System

IBM International Business Machines Corporation

IC Identity Card

ID Identification

IDEA International Data Encryption Algorithm

IDWT Inverse Discrete Wavelet Transform

IP Initial Permutation

ISAC Information System Audit and Control

ISBN International Standard Book Number

ISRC International Standard Recording Code

JPEG Joint Photographic Experts Group

LSB Least Significant Bit

MPEG Moving Picture Experts Group

MSE Mean Square Error

NIST National Institute of Science and Technology

PDF Probability Density Function

PN Pseudorandom Number

PSNR Peak Signal to Noise Ratio

R Radius

RAM Random Access Memory

RC4 stream cipher designed by Rivest for RSA Data Security

RSA Rivest Shamir and Adleman

SNR Signal to Noise Ratio

TIF Tag Image File Format

WSQ Wavelet Scalar Quantization