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 increased a 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 unpredicted 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 hiding 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 of 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 (Intelectual 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 frekuenci 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

3 METHODOLOGY

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page

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