UNIVERSITI PUTRA MALAYSIA

SECURE ACCESS TO AUTHORIZED RESOURCES BASED ON FINGERPRINT AUTHENTICATION

AHMED BABA ELMADANI

FK 2003 17

SECURE ACCESS TO AUTHORIZED RESOURCES BASED ON FINGERPRINT AUTHENTICATION

By

AHMED BABA ELMADANI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirement for the Degree of Doctor of Philosophy

March 2003

UPM

DEDICATION

To the souls of my beloved father and mother in the heavens (Baba and Tabagort), who regretfully did not live to see this work, which resulted from their gift of many years of love, encourage and support to me.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement of the degree of Doctor of Philosophy

SECURE ACCESS TO AUTHORIZED RESOURCES BASED ON FINGERPRINT AUTHENTICATION

By

AHMED BABA ELMADANI

March 2003

Chairman: Veeraraghavan Prakash, Ph.D.

Faculty: Engineering

The Internet makes it convenient for anyone to access publicly available information on the servers. The increased functionality of computers and other technological equipment makes the connectivity easier than ever before, and the need for security more and more important. Passwords are frequently used to control access to restricted functions. Unfortunately, password or personal identification number (PIN) verification suffers an inherent problem. It cannot ensure that the user is the claimed individual. Higher security systems have now veered towards biometric verification in conjunction with passwords. Fingerprints are a practical bodily characteristic to use, as they are unique to each individual and easily collected using image-capture systems.

In this thesis, the methods of fingerprint recognition and classification are investigated. Then, the possible approaches to use are discussed while investigating

the subject. The final choice combines a feature-based and correlation-based approach.

The thesis proposes a novel method of allowing users access after authenticating them by their fingerprints. The method is based on a statistical approach, and is crafted in such a way that the authentication operations are inconspicuous to the user. All the required image processing techniques that make the extraction of the true fingerprint features easier are used: equalization, filtering, binarization and thinning.

A new method for constructing a unique key from the fingerprint image is also presented, with the fingerprint database (fingerprint features, unique fingerprint key, public and private keys) created shown. The database can be manipulated (insertion, retrieving, and deletion) rapidly using the Adelson Velskii and Landis (AVL) tree searching technique. The AVL tree is used to increase the compression ratio as its compression algorithm works efficiently for all types of data. The security is maintained and enhanced by adding a public key system.

Finally, a unique fingerprint based key is constructed using a user's fingerprint image and the key used to access and retrieve the private key. The method successfully recognizes the user fingerprint image even with noisy, translated or rotated images.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia bagi memenuhi syarat untuk mendapatkan ijazah Doktor Falsafah

SECURE ACCESS TO AUTHORIZED RESOURCES BASED ON FINGERPRINT AUTHENTICATION

Oleh

AHMED BABA ELMADANI

Mac 2003

Pengerusi: Veeraraghavan Prakash, Ph.D.

Fakulti: Kejuruteraan

Internet dapat memudahkan seseorang mencapai maklumat yang terkandung di dalam pelayan menggunakan teknologi web. Fungsi komputer dan peralatan teknologi lain yang semakin canggih telah membuatkan sambungan ke Internet menjadi lebih mudah. Kemudahan ini memerlukan ciri-ciri keselamatan agar sesuatu perkhidmatan boleh dipercayai oleh para pengguna.

Kata kunci adalah suatu kaedah yang biasa digunakan untuk menghadkan capaian kepada pengguna yang dibenarkan. Malangnya, pengesahan kata kunci atau PIN mempunyai satu kelemahan yang ketara. Kaedah ini gagal memastikan seseorang yang memasukkan kata kunci atau PIN adalah individu yang dimaksudkan. Sistem keselamatan yang lebih canggih masa kini menggunakan kaedah pengesahan biometrik bersama kata kunci sebagai penyelesaian. Pengesahan cap jari adalah pilihan yang sesuai disebabkan keunikannya dan ia senang diperolehi melalui sistem penangkapan imej.

Tesis ini menyiasat kaedah pengenalan cap jari dan klasifikasi. Kemudian penerangan mengenai pendekatan kajian dilakukan. Tesis ini menggabungkan kaedah pengecaman dan pengelasan cap jari.

Tesis ini mencadangkan suatu kaedah baru untuk memberikan capaian kepada pengguna selepas proses pengesahan menggunakan cap cari. Kaedah yang dicadangkan adalah berdasarkan pendekatan statistik. Pendekatan ini membolehkan operasi pengesahan adalah tersembunyi daripada pengguna sistem. Teknik-teknik pemprosesan imej yang membolehkan pengambilan ciri-ciri dengan lebih mudah telah digunakan seperti penyamaan (*equalization*), penapisan (*filtering*), penduaan (*binarization*) dan penipisan (*thinning*).

Suatu kaedah baru yang membina kekunci unik daripada imej cap jari dipersembahkan dan pengkalan cap jari yang mengandungi ciri-ciri cap jari, kekunci cap jari unik, kekunci awam dan rahsia ditunjukkan.

Maklumat di dalam pengkalan data dicapai secara pantas menggunakan kaedah pencarian pepokok Adelson Velskii dan Landis (AVL). Pepokok AVL digunakan untuk meningkatkan nisbah mampatan secara berkesan untuk sebarang jenis data. Keselamatan dicapai dengan bantuan sistem kekunci awam.

Keputusan seterusnya ialah kekunci unik berdasarkan cap jari telah dibina menggunakan imej cap jari pengguna dan digunakan untuk mencapai kekunci rahsia. Kaedah yang dicadangkan telah berjaya mengenalpasti cap jari pengguna walaupun daripada sumber imej yang mengandungi hingar, teralih atau terpusing.

ACKNOWLEDGMENTS

I would like to thank Allah (S.W.T.) for giving me this opportunity to continue my study and giving me the patience and perseverance to successfully complete my Ph.D. thesis.

I would like also to express my sincere thanks and profound appreciation to the chairman of my supervisory committee, Dr. Veeraraghavan Prakash for his guidance and discussion. Under his supervision, I have received heaps of assistance, who keep advising and commenting throughout this thesis until it turns to real success. Great appreciation is expressed to Dr. Abd Rahman Ramli, who is always present with his valuable remarks, help, advice, encouragement and being as group father in Multimedia and imaging Lab. I am also indebted to Prof. Dr. Borhanuddin Mohd. Ali, Prof. Dr. Kasmiran Jumari, my co-supervisors for their help and guidance. My appreciation and honest thanks to the Department of Computer and Communication Systems Engineering staff members.

Completing this research work owes much to my wife Khadija, for her encouragement and understanding, which made life easy throughout my study. I am very grateful to her. Last but not least, I would like to acknowledge my intimate and loving children, who also donated much time as they exerted great efforts concentrating on their own lessons.

Finally, most profound thanks go to the Libyan government represented by General Secretariat of Education for their financial support and to University Putra

Malaysia for giving me this opportunity to study in their prestigious and reputed institute, thanks to my lab mate Lawan, Jaker. Saiful, and Hanan for their help.

I certify that an Examination Committee met on 23rd June 2003 to condu examination of Ahmed Baba Elmadani on his Doctor of Philosophy thesis entitled "Secure Access to Authorized Resources Based on Fingerprint Authentication" in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the candidate be awarded the relevant degree. Members of the Examination Committee are as follows:

Adznan Jantan, Ph.D.
Associate Professor,
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Veerarghavan Prakash, Ph.D.
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Abdul Rahman Ramli, Ph.D.
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Borhanuddin Mohd. Ali, PhD.
Professor,
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Kasmiran Jumari, PhD.
Professor,
Department of Electronics, Electrical and Systems
Faculty of Engineering
Universiti Kebangsaan Malaysia
(Member)

Ashwani Kumar Ramani Ph.D.
Professor,
International Institute of Professional Studies
Devi Ahilya University INDIA
(Independent Examiner)

GULAM RUSUL RAHMAT ALI, Ph.D.
Professor/ Deputy Dean,
School of Graduate Studies,
Universiti Putra Malaysia

Date: 21 JUL 2003

This thesis submitted to the Senate of University Putra Malaysia has been accepted as fulfillment of the requirement for the Degree of Doctor of Philosophy. The members of Supervisory Committee are as follows:

Veerarghavan Prakash, Ph.D.
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Abdul Rahman Ramli, Ph.D.
Faculty of Engineering
Universiti Putra Malaysia
(Member)

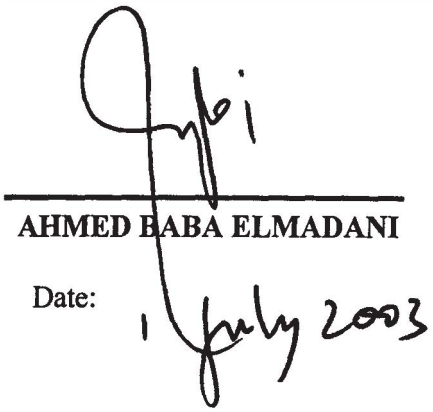
Borhanuddin Mohd. Ali, PhD.
Professor,
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Kasmiran Jumari, PhD.
Professor,
Department of Electronics, Electrical and Systems
Faculty of Engineering
Universiti Kebangsaan Malaysia
(Member)

AINI IDERIS, Ph.D.
Professor/ Dean,
School of Graduate Studies,
Universisti Putra Malaysia

Date: 15 AUG 2003

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.



AHMED BABA ELMADANI

Date: 1 July 2003

TABLE OF CONTENTS

		Page
DEDICATION		ii
ABSTRACT		iii
ABSRAK		v
ACKNOWLEDGEMENTS		vii
DECLARATION FORM		ix
LIST OF TABLES		xvi
LIST OF FIGRURES		xx
LIST OF ABBREVIATIONS		xxiv
CHAPTER		
1	**INTRODUCTION**	1.1
	1.1 Objectives	1.2
	1.2 Motivation for Studying this Problem	1.2
	1.3 Scope	1.5
	1.4 Thesis Organization	1.6
2	**LITREATURE REVIEW**	2.1
	2.1 Authentication	2.1
	2.1.1 Knowledge-based Authentication	2.3
	2.1.2 Token-based Authentication	2.4
	2.1.3 Biometric Based Authentication	2.5
	2.1.4 Password Based Authentication	2.5
	2.1.5 Smart Cards Based Authentication	2.6
	2.2 Encryption and Decryption Algorithms	2.10
	2.2.1 Symmetric Algorithms	2.12
	2.2.2 Asymmetric Algorithms	2.14
	2.2.3 Public Key Infrastructure (PKI)	2.15
	2.2.4 Advantage of Asymmetric Key Cryptography	2.18
	2.2.5 Need for Protecting Transferred Cryptographic Keys	2.19
	2.2.6 Secure Coprocessor	2.20
	2.3 Biometrics	2.20
	2.3.1 Biometric Types and Their Use	2.21
	2.3.2 Biometrics Security Systems	2.25
	2.3.3 Biometrics Systems Performance	2.26
	2.4 Authentication Using Fingerprint	2.26
	2.4.1 Fingerprint History	2.27
	2.4.2 Fingerprint Classification	2.30
	2.4.3 Fingerprint Authentication (Verification) Techniques	2.41
	2.4.4 Fingerprint Pattern-selection Techniques	2.43
	2.4.5 Fingerprint Template or Pattern Storage	2.44
	2.5 Fingerprint Image Processing	2.45
	2.5.1 Imaging	2.45

	2.5.2 Image Preprocessing	2.47
	2.5.3 Image Processing and Analysis	2.51
	2.5.4 Fingerprint Processing	2.57
	2.5.5 Fingerprint Feature Extraction	2.61
	2.5.6 Fingerprint Feature Types	2.62
	2.5.7 Singular Point Extraction Algorithms	2.64
	2.6 Fingerprint Matching Techniques	2.70
	2.7 Fingerprint Image Compression	2.73
	2.8 Tree Based Searching Algorithms	2.74
	2.8.1 Introduction to Trees	2.75
	2.8.2 Binary Tree Search Algorithm	2.75
	2.8.3 AVL Tree Searching Algorithm	2.76
	2.9 Discussion	2.78
	2.10 Conclusion	2.81
3	**METHODOLOGY**	3.1
	3.1 The System	3.1
	3.1.1 Process Flow of the System	3.4
	3.2 Generating Statistical Parameters from the User Fingerprint Image	3.6
	3.2.1 Fingerprint Processing	3.7
	3.2.2 Segmentation	3.11
	3.2.3 Fingerprint Class Assigning Procedure	3.12
	3.2.4 Fingerprint Feature Extraction	3.17
	3.3 User Keys Constructions and Generation	3.18
	3.3.1 Fingerprint Key (FP-key) Construction	3.19
	3.3.2 Public-Private Key	3.19
	3.4 Referenced User Fingerprint Image	3.20
	3.5 User Registry and Matching Procedure	3.21
	3.5.1 User Account Registry	3.22
	3.5.2 Users Database Manipulation	3.23
	3.6 Fingerprint Image Encryption and Compression	3.27
	3.7 Implementation Issues	3.28
	3.7.1 Hardware Requirements	3.28
	3.7.2 Software Requirements	3.29
	3.7.3 Application with Low Security	3.32
	3.7.4 Application with High Security	3.32
	3.8 Conclusion	3.32
4	**RESULTS AND DISCUSSION**	4.1
	4.1 Generating of Statistical Parameters from Fingerprint Images	4.1
	4.1.1 Fingerprint Processing	4.1
	4.1.2 Segmentation	4.9
	4.1.3 Fingerprint Feature Extraction	4.12
	4.2 User Keys Construction and Generation	4.25
	4.2.1 Fingerprint Key (FP-key) Construction	4.25

	4.2.2 Public-private key	4.25
	4.3 User Referenced Fingerprint Image	4.27
	4.4 User Database Manipulation	4.28
	4.4.1 Fingerprint Database Structure	4.28
	4.4.2 Search Algorithm	4.32
	4.4.3 Function of the Used Search Tool	4.33
	4.4.4 Reason for Choosing the Search Algorithm	4.36
	4.4.5 Insertion	4.38
	4.4.6 Locating a User Record	4.40
	4.4.7 Deleting a User Record	4.42
	4.5 User Registry and Matching in the Proposed System	4.44
	4.5.1 User Account Registry	4.44
	4.5.2 Extracting User Fingerprint Information	4.45
	4.5.3 Feature Matching	4.46
	4.5.4 Matching Portions of Images	4.46
	4.6 Giving a User Access to the Private key	4.46
	4.7 Encryption and Compression in the System	4.47
	4.7.1 Fingerprint Image Compression and Reduction of Resource Consumption	4.47
	4.7.2 Fingerprint Image Encryption	4.48
	4.8 Security Enhancement in the System	4.48
	4.9 Testing the System	4.49
	4.9.1 Testing Fingerprint Images from Web Sites	4.51
	4.9.2 Testing Rotated and Translated Fingerprint Images	4.61
	4.9.3 Giving the User Access to Private Key	4.76
	4.9.4 Average Time Taken by the System	4.76
	4.9.5 Recognized Fingerprint Images by the Proposed System	4.78
	4.9.6 User Acceptance-rejection and Security enhancement in the System	4.79
	4.10 Conclusion	4.82
5	**APPLICATION OF BIOMETRICS AUTHENTICATION AND SECURE COPROCESSOR**	5.1
	5.1 State of the Art	5.1
	5.2 Fingerprint Based Payment System Using PDA or Bluetooth.	5.2
	5.3 Fingerprint Based ATM Authentication Gelatin Protection.	5.3
	5.4 Fingerprint Based Online Payment System Using a Secure Coprocessor	5.3
	5.5 Fingerprint Based Authorized Gate	5.4
	5.6 Conclusion	5.4
6	**CONCLUSIONS AND FUTURE RECOMMENDATIONS**	6.1
	6.1 Conclusions	6.1
	6.2 Recommendations for Further Research	6.4

REFERENCES/BIBLIOGRAPHY R.1
APPENDICES A.1
BIODATA OF THE AUTHOR B.1

LIST OF TABLES

Table		Page
1.1	International biometric forum, consortium and biometric journals	1.3
2.1	Estimated times to spend for cracking known symmetric encryption algorithms	2.19
2.2	Biometrics Data Size per Record	2.27
2.3	Error rates for assigned classes of fingerprints	2.40
2.4	Error rates and testing combinations for fingerprint classifiers	2.40
2.5	Efficiency and errors from fingerprint classification systems in cases previously been published	2.40
2.6	Fingerprint extracting features methods	2.80
3.1	Fingerprint class assign based on the number of singular points and delta position.	3.15
3.2	FP-key data fields, user fingerprint unique key	3.19
3.3	Fingerprint-key file data field record	3.20
4.1	Quantized block directions into 4-directions	4.10
4.2	Feature ranges in the fingerprint classes	4.24
4.3	Comparing the system with other systems	4.25
4.4	Construction of User unique fingerprint key (FP-key)	4.25
4.5	Private-key file data record	4.27
4.6	Protected parts of the Fingerprint-key file data field record	4.27
4.7	Users database containing fingerprint-determined class and calculated features: Right-loop class	4.29
4.8	Users database containing fingerprint-determined class and calculated features: Arch class	4.29
4.9	Users database containing fingerprint-determined class and calculated features: Tented-arch class	4.30

4.10	Users database containing fingerprint-determined class and calculated features: Left-loop class	4.31
4.11	Users database containing fingerprint-determined class and calculated features: Whorl class	4.31
4.12	Fingerprint features for unknown Images used for testing Matching in the system	4.53
4.13	FP-key (unique fingerprint user key): calculated using features	4.54
4.14	Matched MSE calculated values for new arch image using stored information (file of Arch images)	4.56
4.15	Arch database: Results from matching two portions of images	4.55
4.16	Matching: MSE values for new Tented-arch images using stored information (file containing Tented-arch images).	4.57
4.17	Tented-arch database: Results from matching two portions of images	4.57
4.18	Matching: MSE values for new Left-loop images using stored information (file containing Left-loop images)	4.58
4.19	Left loop database: Results from matching two portions of images	4.58
4.20	Matching: MSE values for new Right-loop images using stored information (file containing Right-loop images)	4.59
4.21	Right loop database, Results from matching two portions of images	4.59
4.22	Matching: MSE values for new Whorl images using stored information (file containing Whorl images)	4.60
4.23	Whorl database: Results from matching two portions of images	4.61
4.24	Results of assigning fingerprint classes	4.63
4.25	Assigning new names to the fingerprint images	4.64
4.26	MSEs calculated for Y1 and Y2 fingerprint images (Tented arch)	4.65
4.27	Tented arch database refining and selection of proper images	4.65

4.28	Results of matching two portions from two images (Tented arch database)	4.66
4.29	MSEs calculated for Y3 and Y4 fingerprint images (left loop database)	4.66
4.30	MSEs calculated for Y5, Y6, Y7, Y8, and Y9 fingerprint images (Right loop database)	4.67
4.31	Right loop database refining and selection of proper fingerprint images	4.67
4.32	Results of matching two portions of two images (Right loop database)	4.68
4.33a	MSEs calculated for Y10, Y11, Y12, and Y13 fingerprint images (Whorl)	4.69
4.33b	MSEs calculated for Y10, Y11, Y12, and Y13 fingerprint images (Whorl)	4.70
4.34a	MSEs calculated for Y14, Y15, Y16, and Y17 fingerprint images (Whorl)	4.71
4.34b	MSEs calculated for Y14, Y15, Y16, and Y17 fingerprint images (Whorl)	4.72
4.35a	MSEs calculated for Y18, Y19, and Y20 fingerprint images (Whorl)	4.73
4.35b	MSEs calculated for Y18, Y19, and Y20 fingerprint images (Whorl)	4.74
4.36	Whorl database refining and selection of proper fingerprint images	4.75
4.37	Results of matching two portions of two images (Whorl database)	4.75
4.38	Average Time for processing a fingerprint by the system	4.77
4.39	Recognition and Error rates in the system (images received from web sites)	4.78
4.40	Recognition and Error rates in the system (captured images)	4.78
4.41	Recognition and Error rates in the system (used fingerprint images)	4.79

4.42	Three security levels used to test the system	4.81
4.43	Number of registered cases for FAR and FRR by the system	4.81

.

LIST OF FIGURES

Figure		Page
2.1	Authentication required for obtaining services	2.2
2.2	PKI Security architecture	2.17
2.3	Fingerprint Different Pattern	2.31
2.4	Graph based classification	2.35
2.5	Dynamic masks used for fingerprint classification	2.36
2.6	KL and MKL point fingerprint classification approach	2.36
2.7	Fingerprint edging: (a) Original image, (b) Image after removing insignificant parts, (c) image edge	2.51
2.8	Gray scale image and its thinned image.	2.61
2.9	Fingerprint orientation field and fingerprint points (Minutiae, Core and Delta).	2.63
2.10	Fingerprint singular points: (a) Core and (b) Delta	2.63
2.11	Sequence estimation of fingerprint singular point using filter-bank	2.69
2.12	Binary tree structure (a1 – a9 are nodes in binary tree)	2.76
2.13	Balancing of AVL Tree by so called RR rotation (r and x are nodes. T_1, T_2 and T_3 are weight, h is level. RR is right rotation)	2.77
3.1	Proposed Fingerprint Authentication System	3.3
3.2	Fingerprint processing algorithm in the system	3.7
3.3	FFT Wiener filter for enhancing image blocks	3.9
3.4	Orientation Field Computation	3.11
3.4a	Block (16x16 pixels matrix) and its center point $S(i, j)$	3.13
3.5	Middle-delta to the corresponding core determination algorithm	3.14

3.6	Fingerprint image class assigning	3.16
3.7	Fingerprint features extracted in the proposed system	3.18
3.8	FP-key construction procedure, security keys and fingerprint storage algorithm	3.21
3.9	Adding a new user to database	3.24
3.10	Retrieving user record from database	3.25
3.11	Implementation diagram of the proposed system	3.30
4.1	Samples of the fingerprint Images, (a) received from NIST and (b), (c) downloaded from Internet sites	4.2
4.2	Clockwise from top left: (a) original fingerprint image cropped, (b) Histogram of original image, (c) equalized image, and (d) histogram of the Equalized image.	4.3
4.3	Fingerprint image filtered with median filter and its histogram	4.4
4.4	A fingerprint image filtered with a FFT Wiener filter and its Histogram before and after equalization	4.5
4.5	Image interpolation using three different methods	4.6
4.6	Bilinear interpolation compared with other methods	4.7
4.7	Fingerprint original image and its binarized image	4.8
4.8	Thinning by three methods	4.8
4.9	Ranges of Means in the fingerprint classes	4.14
4.10	Ranges of Means in the tented-arch and whorl fingerprint classes	4.15
4.11	Ranges of Standard deviations in the fingerprint classes	4.16
4.12	Ranges of Standard deviations in tented-arch and whorl classes	4.16
4.13	Ranges of Variances in the fingerprint classes	4.17
4.14	Ranges of Variances in tented-arch and whorl classes	4.18

4.15	Ranges of Moments in the fingerprint classes	4.19
4.16	Ranges of Moments in tented-arch and whorl classes	4.20
4.17	Ranges of Coherence in fingerprint classes	4.20
4.18	Ranges of Coherence in tented-arch and whorl classes	4.21
4.19	Whorl class features: differentiating between two images	4.22
4.20	Tented-arch class features: differentiating between two images	4.22
4.21	Arch class features: differentiating between two images	4.23
4.22	Left-loop class features: differentiating between two images	4.23
4.23	Right-loop class features: differentiating between two images	4.24
4.24	Loading FP-key keys by the AVL tree	4.33
4.25	Balancing the AVL tree with right rotation	4.34
4.26	The AVL tree loading FP-key keys from the database	4.35
4.27	Balancing the AVL tree with left rotation	4.36
4.28	Loading the FP-key keys on AVL tree	4.37
4.29	Balancing the AVL tree using left rotation (Note: only two levels between the parental and child nodes)	4.37
4.30	User record insertion in a loaded AVL tree	4.38
4.31	Balancing the AVL tree by left rotation	4.39
4.32	Locating a user record using the AVL tree	4.41
4.33	Locating approximate records to the given FP-key using the AVL tree	4.42
4.34	Deleting a user record from the database using the AVL tree algorithm	4.43
4.35	Balancing the AVL tree after record deletion using right rotation	4.44

4.35a	Sequence of processing and matching new fingerprint image	4.50
4.36	Web fingerprint images used to test the system	4.52
4.37	Average Times taken for the different process in the system	4.77
4.38	False acceptance and false rejection rates resulted by the system	4.82

LIST OF SYMBLOS AND ABBREVIATIONS

FFT	Fast Fourier Transform
$F(u,v)$	Fourier Transform
$f(x,y)$	Inverse FFT
$g(x,y)$	The enhanced block
$G_x(i,j)$	Gradient of x-axis
$Gy(i,j)$	Gradient of y-axis
$\Phi(i,j)$	The direction of a block
I_c	Image with a length equals to 25 pixels
$S(i,j)$	Point in directional matrix
$C(i,j)$	Singular point
H	Directional core or delta point matrix
Pos	Position of delta with corresponding core
$Dist$	Distance between delta and corresponding core
ϖ	Mean feature
$\Re$	Standard deviation feature
η	Moment feature
δ	Variance feature
σ	Coherence feature
FP-Key	Unique fingerprint key
MSE	Mean squire error
CC	Correlation Coefficient
$PR1$	Captured image