DUAL MODEL FOR BIOMETRIC IDENTIFICATION SYSTEM

ALA ABDULHAKIM ABDULAZIZ

UNIVERSITI TEKNOLOGI MALAYSIA

UNIVERSITI TEKNOLOGI MALAYSIA

DECLARATION OF THESIS / UNDERGRADUATE PROJECT PAPER AND COPYRIGHT

Author's full name : ALA ABDULHAKIM ABDULAZIZ
Date of birth : 21/08/1986
Title : DUAL MODEL FOR BIOMETRIC IDENTIFICATION SYSTEM
Academic Session : 1, 2011/2012

I declare that this thesis is classified as :

\	**CONFIDENTIAL**	(Contains confidential information under the Official Secret Act 1972)*
\	**RESTRICTED**	(Contains restricted information as specified by the organization where research was done)*
\	**OPEN ACCESS**	I agree that my thesis to be published as online open access (full text)

I acknowledged that Universiti Teknologi Malaysia reserves the right as follows:

1. The thesis is the property of Universiti Teknologi Malaysia.
2. The Library of Universiti Teknologi Malaysia has the right to make copies for the Purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by :

SIGNATURE	**SIGNATURE OF SUPERVISOR**
01663069	Prof. Dr. Azizah Abd Manaf
(NEW IC NO. /PASSPORT NO.)	**NAME OF SUPERVISOR**
Date :	Date :

"I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of the degree of Master of Computer Science (Information Security)."

Signature	:	_____
Name of Supervisor	:	Prof. Dr. Azizah Abd Manaf
Date	:	3rd January, 2012

DUAL MODEL FOR BIOMETRIC IDENTIFICATION SYSTEM

ALA ABDULHAKIM ABDULAZIZ

A thesis submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

JANUARY 2012

I declare that this thesis entitled *"Dual Model for Biometric Identification System"* is the result of my own research except as cited in references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature	:	
Name	:	ALA ABDULHAKIM ABDULAZIZ
Date	:	03 JANUARY 2012

ACKNOWLEDGEMENT

First and foremost, I would like to express my utmost gratitude and appreciation to my supervisor, Prof. Dr. Azizah Bt Abdul Manaf. Because of her dedicated, and willing to help me, and willing to accept to become my supervisor. Also for her excellent guidance outstanding support, And for being patient with what I did and to advice me, on how I should proceed in this project.

Special thanks to Associate Professor Dr. Zuraini Ismail and Associate Professor Wardah binti Zainal Abidin, Dr. Bharanidharan Shanmugam and Dr. Mazdak Zamani for their comments that make this study more comprehensive and precious. I would like to extend my thanks to staff at UTM AIS for directly or indirectly extending their help during the work.

I also take this opportunity to give thanks for Wu zhili, Libor Masek, Manvjeet Kaur and Mukhwinder Sing for their fingerprint and iris algorithms implementation coding.

ABSTRACT

A biometric system which relies only on a single biometric identifier in making a personal identification is often not able to meet the desired performance requirements. Dual modal has great demands to overcome the issue involved in single biometric identifier. The use of personal identity verification systems with a serial architecture dual-modal biometrics has been proposed using fingerprint and iris pattern in order to increase the performance and security against environmental variations and fraudulent. The dual modal system is based on an empirical analysis of the fingerprint and iris images and it is split in several steps using local image properties. The fingerprint Minutiae extraction steps are loading the finger image, enhancement by histogram equalization and Fourier transform, binarization, segmentation by block direction estimation and region of interest extraction by morphological operations, remove H-break, remove spur, extract minutia and remove false minutia. At the same time, the iris system steps are capturing iris patterns, determine the location of the iris boundaries, converting the iris boundary to the stretched polar coordinate system, extracting the iris code. The dual modal system is achieved at the fingerprint matching score level less than 75%. The implementation of methods, algorithms and the graphical user interface was done by using MATLAB and CASIA database of 11 samples of fingerprint and iris data. Statistical Experimental used in this project on a small sample size, which is very difficult to conduct a full analysis of the observed results and consider as a main limitation of dual modal system. Future work can be done by performing the statistical experiments on a larger sample size, and conduct a full analysis of the observed results.

ABSTRAK

Sistem biometrik yang bergantung hanya pada satu identifikasi biometrik dalam membuat pengenalan peribadi sering tidak mampu untuk memenuhi keperluan prestasi yang diingini. Ragaman Dual mempunyai permintaan besar untuk mengatasi isu yang terlibat dalam pengecam biometrik tunggal. Penggunaan sistem pengesahan identiti peribadi dengan dwi-mod biometrik telah dicadangkan dengan senibina bersiri menggunakan cap jari dan corak iris untuk meningkatkan prestasi dan keselamatan terhadap perubahan alam sekitar dan penipuan. Sistem dua ragaman adalah berdasarkan analisis empirik cap jari dan imej iris dan berpecah dalam beberapa langkah yang menggunakan ciri-ciri imej tempatan. Langkah-langkah pengekstrakan detel cap jari memuatkan imej jari, peningkatan oleh penyamaan histogram dan jelmaan Fourier, binarization, segmentasi oleh anggaran arah blok dan rantau pengekstrakan kepentingan oleh operasi morfologi, mengeluarkan H-rehat, keluarkan merangsang, cabutan minutia dan keluarkan minutia palsu. Pada masa yang sama, langkah-langkah sistem iris menangkap corak iris, menentukan lokasi sempadan iris, mengubah sempadan iris kepada sistem koordinat kutub diregangkan, mengekstrak kod iris. Sistem dua mod dicapai pada tahap cap jari skor yang hampir sama kurang daripada 75%. Pelaksanaan kaedah, algoritma dan antara muka pengguna grafik yang telah dilakukan dengan menggunakan pangkalan data MATLAB dan CASIA 11 sampel cap jari dan data iris.Dari keputusan permerhatian yang dilakukan, uji kaji statistik ke atas saiz sampel yang kecil, adalah sukar untuk menganalisa keputusan yang diperolehi dan ianya merupakan keterbatasan ke atas ragaman dua sistem ini. Pada masa hadapan, diharap sampel uji kaji yang lebih besar dan analisa ke atas hasil keputusan dari pemerhatian dapat dijalankan dengan sepenuhnya.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

FAR	-	False Acceptance Rate
FRR	-	False Rejection Rate
PIN	-	Personal Identification Number
FFT	-	Fast Fourier Transform
MLP	-	Multilayer Perception
ROI	-	Region of Interest
HD	-	Hamming Distance
UML	-	Unified Modeling Language
Matlab	-	Matrix Laboratory
D	-	Distance Measured in Standard Deviations
μs	-	Mean of the Intra-class Distribution
μD	-	Mean of the Inter-class Distribution
ϵs	-	Standard Deviation of the Intra-class
ϵD	-	Inter-class Distributions

CHAPTER 1

INTRODUCTION

1.1 Introduction

Software and computer systems are recognized as a subset of simulated intelligent behaviors of human beings described by programmed instructive information. Biometric information system is one of the finest examples of computer system that tries to imitate the decisions that humans make in their everyday life, specifically concerning people identification and matching tasks. A biometric is a biological measurement of any human physiological or behavior characteristics that can be used to verify the identity of an individual (Wang, 2007).

The evolvements in science and technology have made it possible to use biometrics in applications where it is necessary to establish or verify the identity of individuals. Applications such as passenger control in airports, access control in restricted areas, border control, database access and financial services are some of the examples where the biometric technology has been applied for more reliable identification and verification.

For biometric applications that demand robustness and accuracy higher than that provided by any single biometric trait, Dual model biometric approaches often provide promising results. Dual model Biometric Authentication or Dual model Biometrics is the approach of using two biometric traits from a single user in an effort to improve the results of the authentication process.

In this project the researcher will develop dual model Biometrics identification system by using the fingerprint and iris recognition system. This system will provide robustness, accuracy, reliability, security and stability of the system over its individual unimodal components.

1.2 Overview of biometrics

A biometric provides automatic recognition of an individual based on his/her physical or behavior characteristics. Biometric offer several advantage over using ID cards or PIN numbers. There are so many advantages of the biometrics such as no need to memorize passwords, requires physical presence of the person to be identified , cannot be borrowed, stolen, or forgotten, cannot leave it at home and better than password/PIN or smart cards. Biometric systems have been developed based on facial features, voice, hand geometry, handwriting, the retina and the one presented in this thesis, fingerprints and iris.

1.2.1 Types of Biometrics

Biometric characteristics can be separated into two types:

i. Physiological characteristics

A biometric characteristic based primarily on an anatomical or biological characteristic, rather than a learned behavior. They are related to the shape of the body. The trait that has been used the longest, for over one hundred years, are fingerprints; other examples are face recognition, hand geometry and iris recognition (Ashbourn et al, 2004).

ii. Behavioral characteristics

A biometric characteristic that is learned and acquired over time rather than one based primarily on biology. They are related to the behavior of a person. The first characteristic to be used that is still widely used today is the signature, keystroke and voice (Ashbourn et al, 2004).

1.2.2 Modes by a biometric system

The biometric system has divided into two modes which are general biometric system and biometric system application. The two biometrics systems are explained briefly as follow:

i. General biometric system

Biometric system is an automated system capable of Capturing of biometric sample from an end user. Biometric system is also extracting and processing the biometric data from that sample. Furthermore, the biometric system is storing the extracted information in a database then comparing the biometric data with data contained in one or more references. Finally the biometric system is deciding how well they match and indicating whether or not an identification or verification of identity has been achieved (Jain etc al, 2004).

ii. Biometrics system application

Biometrics system has two type of application which are identification and verfication. However, the identification is a task where the biometric system searches a database for a reference matching a submitted biometric sample, and if found, returns a corresponding identity.in another hand, the verification is a task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample (biometric data) to one or more previously enrolled templates.

the section below is explain more about the two types of biometrics system (Jain etc al, 2004).

a. Identification

The identification method is selecting the correct identity of an unknown person from a database of registered identities. Furthermore, it is one too many matching process, because the system is asked to complete a comparison between the person's biometrics and all the biometric templates stored in a database. The system can take either the best match, or it can score the possible matches, and rank them in order of similarity (Jain etc al, 2004).

b. Verification

The verification method is verifying whether a person is who he or she claims to be. In another hand , It is one to one matching process, as the system has to complete a comparison between the person's biometric and only one chosen template stored in a centralized or a distributed database, e.g. directly on a chip for an identity document. Such a method is applied when the goal is to secure and restrict specific accesses with obviously cooperative users (Jain etc al, 2004).

1.3 Background of the Problem

With the rapid spread of information technologies, data processing and electronic transactions, strong need for new identification and verification practices has emerged. In today world a wide variety of applications requires reliable and secure authentication methods to confirm the identity of an individual requesting their service. In recent years, biometric authentication has seen considerable improvements in reliability and accuracy, with some biometrics offering reasonably good overall performance. The increasing demand of enhanced security systems has led to an unprecedented interest in biometric based person authentication system. Biometric systems based on single source of information are called unimodal systems.

i. Problem of single biometric System

Most of the biometric systems deployed in real world applications are unimodal which rely on the evidence of single source of information for authentication (e.g. fingerprint, face, iris, voice etc.). These systems are vulnerable to variety of problems such as noisy data, intra-class variations, inter-class similarities, non-universality and spoofing (Mane and Jadhav, 2009). It leads to considerably high false acceptance rate (FAR) and false rejection rate (FRR), limited discrimination capability, upper bound in performance and lack of permanence (Mane and Jadhav, 2009). However, even the new biometrics is still facing numerous problems, some of them inherent to the technology itself. In particular, biometric authentication systems generally suffer from enrollment problems due to non-universal biometric traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data acquisition in certain environments (Mane and Jadhav, 2009).

Hence, single biometric may not be able to achieve the desired performance requirement in real world applications. Furthermore, unimodal biometric systems rely on the evidence of only a single biometric trait. The problem that has been faced from a single biometric it has disadvantages regarding accuracy and performance (Maltoni and Cappelli, 2009)**.** Furthermore, Spoofing of biometric data is still facing numerous problems since it is far easier to spoof only one biometric trait (Maltoni and Cappelli, 2009)**.**

However, each biometric technology has its strengths and limitations, and no single biometric is expected to effectively satisfy the requirements of all verification or identification applications. A single biometric sometimes fails to be accurate enough for the identification of a large user population. Another disadvantage of using only one biometric is that the physical characteristics of a person for the selected biometric might not be always available or readable (Ko, 2005). Biometric systems based on one (one-modal) biometric are often not able to meet the desired performance requirements, and have to contend with a variety of problems such as noisy data, intra-class variations, restricted degree of freedom, non-university, spoof

attacks for example finger print spoofing with rubber and unacceptable error rates (Ko, 2005).

ii. Problem of Fingerprint System

Fingerprint recognition is still a complex and very challenging pattern recognition task, designing algorithms capable of extracting effective features and matching them in a robust way is very hard, especially in poor quality fingerprint images and when low-cost acquisition devices with a small area are adopted. One of the open issues in matching two fingerprint samples of the same finger is how to deal with the non-linear distortions, often produced by an incorrect finger placement of the finger over the sensing element, which make a global rigid comparison unfeasible (Maltoni and Cappelli, 2009).

One of the challenges of fingerprint technology is individuals that have poorly defined (or tenuous) ridges in their fingerprints. Furthermore, since the finger actually touches the scanning device, the surface can become oily and cloudy after repeated use and reduce the sensitivity and reliability of optical scanners. Furthermore, Fingerprints can be easily forged from touched surfaces and can be copied in a small amount of time using readily available materials (Kumar and Ryu, 2009).

iii. Problem of Iris System

Another type of access control deals with biometric information is iris biometrics. The iris system has some of the good aspect, but also has some of the disadvantage. The first advantage if the iris is uniqueness since every person has his own iris so it is impossible that two people has the same iris, even the twins don't have the same iris as well. The second advantage of iris is performance since the FAR AND FFR are very low because the scan s very accurate (Cavadini, et al 2008).

At the same time iris has some disadvantages. One of the disadvantage of iris recognition is the acceptability is very low, even if with modern technology an iris

could be photographed from 10cm to few meters away. Moreover, the second disadvantages of the iris if a person does not want to cooperate the iris reading procedure becomes very difficult or the image quality influences the FRR (Cavadini, et al 2008).

1.4 Problem Statement

With the rapid spread of information technologies, data processing and electronic transactions, strong need for new identification and verification practices has emerged. The problem that has been faced from a single biometric sometimes it fails to be accurate enough for the identification of a large user population (Mane and Jadhav, 2009). Furthermore, single biometric has variety of problems such as noisy data, intra-class variations, inter-class similarities, non-universality and spoofing (Mane and Jadhav, 2009). Hence, single biometric may not be able to achieve the desired performance requirement in real world applications (Mane and Jadhav, 2009).

Fingerprint is the newest and most rapidly-developing field of access control deals with biometric information. Since the finger actually touches the scanning device, the surface can become oily and cloudy after repeated use and reduce the sensitivity and reliability of optical scanners. Furthermore, fingerprints can be easily forged from touched surfaces and can be copied in a small amount of time using readily available materials (Kumar and Ryu 2009). Fingerprints can be affected by dirt, dryness and scarring (Maltoni and Cappelli, 2009).

Another type of access control deals with biometric information is iris biometrics. One of the disadvantage of iris recognition is the acceptability is very low, even if with modern technology an iris could be photographed from 10cm to few meters away. Moreover, the second disadvantages of the iris if a person doesn’t want to cooperate the iris reading procedure becomes very difficult or the image quality influences the FRR (Cavadini et al, 2008).

1.5 Research Questions

To develop a dual model biometric identification system it is important to know the following:

i. What are the multimodal biometric and the current research on biometrics?
ii. How can we develop the dual modals of biometrics to achieve reliable biometric system?
iii. How can we make sure the proposed model is working well?

First question answered in Literature review chapter, the rest of the questions which the first one regard how we can develop the dual modals of biometrics to achieve reliable biometric system the answer of it will be in proposed dual model for this project. And the question about How can we make sure the proposed model is working well the answer of it will be after implementing the proposed dual model then the researcher will perform testing.

1.6 Objectives

The objectives of this project are as follows:

i. To examine the multi-modal biometric identification system.

ii. To develop dual model biometric identification system by using serial architecture.

iii. To test dual modal biometric identification system.

1.7 Project Aim

The aim of this project is to examine on the multi-model biometric identification system. That offers reliability by using the fingerprint and iris recognition system. Furthermore, the second aim will be to create an open-source fingerprint and iris recognition system in order to verify the claimed performance of the technology. The development tool used will be MATLAB and use the well known database is the CASIA Iris Image Database (version 1.0) provided by the Chinese Academy of Sciences and UBIRIS Database. Finally, the last aim is to test and evaluate the fingerprint and iris recognition system. This project will tested using on CASIA database of grayscale eye and fingerprint images in order to verify the claimed performance of finger and iris recognition technology.

1.8 Project Scope

This study concerns on the nature of multi-model biometric in terms of its algorithm, techniques, methods and it is effectiveness. This project will also look at the different types of algorithm and techniques which have been implemented in fingerprint and iris. This project will be focus on various algorithm and techniques that have been utilized in order to impalement fingerprint and iris. In this project the researcher going to implement the fingerprint and iris based identification system for access control. However the implementation of methods, algorithms and the graphical user interface will be done using MATLAB and CASIA database of grayscale eye and fingerprint images in order to verify the claimed performance of finger and iris recognition technology.

1.9 Project Requirements

As long as the implementation of this project will be done by using MATLLab, the MATLAB tool is required in order to design and implement of methods, algorithms and the graphical user interface of this project as well as trying to verify the project is matching the objectives which this project has been designed aiming to achieve those objectives. In this project the researcher will use CASIA database of grayscale eye and fingerprint images in order to verify the claimed performance of finger and iris recognition technology.

1.10 Summary

This chapter provides a background on biometrics. The concept of biometrics is defined an automatic recognition of an individual based on his/her physical or behavior characteristics. Most of the biometric systems deployed in real world applications are unimodal which rely on the evidence of single source of information for authentication (e.g. fingerprint, face, iris, voice etc.). These systems are vulnerable to variety of problems such as noisy data, intra-class variations, inter-class similarities, non-universality and spoofing. A quick overview about the biometrics technique is clarified. The problem statement is declared and the objectives of this project are stated.

REFRENCES

Abbad, K. Assem, N. Tairi H. and, Aarab, A.(2010). *Fingerprint Matching Relying on Minutiae Hough Clusters.* ICGST - GVIP Journal, ISSN: 1687-398X, Volume 10, Issue 1.

Abhyankar,A. and Schuckers,S.(2010). *Novel Biorthogonal Wavelet based Iris Recognition for Robust Biometric System.* International Journal of Computer Theory and Engineering, Vol. 2, No. 2 1793-8201.

Adnan,W., Siang ,L.and Hitam ,S. (2004). Fingerprint recognition in wavelet domain . *Jurnal Teknologi*, 41(D) , 25–42.

Al-harby,F., Qahwaji,R. and Kamala, M. (2004). Secure Biometrics Authentication: A brief review of the Literature. *School of Informatics, University of Bradford BD7 1DP, UK 1-2*

Ashbourn,J.(2000). *Biometrics: Advanced Identity Verification: The Complete Guide*. Springer-Verlag, London.

Baig , A ., Bouridane , A . , Kurugollu,F. and Qu ,G .(2009). Fingerprint – iris fusion based identification system using a single hamming distance matcher. *International Journal of Bio- Science and Bio- Technology .1(1),*47.

Bubeck,M.U.(2003).*Multibiometric Authentication An Overview of Recent Developments.* San Diego State University.

Carrasco, M., Pizarro,L. and Mery, D.(2007). *Bimodal Biometric Person Identification System Under Perturbations.* Faculty of Mathematics and Computer Science Saarland University.

Cavadini,D. , Meier,A. and Fasel,D.(2008).Cimasoni,L.Introducing the BiometricalElectronic Passport (ePass). University of Fribourg.

Chandran, j . and Rajesh, R .(2009) . Performance analysis of multimodal biometric system authentication. IJCSNS *Journal of Computer Science and Network Security* ,9(3), 290 .

Chang, K. I., Bowyer,K. W. and Flynn,P. J.(2005). An evaluation of multi-modal 2D+3D face biometrics, IEEE Trans. on PAMI 27 (4), pp. 619-624.

Daugman,J. (2001). Statistical richness of visual phase information: Update on recognizing persons by their iris patterns. *International Journal of Computer Vision* 45(1): 25-38.

Denton, J. W., Peace, A.G. Selection and use of MySQL in a database management course. *Journal of Information Systems Education*, 14(4): 401–407.

Du,Y.E.(2006).Review of iris recognition: cameras, systems,and their applications. *Sensor Review*, 26 (1),66 – 69 .

EECE695C (2003). EECE695C – Adaptive Filtering and Neural Networks Fingerprint Identification. *American University of Beirut*. Retrieved March 2, 2011, from http://www.webfea.fea.aub.edu.lb/dsaf/labs/projectv1.1.pdf.

Hong,L., Wan,Y. and Jain,A.K.(1998). Fingerprint image enhancement: Algorithm and performance evaluation, IEEE Trans. Pattern Anal. Machine Intell, 20 (8), 777-789.

Jain, A. and Nandakumar, K.(2004). Local Correlation-based Fingerprint Matching. Michigan State University, MI 48824, U.S.A.

Jain, N., Bolle, R. and Pankanti, S.(2010). Introduction to biometrics. Michigan State University, 5-15.

Jain,A., Hong, L. and Boler,R.(1997).Online Fingerprint Verification, IEEE trans, PAMI-19, (4), pp. 302-314.

Jain,A.,Hong,L. andKulkarni,Y.(2010). A Personal Identification System Using Faces and Fingerprints. Department of Computer Science, Michigan State University, East Lansing, MI 48824.

Jain,K.,Ross,*A. and* Prabhakar,*S.(2004).* An Introduction to Biometric Recognition. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1.

Kau,M., Sing,M., Girdha,P., Sandh,P(2008). Fingerprint Verification System using Minutiae Extraction Technique, World Academy of Science, Engineering and Technology 46 2008.

Ko,T.(2005). Multimodal Biometric Identification for Large User Population Using Fingerprint, Face and Iris Recognition. Proceedings of the 34th Applied Imagery and Pattern Recognition Workshop (AIPR05) IEEE.

Kumar,D. and Ryu,Y.(2009). A Brief Introduction of Biometrics and Fingerprint Payment Technology.*Department of Computer Software Myongji University, Yongin-Si, Kyonggi-Do, South Korea 449-728,* 4

Kurt Bittner. *Use Case Modeling*. Addison-Wesley Longman Publishing:Boston- USA.2003

Lee,Y., Lee,K., Jee,H., Gil,Y.,Choi,W., Ahn,D. and Pan,S.(2005). *Fusion for Multimodal Biometric Identification*. The University of Suwon, Korea.

Maltoni,D. and Cappelli,R.(2007). Advances in fingerprint modeling. *Biometric System Laboratory – DEIS,* University of Bologna. Sincedirect.

Masek, L. (2003). *Recognition of Human Iris Patternsfor Biometric Identification.* Retrieved January 23, 2011, from http://www.csse.uwa.edu.au/~pk/studentprojects/libor/LiborM asekThesis.pdf

Masek,L.(2003). Recognition of Human Iris Patterns for Biometric Identification.*The University of Western Australia.*

Nain, N., Deepak, M., Kumar, D., Baswal,M. and Gautham, B.(2008). *Optimized Minutiae–Based Fingerprint Matching*. Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.

Object Management Group .*Unified Modelling Language Specification*. 1.3. USA. June 1999.

Paul,P. and Monwar,M(2007). *Human Iris Recognition for Biometric Identification. Ahsanullah University of Science and Technology*, Dhaka, Bangladesh 1-4244-1551-9/07 IEEE.

Prof Mane, M. and Prof Jadhav, V. (2009).*Review of Multimodal Biometrics: Applications, challenges and Research Areas.* International Journal of Biometrics and Bioinformatics (IJBB), Volume 3, Issue 5.

Vatsa,M.,Signh,R.and Gupta,P.(2004).comparison of iris recognition algoritms, IEEE ICISIP, 0-7803-8243-9/04.

Wang,Y. (2007). The theoretical framework of cognitive informatics. *Int. J. Cognit. Informat. Nat. Intell.*, vol. 1, no. 1, pp. 10–22.

Wayman,J.L. and Alyea,L. (2000). *Picking the Best Biometric for Your Applications*, in *National Biometric Test Center Collected Works*. National Biometric Test Center: San Jose. p. 269-275.

Wuzhili,Z (2002). Fingerprint recognition. Hong Kong Baptist University 2002.