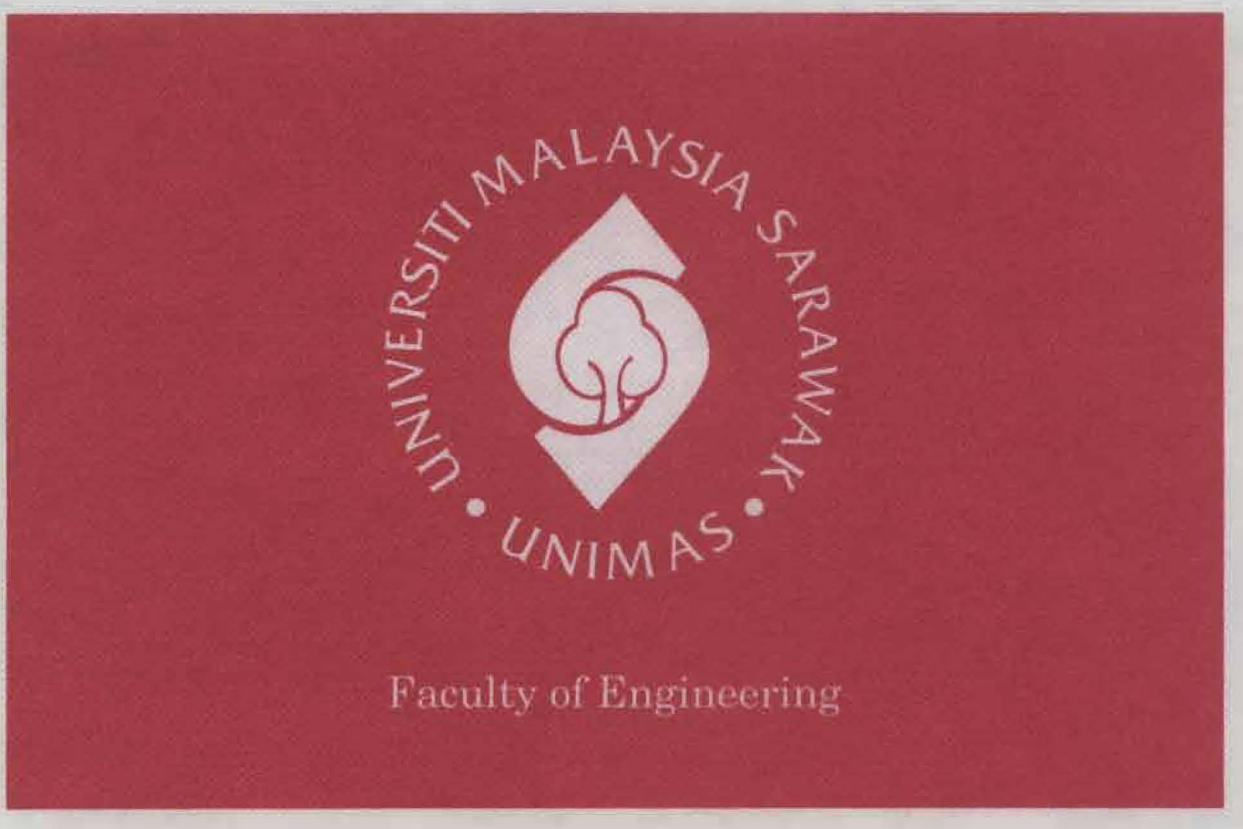

MULTIMODAL BIOMETRICS TECHNIQUE FOR PERSONAL AUTHENTICATION

Ainur Idayu Binti Tumingan

Bachelor of Engineering with Honours
(Electronics and Computer Engineering)
2010

UNIVERSITI MALAYSIA SARAWAK

R13a

BORANG PENGESAHAN STATUS TESIS

Judul: **MULTIMODAL BIOMETRICS TECHNIQUE FOR PERSONAL AUTHENTICATION**

SESI PENGAJIAN: 2009/2010

Saya **AINUR IDAYU BINTI TUMINGAN**
(HURUF BESAR)

mengaku membenarkan tesis * ini disimpan di Pusat Khidmat Maklumat Akademik, Universiti Malaysia Sarawak dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Universiti Malaysia Sarawak.
2. Pusat Khidmat Maklumat Akademik, Universiti Malaysia Sarawak dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Membuat pendigitan untuk membangunkan Pangkalan Data Kandungan Tempatan.
4. Pusat Khidmat Maklumat Akademik, Universiti Malaysia Sarawak dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
5. ** Sila tandakan (✓) di kotak yang berkenaan

☐	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972).
☐	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/ badan di mana penyelidikan dijalankan).
☑	TIDAK TERHAD	

(TANDATANGAN PENULIS)

Alamat tetap: NO. 2, JALAN 11, TAMAN CEMPAKA SARI, 45620 IJOK, SELANGOR DARUL EHSAN

Tarikh: _____

Disahkan oleh

(TANDATANGAN PENYELIA)

MR. TENGKU MOHD AFENDI BIN ZULCAFFLE
Nama Penyelia

Tarikh: 12/5/2010

CATATAN

* Tesis dimaksudkan sebagai tesis bagi Ijazah Doktor Falsafah, Sarjana dan Sarjana Muda.

** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh tesis ini perlu dikelaskan sebagai SULIT dan TERHAD.

This Final Year Project attached here:

Title	: MULTIMODAL BIOMETRICS TECHNIQUE FOR PERSONAL AUTHENTICATION
Student Name	: AINUR IDAYU BINTI TUMINGAN
Matric No	: 17665

has been read and approved by:

b/p

12/5/2010

Mr. Tengku Mohd Afendi Zulcaffle

(Supervisor)

Date

MULTIMODAL BIOMETRICS TECHNIQUE FOR PERSONAL AUTHENTICATION

AINUR IDAYU BINTI TUMINGAN

A Thesis Submitted to

Faculty of Engineering, Universiti Malaysia Sarawak

in Fulfillment of the Requirements

for the Award of the Bachelor Degree

with Honors (Electronic and Computer Engineering) 2010

To my lovely mom and dad

ACKNOWLEDGEMENT

First, I would like to thankful to God as He grants grace, wisdom and patience to accomplish this research. I would like to express my gratitude to my supervisor, Mr. Tengku Mohd Afendi Bin Zulcaffle for the support he has extended to me throughout my work towards this thesis, and for his informed guidance and advice. I also would like to thanks to MR. Ir. David Bong Boon Liang for the he assist and support me on doing this project.

I also extend my sincere gratitude to my lovely parents, my brothers and sister for their unshakable faith in me and for unconditional support and encouragement to pursue my dreams.

Lastly, I offer my regards and blessings to all of those who supported me in any respect during the completion of this project.

ABSTRAK

Teknologi biometrik merujuk kepada teknologi di mana ia mengukur dan menganalisa ciri-ciri fizikal dan kelakuan manusia untuk tujuan pengecaman dan pengesahan. Sistem rantaian modus biometrik merupakan sistem yang lebih dipercayai dan memberikan prestasi yang lebih baik berbanding penggunaan satu modus biometrik. Kertas kerja ini mencadangkan gabungan pengecaman muka dan cap jari sebagai sistem rangkaian modus. Rekabentuk sistem pengesahan ini mengandungi dua peringkat utama iaitu fasa pendaftaran dan fasa pengesahan. Setiap sistem pengesahan ini menggunakan sepenuhnya kaedah Analisis Komponen Utama (PCA) untuk mendapatkan unjuran linear ruang imej sebenar bagi mencapai pengurangan dimensi. Jaringan Saraf Backpropagation (BP-ANN) diaplikasikan dalam projek ini untuk tujuan proses latihan dan pemadanan. BP-ANN adalah yang paling popular digunakan dalam sistem pembuktian.

ABSTRACT

Biometric technology are refers to technologies that measure and analyze human physical and behavioral characteristics for recognition and authentication purpose. A multimodal biometrics system is more reliable and provided better performance than uni-modal biometric. This paper proposes a multimodal biometric systems using face and fingerprint recognition. The design of a verification system consists of two major stages which are enrollment phase and verification phase. Each verification system completely used a Principal Component Analysis (PCA) method to apply linear projection to the original image space to achieve dimensionality reduction. Backpropagation Neural Network (BP-ANN) is adopted in this project for training and matching process. BP-ANN is the most popular used in verification systems.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AFIS	-	Automated Fingerprint Identification Services
AFIVS	-	Automatic Fingerprint Identification And Verification Systems
ANN	-	Artificial Neural Network
BP	-	Backpropagation
BP-ANN	-	Backpropagation Artificial Neural Network
DNA	-	Deoxyribonucleic Acid
FAR	-	False Acceptance Rates
FRR	-	False Rejection Rates
FRS	-	Face Recognition Systems
FYP	-	Final Year Project
IAFIS	-	Integrated Automated Fingerprint Identification Ser
JPEG	-	Joint Photographic Experts Group
LDA	-	Linear Discriminate Analysis
MATLAB	-	Mathematics Laboratory
MIT	-	Massachusetts Institute of Technology
MBP-ANN	-	Momentum Back-propagation
MRTD	-	Machine Readable Table Documents
NN	-	Neural Network
PCA	-	Principal Component Analysis
PIN	-	Personal Identification Numbers
RGB	-	Red Green Blue

CHAPTER 1

INTRODUCTION

1.1 Biometrics Technologies

Biometric recognition is defined as the automatic recognition of individuals based on their physiological/biological or behavioral characteristics [1]. Physiological biometrics is based upon physiology characteristics such as fingerprint, hand geometry, iris, face, retina, and palm vein. While, behavioral biometrics is traits based on data derived from physiology characteristics which are voice recognition, keystroke recognition, signature recognition and DNA biometrics.

Biometrics technologies are concerned with the physical parts of human body or the personal traits of human beings, and the recognition of individuals based on human traits. This technology acts as a front end to a system that requires precise identification before it can be accessed or used.

Multimodal biometrics is combinations of two or more biometric recognition technologies. By using more than one of biometric recognitions, it can operate effectively and more secure to prevent an impostor. It also more reliable and provide better performance than any individual biometrics. This is because a single biometric feature may fail to be accurate enough for identification or verification [2].

Multimodal biometric systems can address the problem of non-universality, since multiple traits ensure sufficient population coverage. Furthermore, it could provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometrics traits of legitimate user.

1.2 Problem Statement

Traditionally, user authenticates based on authentication mechanisms either "something you know" which usually refer to passwords and personal identification numbers (PINs) or "something you have" which usually refer to cards or token [3]. This authentication mechanisms needed user to memorizes a password or PIN also need to brings anyway the token or cards with. These approaches have a number of significant drawbacks. The used of password or PINs are easily guessed, forgotten or compromised, and also for tokens or cards can be stolen or misplaced [4]. Therefore, by using the biometrics authentication which "something you are", it can provide a high degree of security and it convenience for personal authentications.

However, using a single biometric trait for authentication purposes has some limitation [5], as an example, for identical twins. Their faces alone may not distinguish them. Another disadvantage of using only one biometrics is that the chosen biometrics is not always readable, as an example, some people have fingerprints that cannot be recorded because they are obscured by a cut or a scar or arc too fine to show up well in a photograph [6]. Thus, the noisy data, limited degrees of freedom, performance limitation, circumvention via spoofing, and non-

universality all affect the performance, security, and convenience of using such a system [7].

1.3 Motivation

I'm interested in doing this project because most of current verification systems are using the traditional authentication system such as password/PINs or cards. These make them susceptible to problems such as forgetting the password and cards being stolen. One way to overcome these problems is to employ biometrics for authentication. However, verification methods based on a single biometric trait or algorithm may not provide adequate verification performance. For example, some face recognition algorithm cannot perform effectively. We need to verify which better performance algorithm in verification systems. It also in some cases, one biometric may not be applicable at all. For example, some people don't have good enough ridges in their fingerprints to be able to use fingerprint verification systems. Thus, when combined both biometrics, it could improve the accuracy of a biometric system. Therefore, we believe that by using multimodal biometrics, we will achieve not only improved security, but it also reliable and convenience for any people and applications.

1.4 Project Overview

This project is about the multimodal biometrics technique in used for personal authentication. From the evaluation, notice that the fingerprint and face recognition have a very good balance performance. Thus, the fingerprint and face identifier can form a good combination for a multimodal biometric systems. The fingerprint recognition uses the impression made by the unique, minutiae, ridge formations or patterns found on the fingertips. Due to the lack of fund, fingerprint is scanned by using an ink printed fingerprint and then the scanned image is processed to enhance the image. Thus it would useful to extract the features. In face recognition, face is captured by using camera to extract the features. Face recognition system mostly are based on eigenface method and local feature analysis. Both of this input features are manipulated by using neural network. These features then store on the database. By using the Artificial Neural Network, it performs by matching both features to the claimant stored database. The interface and the processing part are done using MATLAB, which is very powerful mathematics and engineering software.

1.5 Project Objectives

The aim of the project is to develop an algorithm that can authenticate a person based on multimodal biometric technique.

At the end of this project, I will be able to achieve this objective:

- To develop a multimodal verification algorithm using fingerprint and face images
- To apply image processing and neural network techniques in multimodal verification.
- To analyze the performance of neural network in multimodal verification
- To verify and evaluate this multimodal verification performances

1.6 Project Outlines

Chapter 1 – This chapter is the introduction to the project with project overview that briefly describes the multimodal biometrics for personal authentication. This chapter also contains problems statement, project objectives and project outlines.

Chapter 2 – The chapter contains literature reviews regarding multimodal biometrics which are combination of fingerprint and face recognition. There are two main part of explanation which in image processing and neural network method. The

image enhancement methods, such a filtering and feature extraction are explained. Types of neural network will also be explained briefly.

Chapter 3 – Research methodology is presented in this chapter. The chapter consists of two major stages which are enrollment stage and verification stage. Each stage is divided into four parts which are image acquisition stage, preprocessing stage, features extraction (fingerprint features and face features) stage and training and matching stage. All stages are covered briefly.

Chapter 4 – This chapter is presents the results and analysis of the project. Experiment is done on the fingerprint and face recognition system and the performance of the system are recorded. Analysis on the performance is done and followed by discussion on the results.

Chapter 5 – The conclusion is drawn based on the whole project and the results of the system. The limitations of the project are elaborated. Furthermore, recommendation is given to improve the system further as well as for future works.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

In this chapter, proposed summary of the previous research on the multimodal biometrics by surveying scholarly papers, conference proceedings and websites that relevant to this area of research. The purposes of this project that to develop an algorithm that can authenticate a person based on multimodal biometrics technique. This chapter closely examined the works that have been conducted in order to understand and investigate the research problem. It is needed to evaluate relevant researches on this topic to show the relationships between different works, how they related to this topic and how there researches can be used in multimodal techniques.

This chapter also presents the comparative better performance in biometric technologies, to produce a high accuracy and reliability systems.

2.2 Overview of Biometrics

The terms of "biometrics" is derived from the Greek words "bio" (life) and "metric" (to measure) [8]. Biometrics refers to technologies for measuring and analyzing a human's physiological or behavioral characteristics. Human biometric characteristics are unique, so it can hardly duplicate [9]. Automated biometric systems have only become available over the last few decades, due to significant advances in field of computer processing. Many of these new automated techniques, however, are based on ideas that were originally conceived hundreds, even thousands of years ago.

In the nineteenth century, law enforcement professionals and researchers, spurred by the need to identify recidivist criminals, was tried to find better ways to identify people. Alphonse Bertillon, is a chief of the criminal identification division of the police department in France, was developed anthropometrics to identify person by using a number of the human body measurements. These measurements were written on cards that could be sorted by height, the length of one foot, arm length or any other parameter. After Bertillon method discovery, the other approach was use fingerprint to recognized dependable identifiers for law enforcement purposes [10]. In the latter of the twentieth century, the true biometrics system was began coincide with the emergence of computer systems. The nascent field experienced an explosion of activity in the 1990s and began to surface in everyday applications in the early 2000s.

2.2.1 Types of Biometrics Technologies

Biometrics is classified into two categories which is passive biometrics and active biometrics. Passive biometric are generally referred to as covert. These types of system are recognizes people without their knowledge or cooperation. Generally, it used in surveillance applications. Examples of passive biometrics are comprises of face recognition, voice recognition and gait recognition. Actives biometrics, on the other hand, required the cooperation of the subject. These types of systems are generally referred to as overt. It generally used in applications that authenticate a user's identity. Examples of these methods include fingerprint authentication, hand geometry authentication, retinal and iris authentication. [11]

According to [12], in biometrics technology there is no single best performance in which can serve all applications in every situation. The effectiveness of a biometric technology is dependent on various factors including location, security risks, task (identification or verification), size of users and other circumstances. Each biometric modality varies in the technology maturity with its own strength and weaknesses that should be evaluated in relation to the application before implementation. Table 2.1 shows the strength and weaknesses of most biometrics.