Information Fusion of Face and Palm-print Multimodal Biometric at Matching Score Level

by

Mohammed Elzaroug Alshrief

(1432321182)

A dissertation submitted in partial fulfillment of the requirements for the degree of Master of Science (Embedded System Design Engineering)

School of Computer and Communication

UNIVERSITI MALAYSIA PERLIS

2014

ACKNOWLEDGMENT

First and foremost, **Alhamdulillah**, the creator, the cherisher, the most wise, the lord of the world. I am extremely thankful to almighty Allah for giving me the chance, strength and courage to complete this work, and without his willing, this thesis would not have been possible.

I would like to express my utmost and deepest gratitude to my advisor, **Dr. Muhammad Imran Ahmad**, for his guidance in academic research and his support in daily life. He has widened my view in research areas, especially in biometrics and image and signal processing. His motivation and support have guided me towards the successful completion of my thesis.

I would like to convey my deepest gratitude and thanks to my family (**my parents, my brothers and sisters**) for their support spiritually and financially in order to finish this project.

I would also like to extend my gratefulness to my entire friends and staff in the **School of Computer and Communication**, UniMAP for their full support to me all these while. Last but absolutely not least, my heartfelt thanks to all those who I forgot but who nevertheless deserve to be thanked.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ATM	Automatic Telling Machines
DWT	Discrete Wavelet transform
ED	Euclidean distance
EER	Equal Error Rate
FAR	False Acceptance Rate
FKP	finger knuckle print
FRR	False Rejection Rate
GAR	Genuine Acceptance Rate
LDA	Linear Discrimination Analysis
PCA	Principle Components Analysis
PIN	Personal Identification Number
PolyU	Poly Technique University
PSO	Particle Swarm Optimization
RBF	Radial Basis Function
RGB	Red, Green, Blue
ROI	Region of Interest
ORL	Olivetti Research Laboratory
SVM	Support Vector Machine

Integrasi Maklumat Biometrik Multimodal Muka Dan Tapak Tangan Pada Tahap Persamaan Skor

ABSTRAK

Sistem biometrik pelbagai mod yang mengintegrasikan ciri-ciri biometrik daripada beberapa input yang dapat mengatasi kekurangan biometrik mod tunggal. Teknik ini menggabungkan maklumat di peringkat pertengahan dengan menyatukan maklumat yang diberikan oleh input biometrik yang berbeza dan boleh memberikan hasil yang lebih baik kerana terdapat maklumat tambahan pada peringkat ini. Dalam tesis ini, gabungan maklumat di peringkat persamaan skor digunakan untuk mengabungkan gambar muka dan tapak tangan . Tiga jenis penggabungan skor yang digunakan adalah sum , product dan minimum. Satu kaedah unjuran statistik linear berdasarkan analisis komponen prinsip (PCA) digunakan untuk memberi maklumat penting dan mengurangkan dimensi vektor. Proses gabungan dilakukan dengan menggunakan skor padanan yang dihasilkan oleh Euclidean distance classifier. Eksperimen ini dijalankan dengan menggunakan dua penanda aras dataset iaitu ORL dan PolyU untuk memeriksa kadar pengecaman. Kadar pengecaman terbaik adalah 98.96 % yang boleh dicapai apabila menggunakan kaedah gabungan sum . Kadar pengecaman juga boleh diperbaiki dengan meningkatkan bilangan imej latihan dan bilangan pekali PCA.

Information Fusion of Face and Palm-print Multimodal Biometric at Matching Score Level

ABSTRACT

Multimodal biometric systems that integrate the biometric traits from several modalities are able to overcome the limitations of single modal biometrics. Fusing the information at the middle stage by consolidating the information given by different traits can give a better result due to the richness of information at this stage. In this thesis, an information fusion at matching score level is used to integrate face and palm-print modalities. Three types of matching score rule are used which is sum, product and minimum rule. A linear statistical projection method based on the principle component analysis (PCA) is used to capture the important information and reduce feature dimension in the feature space. A fusion process is performed using matching score computed using Euclidean distance classifier. The experiment is conducted using a benchmark ORL face and PolyU palm-print dataset to examine the recognition rates of the propose technique. The best recognition rate is 98.96% achieved by using sum rule fusion method. Recognition rate can also be improved by increasing number of training images and number of PCA coefficients.

CHAPTER 1

INTRODUCTION

1.1 Background

Identity management is the challenges faced in the provision of authorized users with a secure and easy access to information and services across several security systems. Reliability of identity management is an important component of several applications that render their services only to authentic users. Telebanking, the control of physical access, computer systems, laptops, and automatic teller machines (ATMs) are important examples of such applications. Traditional approaches make use of passwords, personal cards, PIN numbers and keys to achieve verification. However, one can easily loose, forget or mistakenly disclose the proxy representation of these identities. Therefore, they are not regarded in the modern day world as sufficient form of identity confirmation. In addition, an authentic user may not easily recall his/her password while easy passwords are easier for an imposter to guess. Thus, a dependable and natural authentication method that helps in avoiding the problems associated with conventional methods are provided by the biometrics. Biometrics provides for an establishment of identity base on who a user is rather than what the user possess such as an identification card or what is remembered by the user such as the user's password.

A biometric identification system is defined as the recognition of individual through the use of information about specific physical characteristics or personal attributes held in a database. The achievement of recognition could be attained by

measuring certain attributes using three different categories which are: intrinsic; extrinsic; and hybrid biometric. Individual generic make-up are identified in the intrinsic biometric. Finger prints and iris pattern are good examples of intrinsic biometric. The behaviours such as signatures and the keystrokes that are learnt by the users are regarded as the extrinsic biometrics. While the hybrids biometric combines the physical characteristics of individuals and the personal attributes like the voice (Prabhakar, *et.al* 2003; Ross, *et.al* 2004).

The biometric systems are becoming one of the fastest growing personal identification systems, thanks to their high precision and accuracy in individual identification by using the physiological and behavioural characteristics of individuals. They overcome the limitations of token-based and knowledge-based identification systems. Biometrics is classified into two main groups: 1) physiological: which is based on the person's behavioral traits such as the gait, voice, keystrokes and signature. And 2) behavioural: which relies on the person's physiological traits. These traits include face, palm-print, fingerprint, iris, retina, hand geometry and DNA. Figure 1.1 gives a summary of the various biometric traits currently in use with biometric systems. Moreover, biometric systems are considered as patterns of recognition systems that process such traits to identify the person based on a prior knowledge of his specific biometric data (Ross, *et.al* 2011).

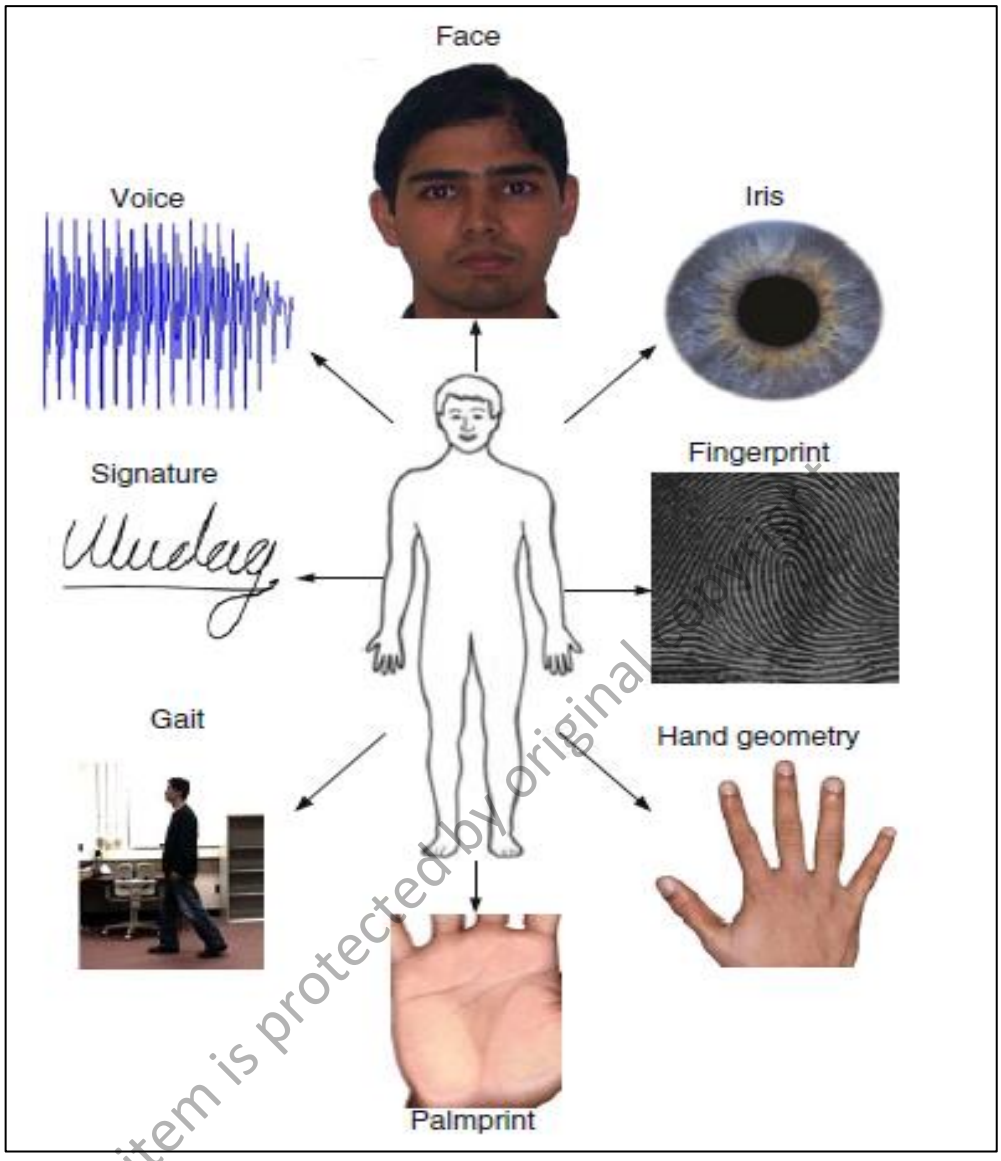

Figure 1.1: Examples of Body Traits for Biometric Recognition.

A biometrics system is basically a pattern of classification process that functions by collecting individual biometric data, extract a set of feature set from the data for comparison with the template data set in the database. Figure 1.2 shows this system that consists of four main modules:

1. Sensor module, which captures the biometric data of an individual.

2. Feature extraction module, in which the acquired biometric data is processed to extract a set of salient or discriminatory features.

3. Matcher module, in which the features extracted during recognition are compared against the stored templates to generate matching scores.

4. Decision module, in which a user's claimed identity is confirmed (verification) or a user's identity is established (identification) based on the matching score.

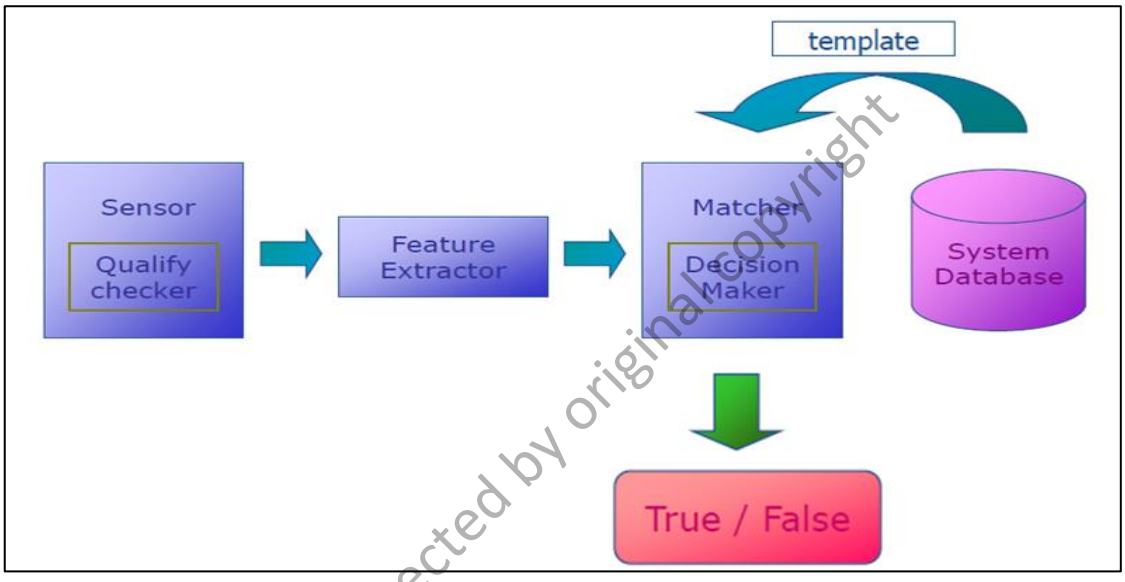

Figure 1.2: Basic Task of A biometrics System

1.2 Biometric Characteristics

In the biometric trait, several issues aside from the recognition or matching performance and accuracy are responsible for the choice of a particular application. (Prabhakar *et al*., (2003) & Jain *et al*., (2004)) assert that the combination of the physiological and the behavioural characteristics can be used for identification in as much as the following requirements are satisfied:

1. Universality: means every person in the population should possess the characteristic.

2. Distinctiveness: it's also known as uniqueness, indicates that each individual within the population should have peculiar traits that is unique and sufficiently varies from one another across the whole population.
3. Permanence: indicates that the biometric should not change or remain the same in relation to the matching algorithm over a period of time.
4. Measurability**:** The ability to measure the biometric quantitatively, in other words, it indicates that there should be a possibility for the acquisition and digitization of the biometric attributes through the use of appropriate means that will not cause undue discomfort to the individual.
5. Performance: refers to efficiency, accuracy, speed, robustness and resource requirements of particular applications based on the biometric.
6. Acceptability: relates to the extent to which a particular biometric identification will be accepted by people in their daily activities.
7. Circumvention: relates to the ease of fooling the system through a fraudulent approach.

The biometric modalities do not have all these properties, or at least have them with different degrees. In other words, there is no ideal biometrics as they are only acceptable to a certain extent. The nature, needs required by an application and the features of a biometric determines the relevance of a particular biometric to a particular application (Sireesha & Sandhyarani, 2013). The application of biometric systems that shown in Figure 1.3 can be categorized into three main groups:

1. Commercial applications such as computer login, electronic data security, e-commerce, Internet access, automated teller machines ATM or credit card use,

physical access control, mobile phone, personal digital assistant PDA, medical records management, distance learning.

2. Government applications such as national ID card, managing inmates in a correctional facility, driver's license, social security, welfare-disbursement, border control, passport control and identification.
3. Forensic applications such as corpse identification, criminal investigation parenthood determination.

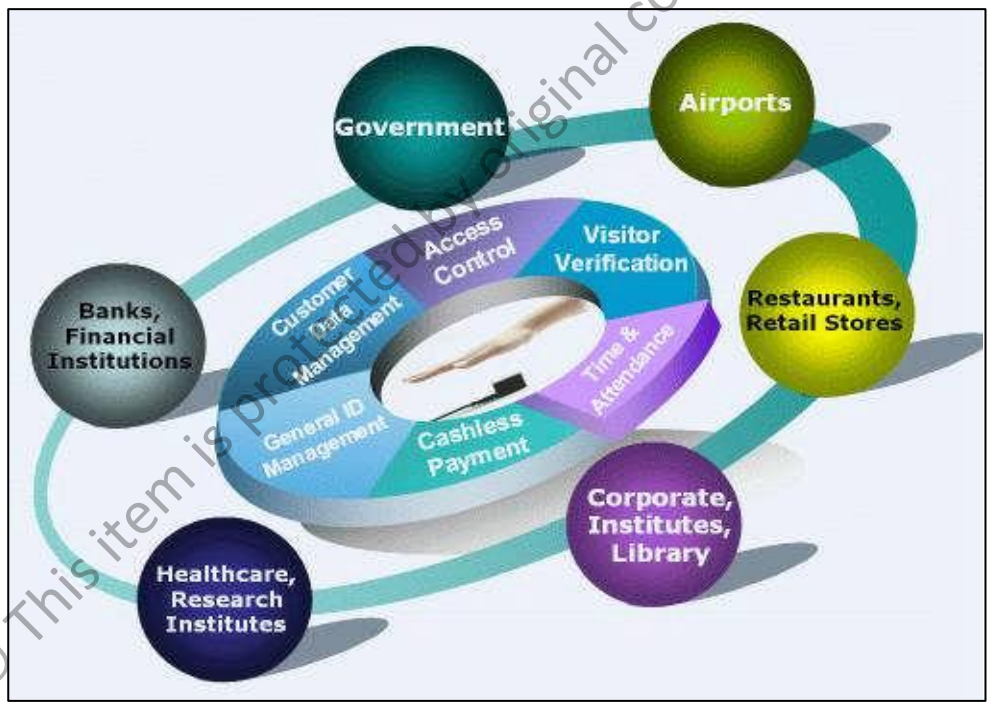

Figure 1.3: Some Biometrics Applications.

1.3 Information Fusion

In multimodal biometric systems we use more than one biometric trait. Fusion is done for biometric traits. Fusion means combining data at various levels. Two or more biometric techniques included in one application are known as multimodal biometric

system. The limitations in unimodal biometric systems can be overcome in multimodal biometric systems. These are expected to be more reliable due to multiple, independent pieces of information. They overcome the problem of non-universality and also spoofing problem. It is difficult for the intruder to spoof multiple biometric traits of an authorized user (Fu *et al*., 2008).

The main rationale behind the use of a multibiometric system is due to the improvement in accuracy, and this is achieved based on two reasons. The first reason is that combining multiple biometric sources increases the effectiveness of the feature space and minimizes the overlay of feature distribution among different individuals. This means that when multiple biometric sources are combined, they produce a unique biometric sample result about individual. The second reason for using multiple biometric sources minimize noise, inaccuracy, or natural drift due to aging in individual and which are alleviated by the biased information produced in the complementary biometric source. However, redundancy and fault-tolerance are produced as the recognition system continues its operation even though the acquisition modules of the biometric system fail. Despite the enhancement of the accuracy in recognising individuals, Faundez-zanuy (2005) stated the following as the added advantages provided by the multibiometric system over the unibiometric systems.

1) Minimises the non-universality problems and errors due to enrolment failure. For example, if an individual is unable to be enrolled in a palm-print system as a result of loss to one harm, the system will still be able to enrol the individual by using the facial recognition or other trait.

2) Provide a certain extent of flexibility in authenticating user. For instance, when a user used several different traits to enrol into an application system, only one of the subset of these traits will be required for authentication based on the application nature

of the system and the ease of the user's authentication. However, the other traits will be useful for continuous monitoring and tracking of the user's situation, and will be used by the multibiometric when that single traits is insufficient for authentication.

3) It enables an efficient computational search of a large biometric database firstly, it uses a relatively simple with poor accuracy method to search the database prior to using a more complex and accurate search method which improves the throughput of the biometric identification system.

4) It helps in improving the resistance towards proof attack. This is achieved because circumventing the multibiometric system becomes more difficult.

1.4 Motivation and Problem Statement

Authentication and verification of the identity of individual user of an application system is becoming an important issues, especially in the automatic access control. Examples of such applications are telebanking, the control of physical access, and automatic teller machines. Traditional approaches make use of passwords, personal cards, PIN numbers and keys to achieve verification. However, loss of access, card, or password compromise exposed security to an easy and a high level of breach. Furthermore, difficult passwords may be hard for a legitimate user to remember and simple passwords are easier for an imposter to guess. Biometric systems based on a single source of information (unimodal systems) are known to suffer from several limitations like the lack of uniqueness, non-universality and noisy data and hence, may not be able to achieve the desired performance requirements of real world applications. In contrast, multibiometric systems combine information from multiple evidences in order to arrive at a more reliable decision in terms of matching and rejection rates (Ross, *et.al* 2006).

Multimodal biometric system has been continually designed and many methods of information fusion have been proposed by researchers. Most of the fusion of this information occurs at the matching score level. This is because the individual modalities provide different types of raw data, and involve different methods of classification to achieved discrimination (Ross & Jain, 2003). Some types of existing feature level fusion use concatenation methods by using a global feature vectors which tend to be associated with dimensionality problems. For example face and palm-print are combined at feature level and RBF classifier is used in the classification process. As per comparison of both unimodal versus multimodal technique, the multimodal biometrics technique is more accurate, robust, challenging, high performance, high security, prevention against spoof attack and remedy over unimodal biometrics system (Bhavsar & Kshirsagar, 2014).

The popularity of using the multibiometric system that combines information from multiple biometric sources are increasing due to the ability of the multibiometric system to overwhelmed the limitations of the uni-biometric systems. Such limitations are the non-universality, noisy sensor data, large variations in intra usage, and its vulnerability to spoof attacks. Thus, the concept issues and the strategies for applying multibiometric system are addressed (Prabhusundhar, *et.al* 2013).

This research develops a methodology of information fusion at matching score level to combine face and palm-print multimodal biometrics which is able to achieve better performance in identification rates.

1.5 Aim and Objectives

The aim of this project is to investigate the fusion of information at matching score level in multimodal biometrics that uses face and palm-print image as the

biometric modalities. The investigation involves several stages relating to feature extraction, fusion and classification. In summary, the main objectives of this research are as follows:

1. To investigate the best fusion rule at matching score level to integrate face and palm-print low frequency information.

2. To develop linear projection technique based on PCA for feature extraction and dimensionality reduction for 2D face and palm-print images.

3. To evaluate the performance of the system in terms of recognition rates using benchmark face and palm-print datasets.

1.6 Scope of Project

The scope and development of this project based on the four processing stages as follows:

1- To specify the numbers of fusion rule at matching score level.

2- To apply image pre-processing technique for better quality of image representation.

3- To utilize linear projection method such as Principle Component Analysis (PCA) to reduce high dimensional feature space to a lower dimensional feature space which have high discrimination power.

4- To implement the Euclidean distance classifier using offline and real-time technique to examine the accuracy and speed of the proposed technique.

1.7 Thesis Organisation

This research focuses on face and palm-print multimodal biometric fusion at the match score level. This research organized with five chapters and the contents of each chapter are as follows:

Chapter 1: introduces the brief background, biometric characteristics, information fusion, motivation and problem statement of the research, aim and objectives and scope of this research.

Chapter 2: this chapter briefly discuss on different levels of fusion and their implementations, some of fusion strategies, the literature review of current research on the fusion technique at various levels.

Chapter 3: presents the multimodal biometrics system, Pre-processing stage, extract the features, information fusion at match score level and classification, and also details of the ORL benchmark face dataset and PolyU benchmark palm-print dataset.

Chapter 4: explains the experimental setup, analysis the results and the discussion, several number of analysis is to validate the proposed method.

Chapter 5: concludes the research findings with the recommendation of future work.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter entails a review of the current technique on palm-print and face information fusion. This includes several different techniques and algorithms for feature extraction, fusion level and classification process.

2.2 Fusion in Multimodal Biometric Systems

Biometric fusion is a mechanism that can associate multiples information from the biometric input. This biometric fusion can be performed at different level with different amount of information. To boost strengths, multimodal biometric fusion associates measurements from different traits of biometric (Yang & Ma, 2007). The problems of non-universality when numerous traits were used to ensure sufficient population coverage can be overcome by multimodal biometric system. Also, multimodal biometrics provides anti-spoofing measures, making it difficult for intruders to concurrently spoof the numerous traits of biometrics of genuine users. Furthermore, using multiple traits, more information can be gained which can eliminate the problem of inter-class similarity in the feature space and thus increase the performance of the recognition rate. The use of independent modalities is expected to have a high significant part in the improvement possible, when features from numerous biometrics modalities are fused. A combined system properly designed which has been trained and tested on huge amount of data was assumed to have performed better than the single