INTEGRATION OF MEDIAN FILTER AND ORIENTED FIELD ESTIMATION FOR FINGERPRINT IDENTIFICATION SYSTEM

NOR'AQILAH BINTI MISMAN

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

Faculty of Computing
Universiti Teknologi Malaysia

JANUARY 2015

ABSTRACT

The Fingerprint Identification System (FIS) has been used and applied into various aspects. The system used identification based on fingerprint to give an authorization and identification to every person that wants to access the system. However, there are some research issues that affect the system accuracy such as noise element and low-quality fingerprint image. To solve this problem, this project will proposed two selection methods; which are Median filter to reduce noise element and Orientation Field Extimation method to enhance the low-quality image. This proposed methods is implement in order to get an accurate result and high performance system. In order to verify the system identification, two experiments has been done which are functional test and accuracy test. This test will used 16 images from FVC2004DB1 set. From this test, there will be three results that being focus on which are the computational time, high peak value, False Rejection Rate (FRR), False Acceptance Rate (FAR) and Matching Rate. These values are used in order to verify high performance in the system, by comparing the proposed system with other existing system. By doing this experiment, it shown that by using the proposed methods it has lower value in average time and FRR value; which is good in order to get a high performance working system.However, for FAR value the other existing work has more accurate result in identifying fingerprint image compared to proposed work. Based from the experimental test, it shown that by using the proposed methods it is effective in order to identify low-quality and noises image with an accurate matching result and high performance system.

ABSTRAK

Sistem Pengenalan Cap Jari (*FIS*) telah lama digunakan dan diaplikasikan ke dalam pelbagai aspek. Sistem ini menggunakan cara pengenalan berdasarkan cap jari untuk memberi kebenaran dan pengenalan kepada setiap orang yang mahu untuk mengakses sistem. Walau bagaimanapun, terdapat beberapa isu penyelidikan yang memberi kesan kepada ketepatan sistem seperti unsur bintikan dan imej cap jari yang berkualiti rendah. Untuk menyelesaikan masalah ini, projek ini akan mencadangkan dua kaedah pemilihan; iaitu penapisan *Median* untuk mengurangkan unsur bintikan dan kaedah *Oriented Field Estimation* untuk meningkatkan imej yang berkualiti rendah. Ini adalah kaedah yang dicadangkan untuk diaplikasikan bagi mendapatkan keputusan yang lebih tepat dan sistem yang berprestasi tinggi. Bagi mengesahkan pengenalan sistem, dua eksperimen telah dilakukan iaitu ujian fungsional dan ujian ketepatan. Ujian ini menggunakan 16 imej dari set FVC2004DB1. Daripada ujian ini, akan ada tiga keputusan yang menjadi tumpuan pada yang masa pengiraan, nilai puncak kolerasi yang tiggi, Kadar Penolakan Palsu (*FRR*), Kadar Penerimaan Palsu (*FAR*) dan Kadar Pemadanan. Nilai-nilai ini digunakan bagi mengesahkan prestasi yang tinggi dalam sistem, dengan membandingkan sistem yang dicadangkan dengan sistem lain yang sedia ada. Dengan melaksanakan eksperimen ini, ia menunjukkan bahawa dengan menggunakan kaedah yang dicadangkan ia mempunyai nilai yang lebih rendah bagi purata masa dan nilai *FRR*, yang baik bagi mendapatkan satu sistem kerja yang berprestasi tinggi. Walau bagaimanapun, untuk nilai *FAR* kerja sedia lain yang sedia ada mempunyai hasil yang lebih tepat dalam mengenal pasti imej cap jari berbanding dengan kerja yang dicadangkan. Berdasarkan daripada ujian uji kaji, ia menunjukkan bahawa dengan menggunakan kaedah yang dicadangkan ia adalah berkesan bagi mengenal pasti imej yang imej berkualiti rendah dan bintikan dengan hasil pemadanan yang tepat dan sistem prestasi tinggi.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Today, many application systems used biometric verification as their medium security for access control. It used to authenticate the authorized persons from the threat, which is that could bring disaster or lost in the system or a person. Biometric technologies have become a base of highly secure human verification and identification solutions (Bharkad and Kokare, 2011).

Biometric system is known as an automatic pattern recognition system. It recognizes the identity by determining their authenticity based on the specific distinction physical or from the behavioural characteristics (Meraoumia, *et al.*, 2009). Biometric technology, there are many types of biometric such as fingerprint, face, hand palm, iris and others. In this project, the biometric technology that will be used is fingerprinted. In general, there are many applications of identification system that based on fingerprint. This application is used as a front end to a system that requires an accurate identification before it can be accessed or not.

The Fingerprint Identification System (FIS) has been applied in various aspects, whether in business or life, such as in computer network security, financial institutions, government organizations or enterprises, border pass control and others. In the government sector, they use a fingerprint identification system to authorize, identifies the verification of staff in safe regions and to manage security control of database access. While in the airport border control, they need an identity and do verification processes, which is not only checking the passports or visas but also checking on individual profile by using fingerprint scan. For some other airports, they also used iris scan for verification. These processes are created to get an accurate identification profiles in the world and to prevent from social engineering access. Furthermore, in the forensic field, the fingerprint identification is important steps that lead the prosecutor and forensic expert in criminal investigation. Besides, it has also become a crucial evidence to prove the person, whether guilty or not in the cases.

1.2 Problem Background

Biometric system is a recognition system that used to identify a human pattern; it determines the authenticity based on their specific characteristics (Meraoumia *et al.,* 2012). However, in order to get an accurate results, some existed system leads to unacceptable error rates in identifying a person.

Moreover, there are several issues need to be addressed in fingerprint image: lack of distinctiveness of the biometric trait, non-universality, spoof attacks and noisy sensor data (Meraoumia *et al.*, 2012). Some of the limitations were imposed by the single point biometric systems can be overcome by using multiple biometric modalities (Jia *et al.*, 2008). While by using biometric techniques, it can hold many desirable features such as distinctiveness, universality permanence, and collectability. Currently, the application by using personal identification and based on fingerprint matching is quite popular in wide

range area. There are multiple biometric systems, which were expected to be more reliable due to the presence of multiple template security (Singh *et al.*, 2008).

In the fingerprint identification system, there are two matching pattern techniques have been used; which is minutiae–based and images-based. The minutiae-based matching relied on less information, also offers a better performance in the matching process for a large dataset. While, by using image-based matching technique, it can provide a good registration in matching area for small datasets. However, fingerprint identification system needs to consume a large storage, a good computing resources and fast performance correlation technique (Souksamay *et al.*, 2011).

In existing FIS, it has a number of drawbacks that cause the system having low performance. For instance, the weakness of reliable minutiae extraction algorithms, which is it has a difficulty in quantitative by defining a reliable match between fingerprint images and fingerprint classification (Vaidehi *et al.*, 2010; Greenberg *et al.*, 2000). Besides, different applications will have different properties and desire in the fingerprint matching algorithm; such as different template size, matching speed and memory requirements. However, based on (Vaidehi *et al.*, 2010), in order to propose FIS, the researcher need to concern the following issues in order to make it an effective system. The first issue is regarding to fingerprint acquisition, which need to acquire and represent fingerprint images in the proper format. The second issue is fingerprint verification by authenticating between two fingerprints is from a same person. The third issue is fingerprint identification, which need to search for fingerprint image in the database query. Lastly, fingerprint classification, which need to assign categories for a given fingerprint based on its geometric appearance.

Based on the related works, there are 4 issues that need to be addressed in developing FIS and become important requirements to the system (Bharkad and Kokare, 2011). There are the accuracy, the adaptive system with non-linear

distortion, speed and the recognition of the overlapped fingerprint. For accuracy, it is challenging to get a minimum value that near to zero when using Equal Error Rate (ERR) (Chen *et al.*, 2009). Whilst, the adaptive system with non-linear distortion, it becomes and issues because of non-linear fingerprint deformation creates spurious minutiae (Diaz and Troyo, 2010). Then in speed issues, it has become an important requirement because the slowness in matching fingerprint images will lead to time consuming process (Chen *et al.*, 2009). Finally is the recognition of the fingerprint images from the overlapped fingerprint image.

1.3 Problem Statement

Among all the mentioned issues in the previous section, this project will focus on accuracy issue. It is quite difficult to get an accurate result because of the poor quality images, which consist of noise, and shape distortion factors such blurring effect (Diaz and Troyo, 2010; Bazen *et al.*, 2000). The noise factor is caused by the capturing device. However, it can be reduced by using an appropriate filtering. While for the shape distortion factor, it is caused by pressing the fingerprint surface on a flat sensor. This factor may result to blurring and stretching image, shear and rotation. They also cannot be compensated easily. These factors can decrease the system performance (Bazen *et al.*, 2000). Such low quality of fingerprint images will affect the accuracy of the fingerprint identification performance. So, in order to enhance the accuracy of fingerprint identification; those factors must be reduced by using suitable techniques.

So, the main question in this project is how to improve the accuracy of the FIS, in the presence of noise and shape distortion factors in fingerprint images.

The supported research questions are:

i. How to reduce noise and synthesis fingerprint template?
ii. How to improve the ridges and valleys of low-quality fingerprint images?
iii. How to evaluate automatic fingerprint identification system?

1.4 Research Goal

Providing the above problem statement, the research goal is:

To proposed an improved FIS in terms of accuracy by integrating 2 correlation techniques which are Median Filter and Orientation Field Estimation even in noisy and blurred fingerprint dataset.

In order to achieve the goal, the research hypothesis is:

"If the integration of are Median Filter and Orientation Field Estimation is effective until other Biometric Identification System with the presence of noise and blurring elements in a dataset, then it should be an effective method to Fingerprint dataset as well in terms of improved performance accuracy"

1.5 Objectives

The following objectives are set to be achieved:

i. To reduce noise and synthesis fingerprint template by using the Median Filter.
ii. To improve the ridges and valleys of low-quality fingerprint images by using Orientation Field Estimation technique.
iii. To propose fingerprint identification system design by integrating Median Filter and Orientation Field Estimation.

1.6 Scopes

The scopes of this project are:

i. This study will use datasets from FVC 2004, DB1 (Mehmet. K, 2013; Hanmandlu. M, 2013; Souksamay. I, 2011).
ii. Fingerprint image must be greyscale.
iii. Fingerprint image must be at 200 X 200 pixels.

1.7 Research Significance

The benefits of this research are:

i. In the government sector, the system will help to manage the security access control of confidential and important area.
ii. In airport border control, it helps them to do the verification in large quantity with accurate and smooth.

iii. In forensic area, it will help the forensic expertise to handle their cases smoothly by getting an accurate result in fingerprint process.

1.8 Project Organization

This research project is organized into five chapters. Chapter one, provide the general overview of the research background topic and focus, problem background, problem statement, and also research objectives and scopes. Chapter two will provide the literature review. The introduction of this chapter will highlight the point discussed of the fingerprint correlation technique, problem issues from these techniques. Besides, this chapter will analyse and overview the techniques of the existing systems that based on the fingerprint correlation identification. In chapter three, present the development phases. This is including the analysis about the system; designing of system needed, flow process of the system, a list of the entire requirement needed and also testing the system. In the chapter four discusses the design and implementation of the system. In chapter five, will show the result of the implementation process. Finally, there will be a conclusion based on the research project.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Based on mapped in figure 2.1, this section will review on fingerprint recognition system, which consists of two research areas; fingerprint identification, fingerprint verification. Then, there are some further surveys on problem and research issues in fingerprint identification. The existing techniques or methods in fingerprint identification also being discussed and the justification on selected techniques are given in the following section. Lastly the criteria for standard performance measurement that used to evaluate the system design and validate the level of accuracy.

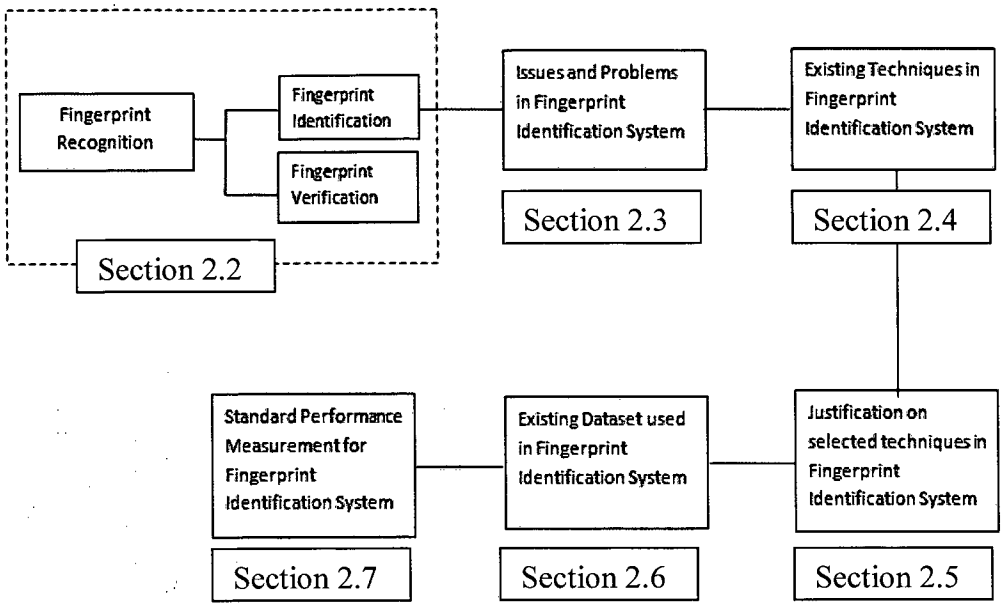

Figure 2.1: Structure of Literature Review

2.2 Fingerprint Recognition

Fingerprint recognition is known as a biometric system that used the physical structure of an individual's fingerprint for authentication or identification purpose. The important requirement that used in fingerprint recognition systems is the minutiae points which consisted of ridges and valleys structure. There are two kinds approach of fingerprint recognition systems. First, fingerprint identification system is by getting users to only offer his or her finger. Then, the system searches the database for a matching print template. If there is a matching print found, the system will identify that person. The other way in identifying fingerprint is through the ID - card such as MyCard for Malaysian citizen.

Based on research, there are two techniques that being used in fingerprint recognition. The techniques are fingerprint verification and identification. In

fingerprint verification technique, it will check the user id whether that person's is whom they claim to be. While for fingerprint identification technique, the user only offers the fingerprint and system will do checking and matching it through the primary database (Asker M. Bazen, 2000). The system will identify the user, if the user's fingerprint is matched or not.

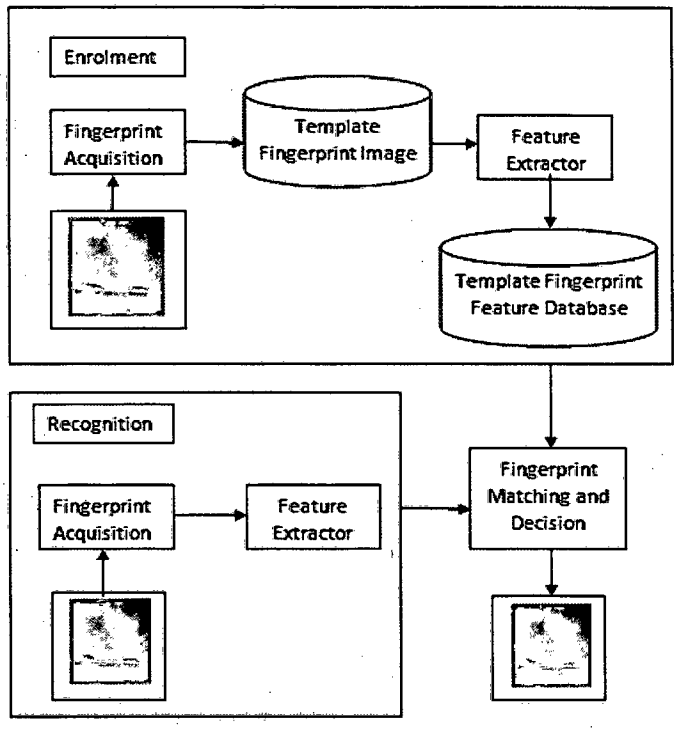

Figure 2.2: System Architecture

Based on Figure 2.2, it shows the system architecture and application of the fingerprint matching. In fingerprint verification, it also refers to this architecture. In fingerprint verification, it works in two phases; fingerprint enrolment phase and fingerprint matching phase. In enrolment phase, a sensor will capture the fingerprint image from various features and stored in 'master template' (Bharkad & Kokare, 2011).

While in fingerprint identification process, it also uses the same processes as verification process. However, it takes two fingerprint templates to determine a similarity score between it in the matching process.

2.2.1 Fingerprint Identification

Since 100 years ago, fingerprint identification has been used in the law enforcement sector. Now, it has become the international standard practices for identifying individuals. For example, it has been applied in the Federal Bureau of Investigation (FBI) for using fingerprint identification since 1928 (GAO, 2003). Fingerprint identification is the tasks that determine a similarity score between two fingerprint images, whether it is matching or not (Bharkad and Kokare, 2011). It required ridges-valleys structures, which were used as the main source of information by extracting from the fingerprints, before do matching process.

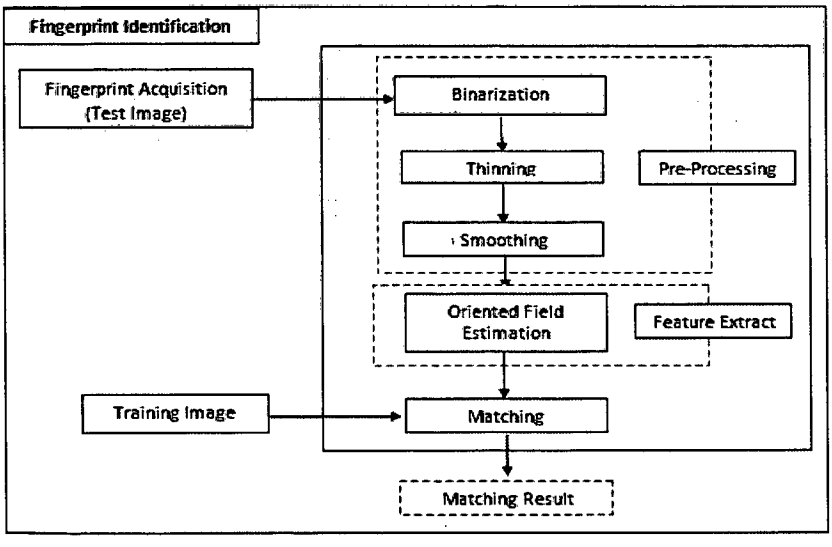

Figure 2.3: General Process

In the fingerprint identification system, there are five processes involved as given in Figure 2.3. The first step is acquiring a fingerprint image step. Usually, in this process requires a sensor device to capture the fingerprint image, and usually the images interrupted by noise element due to device factor or state of finger itself. Table 2.1 below is further explanation of each process in identification system.

Table 2.1: Fingerprint Identification Processes

Processes	Description
i. **Pre-Processing**	This first step uses to remove the noise element from the images. Besides, in order to extract the correct features this step make changes the image to a clear image with obvious edges. This process is one of the important steps in fingerprint identification system, which gives a big impact on the successful identification system (Bahaa-Eldin, 2013; Vaideshi *et al.*, 2010).
ii. **Binarization**	Because of the intensities of the ridges are unique, and have different grey scales. Binarization is to unify the grey scales, and simplified into binary information. Binarization will compress image information, reserves the information of ridges and saves in the storage store space. Besides, it also separates attached ridges and makes provisions for feature exaction and matching (Bahaa-Eldin, 2013; Zhou *et al.*, 2004).

iii. **Thinning**	The purpose of this step, to remove the pixels on ridge edges, and to keep the ridges within one pixel. This is to remove the redundant information .and also to highlight the main features in order to facilitate exaction. However, it shall not change the connectivity, direction or feature points of ridges; neither shall the centre of ridges be changed (Bahaa-Eldin, 2013; Zhou *et al.*, 2004).
iv. **Smoothing**	In this step, the purpose is to filter out the negative element, such as noise from the image content (Steven *et al.*, 2013; Martinez *et al.*, 2010; Kanagalakshmi and Chandra, 2011; Gupta, 2011). This process is will not affect to any changes to the location and orientation of minutiae points. However, the effect of using a filter can cause a disadvantage purpose, such as blur to the image process and computation time (Kanagalakshmi and Chandra, 2011). There are many types of filter that can be used in image processing, such as Low Pass Filter, Median Filter, MACE filter and etc.
v. **Feature Extraction**	There are two exaction methods in this step (Bahaa-Eldin, 2013; Tan and Schuckers, 2010; Zhou *et al.*, 2004): a. To extract from the grey scale image by using an algorithm. Usually, this method used to track the greyscale ridges and finds the location and determines the types of features.