FINGERPRINT RECOGNITION SYSTEM

ROHANI BINTI ABU BAKAR

A report submitted in partial fulfilment
of the requirements for the award
of the degree of

Bachelor Computer Technology (Software Engineering)

....

Faculty of Computer System & Software Engineering
University College of Engineering & Technology Malaysia

MARCH 2005

ABSTRACT

Fingerprint recognition is the oldest method which has been used in numerous applications for identification purpose in many social conditions such as access control and crime investigation. Now a day, in the era of technology the system is still using the password or smart card as an identity character for identification purpose. The problems happen when user forgot their password or lost their smart card. To solve this problem, a prototype for recognition fingerprint was implemented the Fast Fourier Transform (FFT) technique for features extraction and Euclidean Distance for template matching. The waterfall methodology has been used in this prototype because it can provide an orderly sequence of development steps and help to ensure the quality, reliability, and maintainability. Features extraction algorithm will produce the reference number. In addition, template matching algorithm will do the comparison between the fingerprint image based on the reference number either it is similar or not. As a result of this technique, the input fingerprint image will be match with the store fingerprint image if there are the similar images.

ABSTRAK

Pengesanan cap jari adalah merupakan salah satu diantara cara terawal yang diaplikasikan dalam tujuan pengenalpastian sesuatu identiti. Sebagai contoh, pengesanan cap jari telah diaplikasikan didalam sistem kawalan dan pengesanan jenayah. Dewasa ini, di dalam era teknologi terkini, kata laluan atau kad pintar masih digunakan bagi tujuan pengesanan identiti. Masalah akan berlaku sekiranya pengguna terlupa kata laluan atau kehilangan kad pintar mereka. Sekiranya perkara ini berlaku, sistem kawalan yang digunakan sebenarnya masih kurang efektif dan mempunyai banyak kekangan. Bagi mengatasi masalah ini, sebuah prototaip telah di bangunkan dengan mengaplikasikan teknik *Fast Fourier Transform (FFT)* di dalam pengekstrakkan ciri dan *Euclidean Distance* di dalam pemadanan templat. *Waterfall methodology* telah digunakan didalam prototaip ini bagi memastikan kualiti dan penyelenggaraannya berjalan dengan lancar. Algoritma yang digunakan dalam pengekstrakkan ciri ini akan akan menghasilkan ciri-ciri pengekstrakkan bagi setiap tetingkap di dalam imej. Selain dari itu, algoritma bagi pemadanan templat pula akan mengenalpasti sesebuah imej itu mempunyai persamaan ataupun tidak. Apabila sesebuah imej itu diuji, imej tersebut akan dianalisa sama ada imej itu mempunyai persamaan dengan imej yang berada didalam rekod ataupun tidak.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOL

e_x	-	Power
C	-	Constant
L	-	Low pass
H	-	High pass
θ	-	Corner
ENT	-	Obstacle
CON	-	Different
ASM	-	Homogeneous
IDM	-	Roughness
S	-	Average
P	-	Average every block
T	-	Number of filtering
$F(u)$	-	Fast Fourier Transform
σ	-	Standard deviation
g	-	Relative Frequency
q	-	Calculate distance
$\bar{x}$	-	Sum

ABBREVIATIONS

AFIS	-	Automatic Fingerprint Identification System
DFT	-	Discrete Fourier Transform
FFT	-	Fast Fourier Transform
FSR	-	Fingerprint Recognition System
GIF	-	Graphic Interchange Format
JPEG / JPG	-	Joint Photographic Experts Group
LZW	-	Lempel Ziv Welch
MATLAB	-	Matrix Laboratory
Minutiae	-	The characteristic of fingerprint
Ms	-	Microsoft
PDA	-	Personal Digital Assistant
PNG	-	Portable Network Graphics
RGB	-	Red / Green / Blue
TIFF/ TIF	-	Tag Image File Format
KUKTEM	-	Kolej Universiti Kejuruteraan dan Teknologi Malaysia

LIST OF APPENDICES

CHAPTER I

INTRODUCTION

1.1 Introduction

Humans have used fingerprints for a very long time (Stefano Bistarelli et. al, (2004). Fingerprints have long been used for identification in many social conditions such as access control, crime investigation, and personal trust, since they will remain almost constant during people's life time (Qinzhi Zhang et. al, 2004).

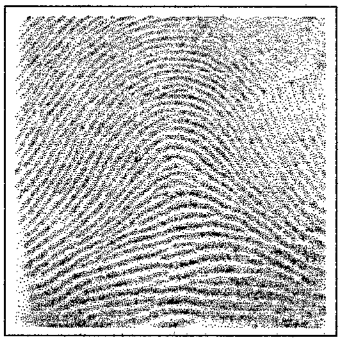


Figure 1.1: An example of fingerprint

Fingerprint recognition is the oldest method which has been successfully used in numerous applications (Qinzhi Zhang et. al, 2004). This is because fingerprint is a unique and never change through out and individual life time. Now a day, in the era of technology, it is possible to manipulate multi dimensional signals from simple digital circuits to advanced parallel computers (John M. Trenkle, 2003). Everybody knows they have a unique and immutable fingerprint (Qinzhi Zhang et. al, 2004). The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. The topic for Undergraduate

Project that is being proposed is "Fingerprint Recognition System (FRS)". The environment that will be used to do the case study is University College of Engineering & Technology of Malaysia (KUKTEM), Gambang, Kuantan. FRS is a verification and recognition of a person fingerprint characteristic that will capture the fingerprint image and match it for identification purposes.

1.2 Problem Statement

As our everyday life is getting more and more computerized automated security systems are getting more and more important. Now days, most personal banking tasks can be performed over the Internet and soon they can also be performed on mobile devices such as cell phones and PDA. There are three main methodologies when performing this verification. The security system could ask the user to provide some information known only to the user, it could ask the user to provide something only the user has access to or it could identify some sort of trait that is unique for the user (Anil K. Jain et. al, 2004).

i. Password is the classical approach. It has been used for decades in computer systems, but unfortunately this methodology has a major drawback. The problem is related to how the human memory works and what is demanded of a password for it to be considered secure. For a password to be considered secure, an imposter should not be able to guess the password within a reasonably large number of attempts. This means that it should be randomly chosen and of a certain minimum length. Humans usually only can hold five to nine digits in their short-term memory at any one time.

ii. Smart card has also been used for a number of years, for example when accessing high security facilities. This methodology also has a major drawback, since what is identified by the security system is not the user but actually the belonging. For example, if an imposter steal an authorized users access card and try to enter a restricted area, there is no way for the security system to know that it is giving access to an imposter and not the user. Of course the method can be combined with a password to get around this problem but then the previously mentioned password problem will be introduced instead.

iii. Identifying some trait that is unique for the user, is known as biometric security and it is an attempt to get around the previously mentioned problems. A biometrics system is a pattern recognition system that establishes the authenticity of a specific physiological or behavioral characteristic possessed by a user.

The current system in KUKTEM is based on “smart card”, where people should bring their own card to enter the door. Sometimes they forget or not remember to bring their own card and sometimes peoples are easy to change and take the card that not belongs to them. When they want to enter, they must put their card to the machine, and system will recognize to enter the door. The problem happens when, user lost their own card, and it is easily for them to borrow from another. That’s mean, the security here still not properly useful.

All the people or student should buy the smart card for their own used. The smart card will be functioning to them to open the door.

1.3 Objective

The objectives to develop this system are:

i. Develop a prototype for features extraction using Fast Fourier Transform.

ii. Develop a prototype for template matching using Euclidean Distance

1.4 Scope

The scope will focus on fingerprint recognition phase. It will recognize the fingerprint after the verification process ended.

The recognition phases consist of:

i. Thinning image.

ii. The format of image is JPEG

iii. Size of image is 240 x 240 pixels.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

Fingerprints are interesting since they show measurable differences in pattern and the pattern is quite stable trough out our lifetime (Chaur-Chin Chen and Yaw-Yi Wang, 2003). Fingerprints have been used in crime investigation for decades now.

Everybody knows they have unique and immutable fingerprint. The uniqueness of a fingerprint can be determined by the pattern of ridges of pattern and furrows as well as the minutiae point which is the local ridge characteristics that occur at either a ridge bifurcation or ridge ending.

Basically, low enforcement agencies used fingerprint for criminal identification (Chaur-Chin Chen and Yaw-Yi Wang, 2003). Today it also be used in several other application such as access control for high security, credit card usage verification and employee identification. In addition it also can improve the security if the system.

Some research of the previous system had been done to gain the knowledge about the important part which is the methodology in recognition, technique and the suitable algorithm.

2.2 The History of Fingerprint

Fingerprints have long been involved in recognition and as signatures (Johan Blomme, 2003):

Table 2.1: The History of Fingerprint

Year	Description
14th century	Official government paper had fingerprint impressions on them in 14th century Persia. One government official (a doctor) also observed that no fingerprints were exactly alike
1686	Marcello Malpighi, a professor of anatomy at the University of Bologna, noted in his treatise; ridges, spirals and loops in fingerprints. He did not address their value as a tool for individual identification.
1856	Sir William Hershel began using fingerprints on contracts with the natives in India. In the beginning the whole handprint was used but later on Hershel only required the right index and middle finger as identification on the contracts. Hershel had a limited experience with fingerprints but his personal conviction was that every fingerprint was unique as well as permanent throughout the individual's life.
1870	Dr. Henry Faulds took up the study of "skin-furrows" after noticing marks on specimens of "prehistoric" pottery. Faulds did not just recognize the importance of fingerprints as means of identification; he also devised a method of classification
1880	Dr. Henry Faulds forwarded an explanation of his classification system and sample forms for recording inked impressions to Sir Charles Darwin. The same year Faulds also published an article in the scientific journal "Nature" where he discussed fingerprints as means of personal identification and the use of ink as a

	method for obtaining these
1883	In Mark Twain's (Samuel L. Clemens) book "Life on the Mississippi" from a murderer was identified with the use of fingerprint identification.
1892	The British anthropologist Sir Francis Galton, cousin of Charles Darwin, began his observations of fingerprints as a means of identification in the 1880's. His observations originated in the book "Fingerprints", establishing the individuality and permanence of fingerprints. This book contained the first classification system for fingerprints. Galton's primary interest in fingerprints was as an aid for determining heredity and racial background. He did however soon discover that there were no real clues for this theory. Instead he ended up scientifically proving that fingerprints do not change during the individual's lifetime and that there are no fingerprints that are exactly alike. Galton also identified the characteristics in which fingerprints can be classified. These characteristics (minutiae) are still today referred to as Galton's Details and their basic use is the same.
1892	Juan Vucetich an Argentine police official made the first criminal fingerprint identification. A woman had murdered her two sons and later cut herself in the throat to place blame on someone else. Her fingerprint in blood was found on the door post, proving her identity as the murderer.
1901	Fingerprints were introduced for criminal identification in England and Wales. The technique was based on Galton's observations, but had been revised by Sir Edward Richard Henry. The Henry Classification System is still used in English speaking countries today.
1918	Edmond Locard wrote that if 12 points (Galton Details) were the same between two fingerprints it would suffice as a positive

	identification. This is where the often quoted "12 point rule" originated. There is still no required number of points for identification and the needed points vary between countries.

2.3 Automatic Fingerprint Identification System (AFIS)

Although no exactly the same fingerprint from distinct identities was found, a perfect system for automatic fingerprint identification does not exist. A minutiae pattern is composed of various minutiae extracted from a fingerprint image. Each minutia is represented by its relative location, a type: ending or bifurcation, and the ridge direction (Chaur-Chin Chen and Yaw-Yi Wang, 2003). The four main components of an AFIS system is the scanner, the recognition algorithm, the search and query algorithm of the data base and the data compression algorithm.

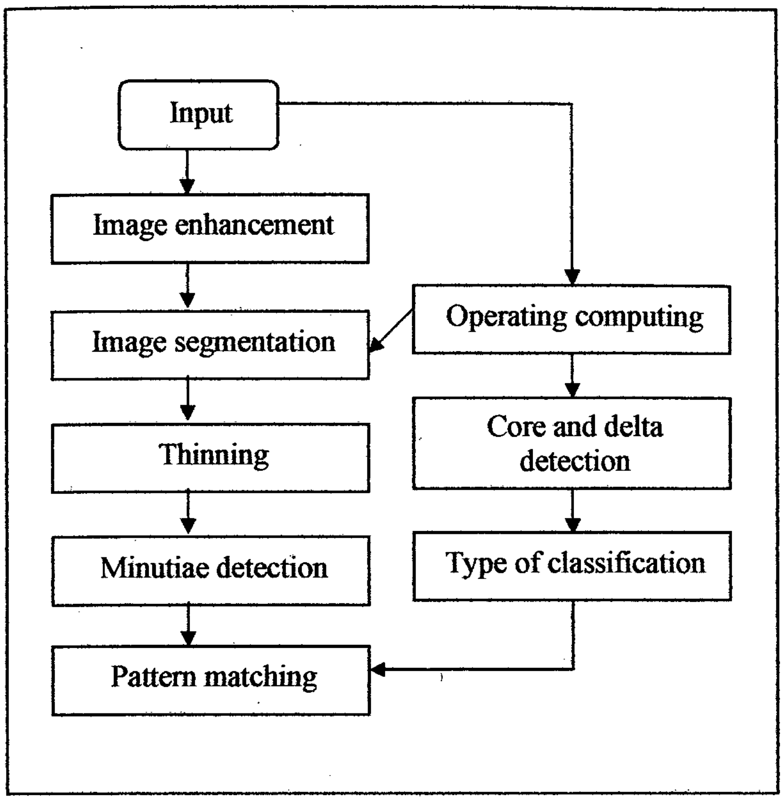


Figure 2.1: An AFIS Paradigm (Chaur-Chin Chen and Yaw-Yi Wang, 2003)

2.4 Fingerprint Classification

There are two categories to define a problem of resolving the identity of a person with different inherent complexities which is (Anil Jain, 2004):

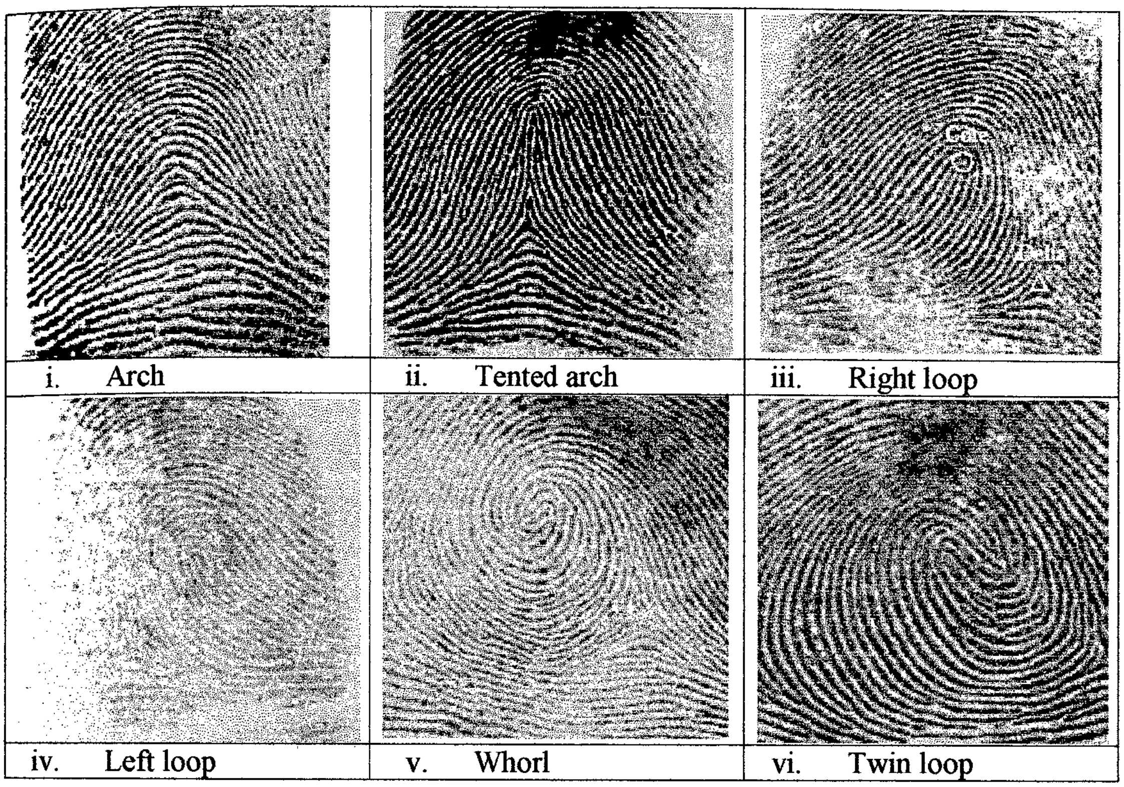
i. Verification

Verification or authentication is refers to the problem of confirming or denying a person's claimed identity

ii. Recognition.

Recognition is refers to the problem of establishing a subject's identity. A reliable personal identification is critical in many daily transactions.

Typically, a person could be identified based on a person's possessions for example permit physical such as smart card to access a building to all persons whose identity could be authenticated by possession of a key.



i. Arch

ii. Tented arch

iii. Right loop

iv. Left loop

v. Whorl

vi. Twin loop

Figure 2.2: Classification of Six Fingerprints (Anil Jain et. al, 2004)

2.5 System Architecture

The architecture of a fingerprint-based automatic identity authentication consists of four components (Chaur-Chin Chen and Yaw-Yi Wang, 2003):

i. User interface

Provides mechanisms for a user to indicate his or her identity and input his or her fingerprints into the system.

ii. System database

It consists of a collection of records, each of which corresponds to an authorized person that has access to the system. Each record contains the following fields which are used for authentication purpose: User name of the person minutiae templates of the person's fingerprint

iii. Enrollment module

Enroll persons and their fingerprints into the system database.

iv. Authentication module.

To authenticate the identity of the person who intends to access the system.

2.6 Fingerprint Sensing

There are two primary methods of capturing a fingerprint image (Anil Jain, 2004).

i. Inked (off-line)

An inked fingerprint image is typically acquired in the following way: a trained professional obtains an impression of an inked finger on a paper and the impression is then scanned using a flat bed document scanner.

ii. Live scan (ink-less).

The live scan fingerprint is a collective term for a fingerprint image directly obtained from the finger without the intermediate step of getting an impression on a paper.

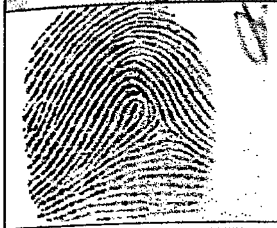
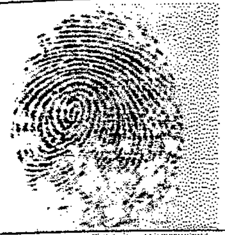
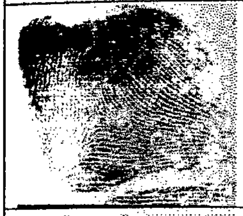
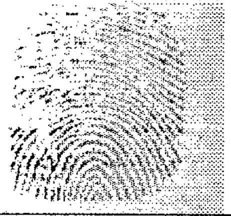
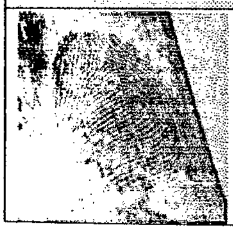
Image	Description
	An inked fingerprint image could be captured from the inked impression of a finger
	A live scan fingerprint is directly imaged from a live finger based on optical total internal reflection principle
	Rolled fingerprints are images depicting nail-to-nail area of a finger
	Fingerprints captured using solid state sensors show a smaller area of finger than a typical fingerprint dab captured using optical scanners.
	A latent fingerprint refers to partial print typically lifted from a scene of crime.

Figure 2.3: Fingerprint Sensing (Anil Jain, 2004)

2.7 Software Development Tools

Software development tools describe the tools that can be used to apply the Software development methodology.