FINGERPRINT DATABASE

NUR AMIRA BINTI ARIFFIN

THESIS SUBMITTED IN FULFILMENT OF THE DEGREE
OF COMPUTER SCIENCE

(COMPUTER SYSTEM AND NETWORKING)

FACULTY OF COMPUTER SYSTEM AND SOFTWARE
ENGINEERING

2015

TABLE OF CONTENT

CHAPTER	TITLE	PAGE
	TABLE OF CONTENT	vi
	LIST OF TABLE	viii
	LIST OF FIGURE	ix
	LIST OF DIAGRAM	xi
	LIST OF ABBREVIATION	xii
	ABSTRACT	xiii
1	INTRODUCTION	
	1.1 Project Background	1
	1.2 Problem Statements	1
	1.3 Objective	2
	1.4 Scope	2
	1.5 Thesis Organization	2
2	LITERATURE REVIEW	
	2.1 Existing System Review	4
	2.1.1 Fingerprint Recognition System	4
	2.1.2 Fingerprint Matching	7

2.1.3 Adaptable Fingerprint Minutiae Extraction Algorithm Based-On Crossing Number Method For Hardware Implementation Using Fpga Device 11

2.2 Propose System 14

2.3 Comparison between Existing System and Propose System 14

3 METHODOLOGY

3.1 Introduction 16

3.2 Requirement 17

3.3 Design 17

3.3.1 Flowchart 18

3.3.2 Use case Diagram 20

3.3.3 System structure 20

3.4 Implementation 21

3.5 Verification 22

3.6 Hardware and Software Requirements 22

4 DESIGN & IMPLEMENTATION

4.1 Introduction 24

4.2 Developing Interface System 24

4.2.1 Device Setup 27

5 RESULT AND DISCUSSION

5.1 Enroll Process 28

5.2 Verify Process 30

6 CONCLUSION 32

References 33

Appendix 34

LIST OF TABLES

NO	TITLE	PAGE
Table 2.1	Comparison between existing systems	16
Table 3.1	Biomini fingerprint specification	20
Table 3.2	Hardware Requirements	20
Table 3.3	Software Requirements	25

LIST OF FIGURES

NO	TITLE	PAGE
Figure 2.1	Algorithm for fingerprint registration	7
Figure 2.2	Fingerprint Image Enhancement	8
Figure 2.3	Binarization, Orientation & ROI	8
Figure 2.4	Thinned ridge map & Removed H Breaks and Spikes	9
Figure 2.5	All Extracted Minutiae & Real Minutiae	10
Figure 2.6	A typical automated fingerprint recognition system. The system determines the user's identity by comparing the match score to a threshold.	11
Figure 2.7	Feature levels in a fingerprint with the second and third images are magnified versions of the fingerprint regions indicated by green boxes in the corresponding preceding images.	12
Figure 2.8	Flow chart of a typical minutiae feature extraction algorithm.	15
Figure 2.9	Typical minutiae matching algorithm. The algorithm first uses local minutiae descriptors to coarsely align two fingerprints and then computes a global match score based on minutiae correspondences.	
Figure 2.10	Structure of Fingerprint Image	23
Figure 2.11	Thinning result	24

Figure 2.12	Image enhancement result	25
Figure 3.1	System structure	26
Figure 3.2	Suprema biomini	27
Figure 3.3	Microsoft Visual Basic 2010	28
Figure 4.1	Start Visual Basic	29
Figure 4.2	Main form	31
Figure 4.3	Choose scanner form	32
Figure 4.4	Enroll form	33
Figure 4.5	Busy form	34
Figure 4.6	User info form	38
Figure 4.7	Choose Suprema Scanner	39
Figure 4.8	No scanner connected	39
Figure 5.1	Enroll	40
Figure 5.2	Waiting for fingerprint	40
Figure 5.3	Scanner timeout	41
Figure 5.4	Fingerprint enrollment	42
Figure 5.5	Waiting for fingerprint	43
Figure 5.6	Scanner timeout	44
Figure 5.7	Fingerprint not verified	45
Figure 5.8	Fingerprint verified	45

LIST OF DIAGRAM

NO	TITLE	PAGE
Diagram 2.1	Schema of fingerprint minutiae extraction algorithm.	14
Diagram 3.1	Waterfall model	18
Diagram 3.2	Flowchart of system	
Diagram 3.3	Flowchart for enroll	
Diagram 3.4	Flowchart for verify	
Diagram 3.5	Use Case Diagram of system	
Diagram 3.6	System structure	

LIST OF ABBREVIATION

ROI - Region of Interest

FPGA – Field Programmable Gate Array

ABSTRACT

This project aims to save a fingerprint in the database. Fingerprints contain many details, which are known as minutiae, that can be used for identification marks in fingerprint verification. Fingerprint recognition is one of the biometric techniques. Each person has a different pattern of fingerprint make it unique and different from each other. Therefore, it can be used for personal identification. Using fingerprint recognition makes a guarantee to be more secure because of unchangeable fingerprint. There are many applications that used fingerprint recognition like fingerprint recognition to replace password and also used fingerprint recognition to recognize the individual identity card for a long period. This project needs the user to thumbprint their finger to be save in database and later their fingerprint is compared and match to retrieve the information.

ABSTRAK

Projek ini bertujuan untuk menyimpan cap ibu jari di dalam pangkalan data. Cap jari mengandungi banyak maklumat yang dikenali sebagai detel yang boleh digunakan untuk tanda pengenalan dalam pengesahan cap jari. Pengiktirafan cap jari adalah salah satu teknik biometrik. Setiap orang mempunyai corak cap jari yang berbeza menjadikannya unik dan berbeza antara satu sama lain. Oleh itu, ia boleh digunakan untuk pengenalan diri. Menggunakan cap jari pengiktirafan memberi jaminan untuk menjadi lebih selamat kerana cap jari tidak berubah-ubah. Terdapat banyak aplikasi yang menggunakan pengiktirafan cap jari seperti pengiktirafan cap jari untuk menggantikan kata laluan dan juga digunakan pengiktirafan cap jari untuk mengenali kad pengenalan individu untuk tempoh masa yang panjang. Projek ini memerlukan pengguna untuk cap ibu jari mereka untuk disimpan dalam pangkalan data dan kemudian cap jari mereka dibandingkan dan sepadan untuk mendapatkan maklumat.

CHAPTER 1

INTRODUCTION

1.1 Project Background

Security is important, especially in networking. Network security works to protect our network from an unauthorized users to access the resources and to ensure only authorized user can access the resources. Authorized is a process to identify the correct user to access the resources. There are many ways to log onto the network such as by using a password, smart cards and many more.

For this project, fingerprint is choosing rather than other methods because it is more secure. Fingerprint is unique for each person because it can be used for authentication purposes. Other than that, fingerprint is biological credentials, which are never left at home.

1.2 Problem Statements

i. Security authentication type.
ii. Fewer databases can be used for storing fingerprint.
iii. Difficult to create database for fingerprint.

1.3 Objectives

i. To develop fingerprint database.
ii. To test the fingerprint in a database.
iii. To verify a fingerprint from the database.

1.4 Scope

i. A prototype for a fingerprint.
ii. Only small group of student involved for testing.
iii. Only several information of user.

1.5 Thesis Organization

This thesis consists of five chapters. First chapter will discuss on introduction to the project. This chapter contains an overview of the project, problem statements, objective, scope and thesis organization.

The next chapter is chapter two will describe about literature review that related on the selected project. This chapter consists of two parts on research. There are existing research or system and technique, method, hardware or technologies, which are suitable for the project.

For the third, chapter will describe the methodology of overall approach and framework of research. It covers method, technique or approach to be used. There are also the methods during design and implementation phase that is important to the project. The information contains an introduction to the activities during research development, methodology phase, hardware and software that uses in the project and lastly Gantt chart which shows research phases from starting on a project complete.

Fourth chapter is design and implementation. It shows the development within the framework and model through flow work. Other than that is the planning of data analysis when designing the research with shows the workflow and model to be implemented into an algorithm.

While in chapter, five shows the result/system/output from the project that consists of result analysis and research constraints.

Finally on the last chapter contains the overall conclusion to the project.

CHAPTER 2

LITERATURE REVIEW

2.1 Existing System Review

There are many existing systems using a fingerprint recognition system for network access.

2.1.1 Fingerprint Recognition System [1]

Fingerprint is a form of biometric identification. The identification mark which are a minutiae points is used for fingerprint recognition based on minutiae extracting and matching. There are many variations of fingerprint when the place in image acquisition device plane such as rotation in right, rotation to the left, shift in left, shift in right, high pressure, low pressure, shift down and shift up. It is necessary to minutiae extraction to match the fingerprints.

A fingerprint consists of different types of components, which are ridges, furrows, termination, bifurcation, dots, islands, ponds or lakes, bridges, crossover, core and delta. There are various steps in fingerprint registration algorithm.

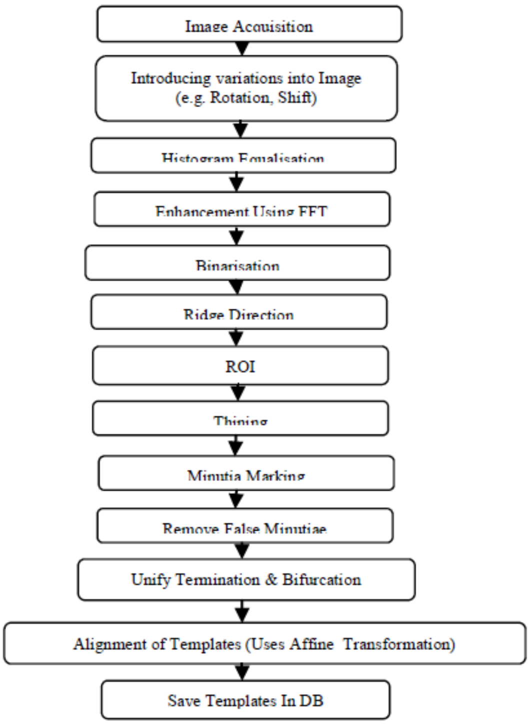
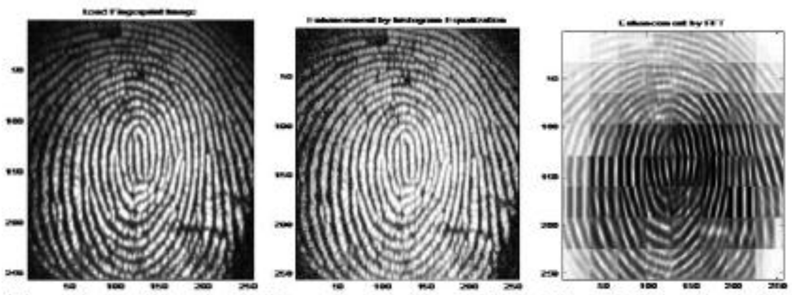


Figure 2.1: Algorithm for fingerprint registration

To register a fingerprint into a database its follow algorithm level design, which is pre-processing stage, minutia extraction stage and lastly post processing stage.

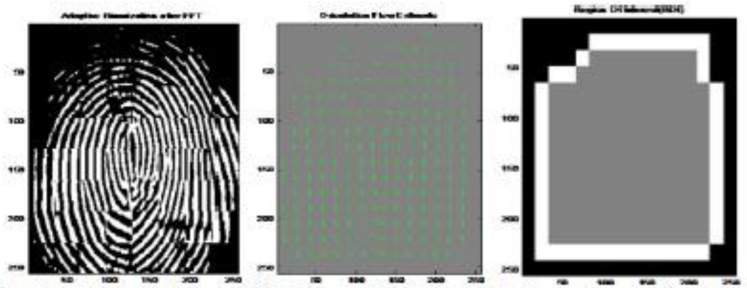
There are three stages is pre-processing stage, which is image enhancement, image binarization, and image segmentation. In image enhancement, there are two methods like histogram equalization and Fast Fourier transforms whereas in an image segmentation followed three steps such as block direction estimation, segmentation by direction intensity and Region of Interest (ROI) extraction by Morphological operations.



(a) Original Image (b) Enhancement by Histogram equalization (c) Enhancement by FFT

Figure 2.2: Fingerprint Image Enhancement

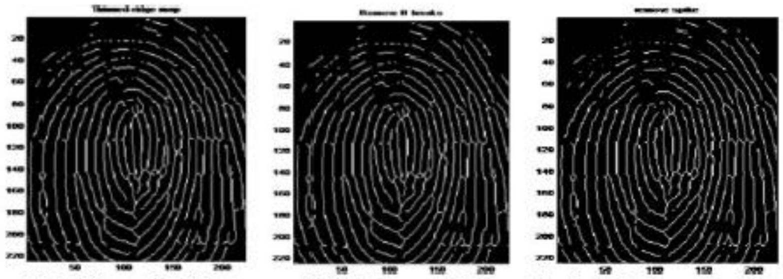
The next stage is binarization of image by extracting the lightness of the image.



(a) Adaptive Binarization (b) Orientation Field Estimation (c) Region of Interest

Figure 2.3: Binarization, Orientation & ROI

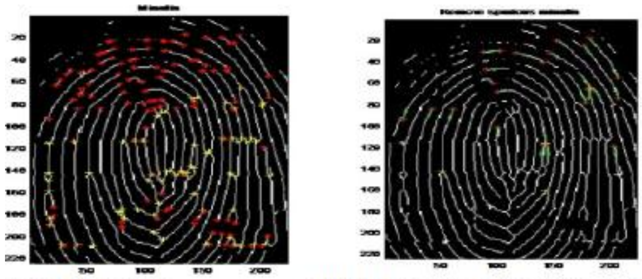
After the fingerprint, image is enhanced and is converting into a binary form, it will be submitted into thinning algorithm that reduces the ridge thickness.



(a) Thinned Ridge map (b) Remove H breaks (c) Remove spikes

Figure 2.4: Thinned ridge map & Removed H Breaks and Spikes

Post processing steps have two, which are the removal of false minutia and unifies termination and bifurcation.



(a) Minutiae (b) Removed Spurious minutiae

Figure 2.5: All Extracted Minutiae & Real Minutiae

2.1.2 Fingerprint Matching [2]

Fingerprint recognition systems are used for verification and identification. In verification, a fingerprint of a user is compared to specify the identical fingerprint from an enrolled fingerprint whereas in identification, a fingerprint with the prints of user who are enrolled in the database is specified if it is duplicated or false identity of a user.

2.1.2.1 Automated Fingerprint Recognition

In enrollment phase, the sensor scans the fingerprint of a user and then converts it into a digital image. The minutiae extractor processes the image of fingerprint to identify special details of minutia points that are used to differentiate multiple users. Minutia points show the locations where friction ridges end abruptly or where a ridge branches into two or more ridges. The quality of good fingerprint image has 20 to 70 minutiae points where the actual number depends upon the surface size of the sensor and how the user placed their finger on the sensor. The system stores the minutiae information which is its location and direction with the user’s demographic information about the enrollment database.

At identification phase, the user touches the same sensor, produce the new fingerprint image called query print. Minutia points are extracted from the query print, and the matcher module compares the query minutia set with the stored minutia in the enrollment database to find the number of same minutia points. There are many variation's placement and pressure of finger on the sensor by the user. The minutia points are extracted from the template and query fingerprints must be aligned or registered before matching. After that, the matcher determines the number of pairs of matching minutiae of two minutia points that have same location and directions. The system determines the identity of a user with compare the match score to a threshold set by the administrator.

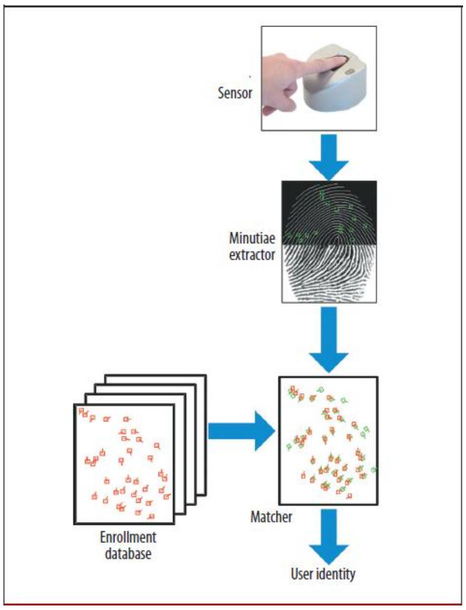


Figure 2.6: A typical automated fingerprint recognition system. The system determines the user's identity by comparing the match score to a threshold.

2.1.2.2 Feature extraction

There are three levels of features extracted from a fingerprint image. Firstly, features capture macrodetails like friction ridge flow, pattern type and singular points. Secondly, features refer to minutiae like ridge bifurcations and endings. Lastly, features include all dimensional attributes of the ridge like ridge path deviation, width, shape, pores, edge contour and other details, including incipient ridges, creases and scars.

Level 1 features can be applied to categorize the fingerprints into major pattern types such as arch, loop or whorl wheres level 2 and level three features can be applied to create a uniqueness of fingerprint with high resolution. A flow chart of a typical minutia features extraction algorithm by estimates the friction ridge orientation and frequency from the image.

It then performs contextual filtering based in the value to improve the image quality and facilitate ridge extraction. To trace the ridge lines, the algorithm obtains binary ridge skeletons from the enhanced image. Ridge endings and bifurcation points are getting from the ridge skeleton and referred to as minutiae. The algorithm uses heuristic rules to detect and remove false minutiae resulting from an imperfect skeleton image.

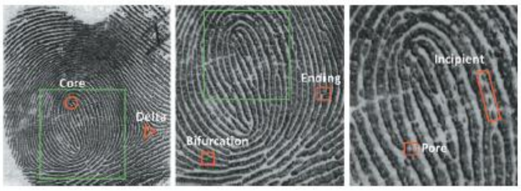


Figure 2.7: Feature levels in a fingerprint with the second and third images are magnified versions of the fingerprint regions indicated by green boxes in the corresponding preceding images.

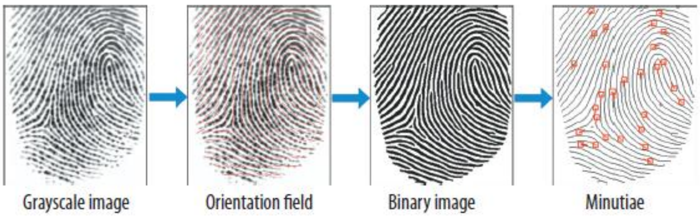


Figure 2.8: Flow chart of a typical minutiae feature extraction algorithm.

2.1.2.3 Matching

A fingerprint matching module counts a match score between two fingerprints, which is high from the same finger and low from different fingers for fingerprints. Fingerprint matching is a difficult pattern recognition problem because too-large intraclass variations in fingerprint images of the same finger and large interclass similarity between fingerprint images from different fingers. Intraclas's variations caused by finger pressure and placement like rotation, translation and contact area relate to the sensor and condition of the finger, including skin dryness and cuts. Interclass similarity probably large because there are only three types of major fingerprint patterns, which are arched, loop and whorl.

Fingerprint matching algorithms adopt one of four approaches, whether image correlation, phase matching, skeleton matching and lastly minutiae matching.

Nowadays, local minutiae structure is used in minutiae matching to quickly find a rough alignment of two fingerprints and then combine the local matching results at a global level that consists of four steps. Firstly, the algorithms counts and compare a pair of similarity between minutiae of two fingerprints to rotation and translation. Secondly, two fingerprints are aligning based on the most similar minutiae pair. Thirdly, the algorithms create minutiae correspondence that is close enough in location and Directions are considered to be corresponding minutiae. Finally, the algorithm counts the similarity score to show the match between two fingerprints based on factors, which is the number of matching minutiae, the percentage of matching minutiae in the overlapping area of two fingerprints and the consistency of ridge count between matching minutiae.

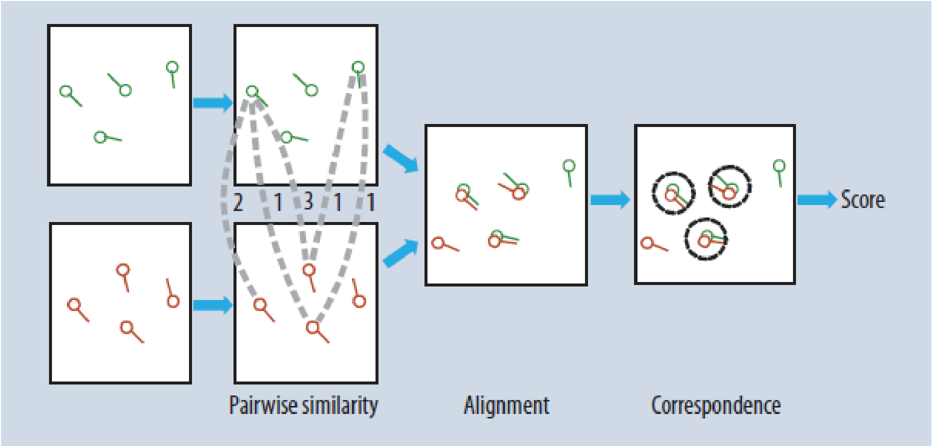


Figure 2.9: Typical minutiae matching algorithm. The algorithm first uses local minutiae descriptors to coarsely align two fingerprints and then computes a global match score based on minutiae correspondences.

2.1.3 Adaptable Fingerprint Minutiae Extraction Algorithm Based-On Crossing Number Method For Hardware Implementation Using Fpga Device [3]

This fingerprint recognition system focused in developing and implementing fingerprint extraction and matching algorithms. There are two steps, which develop a simple algorithm with extracting fingerprint features to test algorithm at PC and implement the algorithm using FPGA devices.

2.1.3.1 Fingerprint Minutiae Extraction Algorithm

The algorithm consists of several processes based on crossing number method. The process includes image enhancement process, binarization, thinning process, fingerprint feature extraction and angle calculation block.

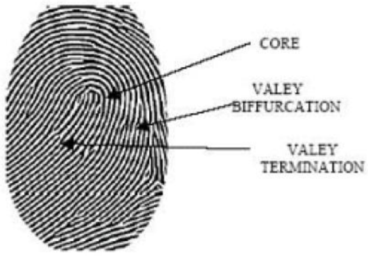
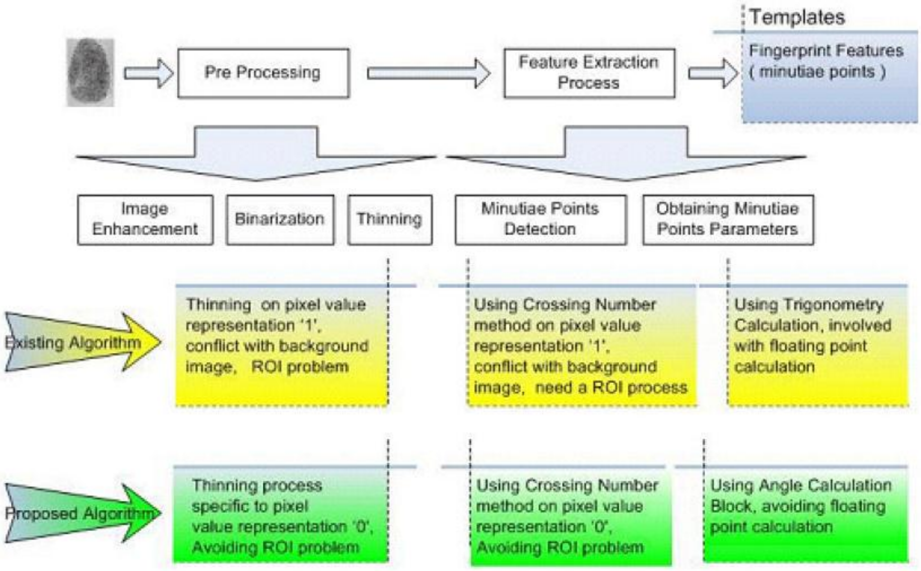


Figure 2.10: Structure of Fingerprint Image

In the image enhancement processes, the fingerprint is enhanced for better quality to the fingerprint image to provide good results in detecting minutiae points as templates. Binarization process converts fingerprint images from gray scale to binary image. At thinning process, one pixel width representation of fingerprint structure. Minutiae points' detection will detect the minutiae points that exist and define the type of the minutiae based on Crossing Number. Lastly in order to obtain minutiae point's parameters the calculation of the direction of minutiae point is defined in using angle calculation block.



Templates
Fingerprint Features (minutiae points)
Pre Processing
Feature Extraction Process
Image Enhancement
Binarization
Thinning
Minutiae Points Detection
Obtaining Minutiae Points Parameters
Existing Algorithm
Thinning on pixel value representation '1', conflict with background image, ROI problem
Using Crossing Number method on pixel value representation '1', conflict with background image, need a ROI process
Using Trigonometry Calculation, involved with floating point calculation
Proposed Algorithm
Thinning process specific to pixel value representation '0', Avoiding ROI problem
Using Crossing Number method on pixel value representation '0', Avoiding ROI problem
Using Angle Calculation Block, avoiding floating point calculation

Diagram 2.1 : Schema of fingerprint minutiae extraction algorithm.

2.1.3.2 Thinning Algorithm Experimental Result

The thinning algorithm is customized to match with the image of the fingerprint.

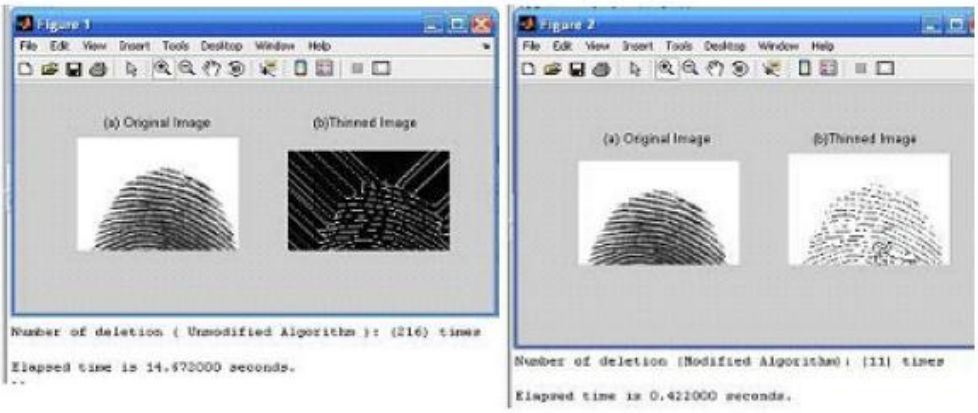


Figure 1
File Edit View Insert Tools Desktop Window Help
(a) Original Image
(b)Thinned Image
Figure 2
File Edit View Insert Tools Desktop Window Help
(a) Original Image
(b)Thinned Image

```
Number of deletion ( Unmodified Algorithm ): (216) times

Elapsed time is 14.672000 seconds.
```

```
Number of deletion (Modified Algorithm): (11) times

Elapsed time is 0.422000 seconds.
```

Figure 2.11: Thinning result, (a) original thinning algorithm (b) modified thinning algorithm.

2.1.3.3 Minutiae Points Extraction Algorithm Experimental Result

Pre-processing in minutiae points extraction algorithm shows the minutiae extraction process result from fingerprint image without enhancement to better results. The result is better in the enhancement process.

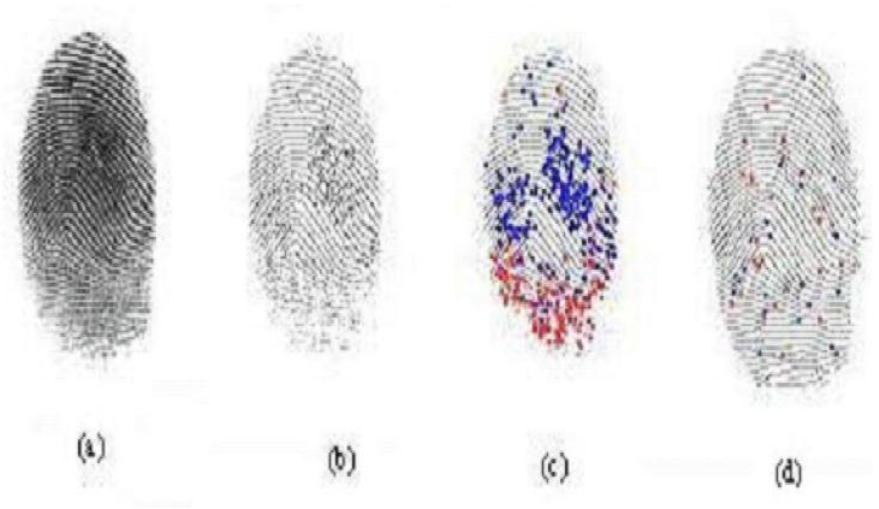


Figure 2.12: Image enhancement result, (a) original image 101 2.tif, (b) thinned image without enhancement (c) minutiae point detected without enhancement and (d) minutia point detected with image fingerprint enhancement.

2.2 Propose System

There are several goals in using computer and network security. Firstly, is to keep from an unauthorized user by accessing to the resources and secondly is to ensure only authorized people can access to the resources. Authentication types such as using password, smart cards and biometrics.

As known fingerprint is one example of biometrics, which have their uniqueness and permanent over time from each person. Fingerprint is used for identification due to development in computing capabilities. There are many advantages when using fingerprint for authentication. Fingerprint is more secure used as a replacement of the personal identification.

For the hardware, there is a variety of types of sensor used to collect digital image of a fingerprint surface. In software, there are two categories for fingerprint matching, which is minutiae-based matching and pattern matching techniques.

In this system, users need to register all of their information in enrollment form. Fingerprints are then taken and are saving in a database. Next users just need to thumbprint their finger, and the information are retrieved.

2.3 Comparison between Existing System and Propose System

Table 2.1 Comparison between existing systems

	Algorithm level	**Challenges**
i. **Fingerprint Recognition System**	• Pre-processing stage • Minutia extraction stage • Post processing stage.	• Robust feature extraction from low quality fingerprints • Matching elastically deformed fingerprints • Efficient search of fingerprint in a database