TABLE OF CONTENTS

CERTIFICATION OF APPROVAL

UTP Cafeteria Cashless Payment System using Fingerprint Recognition

by

Nurul Hafiah Binti Ahmad

A project dissertation submitted to the
Computer and Information Sciences Programme
Universiti Teknologi PETRONAS
in partial fulfillment of the requirement for the
BACHELOR OF TECHNOLOGY (Hons)
(BUSINESS INFORMATION SYSTEM)

Approved by,

Mr Yew Kwang Hooi

UNIVERSITI TEKNOLOGI PETRONAS
TRONOH, PERAK
OCTOBER 2007

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contain herein have not been undertaken or done by unspecified sources or persons.

-Nurul-

NURUL HAFIAH BINTI AHMAD

ABSTRACT

Cashless payment system is one of the most significant improvements in food service and is transforming today's quick service especially for campus or high school cafeteria. There are several medium for cashless payment system which include using smart cards or credit cards and biometric technologies. There are many problem associated with smart cards and credit cards technologies since people might forget the password. With cards to identify a person, whoever has possession of the card can again access. Biometric technologies have its different features to remedy this problem. A biometric system cannot be implemented the same way as one utilizing password since there will be no physical items. One reason a biometric system is valuable is in the way it authenticate users. A biometric system offers levels of physical security, integrity and confidentiality. This research focuses on the development of Cashless Payment System for UTP Cafeteria using fingerprint recognition, a system which enables students to make payment for foods that they purchased using the touch of their finger. Intensive research and literature review had been done in order to obtain as much information to develop the project. Surveys had been done over some group of students to obtain data on their feedback regarding the development of the system. The project will solve problems that arise from the cash based system which is currently used by all café owners in UTP.

ACKNOWLEDGEMENT

Thank you All Mighty Allah for lending me the strength to complete this Final Report and above all completing the Final Year Project (FYP) Part One and Part Two. This page is dedicated to give my fullest appreciation and thank you to all the people involved directly or indirectly during two semester's period of Final Year Project (FYP) Part One and Part Two.

First and foremost, I would like to convey my gratitude to my Final Year Project (FYP) Supervisor, Mr Yew Kwang Hooi, for offering me his supervision under the Multimedia and Communication System cluster of the Computer and Information Sciences Department. He is a supportive and highly motivated supervisor who monitored my progress along the two semester period. Because of his ideas and critics, I was able to successfully complete Final Year Project in UTP. He showed flexibility in the correct way but at the same time made sure that I am conscious with the requirements to complete and submit deliverables before deadline.

Secondly, I would like to thank my parents for being so supportive during my completion of my Final Year Project. They supported me all the way, in terms of motivation, financial and other important aspects. They are also very concern on how I have been doing for my project.

Last but not least, to all of my friends who had been very contributive and helpful in terms of ideas, technical knowledge and keep me encouraged at the fullest level at all times.

LIST OF FIGURES:

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1. INTRODUCTION

1.1 Background of Study

The implementation of cashless payment system using biometric technologies has been emerging recently. It is not only implemented within campus environment but also in government agencies and hypermarket including the largest hypermarket in the world which is Wal-Mart.

Not all people have come across the words and understand what biometric technologies are. Biometric refers to the use of an automated system to verify personal identity through physiological or behavioral characteristics. Biometric technologies form the basis for highly secure identification and verification systems. With identity theft and fraudulent activity increasing, biometric-based solutions can provide increased security and confidentiality of personal and financial data.

More secure than PIN numbers, passwords, social security numbers and signatures, biometrics can authenticate an individual based on unique physical attributes that are difficult, if not impossible, to copy or forge. Fingerprints are the most popular biometric characteristic used but there are also other measurable traits include: hand, retina, iris, facial, voice and handwriting recognition

Cashless payment system using fingerprint recognition will now be implemented in UTP cafeteria and this will enable students to make food payment using the touch of their finger. We would never imagine how convenient the transaction would be by implementing this system. With cashless payment system, as the name implied cashiers are no longer able to accept cash on student's meals.

Instead of using cards or ID to recognize a user and to activate their account, it is now possible to recognize user by scanning their fingerprint. At the initial recognition stage, each user has their fingerprint scanned, converted into digital data and recorded. The image of the print itself is not recorded and cannot be regenerated from the digital data which cannot be compared to existing records of fingerprint images.

1.2 Problem Statement

1.2.1 Problem Identification

Currently, UTP does not have any system which enables students to pay for food that they purchase. The weaknesses which have been identified on the manual system are: students need to queue for more than 5 minutes while waiting for their food to be charged and paid to the café cashier and this definitely requires longer time. This usually happen during peak hours at 12.00 to 1.00PM on weekdays.

Other than that, we can see that the café cashier tends to charge more and there is also possibility of giving students the wrong balance. With the condition of rushing for classes, students usually are not aware of the wrong balance and their only concern is to have their meal. Based on the research done, payment system using fingerprint recognition would be efficient and convenient enough if some modifications in terms of functions and security elements can be made to better served students.

1.2.2 Significant of the Project

The system to be developed will provide more convenient environment to both cashier and also students. Students do not have to worry of having a long queue during lunch hours which will consume more of their time. They are also able to purchase foods and drinks even if they accidentally forget to bring along their money. Other than that, wrong balance problem or money change unavailability (where cashiers have to change the money with other café owner) will also be solved by having such system.

1.3 Objectives and Scope of Study

1.3.1 Relevancy of the Project

The objective is to develop a practical system which would be convenient not only to café cashier but also students. Using such a system will help to improve performance of daily cafeteria transaction. No cash involved, transaction will be much faster than the manual based.

Database is also important in this project. It will be used to store student's particulars as well as the transaction details such as price of foods purchased and the current balance of student's account.

Since the system involved payment for every transaction, security elements are also emphasized in this project. No students would be able to use other students account since the scheme of payment is using fingerprint recognition which is unique for every individual. The system also provides flexibility whereby if fingerprint scanner is not able to read the image due to finger condition, students will provide cashier with their account ID which has been associated with the template image during registration of their fingerprint.

CHAPTER 2
LITERATURE REVIEW

2. LITERATURE REVIEW

2.1 Approaches of biometric technologies:

The following explains the basic concept of each technology with their advantages and disadvantages:

Finger-Scan Technology

Finger-scan biometrics is based on the distinctive characteristics of human fingerprint. A fingerprint image is read from a capture device, features are extracted from the image and a template is created. Fingerprint matching techniques can be placed into two categories: minutiae based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties for this approach when the fingerprint is of low quality such that accurate extraction of minutiae points is difficult. This method also does not take into account the global pattern of ridges and furrows. In contrast, the correlation-based method is able to overcome the problems of minutiae-based approach. However it requires the precise location of a registration points and are affected by image translation and rotation.

Hand-Scan Technology

This approach uses the geometric shape of the hand for authentication. Authentication of identity using hand geometry is challenging work as hand features are not very descriptive. Hand-scan is a relatively accurate technology but does not draw on as rich a data set as finger, face or iris-scan. Hand-scan does not perform one-to-many identification very well, as similarities between hands are not uncommon.

Organizations use hand geometry readers in various scenarios including time and attendance recording for the following benefits: cards and associated administration costs can be eliminated and buddy punching is impossible.

Retina-Scan Technology

Along with iris recognition technology, retina scan is perhaps the most accurate and reliable biometric technology. However, it is difficult to use and is perceived as being moderately to highly intrusive. Retina-scan biometrics requires a cooperative, well-trained, patient audience, or else performance will fall dramatically. Retina-scan devices read through the pupil, this requires user to situate their eye within ½ inch of the capture device, and to hold still while the reader ascertains the patterns. User will look at a rotating green light as the patterns of the retina are measured at over 400 points. Retina-scan can be quite accurate but requires user to look into a receptacle and focus on a given point. This is not particularly convenient if user wears glasses or is concerned about having close contact with the reading device. For these reasons, retina scanning is not warmly accepted by all users even though the technology itself works well.

Iris-Scan Technology

Iris recognition uses the unique features of the human iris to provide an unmatched identification technology. The algorithms used in iris recognition are accurate that the entire planet could be enrolled in an iris database with only a small chance of false acceptance or false rejection. Iris-based biometric involves analyzing features found in the colored ring of tissue that surrounds the pupil. Iris-scan undoubtedly the less intrusive of the eye-related biometrics uses a fairly conventional camera element and requires no close contact between user and the reader. Iris biometrics work with glasses in place and it is one of the few technologies that can work well in identification mode. Ease of use and system integration has not traditionally been strong points with iris-scanning devices but we can expect improvements in these areas as new products emerge.

Facial-Scan Technology

Similar to finger-scan and voice-scan biometrics, there are various methods by which facial-scan technology recognizes people. All share certain commonalities, such as emphasizing those sections of the face that are less susceptible to alternation including the upper outlines of the eye socket, the areas surrounding the cheekbones and the sides of the mouth. Facial-scan can be used to control entry to buildings or computer networks by comparing the image of a person seeking access against the scan taken of that person at an earlier date that is one-to-one check. Because facial scanning needs an extra peripheral not customarily included in basic PCs, it is more of a niche market for network authentication.

Voice-Scan Technology

Of all human traits used in biometrics, the one that humans learn to recognize first is the voice characteristics. Furthermore, the bandwidth associated with speech is much smaller than the other image-based human traits. This implies faster processing and smaller storage space. A speaker-recognition system can be divided into two categories, namely text-dependent and text-independent systems. In text-dependent systems, use is expected to use the same text (keyword or sentence) during training and recognition sessions. A text-independent system does not use training text during recognition session. Both systems perform the following tasks: feature extraction, similarity analysis and selection. Texture extraction uses the spectral envelope to adjust a set of coefficients in a predictive system. One voice sample can then be compared for similarity with another sample by computing the regression between coefficients and this is a similarity analysis. A number of normalization techniques have been developed to account for variation of speech signals. Voice biometrics has the most potential for growth because it does not require new hardware since most PCs nowadays come together with a microphone. However, poor voice quality and ambient noise can affect verification. In addition, enrollment procedure has often been more complicated than with other biometrics. This leads to the perception that voice verification is not user friendly

Table 1.1 below shows comparison of various biometrics techniques based on several technical factors:

Technical Factor	**Iris**	**Retina**	**Face**	**Finger-scan**	**Voice**
Level of accuracy	Very High	Very High	High	High	High
Ease of use	Medium	Medium	Medium	High	High
Vulnerability to fraud	Very high	Very high	Medium	High	Medium
Intrusive for human beings	Medium	Medium	High	Medium	High
Long-term stability	High	High	Medium	High	Medium
Factors that may affect performance	Glasses worn by end user	none	Poor lighting, aging of face	Dry, dirty or damaged finger	Background and network noise

Table 1.1: Comparison of various biometrics techniques

Of all the biometric technologies mentioned before, fingerprints have been used for a long time and their accuracies have been proven widely. Meanwhile, other biometric system such as face scanning is newcomer to this area and need to be proven in real-time application. Fingerprint biometric has a low data-collection-error-rate and high user acceptability. Furthermore, it has also been heavily invested and applied to both the identification and the authentication problem. Finally, fingerprint biometric has the highest acceptance in the identification of community and virtually every large biometrics system in operation today uses fingerprint biometric.

Before using any biometric recognition system, user needs to enroll their features. The sensor captures three different images and changes them into mathematical algorithms that identify each finger. These algorithms help the system develop a reference template, which is stored in a secure part of a network or hard drive. When user completes this enrollment process they can use the touch of their finger to identify themselves during payment.

2.2 Introduction to fingerprint recognition:

Fingerprint identification is based on two basic premises:

- Persistence: The basic characteristics of fingerprints do not change with time. The validity of this first premise has been established by the anatomy and morphogenesis of friction ridge skin.
- Individuality: The fingerprint is unique to an individual. This second premise has been generally accepted to be true based on empirical results; the underlying scientific basis of fingerprint individuality has not been formally tested.

In order to come out with cashless payment system using fingerprint recognition for UTP cafeteria, we must first understand how basically fingerprint recognition works:

1) **Scanning:**

Users scan their finger on the fingerprint scanner. The scanner captures a 3D image of the fingertips and this sample image is sometimes called the live-scan template.

Figure 1.1: User scans finger

2) **Feature Extraction:**

The system extracts unique data (minutiae) from the sample that user has just provided and converts that sample into code (or template) using a complex algorithm. After the computer extracts these features, it discards the actual 3D image of the finger. That means no one can retrieve the actual fingerprint for potential misuse.

Figure 1.2: Data extracted from sample

3) **Association or Comparison:**

The system compares the live-scan template with the reference templates stored in the database. In most systems this step is nearly instantaneous. In some cases, however, there are a couple of factors that may cause problems. First is the quality of the fingerprint scanner. Some scanners cost next to nothing to manufacture, and thus, do not capture clear print samples for database comparison.

Second, if the reference templates were not exceptionally clear to begin with, the system may have trouble finding a match for the live-scan. The speed of identification for fingerprint would be around 2 seconds and the maximum of 20 seconds.

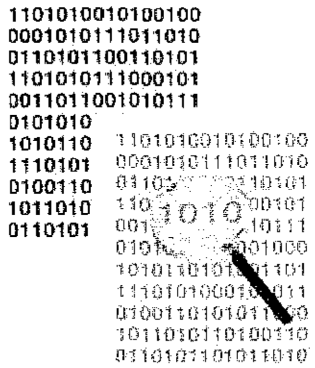


Figure 1.3: Live-scan template compared with reference template

4) **Decision:**

The system locates near matches and begins analyzing the live-scan template to determine if it has sufficient biometrics for an exact match. The entire process takes only a second or two, because the system compares the live-scan template with the stored reference templates at a rate of approximately 200 to 500 templates per second. If the lives-can template meets the predetermined threshold the identification is successful.

2.3 Algorithms for fingerprint recognition:

Fingerprint Recognition Algorithm

The fingerprint recognition algorithm composed of two main technologies which are *image processing technology* that captures the characteristics of the corresponding fingerprint by having the image under-going several stages, and *matching algorithm technology* that authenticates the identity by comparing feature data comprised of minutiae with templates in a database.

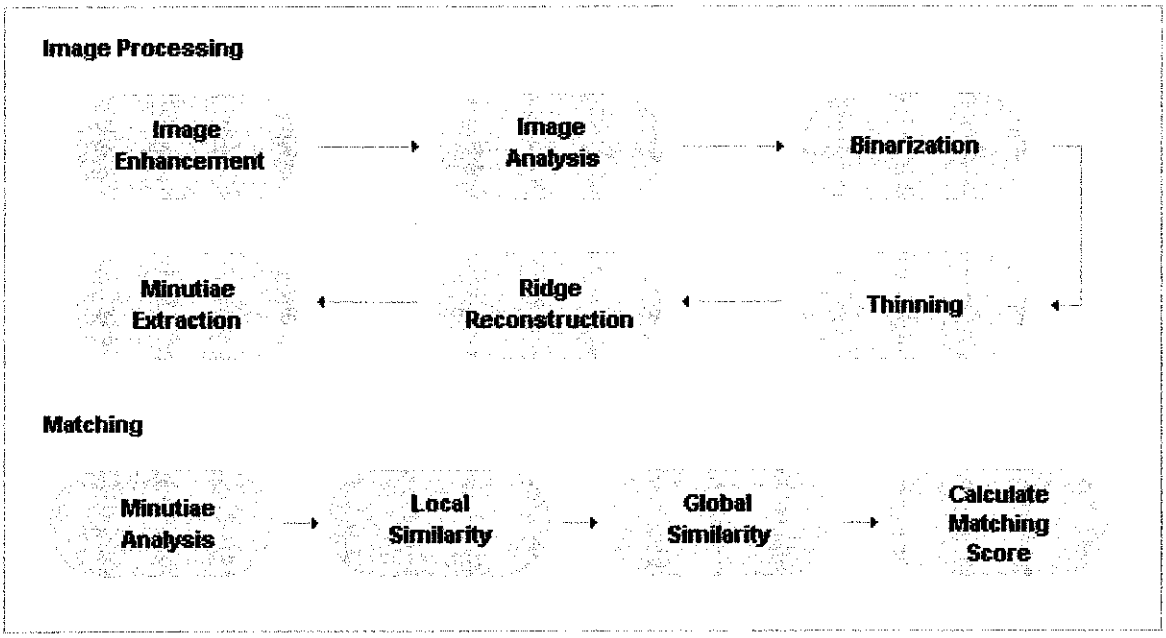


Figure 1.4: Block map of the fingerprint recognition algorithm consisting of the two technologies

1) Image Processing Algorithm

This part consists of six stages. At the image enhancement stage, noise on the input fingerprint image is eliminated and contrast is fortified for the sake of successive stages. At the image analysis stage, area where fingerprint is severely corrupted is cut out to prevent adverse effects on recognition. The binarization stage is designed to binarize a gray-level fingerprint image. The thinning stage thins the binarized image.

The ridge reconstruction stage reconstructs the ridges by removing pseudo minutiae. At the last stage, minutiae are extracted from the reconstructed ridge image.

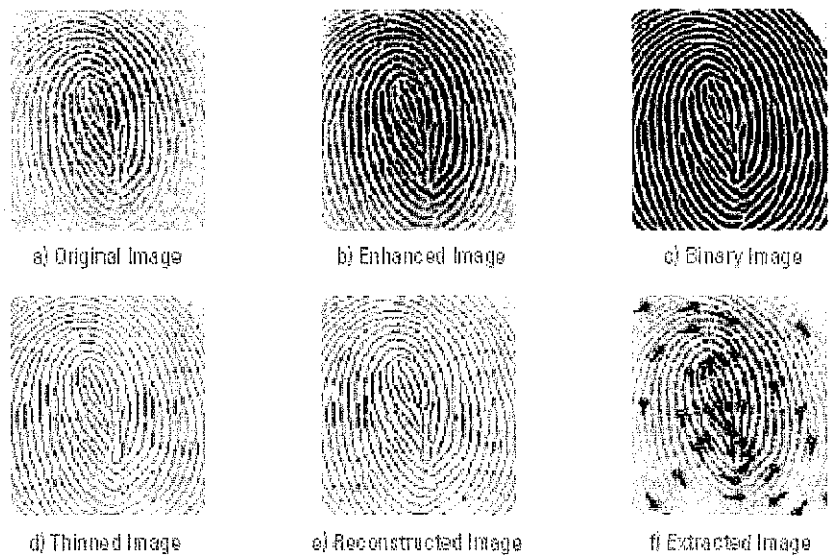


Figure 1.5: Stages involved in image processing technology algorithm

2) Matching Algorithm

There are 2 common matching algorithms which are *minutia based* and *pattern-based.* Minutia matching compares specific details within the fingerprint ridges while pattern matching compares the overall characteristics of the fingerprints.

After obtaining feature data of a specific fingerprint, compare them with the template stored in the database. If the fingerprint is immensely destructed and only general ridges, not minutiae, can be recognized, two algorithms can be used in parallel: an algorithm based on minutiae and an algorithm based on the overall ridge shape.

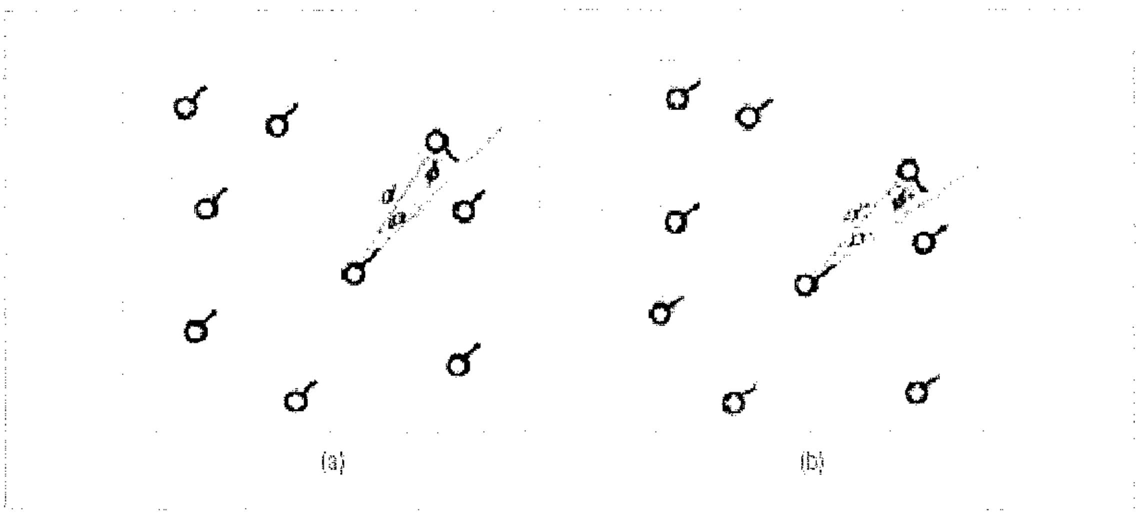


Figure 1.6: Picture (a) shows feature data of the input fingerprint, and (b) shows the already stored template.

Matching stages show big differences according to their types although they are based on the same minutiae. Here, the most well-known matching algorithm will be briefly explained. The matching process consists of four main stages:

First of all, the minutiae analysis stage analyzes the geometric characteristics such as distance and angle between standard minutiae and its neighboring minutiae based on the analysis of the image-processed feature data. After the analysis, all the minutiae pairs have some kind of geometric relationship with their neighboring minutiae, and the relationship will be used as basic information for local similarity measurement.

Finding a similar minutiae pair in (b) against a minutiae pair in (a) is the local similarity measurement. Global similarity measurement means calculating similarity of two fingerprints by finding minutiae pairs in the local similarity measurement in both feature data and selecting the greatest matching minutiae pairs in the feature data.

Lastly, calculating final matching scores with the global similarity value and comparing them with the previously set critical value verifies the identity of the user.

Minutia Based

Every fingerprint consists of a number of ridges and valleys. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form so-called minutia points; ridge ending where a ridge ends and ridge bifurcations where a ridge splits.

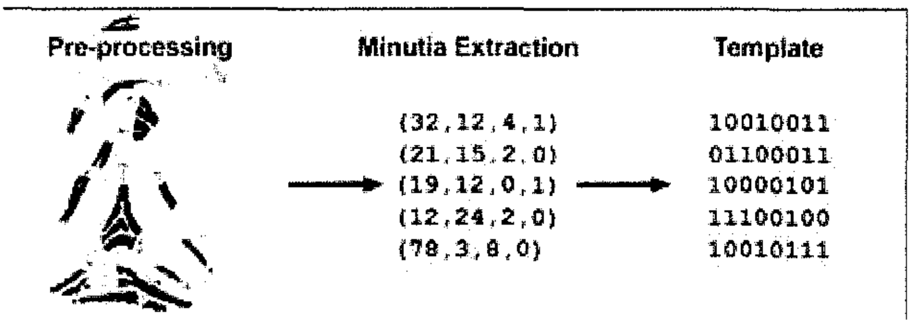


Figure 1.7: Enrolment of minutia points

At registration enrollment, the minutia points are located (Figure 1.7) and the relative positions to each other and their directions are recorded. This data forms the template, the information later used to authenticate a person. At the matching stage (Figure 1.8), the incoming fingerprint image is pre-processed and the minutia points are extracted. The minutia points are compared with the template stored in the database, trying to locate as many similar points as possible within a certain boundary. The result of the matching is usually the number of matching minutiae. A threshold is then applied, determining how large this number needs to be for the fingerprint and the template to match.

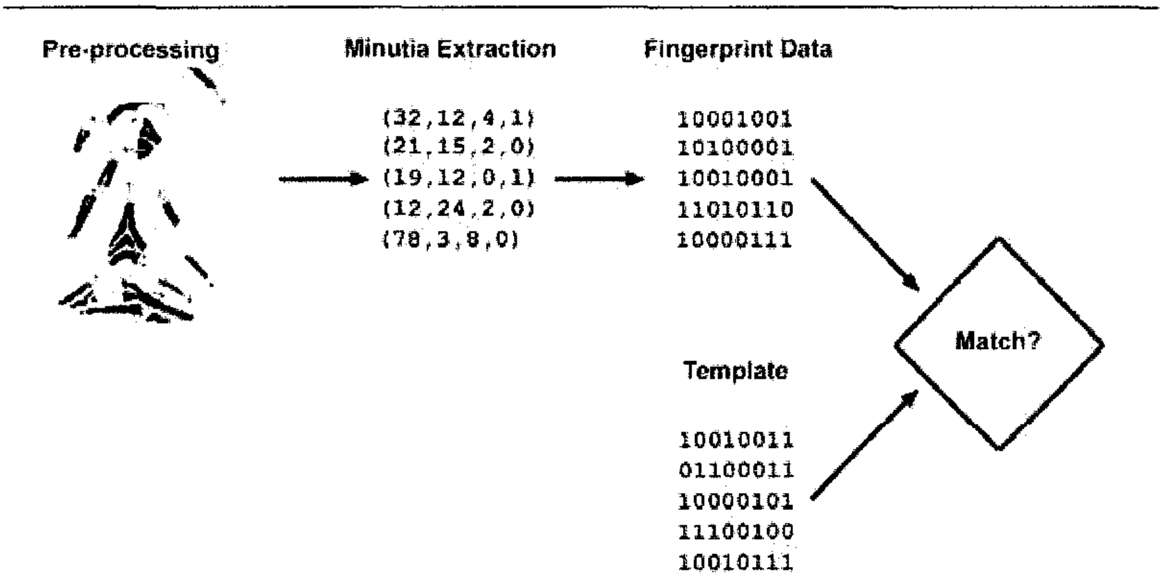


Figure 1.8: Verification using minutia points

A minutiae based fingerprint matching system usually returns the number of matched minutiae on both query and reference fingerprints and uses it to generate similarity scores. Generally, more matched minutiae yield higher similarity scores. That is when the number of minutiae on both fingerprints is large and we can confidently distinguish the genuine and imposter fingerprint using the number of matched minutiae.

Pattern Based

One intrinsic property of pattern matching algorithms is that overall fingerprint characteristics are taken into account, not only individual points. Fingerprint characteristics can then include sub-areas of certain interest including ridge thickness, curvature, or density. Due to this increased depth of data, a pattern-based algorithm is less dependent on the size of the fingerprint sensor and is independent of the number of minutiae points in a fingerprint. Pattern-based algorithms do not, to the same extent as minutia-based methods, suffer from difficulties of recognizing a finger with varying fingerprint quality.

1) Precise Pattern-Based Algorithm

During enrollment, precise biometrics' patented pattern matching algorithm locates sub-areas of the fingerprint image instead of registering minutia points. Small sections of the fingerprint and their relative distances are extracted from the fingerprint (Figure 1.9) in order to maximize the amount of unique information. Areas of certain interest are for example the area around a minutia point and areas with low curvature radius. The main structure and unusual combinations of ridges are also valuable data.

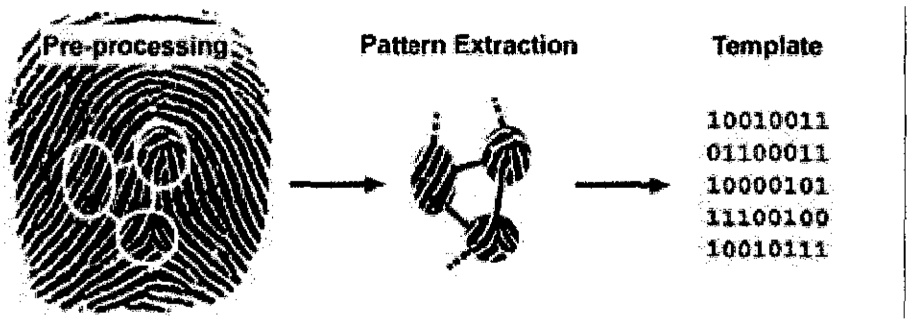


Figure 1.9: Enrolment with pattern-based algorithm

The verification procedure (Figure 2.0) begins with the pre-processing of the incoming fingerprint image. The registered small images from the template are then compared with the fingerprint image to determine to what degree the template matches the image. A threshold describing the smallest allowable deviation is then used to decide if the finger matches the stored template.

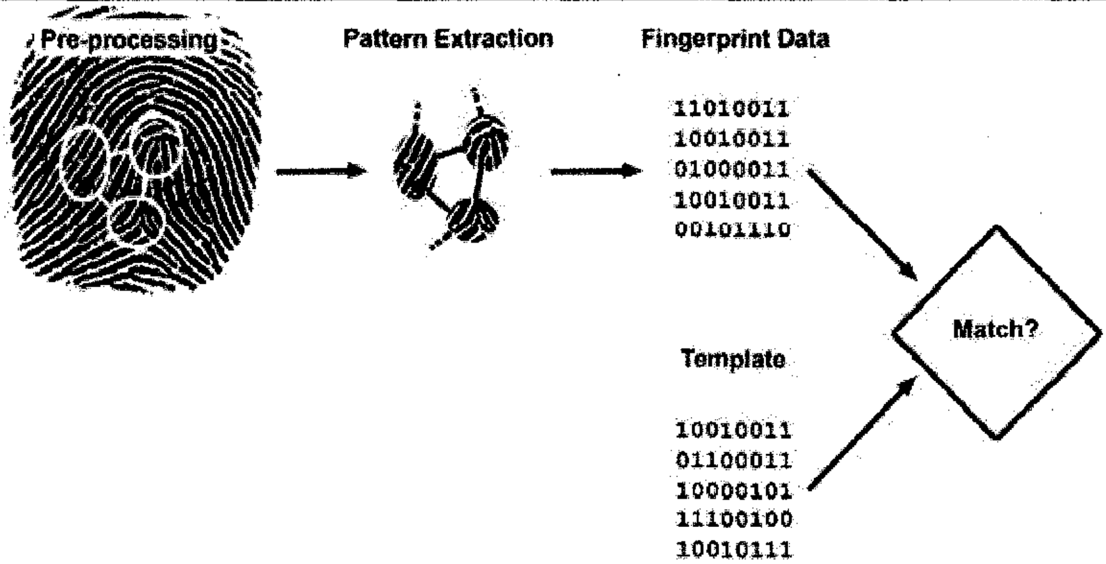


Figure 2.0: Verification using pattern-based algorithm

2.4 Minutia based partial fingerprint issue:

Another concern for this project that we need to observe is, if we are having fingerprint scanners with a sensing area smaller than 0.5"x0.7", which is considered to be the average fingerprint size and can only capture *partial* fingerprints. Matching partial fingerprints to full pre-enrolled images in the database has several problems:

i) The number of minutia points available in such prints is few, thus reducing its discriminating power
(ii) Loss of singular points (core and delta) is likely and therefore, a robust algorithm independent of these singularities is required
(iii) Uncontrolled impression environments result in unspecified orientations of partial fingerprints, and distortions like elasticity and humidity are introduced due to characteristics of the human skin

According to forensic guidelines, when two fingerprints have a minimum of 12 matched minutiae they are considered to have come from the same finger. However, it is not reasonable to use an absolute number of matched minutiae alone in case of partial fingerprints. We must also consider the overlapped areas on both prints and the total distance between all the matched minutiae to obtain a similarity score.

2.4 Fingerprint scanner selection:

It is important for this project that we use appropriate fingerprint scanner during implementation stage. Certainly, the main characteristics of a fingerprint scanner depend on the specific sensor mounted which in turn determines the image features (dpi, area, and dynamic range), size, cost, and durability. However the following features should also be taken into account when a fingerprint scanner has to be chosen for a specific application:

1) ***Interface***: FBI-compliant scanners often have analogue output and a frame grabber is necessary to digitize the images. This introduces an extra cost and usually requires an internal board to be mounted in the host. On the other hand, in non-AFIS devices, the analogue-to-digital conversion are performed by the scanner itself and the interface to the host is usually through a simple Parallel Port or USB connection
2) ***Frames per second***: This indicates the number of images the scanner is able to acquire and send to the host in a second. A high frame rate (e.g., larger than 5 frames/sec) better tolerates movements of the finger on the sensors and allows a more friendly interaction with the scanner. It can also provide a natural visual feedback during the acquisition
3) ***Automatic finger detection***: Some scanners automatically detect the presence of a finger on the acquisition surface, without requiring the host to continually grab and process frames. This allows the acquisition process to be automatically initiated as soon as the user's finger touches the sensor
4) ***Encryption***: Securing the communication channel between the scanner and the host is an effective way of securing a system against attacks. For this purpose, some commercial scanners implement state-of-the-art symmetric and public-key encryption capability
5) ***Supported operating systems***: Depending on the application and the infrastructure where the fingerprint scanners have to be employed, compatibility with more operating systems, and in particular the support of open-source operating systems such as Linux, could be an important feature

2.5 Common method of fingerprint scanning:

There are a number of different ways to get an image of somebody's finger. The most common methods today are *optical scanning* and *capacitance scanning*. Both types come up with the same sort of image, but they go about it in completely different ways.

1) ***Optical Scanner***

A fingerprint scanner system has two basic jobs: It needs to get an image of the finger, and it needs to determine whether the pattern of ridges and valleys in this image matches the pattern of ridges and valleys in pre-scanned images.

The heart of an optical scanner is a *charge coupled device* (CCD), the same light sensor system used in digital cameras and camcorders. A CCD is simply an array of light sensitive diodes called photo sites, which generate an electrical signal in response to light photons. Each photo site records a pixel, a tiny dot representing the light that hit that spot. Collectively, the light and dark pixels form an image of the scanned scene (a finger, for example). Typically, an analog-to-digital converter in the scanner system processes the analog electrical signal to generate a digital representation of this image.

The scanning process starts when a person place their finger on a glass plate and a CCD camera takes a picture. The scanner has its own light source, typically an array of light-emitting diodes, to illuminate the ridges of the finger. The CCD system actually generates an inverted image of the finger, with darker areas representing more reflected light (the ridges of the finger) and lighter areas representing less reflected light (the valleys between the ridges).

Before comparing the print to stored data, the scanner processor makes sure the CCD has captured a clear image. It checks the average pixel darkness, or the overall values in a small sample, and rejects the scan if the overall image is too dark or too light. If the image is rejected, the scanner adjusts the exposure time to let in more or less light, and then tries the scan again.

If the darkness level is adequate, the scanner system goes on to check the image definition (how sharp the fingerprint scan is). The processor looks at several straight lines moving horizontally and vertically across the image. If the fingerprint image has good definition, a line running perpendicular to the ridges will be made up of alternating sections of very dark pixels and very light pixels. If the processor finds that the image is crisp and properly exposed, it proceeds to compare the captured fingerprint with fingerprints in file

2) ***Capacitive Scanner***

Like optical scanners, capacitive fingerprint scanners generate an image of the ridges and valleys that make up a fingerprint. But instead of sensing the print using light, the capacitors use electrical current.

The sensor of capacitive scanner is made up of one or more semiconductor chips containing an array of tiny cells. Each cell includes two conductor plates, covered with an insulating layer. The cells are tiny and smaller than the width of one ridge on a finger. The sensor is connected to an integrator, an electrical circuit built around an inverting operational amplifier. The inverting amplifier is a complex semiconductor device, made up of a number of transistors, resistors and capacitors. The details of its operation would fill an entire article, but here we can get a general sense of what it does in a capacitive scanner.

Like any amplifier, an inverting amplifier alters one current based on fluctuations in another current. Specifically, the inverting amplifier alters a supply voltage. The alteration is based on the relative voltage of two inputs, called the inverting terminal and the non-inverting terminal. In this case, the non-inverting terminal is connected to ground, and the inverting terminal is connected to a reference voltage supply and a feedback loop. The feedback loop, which is also connected to the amplifier output, includes two conductor plates.

The two conductor plates form a basic capacitor, an electrical component that can store up charge. The surface of the finger acts as a third capacitor plate, separated by the insulating layers in the cell structure and, in the case of the fingerprint valleys, a pocket of air. Varying the distance between the capacitor plates (by moving the finger closer or farther away from the conducting plates) changes the total capacitance (ability to store charge) of the capacitor. Because of this quality, the capacitor in a cell under a ridge will have a greater capacitance than the capacitor in a cell under a valley.

To scan the finger, the processor closes the reset switch for each cell, which shorts each amplifier's input and output to balance the integrator circuit. When the switch is opened again, and the processor applies a fixed charge to the integrator circuit, the capacitors charge up. The capacitance of the feedback loop's capacitor affects the voltage at the amplifier's input, which affects the amplifier's output. Since the distance to the finger alters capacitance, a finger ridge will result in a different voltage output than a finger valley.

The scanner processor reads this voltage output and determines whether it is characteristic of a ridge or a valley. By reading every cell in the sensor array, the processor can put together an overall picture of the fingerprint, similar to the image captured by an optical scanner.

The main advantage of a capacitive scanner is that it requires a real fingerprint-type shape, rather than the pattern of light and dark that makes up the visual impression of a fingerprint. This makes the system harder to trick. Additionally, since they use a semiconductor chip rather than a CCD unit, capacitive scanners tend to be more compact that optical devices.

2.6 Risk Analysis for Fingerprint Systems

Generally, fingerprint systems capture images of fingerprints, extract features from the images, encrypt the features, transmit them on communication lines, and then store them as templates into the database. Some systems encrypt templates with a secure cryptographic scheme and manage not whole original images but compressed images. Therefore, it is said to be difficult to reproduce valid fingerprints by using the templates. Some systems are secured against a so-called replay attack in which an attacker copies a data stream from a fingerprint scanner to a server and later replays it, with a one time protocol or a random challenge response device.

In this section, the concern is the security of fingerprint scanners. When a legitimate user has registered her/his live finger with a fingerprint system, there would be several ways to deceive the system. In order to deceive the fingerprint system, an attacker may present the following things to its fingerprint scanner:

1) ***The registered finger***: The highest risk is being forced to press the live finger against the scanner by an armed criminal, or under duress. Another risk is being compelled the legitimate user to fall asleep with a sleeping drug, in order to make free use of her/his live finger. There are some deterrent techniques against these crimes. Combination with another authentication method, such as PIN number, passwords, or ID cards, would be helpful to prevent the crimes. Furthermore, a duress control enables the users to alarm "as under duress" with a secret code or manner, which is different with a PIN or usual manner respectively. Combining a duress control with a fingerprint system would provide a helpful measure to apply to someone for protection.

2) ***An unregistered finger (an imposter's finger)***: An attack against authentication systems by an imposter with his own biometrics is referred to as non-effort forgery. Commonly, accuracy of authentication of fingerprint systems are evaluated by the false rejection rate (FRR) and the false acceptance rate (FAR).

The FAR is important indicator for the security against such a method as with an unregistered finger. Moreover, fingerprints are usually categorized as "loops," "whorls," "arches," and others. If an attacker knows what category of the registered finger is, an unregistered finger of which pattern is similar to the registered one would be presented to the scanner. In this case, the probability of the acceptance may differ from the ordinary FAR. From this point of view, the accuracy of authentication for the system should be evaluated not only for fingers throughout the categories of fingerprints but also for fingers within each category. Another attacker may modify his fingerprint by painting, cutting, or injuring his own fingertip. However, it is thought to be very difficult to deceive the fingerprint system with such a modified finger. The reason for this is that fingerprints are so random the attacker cannot identify which patterns should be modified. Ordinarily, ten-odd features, such as ridges and valleys distinctive patterns are used for the authentication.

3) ***A severed fingertip from the registered finger***: A horrible attack may be performed with the finger which is severed from the legitimate user's hand. Even if the finger severed from the user's half-decomposed corpse, the attacker may use a scientific crime detection technique to clarify its fingerprint for the wrong purpose. In the same way as the above mentioned registered finger, combination with another authentication method, or a duress/two-persons control would be helpful to prevent these crimes. The detection whether the finger is alive or not would be helpful as well.

4) ***A genetic clone of the registered finger***: In general, it is said that identical twins do not have the same fingerprint, and neither would clones. The reason is that fingerprints are not entirely genetically determined, and rather determined in part by its pattern of nerve growth into the skin. As a result, this is not exactly the same even in identical twins. However, it is also said that fingerprints are different in identical twins, but only slightly different. If the genetic clone's fingerprint is similar to the registered fingers, an attacker may try to deceive fingerprint systems by using it. We must keep a close watch on such possibility with genetic engineering.

5) ***An artificial clone of the registered finger***: More casual attacks against fingerprint systems may use an artificial finger. An artificial finger can be produced as a printed fingerprint with a copier or a desk top publishing (DTP) technique as well as forged documents. If an attacker can make a mold of the registered finger directly modeling it, s/he can produce an artificial finger with some materials. Even if not, s/he may make a mold of the registered finger modeling its residual fingerprint at second hand, so as to produce an artificial finger. And, if an attacker can make an artificial finger which can deceive a fingerprint system, one of countermeasures against the attack obviously is the detection whether or not the finger is real. Again, combination with another authentication method, or two-person control would be also helpful to deter the crimes.

6) ***The others***: In some fingerprint systems, an error in authentication may be caused by making noise or flashing a light against the fingerprint scanner, or by heating up, cooling down, humidifying, impacting on, or vibrating the scanner outside its environmental tolerances. Some attackers may use the error to deceive the system. This method is well-known as a "fault based attack," and may be carried out with above-mentioned attacks. Furthermore, a fingerprint image may be stood out in strong relief against the scanner surface, if we spray some materials on the surface. The image would be the residual fingerprint of a registered finger. In this case, a bald thing or finger, regardless of real or not, which are pressed on the surface, may be accepted by the fingerprint system.

CHAPTER 3
METHODOLOGY / PROJECT WORK

3. METHODOLOGY / PROJECT WORK

3.1 Procedure Identification

In this project, Spiral Development Model is chosen as the development methodology. Spiral Methodology takes advantage of the fact that development projects work best when they are both incremental and iterative, where developer benefit from enlightened trial and error along the way. The spiral methodology reflects the relationship of tasks with rapid prototyping, increased parallelism, and concurrency in design activities (Refer Figure 3).

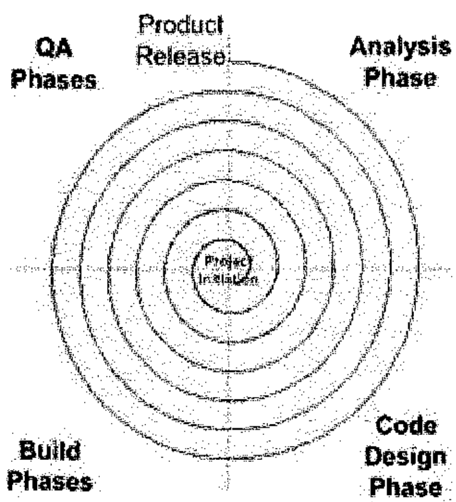


Figure 2.1: Spiral Development Model

Basic Principles of Spiral Development Model:

1. Focus is on risk assessment and on minimizing project risk by breaking a project into smaller segments and providing more ease-of-change during the development process

2. Each cycle involves a progression through the same sequence of steps, for each portion of the product and for each of its levels of elaboration

3. Each trip around the spiral traverses four basic quadrants: (1) determine objectives, alternatives, and constraints of the iteration; (2) evaluate alternatives; identify and resolve risks; (3) develop and verify deliverables from the iteration; and (4) plan the next iteration.

3.2 Tools / Software

The tools and software used to complete this project is listed below (Refer Table 1.2)

Software / Hardware	Minimum Requirement
Programming Language	Visual Basic
Software	Visual Basic 6.0
Database	Microsoft Access
Fingerprint Scanner	None

Table 1.2: Software and Hardware requirements

Microsoft Access: MS Access will be the database chosen for this project. It allows relatively quick development because all database tables, queries, forms, and reports are stored in the database. MS Access can be applied to small projects which do not involve multiple concurrent users because it is a desktop application. Therefore, it is most appropriate to be used for this project.

Visual Basic 6.0: Visual Basic was chosen since it is easy to learn and also to use. The language allows programmers to create GUI applications, which range from simple to fairly complex applications.

Other than software and hardware, other resources listed below have also being used for research purposes. Main access would be from the Information Resource Center (IRC).

- **Internet**
- **Text Books**
- **Journals**

3.3 System Architecture

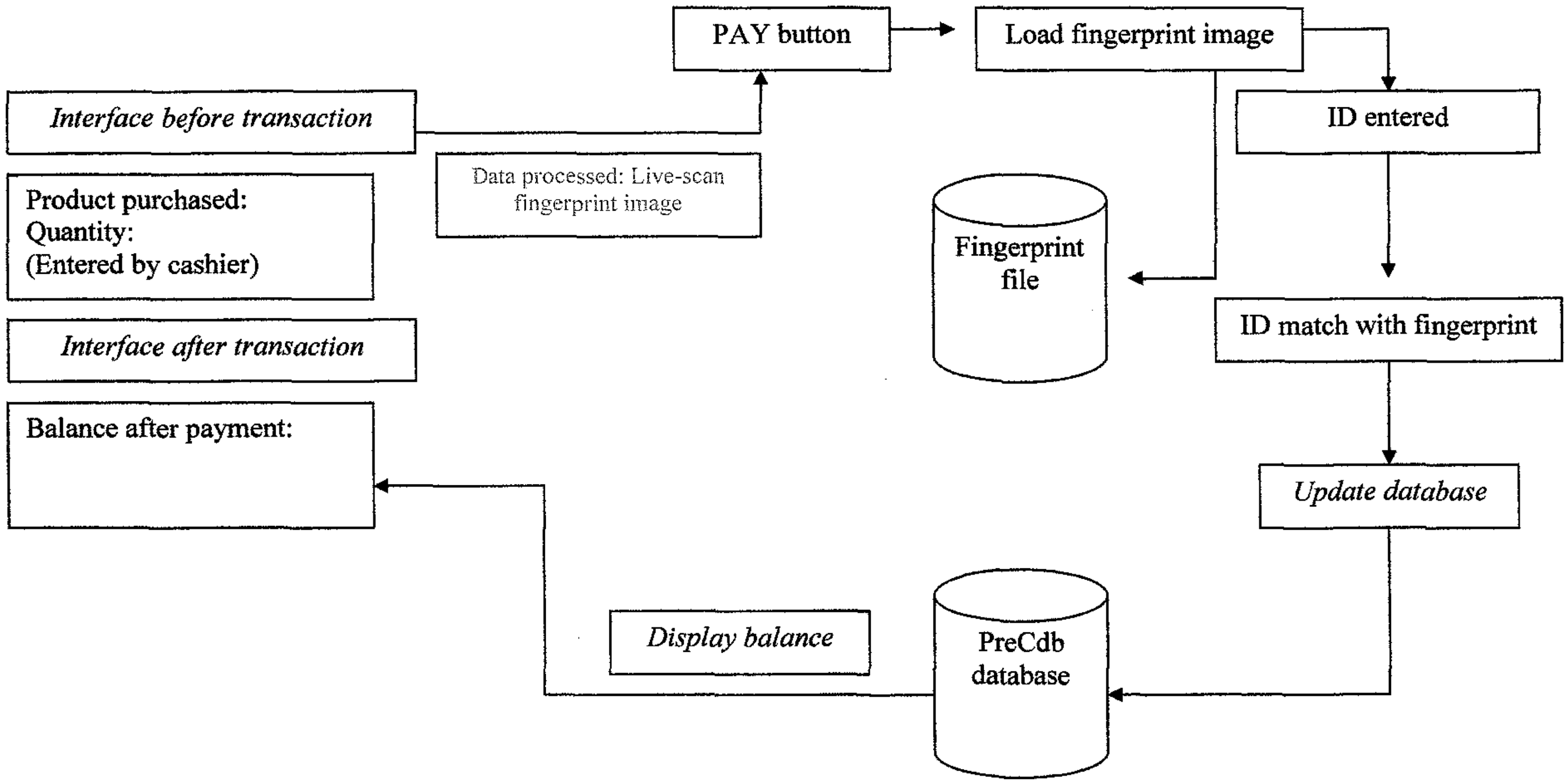


Figure 2.2: System Architecture

CHAPTER 4
RESULTS AND DISCUSSION

4. RESULTS AND DISCUSSION

4. 1 Data Gathering and Analysis

Semester 1 of FYP, for Data Gathering and Analysis, a survey was conducted for the purpose of getting adequate information on the current payment system from future user and plan to upgrade the system to cashless payment system using fingerprint for UTP cafeteria. Feedback from the respondent will help the developer to come out with a system which is able to meet the expected functionality and solve the weaknesses of the cash based system. The results of the survey involving 20 UTP students were then presented in the form of graph, pie chart and table.

4.2 Results and Discussion

4.2.1 Research Questionnaire Results

Question 1 is to see whether students are convenient with the current payment and based on the feedback received, 75% of respondents feel moderate on the current system while other 25% feel very convenient with it.

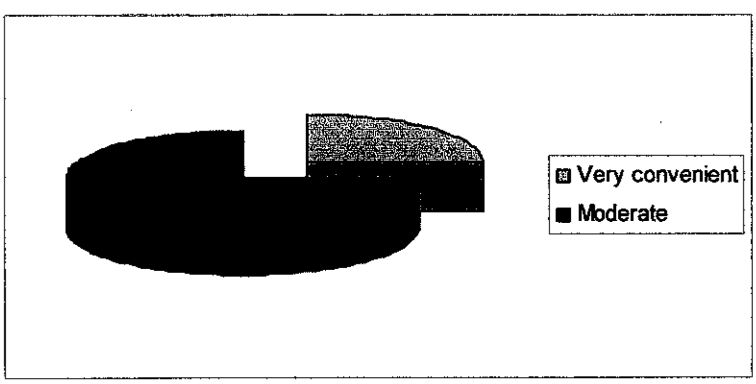


Figure 2.3: Respondents comment on the cash based payment

Question 2 asked about any problems that respondents faced with the current payment system. If respondents faced problems, they are allowed to state and elaborate the problems briefly. 60% of respondents face problem with the manual payment and the most common problem that they faced is the efficiency of the transaction. There are times when cashier is not able to provide students with enough balance and caused them to wait for the cashier to look for the remaining balance.

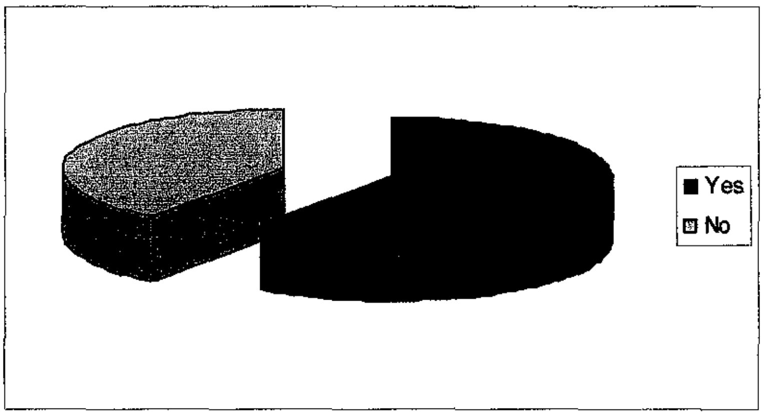


Figure 2.4: Problems faced by students

Question 3 asked whether the current manual payment consume much of respondents time during lunch hours specifically during weekdays. 50% said that manual system consume much of their time since they have to wait for other students along the line to pay for their foods.

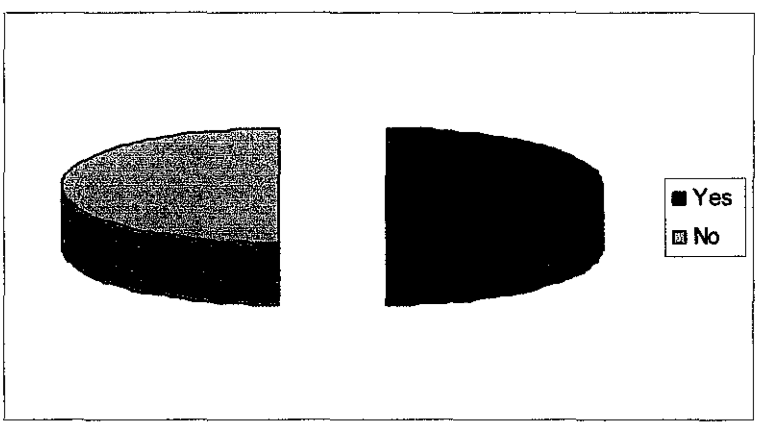


Figure 2.5: Students responds on manual system

Question 4 is to see if respondents have information or know generally about cashless payment system. 40% of respondents ever heard of cashless payment system and Question 5 which is related to the previous question asked where they get the information from. 60% get information from reading while other 40% get information from internet search and relative friends.

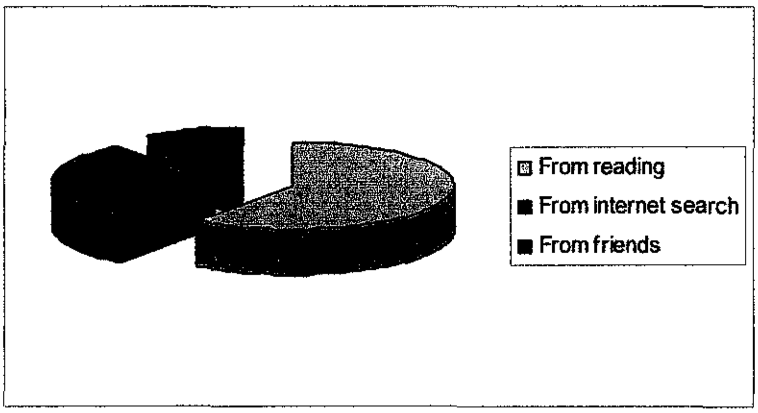


Figure 2.6: Source of information on Cashless Payment System

Question 7, 8 and 9 relate to one another. Question 7 asked whether respondents are willing to use the system once it has been implemented and 85% of them respond by definitely saying yes. Question 8 asked the relevancy of having such system for UTP café and again 85% of responds looking forward to use such system in the future. The last question asked whether cashless payment would be helpful to UTP students and the same percentage of respondents answer yes. The green color indicates answers for Question 7 and the two other colors indicate Question 8 and 9 accordingly.

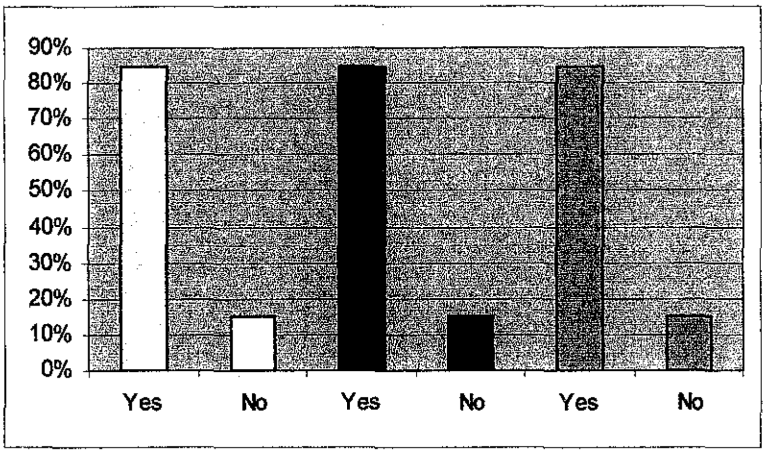


Figure 2.7: Responds towards Cashless Payment System for UTP Cafeteria

Based on the implementation framework of biometric authentication, author identified that future user of this system is the main determination of the new system success. Therefore, the analysis done under this section really helps developer to come out with the new system which is of high user acceptability.

4.2.2 Evaluation Questionnaire Results

Semester 2 of FYP, once the system has been developed, user acceptance testing was conducted by having user to use the system and later gives their feedback by answering the evaluation questionnaire to see how well they accept the developed system. The questionnaire also allows users to specify any ideas or suggestions in order to enhance and improve the system. The results from the testing were summarized and presented in tables and pie chart on the next page.

Users rated the system based on 2 main characteristics which are:

1) Functionality
2) Performances

1) Functionality

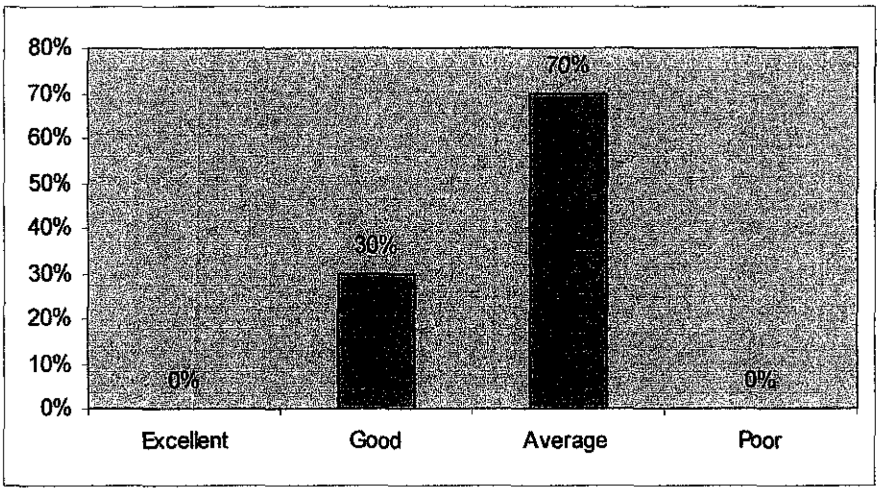


Figure 2.8: Result on functionality of the system

Based on the result shown in Figure 2.8, students mostly rated the system on average while others rated the system as good. This testing is done by having user to give their student id number to the café cashier. The average rating comes from students might probably because they feel insecure on the id being used since others who knows their id might use their account.

2) Performances:

Does the system improve transaction process	Percentage/total
Yes	80%
No	15%
Not Sure	5%
Total	100%

Table 1.3: Result on transaction process to make payment

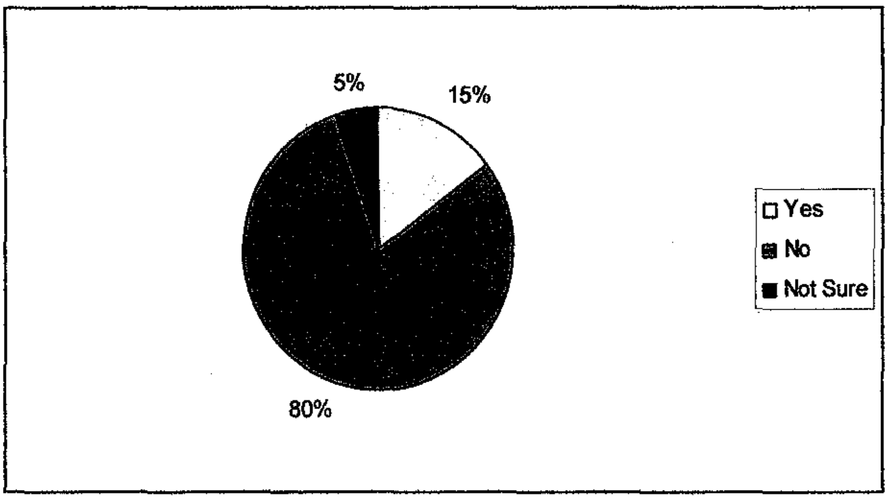


Figure 2.9: Pie chart on transaction process to make payment

Result in Figure 2.9 indicates student's rating on the transaction process to make payment. More than half students who involved in the system testing respond that the system improved the transaction process in terms of time and efficiency.

Based on the result too, it shows that the system is able to overcome the problem identified from the current cash based system whereby students do not have to queue for longer time since the transaction process is much faster.

Did you faced difficulty while using the system	Percentage/total
Yes	90%
No	10%
Not Sure	0%
Total	100%

Table 1.4: Result on whether students faced difficulty while using the system

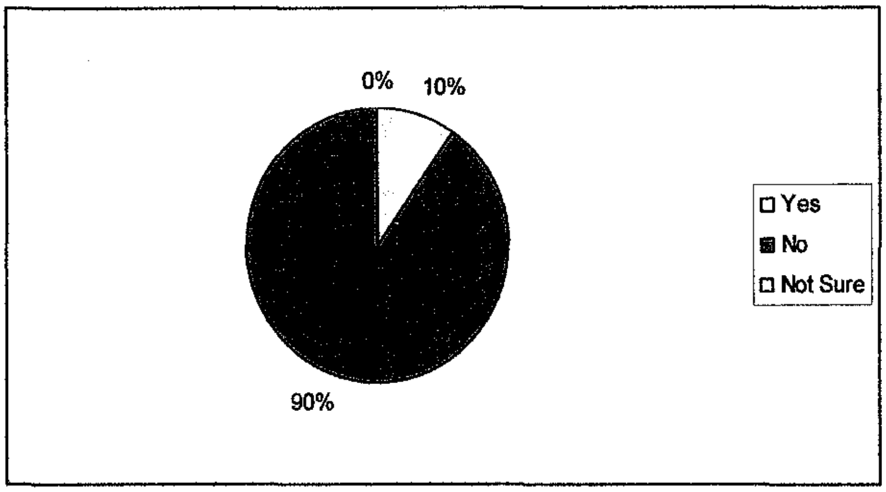


Figure 3.0: Pie chart on whether students faced difficulty while using the system

Figure 3.0 on the other hand shows that most students do not have any difficulty while using the system as the system is simply easy to use by only having them to give their student id to the café cashier.

3) Respondent Opinion

There are many ideas received from students through the evaluation questionnaire to enhance or make little modifications on the system. This shows that there are still improvements and adjustments which can be made to the system. All ideas are included under Recommendation Section in Chapter 5 of this report.

4.3 Development of Cashless Payment System

Semester 2 is continued by starting the development of the project based on the numerical and statistical data obtained from survey during the first semester using Visual Basic 6.0 and Microsoft Access.

4.3.1 Database Design

Database for this project is created using Microsoft Access. The system contains 2 databases as follows:

1) Point of sales database: This database manages every transaction that takes place. It consists of the following tables; Category, Invoice and Product

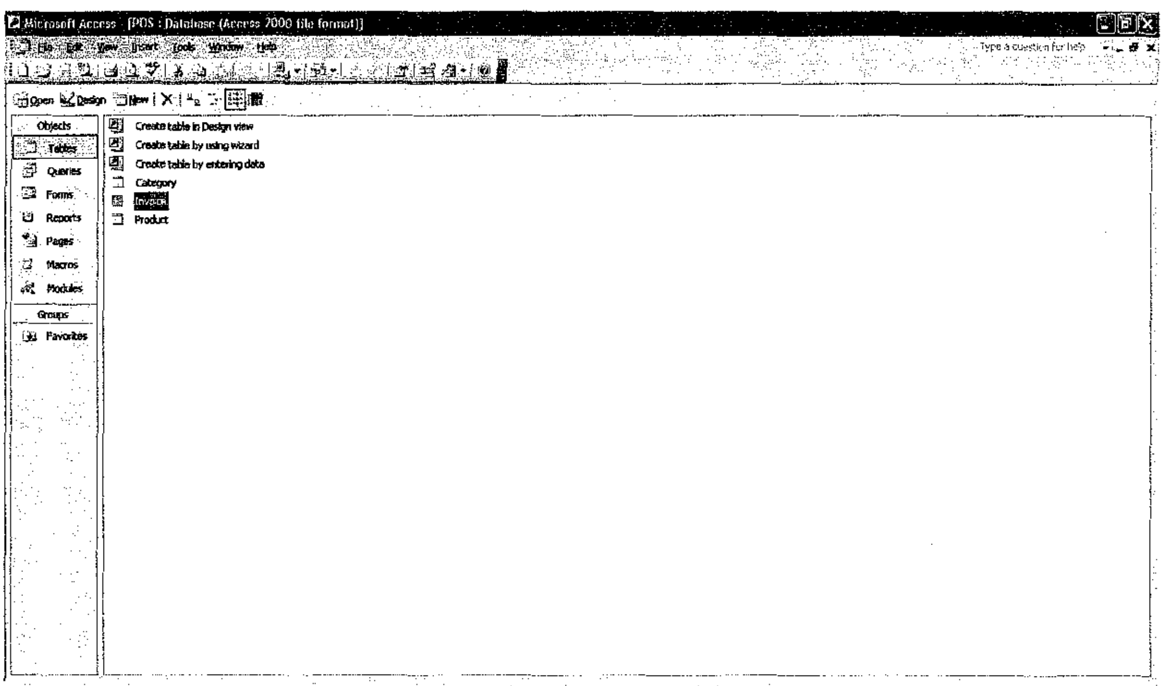


Figure 3.1: Sales database

2) PReCdb database: This database manage user of the system and store user's particulars

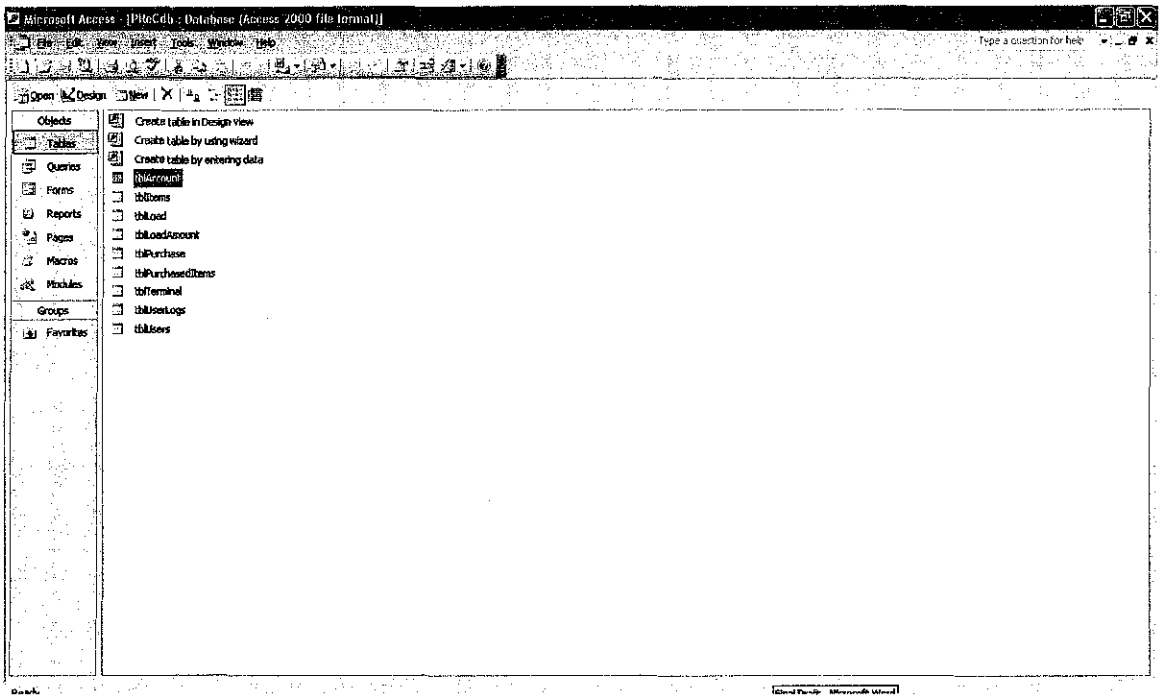


Figure 3.2: User account database

4.3.2 System Interface

The transaction and verification interface were designed and coded using Visual Basic 6.0. For the transaction interface, it basically shows the type of product and the quantity of items that student purchased.

Button PAY links the transaction interface to the verification interface to complete the process of food payment. The entire interfaces were included as a screen shot in appendices section.

During project implementation and testing, fingerprint scanner is not used to capture live-scan template due to unavailability of device. Therefore, the project is tested based on the reference image stored in the file and match with a unique ID associated with the image.

Figure 2.2 in Chapter 3 shows the system architecture of UTP Cafeteria Cashless Payment System. The following explains the flow of the system from one step to another excluding the step of capturing live-scan template:

1) During transaction, cashier entered product ID and the quantity of product purchased by students. Each product available in the cafeteria has product ID.

2) Upon payment for the product that they purchase, cashier click on PAY button in the interface and another window appear for payment transaction. Cashier will then load and select fingerprint image from file.

3) After loading fingerprint image, cashier need to select the resolution of image. Only 500 dpi will be accepted by the system. Student ID entered and we are able to see if the ID match the fingerprint image stored in the database.

4) If student ID match with the fingerprint image stored in the database, the payment for products purchased is successful. 'Verified' is displayed on the screen to indicate the match. The system will display student's current balance after the transaction.

5) If student ID entered does not match with the fingerprint image in the database, the system will display 'Not verify'.

CHAPTER 5
CONCLUSION AND RECOMMENDATION

5.0 CONCLUSION AND RECOMMENDATION

5.1 Conclusion

Cashless Payment System using fingerprint recognition for UTP cafeteria provides convenient and faster transaction process for students in terms of payment. Developing this system is not solely focusing on the functionality of the system but also the security and privacy of data being processed and manipulated by the system.

Fingerprint technology like other cashless payment system using smart cards or PIN numbers does have its own drawbacks. But even with the significant drawback, fingerprint systems are an excellent means of identification. In the future, they'll most likely become an integral part of most peoples' everyday life, just like keys, ATM cards and passwords. In the future, author also hoped that research and development of fingerprint system in Malaysia will grow and expand to a larger and more practical application which can benefit everyone.

5.2 Recommendation

Having students to make payment for items that they purchased without money or cash involved is an effective way to solve the problem identified in Chapter 1 whereby students do not have to queue along the line for longer time. In addition, cashless payment system for campus cafeteria has not been widely developed within institutional education in Malaysia.

However, some enhancements and modifications need to be made to the system. Looking at the environment of the cafeteria itself, the use of fingerprint recognition is not that practical since outsiders who do not have their fingerprint registered would not be able to make any transaction in the cafeteria. Fingerprint would be more appropriate to be used within a larger environment for application such as time attendance for organization since the fingerprint scanner available in the market nowadays is not that cheap to be used for such small environment like UTP Cafeteria.

Other than that, many ideas received from students suggest that they prefer to use other medium for the transaction such as using cards which can be scanned to make the payment. This card will bring more benefits if it can be used for multiple purposes such as make payment for cafeteria services, library services and laundry services.

REFERENCES

Book:

Weidong Kou 2003, *Payment Technologies for E-commerce*, Springer-Verlag Berlin Hiedelberg New York

Articles research:

1) Austine Jay Harris, Davis C. Yen. 2002," *Biometric authentication: assuring access to information,*" Journal of Information Management & Computer Security, Emerald 10/1 12-19

2) V. Zorkadis, P. Donos, *"On biometrics-based authentication and identification from a privacy-protection perspective, "* Information Management & Computer Security, Volume 12 Number 12004 pp.125-137

3) D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, "*Handbook of Fingerprint Recognition,*" Springer, New York, 2003

4) Anil K.Jain,"*Fingeprints: Proving Ground for Pattern Recognition, "*

5) Ola Svedin, Marten Obrink, Jerker Bergenek, "*Precise Biomatch Fingerprint Technology,*" April 2004

6) Ying HAO, Tieniu TAN, Yunhong WANG, "*An effective algorithm for fingerprint matching, "* National Lab of Pattern Recognition, CAS, Institute of Automation, Beijing, P. R. China, 100080

7) Tsai-Yang Jea and Venu Govindaraju," *A minutia-based partial fingerprint recognition system,* " Center for Unified Biometrics and Sensors, University at Buffalo, State University of New York Amherst, NY USA 14228

8) Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, Satoshi Hoshino. *"Impact of Artificial Gummy Fingers on Fingerprint Systems,"* Graduate School of Environment and Information Sciences, Yokohama National University, 79-7 Tokiwadai, Hodogaya, Yokohama 240-8501, Japan

9) Koichi Ito, Ayumi Morita, Takafumi Aoki, Tatsuo Higuchi, Hiroshi Nakajima, and Koji Kobayashi, "*A Fingerprint Recognition Algorithm Using Phase-Based Image Matching for Low-Quality Fingerprints,*" Faculty of Engineering, Tohoku Institute of Technology, Sendai-shi 982-8577, Japan, Yamatake Corporation, Isehara-shi 259-1195, Japan

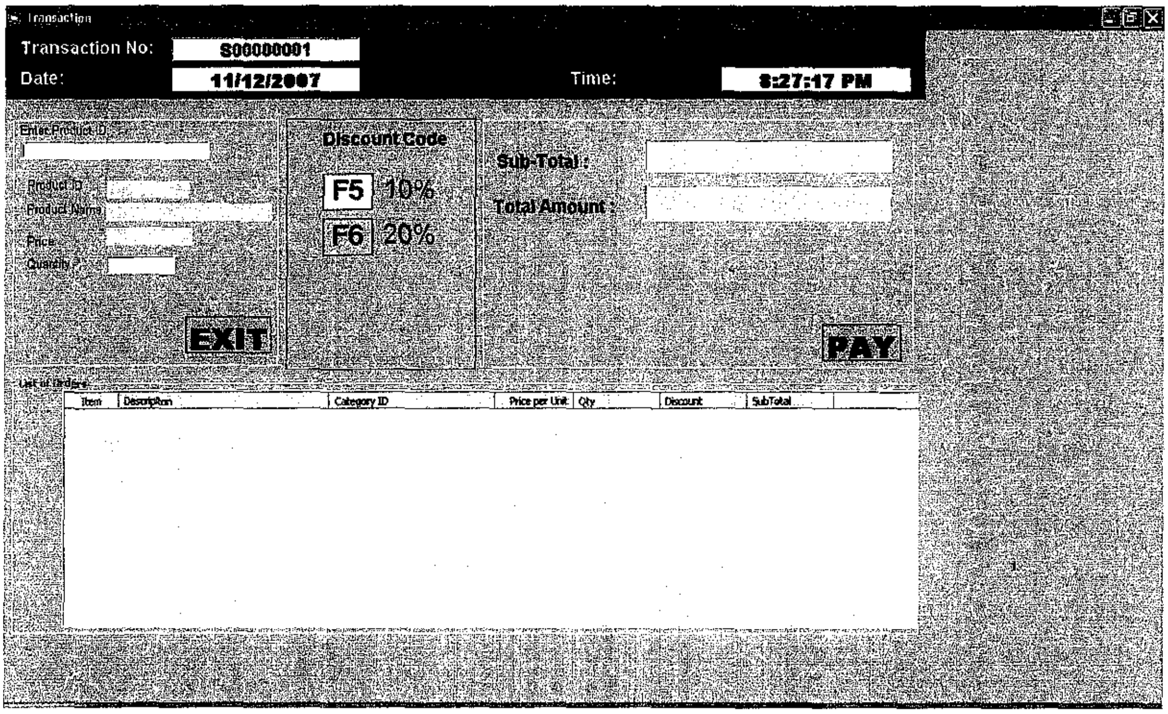
Internet Research:
http://onin.com/cgi-bin/fp/discus.cgi?pg=next&topic=1833&page=240

Wal-Mart, Costco weigh merits of allowing customers to pay by scanning fingerprints
<http://www.money.cnn.com/2006/01/24/magazines/fortune/pluggedin_fortune_biometrics/index.htm?>

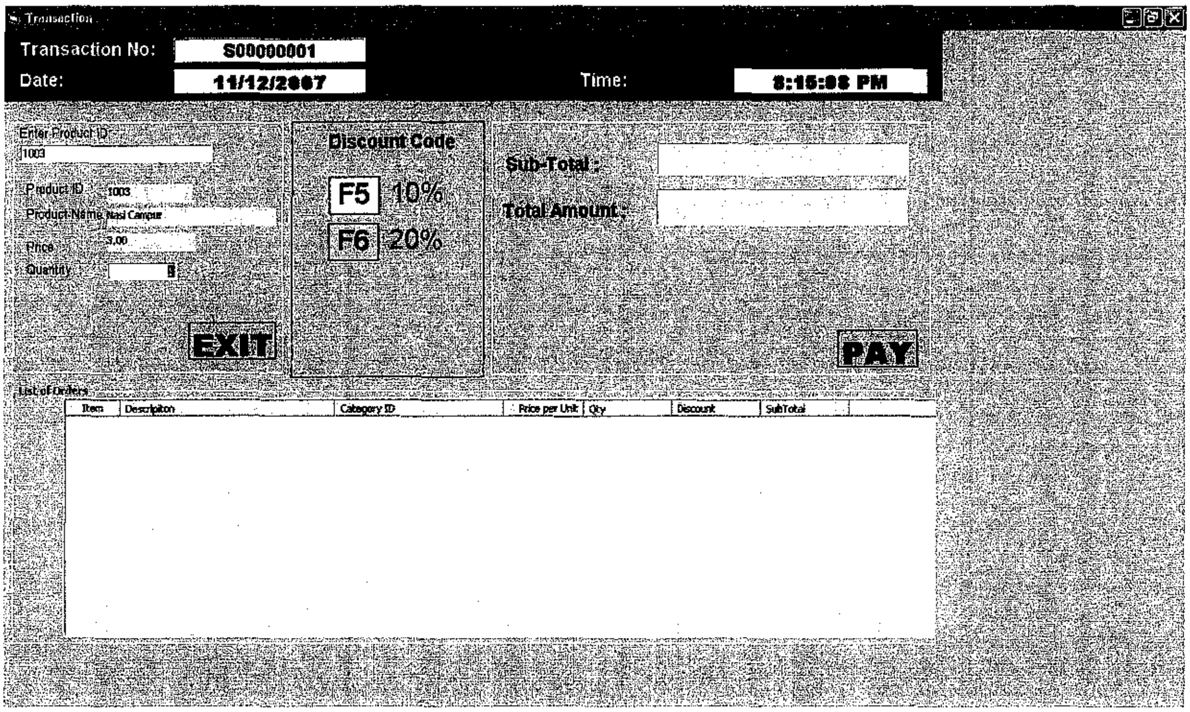
APPENDICES

Screen shots of UTP Cafeteria Cashless Payment System:

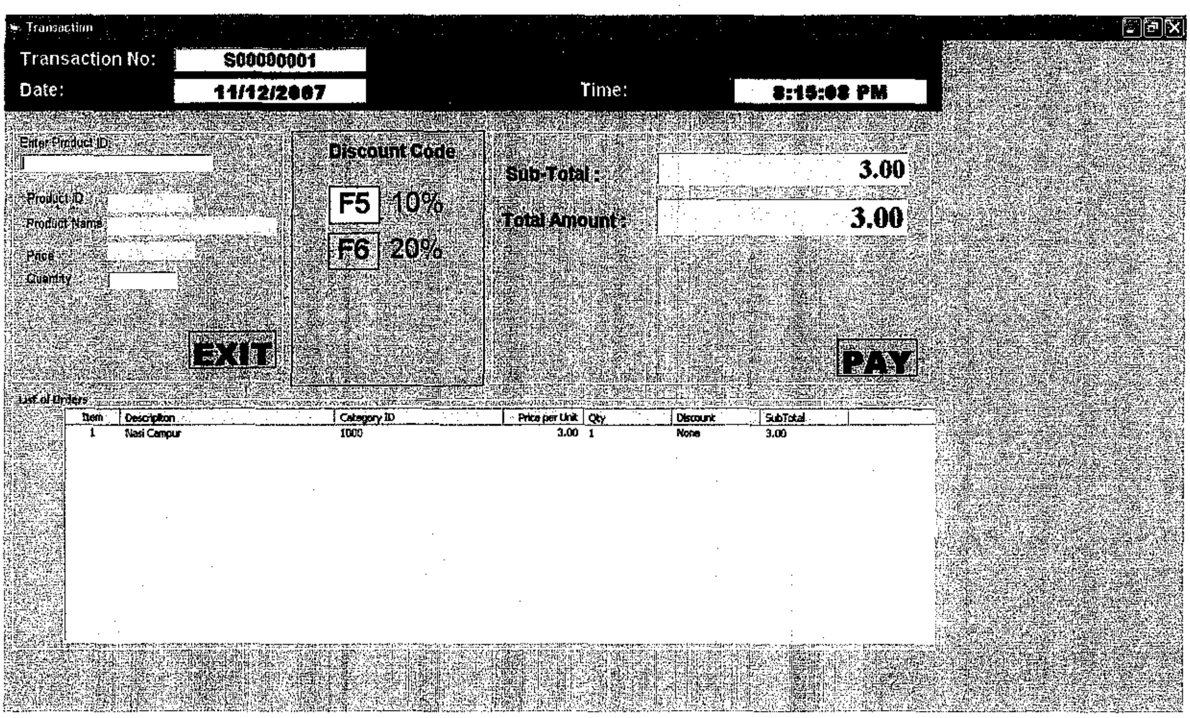
Transaction Interface



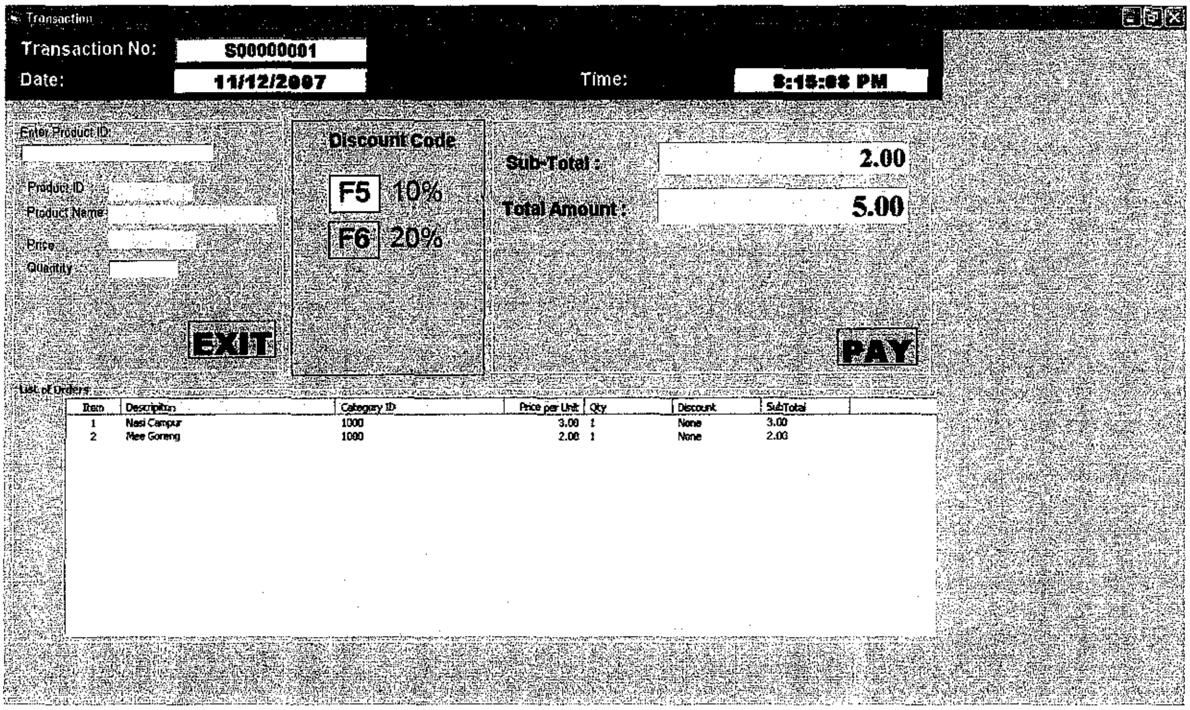
Product ID and quantity entered



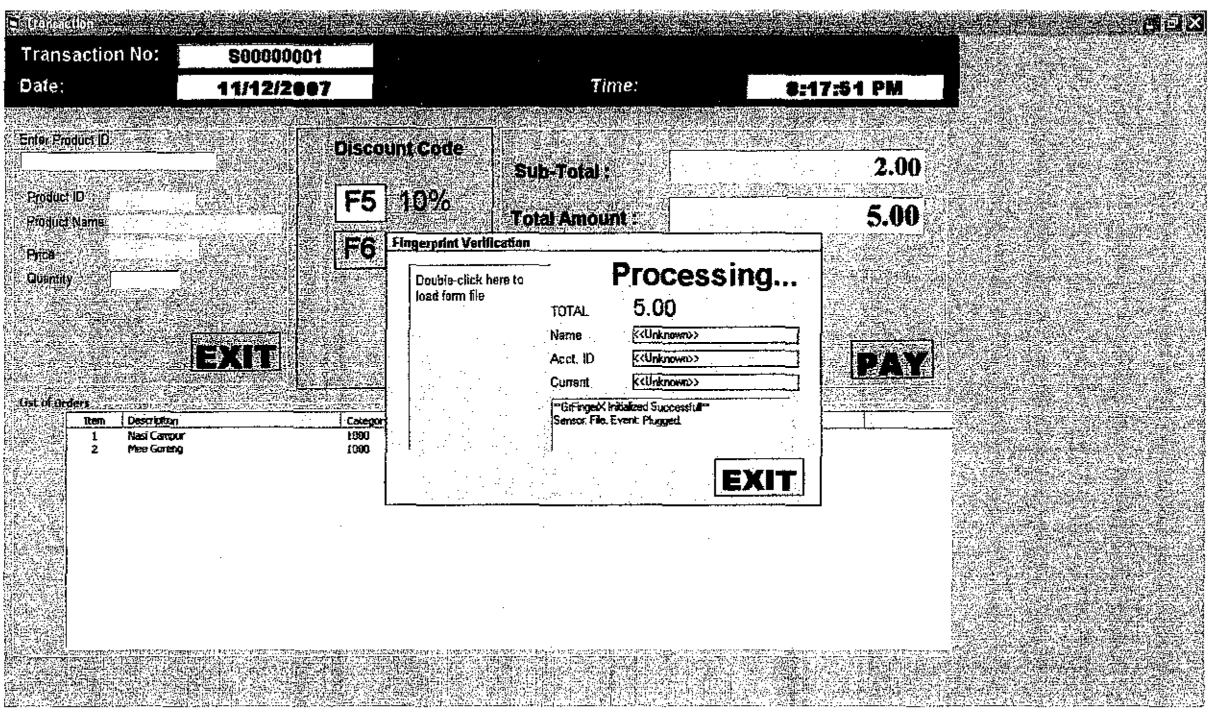
Product details appear under list of orders



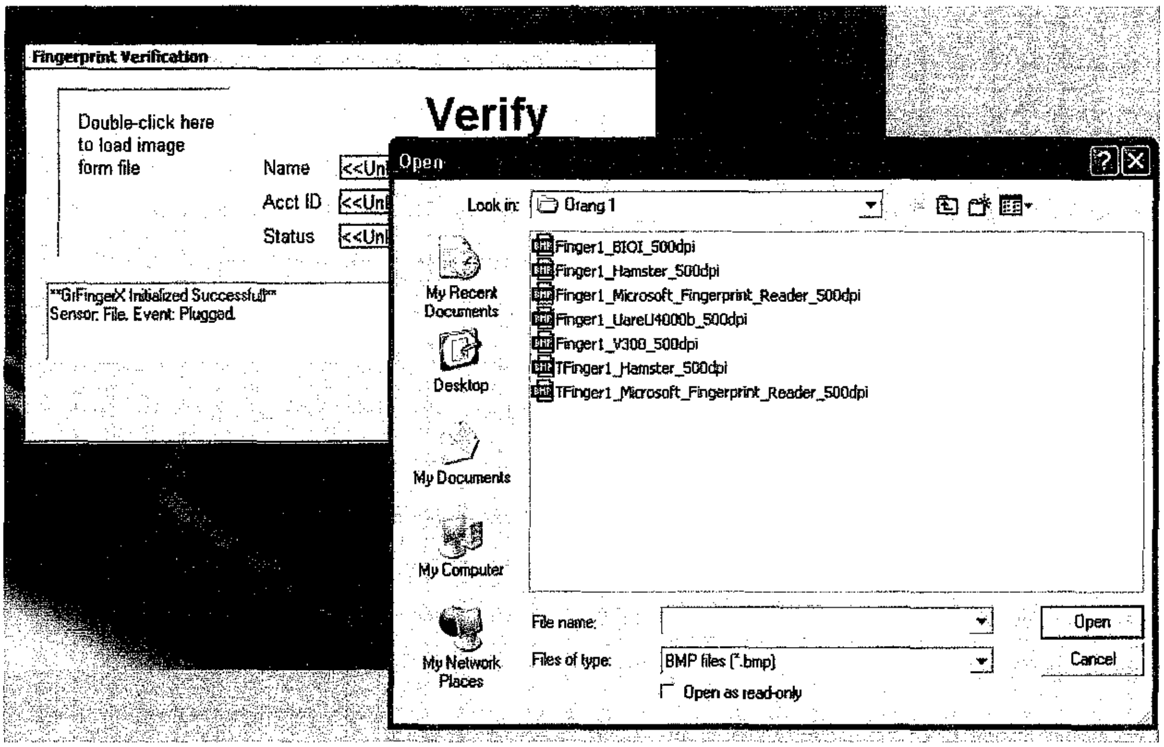
New product added under the list of orders



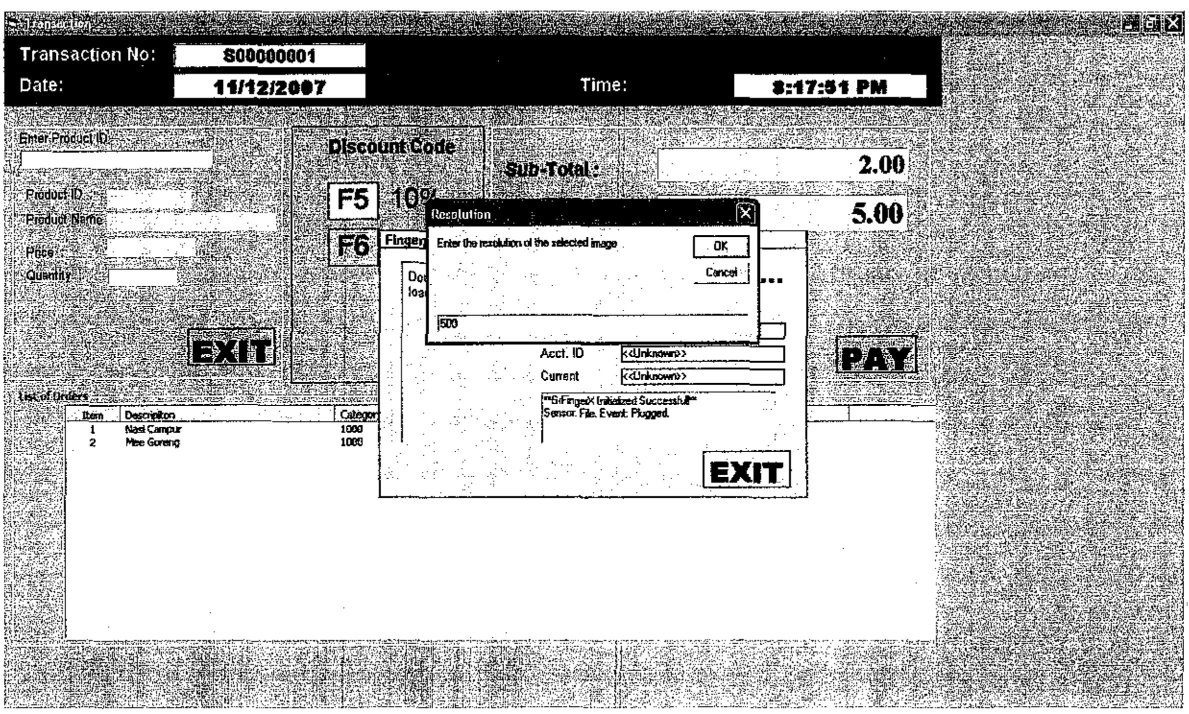
Fingerprint verification interface



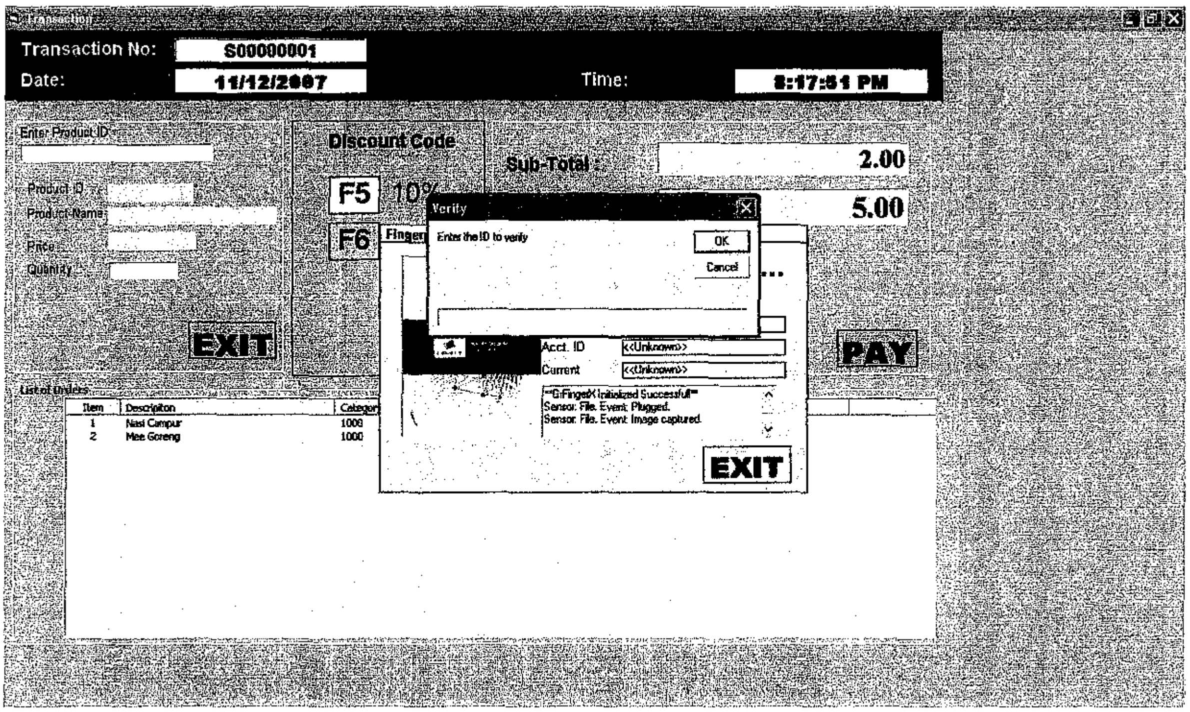
Load and select fingerprint image from file



Enter resolution of fingerprint image

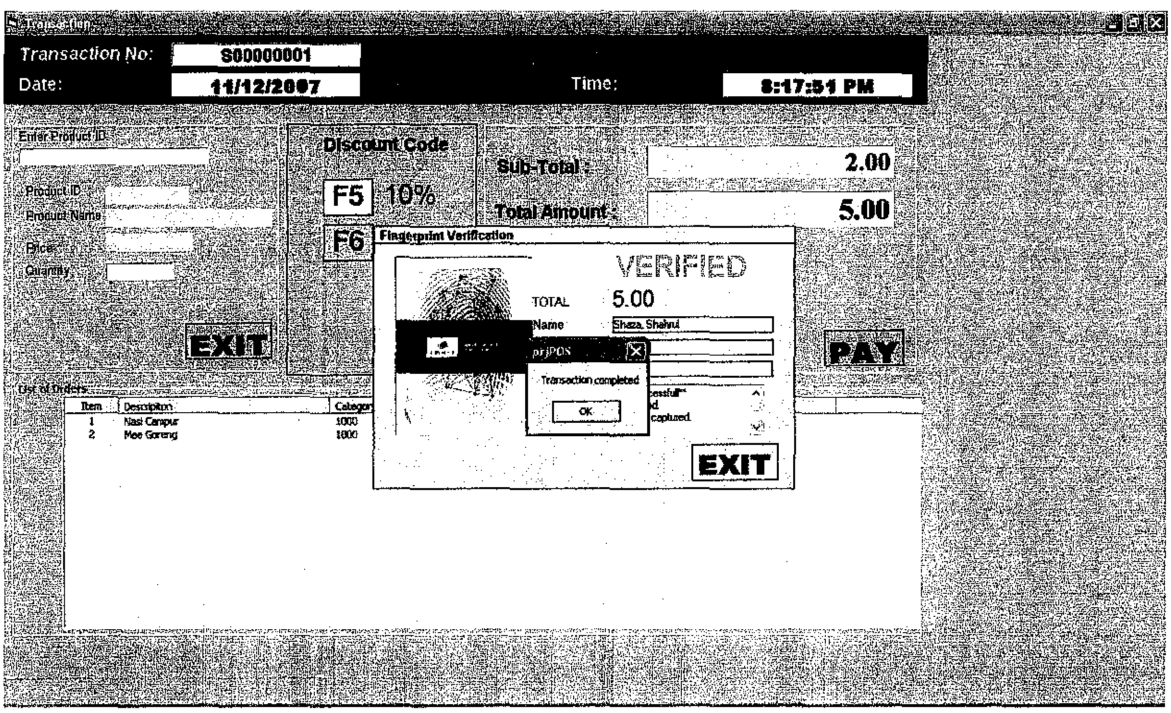


Enter student ID to complete transaction process

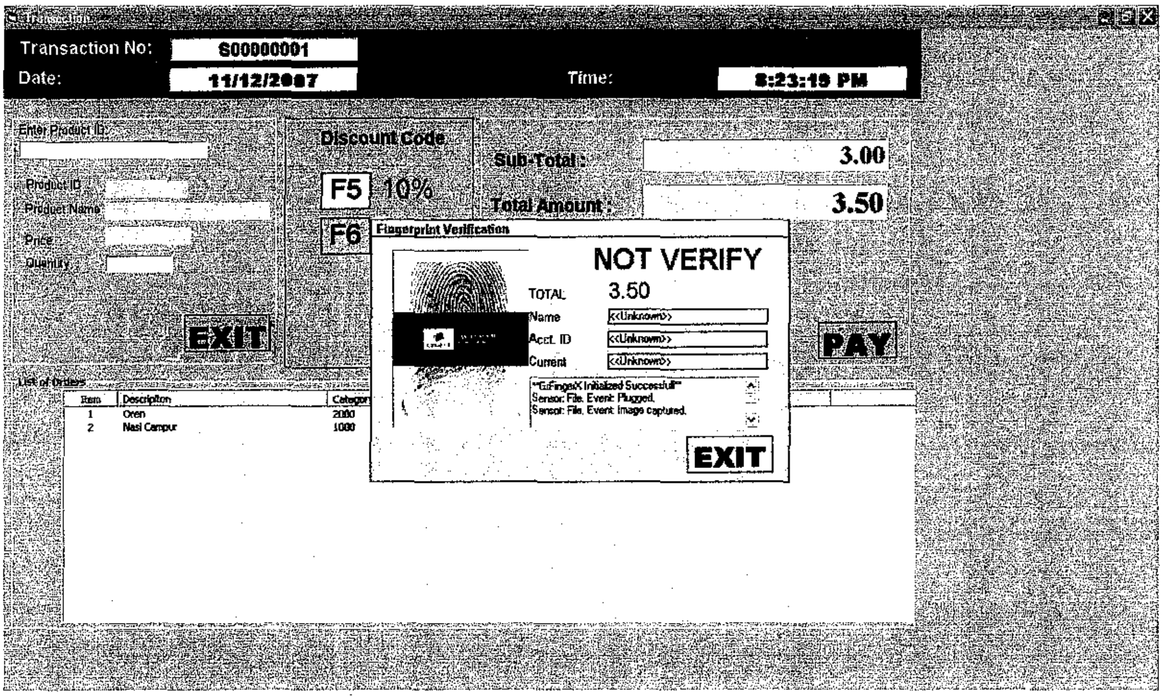


Student ID match with the fingerprint image stored in the database

Transaction completed



Student ID does not match with the fingerprint image in the database



Fingerprint image sample captured from different scanner

Using BIO 1 scanner

Using Hamster scanner

Using Microsoft scanner

Using UARE400b scanner

Using V300 scanner

Project Timeline and Milestone (FYP Part II)															
#	Detail / Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	**System Development**	■	■	■	■	■	■								
	i) Programming and Coding														
	ii) Database Design														
2	**Submission of Progress Report 1**			▒											
3	**Implementation and Testing**							■	■						
	i) Set-up system														
4	**Maintenance**								■						
	i) Correcting error														
6	**Submission of Progress Report 2**								▒						
5	**Seminar**									▒					
7	**Submission of Final Draft**										▒				
8	**Pre-EDX (Exhibition)**											▒			
9	**Oral Presentation**													▒	
10	**Submission of Dissertation**														▒

■ **PROCESS** ▒ **MILESTONE**

RESEARCH QUESTIONNAIRES

Project Title: UTP Cafeteria Cashless Payment System using Fingerprint Recognition

Please answer the following questions.

Your feedback will help in implementing the Cashless Payment System.

1. How convenient are you with the current payment system for UTP Café?

- Very convenient
- Moderate
- Not convenient

2. Do you face any problem with the current payment system? (If yes please state the problem that you faced)

- Yes ____
- No

3. Do you think food payment consume much of your time during lunch hours on weekdays?

- Yes
- No

4. Have you ever heard of Cashless Payment System?

- Yes
- No

5. From whom do you hear about the Cashless Payment System?

- From reading
- From a friend
- From the lecturer
- From search on the internet

6. Have you ever used the Cashless Payment System?

- Yes
- No

7. If UTP implement the Cashless Payment System, are you willing to use the system?

- Yes
- No

8. Is it relevant for UTP to implement Cashless Payment System?

- Yes
- No

9. Do you think the system would be helpful for UTP student?

- Yes
- No

Thank you for your cooperation.

EVALUATION QUESTIONNAIRE

Project Title: UTP Cafeteria Cashless Payment System using Fingerprint Recognition

This survey is to evaluate UTP Cafeteria Cashless Payment System. This evaluation survey will focus on the functionality and performance of the system.

Functionality

1. How do you rate the functionality of the system?

1	2	3	4
Poor	Average	Good	Excellent

Performances

2. Are you satisfied with the transaction process?

   a) Yes b) No c) Not sure

3. Is there any difficulty that you faced while using the system?

   a) Yes b) No c) Not sure

Respondent Opinion

4. What are other suggestions that you think can make the system more useful?

   ____

   ____

Thank you for your cooperation.