**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

***IJCSMC, Vol. 3, Issue. 12, December 2014, pg.397 – 409***

**RESEARCH ARTICLE**

# Portable Fingerprint-Based Attendance Recording & Monitoring System

**M. S. I. M. Zin[1], A. A. M. Isa[2], M. S. M. Isa[3]**

[1,2,3] The Centre for Telecommunication Research and Innovation (CeTRI), Faculty of Electronic & Computer Engineering, Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia

[1] shahril@utem.edu.my

***Abstract— This paper presented the development of a portable attendance monitoring system based on fingerprint identification that can be used by lecturers to monitor attendance of students. Fingerprint-based identification is one of the oldest method among all biometric or security techniques which has been successfully used in numerous applications. Every person has unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The distinctiveness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. A portable fingerprint scanner has been utilized as the input to acquire fingerprint images and a laptop equipped with attendance recording and monitoring software as a mobile terminal to process the fingerprint images and record the attendance. This system can be used by lecturers to replace the old method of attendance recording, so that the integrity of the attendance record can be upheld. The actual student's attendance can be recorded and stored in database. The system is also capable of processing the record to determine students who do not fulfil the attendance percentage requirement.***

***Keywords— Fingerprint, biometrics identification, attendance monitoring, portable***

## I. INTRODUCTION

Reliable personal authentication has become an important human computer interface activity in an increasingly digital world [1]. National security, electronic banking, access to computer networks and attendance monitoring and verifications are some examples where establishing a person's identity is very important. Typical security measures rely on knowledge-based approaches like passwords or token-based approaches such as swipe cards and passports to regulate access to physical and virtual spaces. Though ever-present, such approaches are not very secure [2] Tokens such as access cards and badges may be shared or stolen. Passwords and personal identification number (PIN) may be stolen electronically while signatures can be easily forged [3]. Furthermore, those approaches cannot differentiate between authorized user and a person having access to the tokens or knowledge. Biometrics such as fingerprint offers means of reliable personal authentication that can address these problems and is gaining public confidence [4].

This paper presented the development of a portable attendance monitoring system based on fingerprint identification that can be used by lecturers to monitor attendance of students. The system utilizes portable fingerprint scanner as the input to acquire fingerprint images and a laptop equipped with attendance recording and monitoring software as a mobile terminal to process the fingerprint images and record the attendance. A web camera is used to capture student pictures that will be stored together with the fingerprint image and student details in the system's database.

Lecturers can used this system to replace the old method of attendance recording, so that the integrity of the attendance recording can be upheld and the actual student's attendance can be recorded and stored in database. The system will also be capable of processing the record to determine students who do not fulfil the attendance percentage requirement.

## II. BIOMETRICS

Biometrics is the science of verifying the identity of an individual through physiological measurements or behavioural traits [5]. Since biometric identifiers are related permanently with the user, they are more reliable than token or knowledge based authentication methods. Several benefits of biometrics over typical security measures are:

(a) Non-repudiation: With token and password based approaches, the perpetrator can always deny committing the crime pleading that his/her password or ID was stolen or compromised even when confronted with an electronic audit trail. There is no way in which his claim can be verified effectively. This is known as the problem of deniability or of 'repudiation'. However, biometrics is indefinitely associated with a user and hence it cannot be lent or stolen making such repudiation infeasible [6].

(b) Accuracy and Security: Password-based systems are susceptible to brute force attacks. Such systems are as exposed as their weakest password. In contrast, biometric authentication requires the physical presence of the user and therefore cannot be circumvented through brute force style attack. Biometrics has also been shown to possess a higher bit strength compared to password-based systems and is therefore inherently more secure.

(c) Screening: In screening applications, users are prevented from assuming multiple identities, for example, a terrorist using multiple passports to enter a foreign country. This requires a process to ensure a person has not been enrolled under another assumed identity before adding the new record into the database. Such screening is not feasible using typical authentication mechanisms and biometrics provides a viable solution.

Biometric modalities can be generally categorized as [5]:

(a) Physical biometrics, involving some form of physical measurement and include modalities such as face, fingerprints, iris-scans and hand geometry.

(b) Behavioural biometrics, which are usually temporal in nature and involve measuring the way in which a user performs certain tasks such as speech, signature, gait, keystroke dynamics etc.

(c) Chemical biometrics which involves measuring chemical cues such as odour and the chemical composition of human perspiration.

It is also useful to compare the relative advantages and disadvantages of biometric and password or cryptographic key based systems [5]. Table 1 provides a summary of the comparison.

TABLE I
COMPARISON OF BIOMETRIC AND PASSWORD/KEY BASED AUTHENTICATION

| Biometric Authentication | Password/Key based authentication |
|---|---|
| Based on physiological measurements or behavioral traits | Based on something that the user 'has' or 'knows' |
| Authenticates the user | Authenticates the password/key |
| Is permanently associated with the user | Can be lent, lost or stolen |
| Biometric templates have high uncertainty | Have zero uncertainty |
| Utilizes probabilistic matching | Requires exact match for authentication |

Biometrics can be used for identification or for verification, depending on the application. Biometric is used in verification to validate the claim made by an individual. The biometric of the user is compared with the biometric of the claimed individual in the database and the claim is rejected or accepted based on the match. In identification, the system recognizes an individual by comparing his biometrics with every record in the database [7].

In general, biometric verification consists of two stages, enrolment and authentication as shown in Fig. 1. During enrolment, the biometrics of the user is captured and the extracted features (template) are stored in the database. During authentication, the biometrics of the user is captured again and the extracted features are matched with the ones already existing in the database to determine a match [8]. The exact record to fetch from the database is determined using the claimed identity of the user. The database may be centralized or distributed with each user carrying his template on a smart card.

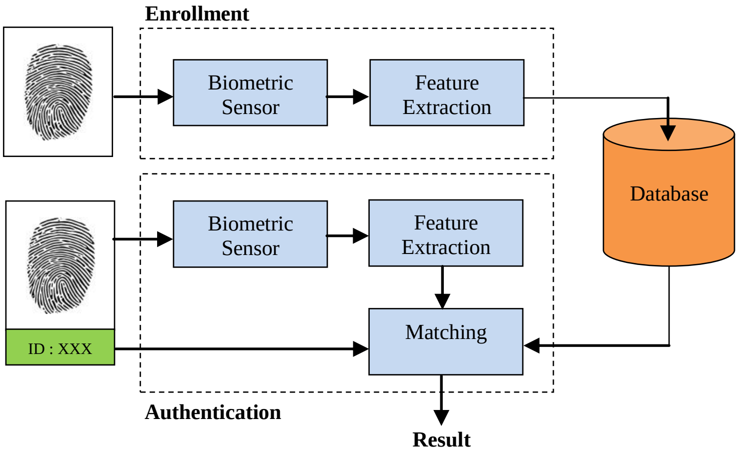


Fig. 1 General Architecture of a Biometric System

## III. FINGERPRINT VERIFICATION SYSTEM

A typical fingerprint recognition system consists of several stages as shown in Fig 2. The fingerprint image can be acquired either by using off-line methods such as creating an inked impression on paper or through a live capture device consisting of an optical, capacitive, ultrasound or thermal sensor [3]. The first stage consists of standard image processing algorithms such as noise removal and smoothening. However, it is to be noted that unlike regular images, the fingerprint image represents a system of oriented texture and has very rich structural information within the image [4]. Furthermore, the definition of noise and unwanted artefacts are also specific to fingerprints. The fingerprint image enhancement algorithms are specifically designed to exploit the periodic and directional nature of the ridges. Finally, the minutiae features are extracted from the image and are subsequently used for matching.

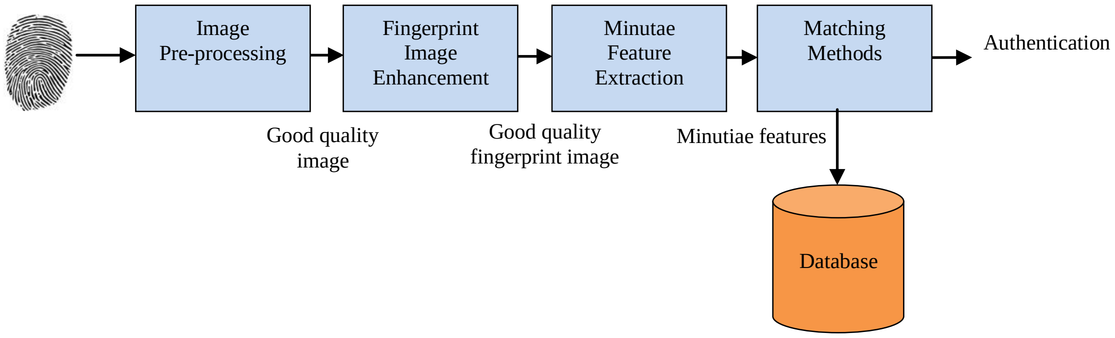


Fig 2 General Architecture of a Fingerprint Verification System

Traditionally fingerprints were acquired by transferring the inked impression onto the paper. This process is termed as off-line acquisition. Existing authentication systems are based on devices that capture the fingerprint image in real time. The live-scan devices can be based on one of the following sensing schemes:

(a) Optical sensors
(b) Capacitive sensors
(c) Ultra-sound sensors
(d) Thermal sensors

Optical sensors are the oldest and most widely used in fingerprint acquisition technology. In most devices, image of the fingerprint with dark ridges and light valleys is converted by a charged coupled device (CCD) into a digital signal. These devices are inexpensive and can provide resolutions up to 500 dpi. Most of the sensors acquire the image by using Frustrated Total Internal Reflection (FTIR) technique where a source illuminates the fingerprint through one side of the prism as shown in Fig. 3 and Fig. 4. Most of the light is reflected back to the other side due to internal reflection phenomenon, where it is then recorded by a CCD camera. In regions where the fingerprint surface touches with the prism, the light is diffused in all directions and consequently does not reach the sensor, resulting in dark regions. Furthermore, a wet fingerprint may affect the quality of the image.

Optical sensors also faced another problem which is the residual patterns left by the previous fingers. It has also been shown that fake fingers are able to fool most low-grade commercial sensors [9]. Due to the optics involved, optical sensors are also among the bulkiest sensor.

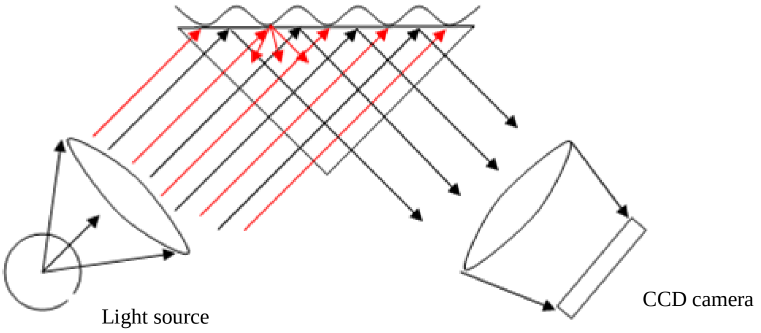


Fig. 3 FTIR Based Optical Sensor

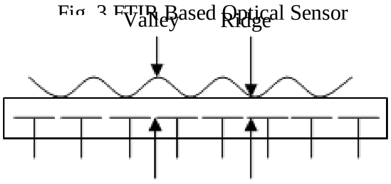


Fig. 4 Capacitive Sensor

In capacitive sensors, the silicon sensor acts as one plate of a capacitor while the finger acts as another other plate [10]. The capacitance between the plate and the finger depends inversely with the distance between them. Since the ridges are closer, they relate to increased capacitance and the valleys relate to smaller capacitance. This variation is transformed into an 8-bit greyscale digital image. Due to its small size, most of the electronic devices featuring fingerprint authentication utilize this form of solid state sensors. However, sensors that are smaller than 0.5”x0.5” are not useful because it reduces the recognition accuracy [11].

Ultrasound technology is possibly the most accurate fingerprint sensing technologies where it utilizes ultrasound waves and measures the distance based on the impedance of the finger, the plate, and air [12]. The sensors are capable of very high resolution of 1000 dpi or more. However, these sensors tend to be very huge and contain moving parts.

Thermal sensors are made up of pyro-electric materials whose properties change with temperature [13]. These are usually manufactured in the form of strips. As the fingerprints are swiped across the sensor, there is differential conduction of heat between the ridges and valleys (since skin conducts heat better than the air in the valleys) that is measured by the sensor. Full size thermal sensors are not practical since skin reaches thermal equilibrium very quickly once placed on the sensor leading to loss of signal. This would require us to constantly keep the sensor at a higher or lower temperature making it very energy inefficient. The sweeping action prevents the finger from reaching thermal equilibrium leading to good contrast images. However, since the sensor can acquire only small strips at a time, a sophisticated image registration and reconstruction scheme is required to construct the whole image from the strips.

Fig. 5 shows various sensors for live capture of fingerprints that are available commercially.

Digital Persona
www.crossmatch.com

SecuGen
www.secugen.com

APC
www.apc.com

Lumidigm
www.lumidigm.com

Fig. 5 Various Commercial Sensors Available for Live Capture of Fingerprints

## IV. SYSTEM DEVELOPMENT

The project was started with gathering of information related to the project from various sources. The main important aspect of this project is about biometric recognition, particularly regarding fingerprint recognition [14]. Much study needed to be done on fingerprint especially on fingerprint theory, classification, identification, matching, match algorithm and verification before any works on developing the software can be started [15].

For software and hardware development, several decisions also need to be made based on the study that has been done, such as type of programming language and database that will be used and type of fingerprint scanner that will be utilized. These decisions were important to make sure that the project could be executed and completed without any major problems.

After careful consideration, Visual Basic 2010 has been selected as the main programming language of this project because it is one of the most productive tool for creating high performance and robust applications. Visual Basic was designed to be easy to learn and use. The language not only allows programmers to create simple GUI applications, but can also develop fairly complex applications as well. Programming in VB is a combination of visually arranging components or controls on a form, specifying attributes and actions of those components, and writing additional lines of code for more functionality. Since default attributes and actions are defined for the components, a simple program can be created without the programmer having to write many lines of code. Performance problems were experienced by earlier versions, but with faster computers and native code compilation this has become less of an issue.

The software also needed to connect to database that stores the required information such as student details and fingerprint information. The database will be created by using Microsoft Office Access. Access is chosen because of its simplicity and ease of use. Access allows relatively quick development because all database tables, queries, forms, and reports are stored in the database. For query development, Access utilizes the Query Design Grid, a graphical user interface that allows users to create queries without knowledge of the SQL programming language.

Several types of fingerprint scanner have been evaluated to determine which scanner is best suited for integration with the software that will be developed. There are four types of fingerprint scanner which are optical sensors, capacitive sensors, ultra-sound sensors and thermal sensors. Optical sensor has been chosen because it is the oldest and most widely used technology in fingerprint scanner. It is also fairly inexpensive and can provide resolutions up to 500 dpi. In optical sensor devices, a charged coupled device (CCD) converts the image of the fingerprint, with dark ridges and light valleys, into a digital signal.

There are several types of optical fingerprint scanner available commercially in the market. In this project, Fingerprint Reader DG2-00002 by Microsoft has been chosen as the fingerprint scanner to acquire fingerprint images and passed to the software for fingerprint identification, matching and verification. This fingerprint scanner has been chosen because it is small and light, therefore making it suitable for this project.

For fingerprint identification, matching, match algorithm and verification, a third-party system development kit (SDK) was used. GrFinger Fingerprint SDK is a fingerprint recognition SDK that supports several existing fingerprint scanners including Microsoft Fingerprint Reader which will be used in this project. GrFinger Fingerprint SDK is used to integrate the Microsoft Fingerprint Reader into the software that would be developed.

## V. **RESULTS**

The outcome of this project is a portable fingerprint-based attendance recording & monitoring system. Among the features of this system are:

(a) portable and easy to use
(b) provides an efficient & effective way to record attendances by using secured method
(c) acquires fingerprint patterns and store in the fingerprint database
(d) records attendances in attendance database by comparing the fingerprint pattern from the fingerprint scanner to the fingerprint database
(e) processes the data in the attendance database to determine specific requirements such as percentage of attendance

The hardware part of the portable fingerprint-based attendance recording & monitoring system developed in this project consists of three main components, portable fingerprint scanner, portable terminal and web camera. Fig. 6 shows the hardware setup for this project.

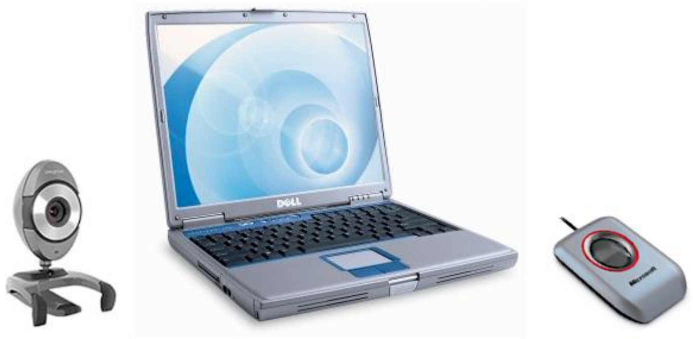


Fig. 6 Hardware Setup

The software is divided to five parts to make the system functioning effectively and efficiently. The parts are:

(a) Login
(b) Main Menu
(c) New Attendance Record
(d) Past Attendance Records
(e) Fingerprint & Data Enrolment

The login page is the first page that a lecturer will see when the software is executed. In this page, lecturers will be required to enter their username and password before they can enter the system and proceed to the main menu. Fig. 7 shows the login page.

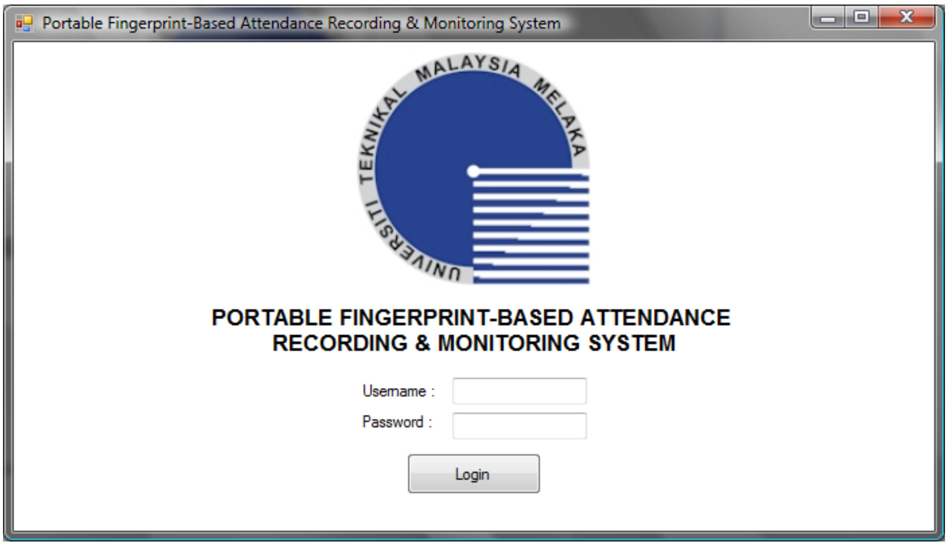

Portable Fingerprint-Based Attendance Recording & Monitoring System
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
PORTABLE FINGERPRINT-BASED ATTENDANCE RECORDING & MONITORING SYSTEM
Username :
Password :
Login

Fig.7 Login Page

After the lecturer has successfully entered the correct username and password, the main menu page will be displayed. The name of the lecturer will be displayed in the page, together with 4 buttons that represent different functions. The lecturer can choose whether to create new attendance record, view past attendance records, enrol new fingerprint and data or logout to the login page by clicking the appropriate button. At bottom right of the page, the current time and date will be displayed. The time and date will be displayed on the entire page except login page. Fig. 8 shows the main menu page of the system.

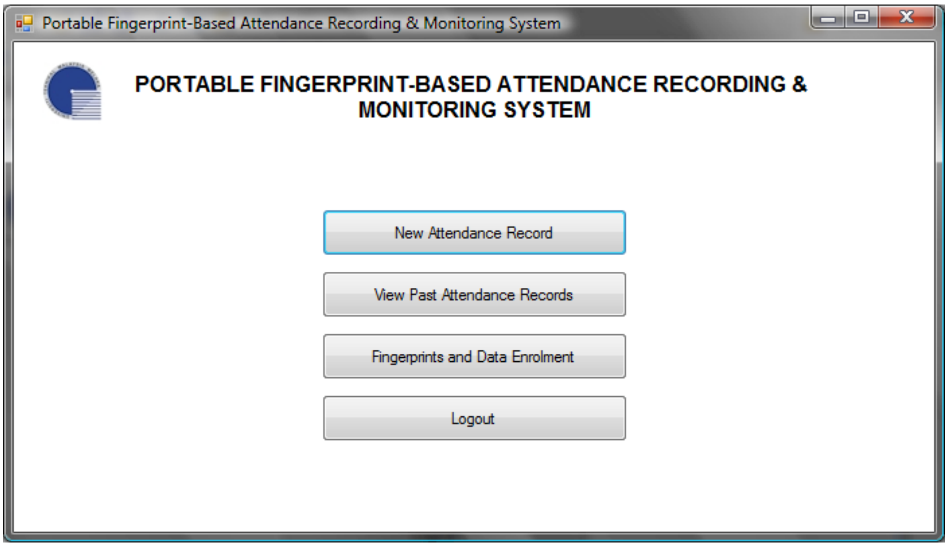
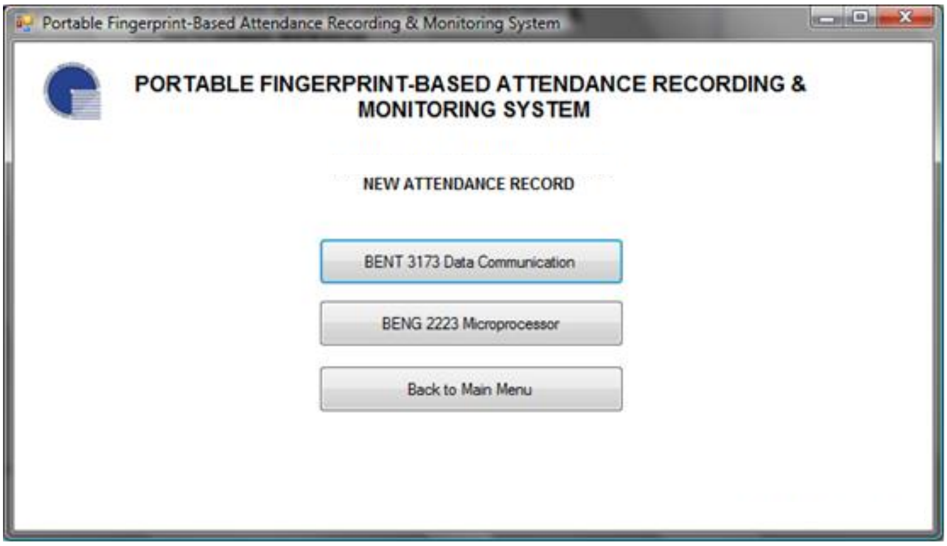

Portable Fingerprint-Based Attendance Recording & Monitoring System
PORTABLE FINGERPRINT-BASED ATTENDANCE RECORDING & MONITORING SYSTEM
New Attendance Record
View Past Attendance Records
Fingerprints and Data Enrolment
Logout

Fig. 8 Main Menu

The main page of new attendance record will be displayed if the lecturer clicks the first button on the main menu page. This main page will display list of subjects associated with the lecturer. For example, if the lecturer teaches 2 different subjects, both of the subjects will be displayed on the page. The lecturer then needs to select the appropriate subject. Fig. 9 shows the main page of new attendance record.



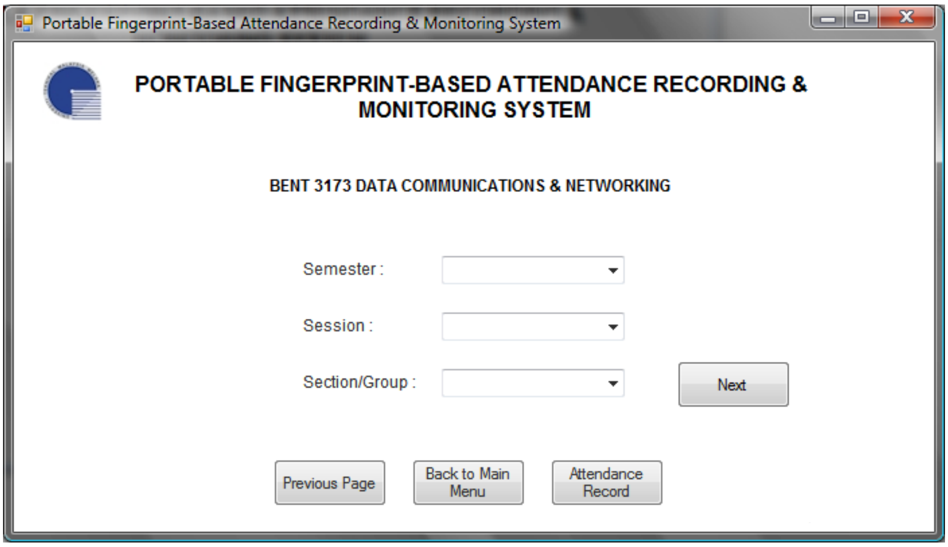
Portable Fingerprint-Based Attendance Recording & Monitoring System

PORTABLE FINGERPRINT-BASED ATTENDANCE RECORDING & MONITORING SYSTEM

NEW ATTENDANCE RECORD

Fig. 9 New Attendance Record.

After selecting the appropriate subject, the lecturer will need to select several details related to the subject such as semester, session and section/group. From the drop-down menus, the lecturer can define the semester in which the subject is currently taught, the session in which the student's attendance need to be recorded and the section and group of the students. The option in the Session drop-down menu are lecture, tutorial, laboratory, test and miscellaneous. After selecting all the appropriate details, the lecturer needs to click the 'Next' button to proceed. The lecturer also have the options to go back to the previous menu, go back to the main menu or view the current attendance record for the subject by clicking the appropriate buttons at the bottom part of the page. Fig. 10 to Fig. 13 shows the page & options for each drop-down menu.



Portable Fingerprint-Based Attendance Recording & Monitoring System

PORTABLE FINGERPRINT-BASED ATTENDANCE RECORDING & MONITORING SYSTEM

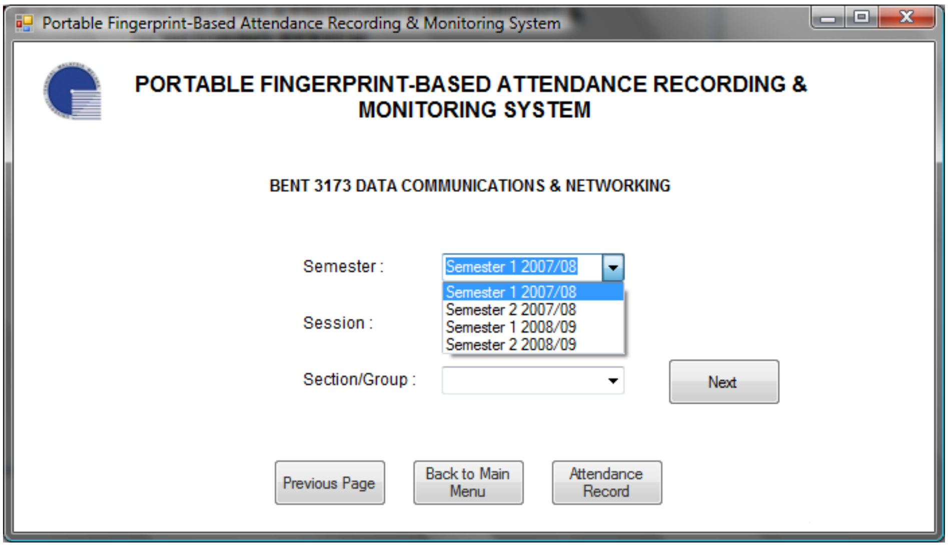
BENT 3173 DATA COMMUNICATIONS & NETWORKING

Semester :

Session :

Section/Group :

Fig. 10 Subject's Details


Portable Fingerprint-Based Attendance Recording & Monitoring System

PORTABLE FINGERPRINT-BASED ATTENDANCE RECORDING & MONITORING SYSTEM

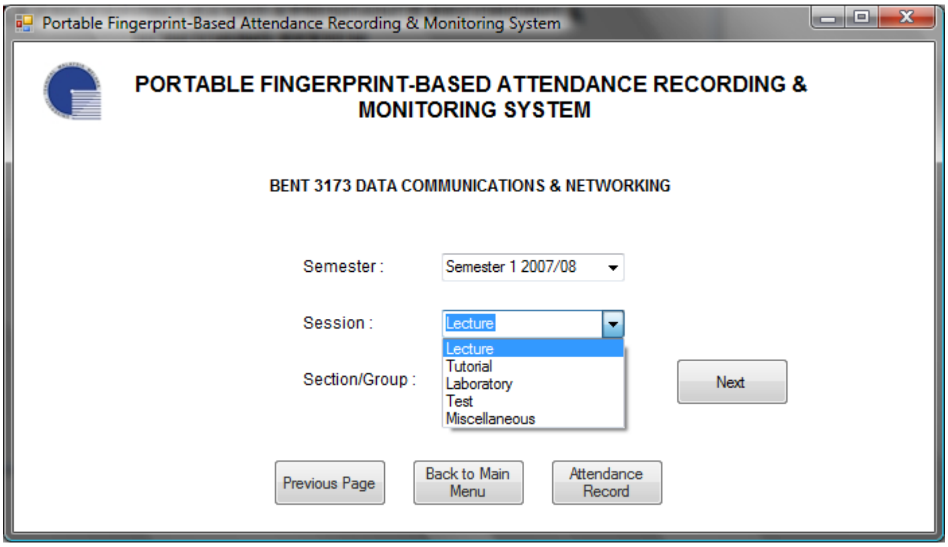
BENT 3173 DATA COMMUNICATIONS & NETWORKING

Semester : Semester 1 2007/08

Session :

Section/Group :

Fig. 11 Selecting Semester


Portable Fingerprint-Based Attendance Recording & Monitoring System

PORTABLE FINGERPRINT-BASED ATTENDANCE RECORDING & MONITORING SYSTEM

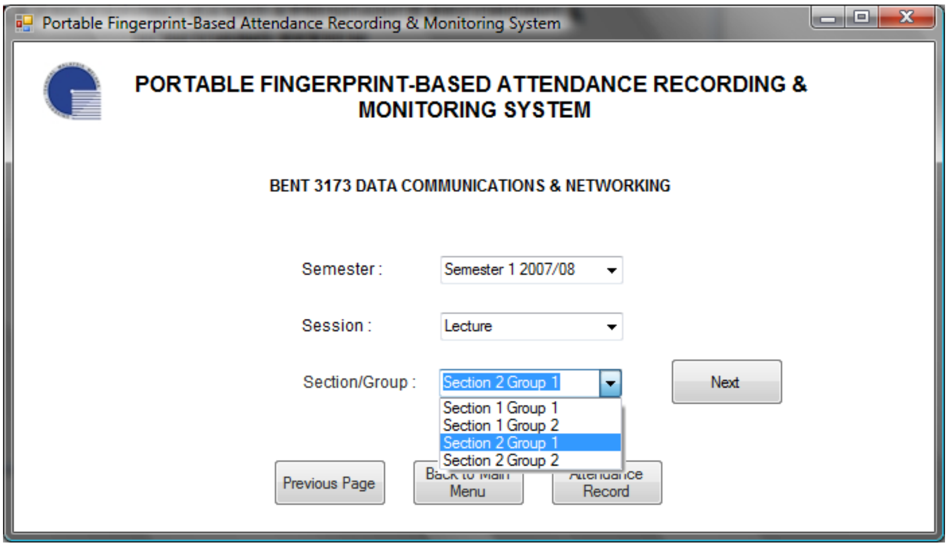
BENT 3173 DATA COMMUNICATIONS & NETWORKING

Semester : Semester 1 2007/08

Session : Lecture

Section/Group :

Fig. 12: Selecting Session


Portable Fingerprint-Based Attendance Recording & Monitoring System

PORTABLE FINGERPRINT-BASED ATTENDANCE RECORDING & MONITORING SYSTEM

BENT 3173 DATA COMMUNICATIONS & NETWORKING

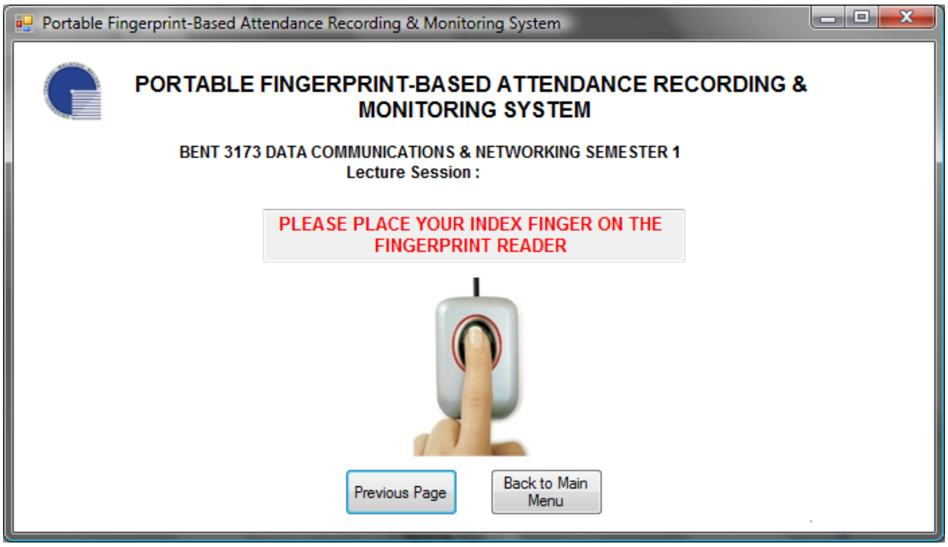
Semester : Semester 1 2007/08

Session : Lecture

Section/Group : Section 2 Group 1

Fig. 13 Selecting Section/Group

After selecting the appropriate parameters, the lecturer can now let students to scan their fingerprints. Students need to place their index finger on the fingerprint scanner for about 5 seconds. The fingerprint scanner will capture the fingerprint image of the student and compare it with the fingerprint images in the database to find any match. Fig. 14 shows the page to acquire fingerprint image.


Portable Fingerprint-Based Attendance Recording & Monitoring System

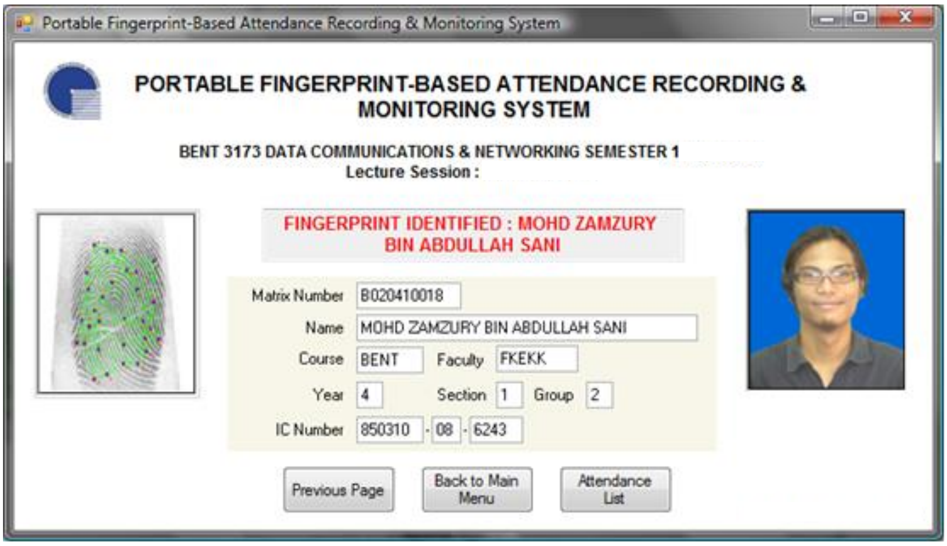
PORTABLE FINGERPRINT-BASED ATTENDANCE RECORDING & MONITORING SYSTEM

BENT 3173 DATA COMMUNICATIONS & NETWORKING SEMESTER 1
Lecture Session :

PLEASE PLACE YOUR INDEX FINGER ON THE FINGERPRINT READER

Fig. 14 Acquiring Fingerprint Image

There are 2 possible outcomes after any fingerprint has been scanned. If there is positive identification, where the fingerprint image scanned match with any fingerprint images stored in the database, the next page will notify that the fingerprint has been identified. The attendance for that student will be recorded in the database together with the timestamp. The fingerprint image, student details and pictures will also be displayed. The details of a student include name, matrix number, course, faculty, year, section, group and IC number. Fig. 15 shows the page displayed for positive identification.


Portable Fingerprint-Based Attendance Recording & Monitoring System

PORTABLE FINGERPRINT-BASED ATTENDANCE RECORDING & MONITORING SYSTEM

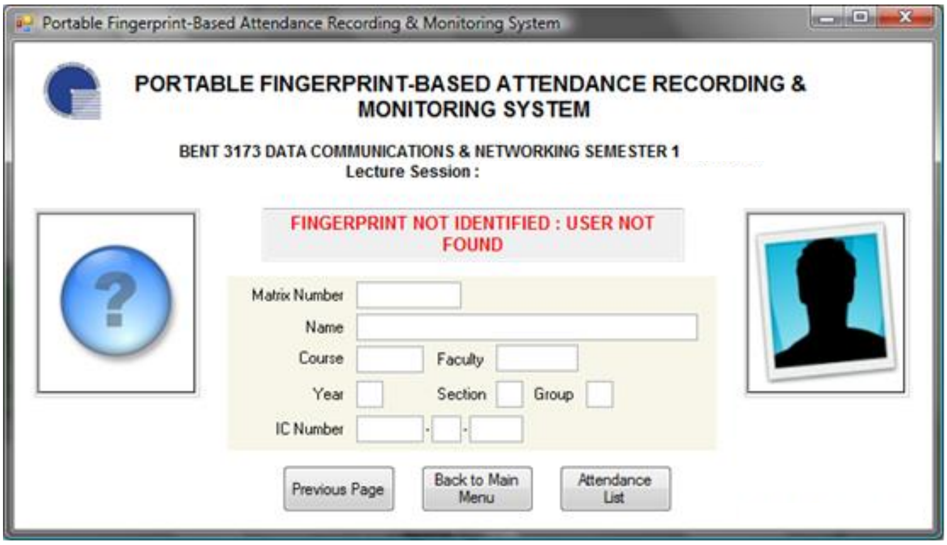
BENT 3173 DATA COMMUNICATIONS & NETWORKING SEMESTER 1
Lecture Session :

FINGERPRINT IDENTIFIED : MOHD ZAMZURY BIN ABDULLAH SANI

Matrix Number: B020410018
Name: MOHD ZAMZURY BIN ABDULLAH SANI
Course: BENT Faculty: FKEKK
Year: 4 Section: 1 Group: 2
IC Number: 850310 - 08 - 6243

Fig. 15 Positive Identification.

If there is negative identification, where the fingerprint image scanned does not match with any fingerprint images stored in the database, the next page will notify that the fingerprint has not been identified. This situation can happen if the student did not put his finger properly on the fingerprint scanner, thus affecting the quality of the fingerprint image acquired. If this happen, the student need to put the index finger back on the fingerprint scanner for a second scan. If there is still negative identification, then most probably the student is not registered for the subject. Fig. 16 shows page displayed for negative identification.



Portable Fingerprint-Based Attendance Recording & Monitoring System

PORTABLE FINGERPRINT-BASED ATTENDANCE RECORDING & MONITORING SYSTEM

BENT 3173 DATA COMMUNICATIONS & NETWORKING SEMESTER 1
Lecture Session :

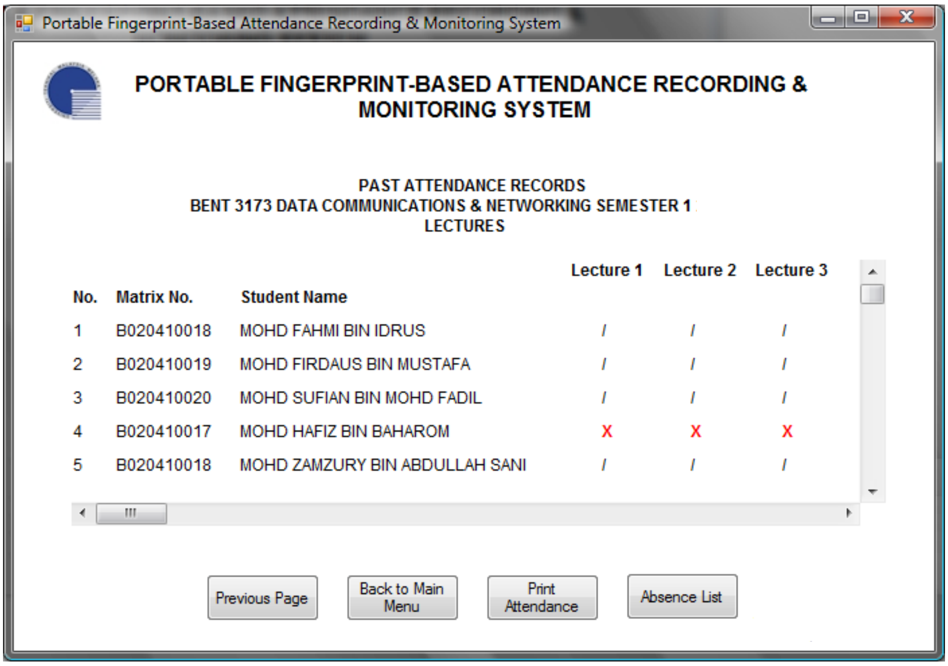
FINGERPRINT NOT IDENTIFIED : USER NOT FOUND

Matrix Number
Name
Course
Faculty
Year
Section
Group
IC Number

Fig. 16 Negative Identification.

At any time, the lecturer can click on the attendance list button to view list of student that have their fingerprint scanned successfully and their attendance recorded. The lecturer also has the option to go back to previous page or go back to the main menu.

The absence list will display the summary of absent records for each student for all the sessions for that particular subject. It will display the number of times a student has failed to attend lecture, tutorial, laboratory, test and miscellaneous session. From this page, lecturers can determine which student that needs to be served the warning letter. Lecturers have the option to print warning letter by clicking the 'Print Warning Letter' button. Fig. 17 shows the absence list page.



Portable Fingerprint-Based Attendance Recording & Monitoring System

PORTABLE FINGERPRINT-BASED ATTENDANCE RECORDING & MONITORING SYSTEM

PAST ATTENDANCE RECORDS
BENT 3173 DATA COMMUNICATIONS & NETWORKING SEMESTER 1
LECTURES

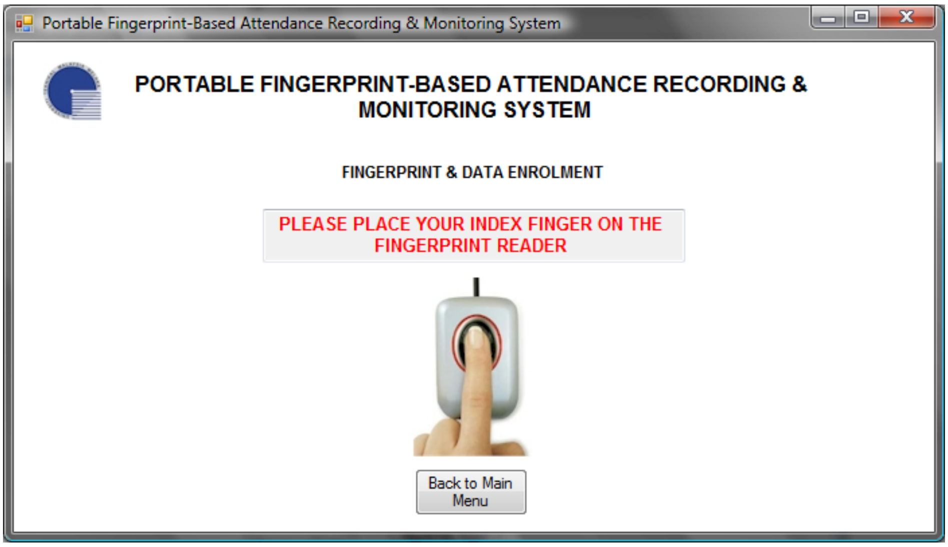
| No. | Matrix No. | Student Name | Lecture 1 | Lecture 2 | Lecture 3 |
|---|---|---|---|---|---|
| 1 | B020410018 | MOHD FAHMI BIN IDRUS | / | / | / |
| 2 | B020410019 | MOHD FIRDAUS BIN MUSTAFA | / | / | / |
| 3 | B020410020 | MOHD SUFIAN BIN MOHD FADIL | / | / | / |
| 4 | B020410017 | MOHD HAFIZ BIN BAHAROM | X | X | X |
| 5 | B020410018 | MOHD ZAMZURY BIN ABDULLAH SANI | / | / | / |

Fig. 17 Specific Attendance Record

At the start of each semester, fingerprint and data for each student for particular subject need to be enrolled in the system and save into the database. This is to make sure that the system can function properly without problems. To enrol new fingerprint and data, lecturers need to access the fingerprint and data enrolment function. This function can be accessed by clicking the third button in the main menu page. A page will be displayed that requires a student to place his index finger on the fingerprint reader as shown in Fig. 18.

The fingerprint scanner will scan and acquire the fingerprint image. A new page will be displayed that requires the student to enter his particulars such as name, matrix number, course, faculty, year, section, group and IC number. The picture of the student also can be captured using the attached web camera by clicking the

'Capture Picture' button. After all the particulars have been filled in and the picture has been captured, the lecturer needs to click the 'Enrol Data' button. After clicking the button, the fingerprint image, particulars and picture will be stored in the system. Fig. 19 shows the data enrolment page.

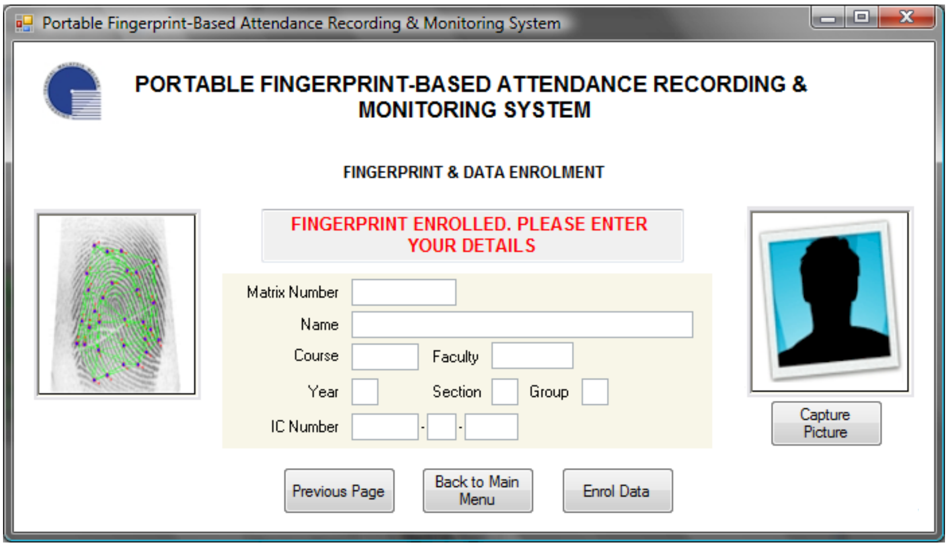

Portable Fingerprint-Based Attendance Recording & Monitoring System

PORTABLE FINGERPRINT-BASED ATTENDANCE RECORDING & MONITORING SYSTEM

FINGERPRINT & DATA ENROLMENT

PLEASE PLACE YOUR INDEX FINGER ON THE FINGERPRINT READER

Fig. 18 Fingerprint Enrolment


Portable Fingerprint-Based Attendance Recording & Monitoring System

PORTABLE FINGERPRINT-BASED ATTENDANCE RECORDING & MONITORING SYSTEM

FINGERPRINT & DATA ENROLMENT

FINGERPRINT ENROLLED. PLEASE ENTER YOUR DETAILS

Matrix Number

Name

Course Faculty

Year Section Group

IC Number - -

Fig. 19 Data Enrolment

## VI. CONCLUSIONS

A portable attendance monitoring system based on fingerprint identification that can be used by lecturers to monitor attendance of students has been successfully developed. The system is portable, easy to use and provides an efficient & effective way to record attendances by using secured method. The system acquires fingerprint patterns and store in the fingerprint database, records attendances in attendance database by comparing the fingerprint pattern from the fingerprint scanner to the fingerprint database and processes the data in the attendance database to determine specific requirements. This system can be used to replace the old method of attendance recording, so that the integrity of the attendance recording can be upheld and the actual student's attendance can be recorded and stored in database. The system utilizes a portable fingerprint scanner as the input to acquire fingerprint images and a laptop equipped with attendance recording and monitoring software as a mobile terminal to process the fingerprint images and record the attendance. The software has been successfully developed in this project although the functionality of the software still has rooms for improvement. However, there are still rooms for improvement. One of the improvements that can be done is on the hardware part. The fingerprint reader can be designed to connect wirelessly to the terminal by using

Bluetooth, Zigbee or any suitable UWB technology that offer low-power high data rate connection [16]. This improvement will increase the mobility of the system and also provide a more seamless user experience in using the system [17].

## ACKNOWLEDGEMENT

The authors would like to express gratitude to Universiti Teknikal Malaysia Melaka (UTeM) for the funding and support through short term grant PJP/2012/FKEKK(5B)/S01095.

## REFERENCES

[1] Henry C. Lee., “Advances in Fingerprint Technology,” 2nd Edition. Florida: CRC Press. 2001.

[2] John Chirillo, Scott Blaul, “Implementing Biometric Security,” 1st Edition, Indiana: Wiley, 2003.

[3] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, “Handbook of Fingerprint Recognition,” 2nd Edition. New York: Springer. 2003.

[4] John D. Woodward Jr., Nicholas M. Orlans, Peter T. Higgins, “Biometrics,” McGraw-Hill. 2002.

[5] Sharat S. Chikkerur, “Online Fingerprint Verification System,” Thesis, State University of New York at Buffalo, June 2005.

[6] Ruud Bolle, Jonathan Connell, Sharanthchandra Pankanti, Nalini Ratha, Andrew Senior, “Guide to Biometrics,” 1st Edition, New York: Springer, 2003.

[7] Gary W. Jones, “Introduction to Fingerprint Comparison,” Staggs Pub, 2000.

[8] James Wayman, Anil Jain, Davide Maltoni, Dario Maio, “Biometric Systems: Technology, Design and Performance Evaluation,” 1st Edition, New York: Springer, 2004.

[9] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, “Impact of artificial gummy fingers on fingerprint systems,” Proceedings of SPIE, Optical Security and Counterfeit Deterrence Techniques IV, Vol. 8577, 2002.

[10] M.Tartagni and R. Guerrieri, “A Fingerprint Sensor Based on the Feedback Capacitive Sensing Scheme,” IEEE Journal of Solid-State Circuits, Vol. 33, No. 1, January 1998.

[11] S. Pankanti, S. Prabhakar, and A. K. Jain, “On the individuality of fingerprints,” Transactions on PAMI, 24(8):1010–1025, 2002.

[12] John K. Schneider, “Ultrasonic Fingerprint Sensors,” Advances in Biometrics, Springer London, pp 63-74, 2008.

[13] H. Han and Y. Koshimoto, “Characteristics of thermal-type fingerprint sensor,” Proceedings of SPIE, Vol. 6944, 2008.

[14] Samir Nanavati, Michael Thieme, Raj Nanavati, “Biometrics: Identity Verification in a Networked World,” Indiana: Wiley, 2002.

[15] Bir Bhanu, Xuejun Tan, “Computational Algorithms for Fingerprint Recognition,” 1st Edition. New York: Springer, 2001.

[16] M. S. I. M. Zin, M. Hope, Finding the Optimal MAC Protocol for Low-Power High Data Rate Ultra Wideband (UWB) Networks, 9th Postgraduate Symposium on the Convergence of Telecommunication, Networking and Broadcasting, June 2008.

[17] M. S. I. M. Zin, M. Hope, A Review of UWB MAC Protocols, 2010 Sixth Advanced International Conference on Telecommunications (AICT), pp.526-534, 9-15 May 2010.