BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Artificial Intelligence Advances
https://ojs.bilpublishing.com/index.php/aia

ARTICLE

School Debit Transaction Using Fingerprint Recognition System

Wai Kit Wong* **Thu Soe Min** **Shi Enn Chong**

Faculty of Engineering and Technology, Multimedia University (MMU), Jalan Ayer Keroh Lama, Melaka, 75450, Malaysia

ARTICLE INFO

Article history
Received: 11 September 2019
Accepted: 22 October 2019
Published Online: 30 October 2019

Keywords:
Fingerprint recognition
Biometric Authentication
Image processing

ABSTRACT

This paper proposed a fingerprint based school debit transaction system using minutiae matching biometric technology. This biometric cashless transaction system intensely shortens the luncheon line traffic and labour force compared to conventional cash payment system. Furthermore, contrast with card cashless transaction system, fingerprint cashless transaction system with benefit that user need not carry additional identification object and remember lengthy password. The implementation of this cashless transaction system provides a more organize, reliable and efficient way to operate the school debit transaction system.

1. Introduction

Nowadays, parents need not to give cash directly to their primary/secondary schools' children. Some schools already practice to use their own debit card system, whereby students or their parents just need to bank in/ deposit the money to the school treasury department, the school treasury department will issue a debit card to students for purchasing food in canteen, stationaries, fees etc. This debit card system in favour by parents because they can monitor their children better due to the reason no cash for students to be get lost/stolen or purchasing outside drugs, tit-bit or unhealthy entertainment.

However, parents still have concerns, such as debit cards being stolen or misplaced by their children. There were a lot of wasteful resources for the system maintainer, as a new card had to be made for them who losing it. Besides that, students would also share their cards among friends, and sometimes the card can be scanned twice, lead to a double charged for a single transaction. Another concerning issue is if students forgot their identification number and PIN number of their card upon transaction, it might lead to a longer queuing time for other students, as primary and secondary students normally have 15-20 minutes' break, the heavy traffic might lead to a waste of food and time. Therefore, a higher level of security and reliable system should be implemented to replace the conventional debit card transaction system, in order to create a convenient and safer environment for the children. Thus, biometric based debit transaction system is being proposed by researchers to overcome the above issues [1,2].

Biometric authentication is a method of recognizing a human being according to the physiological measurements or physically features and traits [3]. The human physical characteristics such as fingerprints, face, hand geometry, voice and iris are known as biometrics. Biometric technologies are becoming the foundation of an

**Corresponding Author:*
Wai Kit Wong,
Faculty of Engineering and Technology, Multimedia University (MMU), Jalan Ayer Keroh Lama, Melaka, 75450, Malaysia;
Email: wkwong@mmu.edu.my

DOI: https://doi.org/10.30564/aia.v1i2.1202

extensive array of highly secure identification and personal verification solutions. Since biometric identifiers are associated permanently with the user, it is more reliable than the conventional authentication methods such as PIN and password. Thus, biometric based authentication can provide extra confidential in transactions by securing the personal information and privacy data.

In fact, there are many methods for biometric authentication. The most commonly used methods for biometric authentication are iris scanning [4], hand scanning [5], fingerprint recognition [6], face recognition [7], and voice recognition [8]. The biometric information will never ever match with another individual because everyone has their own unique biometric features. Researchers [9,10,11] had conducted numerous analysis and comparison among different types of biometric recognition methods. The comparison of biometric methods is mainly based on characteristics such as universality, uniqueness, performance, permanence, and measurability.

Based on the researchers' results [9,10,11], fingerprint recognition has the highest market share among the technologies of biometric security system in the market. The preference of fingerprint recognition in the current market is mostly due to its high accuracy, performance and stability. Besides that, fingerprint recognition has a moderate pricing compare to iris scan which required a high capital cost and level of skills to operate and maintain. Moreover, it also has a relatively low percentage of False Acceptance Rate (FAR) and False Reject Rate (FRR) [12] which make it more reliable to use either in police or industrial area. Thus, fingerprint biometric recognition is widely acceptable and preferable compare to the other biometric security systems.

In this paper, a fingerprint recognition system will be proposed for replacing the debit card in business transaction system. This can provide an even more secure studying environment for students, since debit card can be stolen and use within the school too. With the fingerprint recognition system, the student's fingerprint itself is the debit card. Nobody can steal it. Fingerprint scanning devices in hardware and recognition algorithm in software will be developed to verify and identify the identity of a student's debit account through fingerprint scan. This will enable the student to do transaction by fingerprint scan in the school and does not need to go through the hassle of showing the debit card or paying by cash.

The paper is organized in the following way: Section II will be briefly comments on the fingerprint recognition school debit transaction system. Section III presents the proposed Hough Transform Minutiae Pairing Fingerprint Matching (HTMP) technique applies in identifying the correct person and section IV reports some experimental results. Finally, in section V, some conclusion and envision future developments is drawn.

2. Fingerprint Recognition School Debit Transaction System Design

This section outlines the system design for the fingerprint recognition school debit transaction system. It consists of the hardware architecture and software modules of the system as discuss in section 2.1 and section 2.2 below.

2.1 Hardware Architecture

Figure 1 shows the hardware architecture for the proposed fingerprint recognition school debit transaction system. The overall system consists of fingerprint collection module and PC/tablets placed at each shop/stall, all linked to a centre hub (server) with students' information database for info matching and business transaction.

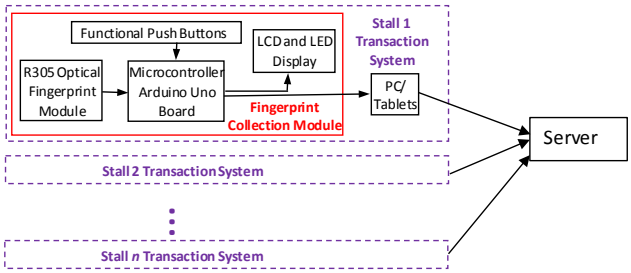


Figure 1. Fingerprint Recognition School Debit Transaction System

2.1.1 R305 Optical Fingerprint Module

It is an optical biometric fingerprint sensor with a TTL UART interface for direct connection to the PC. The user is allowed to store fingerprint data and verify identity with the module. The module consists of two main function which are enrolment and matching of fingerprint. However, in this project, only the enrolment of fingerprint function is in used. The build in fingerprint matching function of R305 is slow when datasets achieving 1000 or more. There is an advance algorithm, namely the Hough Transform Minutiae Pairing (HTMP) fingerprint matching technique is proposed in the computing side (PC/tablet) to run the fingerprint matching task. Besides that, the optical fingerprint module will capture the image of a finger by utilizing the light ray. However, the image of the fingerprint can be affected by external environment such as dirt, wet, quality of skin and humidity. It will be more easy to study and trouble shoot the fingerprint mismatch in the proposed external matching algorithm (HTMP), rather than using the R305 build in matching algorithm.

 DOI: https://doi.org/10.30564/aia.v1i2.1202

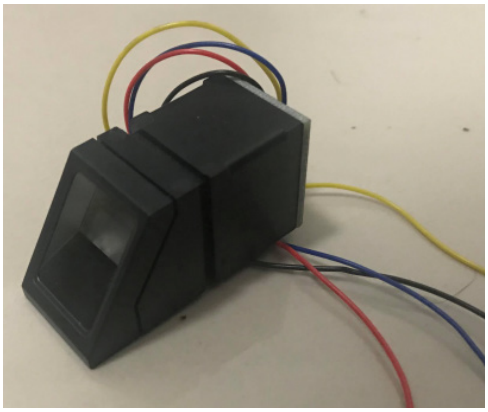


Figure 2. R305-optical fingerprint module

2.1.2 Arduino UNO

The R305 fingerprint module is interfacing by Arduino UNO board. There are several types of Arduino board such as Uno, Mega, Nano, and etc. However, Arduino Uno which based on ATmega328 microcontroller was selected due to its inexpensive cost, cross platform, simple and clear programming environment, with open source and extensive software, together with large support of community. The proposed Arduino UNO board is supplied with multiple sets of digital and analog input/output pins. The operating voltage of the Arduino Uno will be 9Vby connecting to the power supply of PC/tablet. The four digital pins (TXD, RXD, VIN and GND) of the R305 fingerprint module are connected to the Arduino UNO board, as shown in Figure 3 below. The Transmit Data (TXD) pin is connected to pin D3 of Arduino UNO board for data output, the Receive Data (RXD) pin is connected to pin D2 of Arduino UNO board for data input. The Input Voltage (VIN) pin is connected to pin 5V of Arduino UNO board for a constant 5V supply to fingerprint module, and the Ground (GND) pin is connected to pin GND of Arduino UNO board for ground.

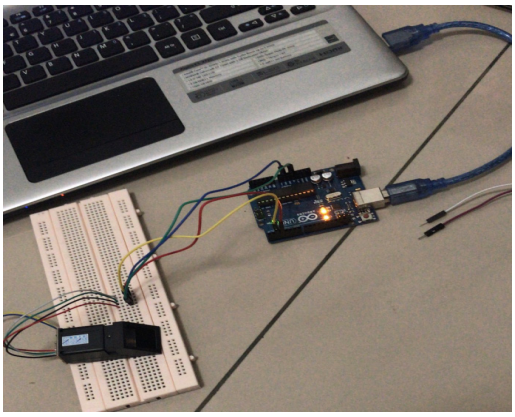


Figure 3. Fingerprint module connected to Arduino UNO board

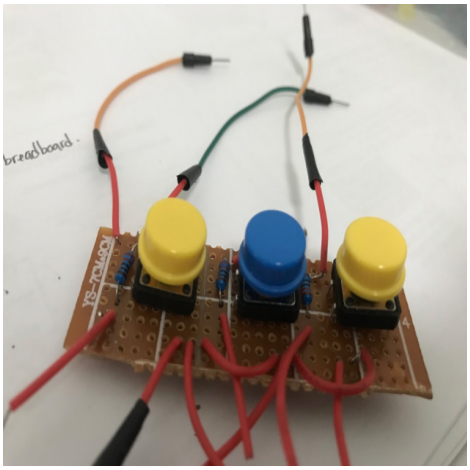


Figure 4. Push buttons for Enrolment, Verification and Delete

2.1.3 Functional Push Buttons

There will be three push buttons as shown in Figure 4, placed on the fingerprint collection module for three important functions, namely: Enrolment, Verification and Delete. The three buttons are connected each with a 1kΩ pull up resistor to the Arduino UNO board.

2.1.4 LED and LCD Display

One red LED, one green LED and three yellow LEDs are used as indicators on the fingerprint collection module. The three yellow LEDs are connected to pin number 12, 10 and 4, as shown in Figure 5, indicate the mode selection of Enrolment task, Verification task and Delete task respectively. The red LED is connected to digital pin 13 to indicate task failure, the green LED is connected to digital pin 11 to indicate task successful. The (I^2C) LCD display is used to display the short messages to the shopkeepers about the task execution of the fingerprint collection module, as shown in Figure 6 below.

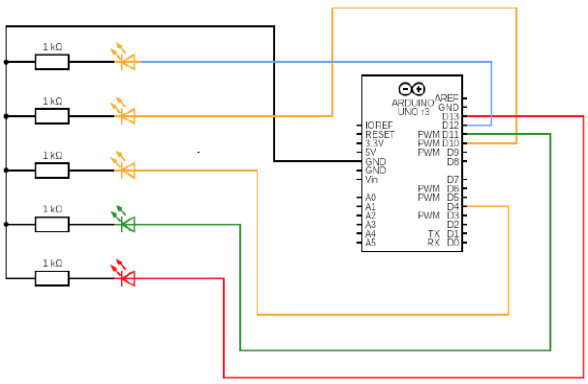


Figure 5. Circuit Diagram of the LED Indicators and Arduino UNO Board

DOI: https://doi.org/10.30564/aia.v1i2.1202

Figure 6. A working (16*2) LCD Display

2.1.5 PC/Tablet

The PC, laptop or tablet will read in fingerprint signals transferred from the Arduino UNO and perform the fingerprint image processing for users' identity matching. It comes with Graphic User Interface to registration page, selling products menus, purchase histories etc. Other than that, it can display the product database, and allow other operations such as viewing employees clock in-out times, sales report, etc.

2.1.6 Server

The server work as a centre hub which manages the access of multiple stall stations to a centralized resource (users' personal information, databases of selling products name lists, price, credit balance, top-up and purchase histories etc.)

2.2 Software Implementation

The fingerprint based school debit transaction system begin with a graphical user interface that authorize the users to register their personal information into the database 1. After that, user is required to enrol their fingerprint into the system for future verification purpose. When the user wishes to proceed for credit transaction (top-up credit or purchase items/services), a verification of fingerprint is needed. There are only two possibilities for the verification results: Successful or Fail. Only the user with a valid fingerprint stored in the database can proceed to further operations such as top-up credit or purchase items/services. After the transactions being performed, the system will update the latest account balance into the database. The overall software architecture for fingerprint based school debit transaction system is shown in Figure 7 below.

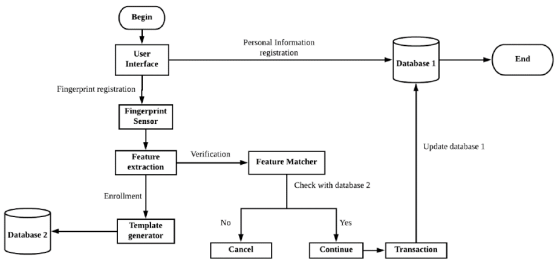


Figure 7. Software Architecture for Fingerprint based school debit transaction system

2.2.1 Activity Diagrams

Activity diagrams are used to demonstrate the processes carried out in the system. Generally, there are five activity diagrams used in the proposed fingerprint based school debit transaction system: (1) Activity diagram of fingerprint enrolment, (2) Activity diagram for fingerprint verification, (3) Activity diagram for top-up process, (4) Activity diagram of transaction process (5) Activity diagram for checking purchase history.

The fingerprint enrolment needs at least two identical fingerprint inputs for the sake of wipe out potential errors during the feature extraction process. The image processor (PC/laptop/tablet) will match the fingerprints to determine whether the two inputs are from the same user's finger. If yes, the template will be saved. Else, if the second fingerprint input is not match with the initial one, the system might not generate the template. The complete fingerprint enrolment process is shown in Figure 8.

For fingerprint verification process, the quality of the fingerprint will be enhancing by some pre-processing steps like classifying fingerprint image into the 8 major pattern categories, identify the essence point in the fingerprint image and crop the core region concentrated in the essence point, so that the important features like minutiaes, ridges and bifurcation points can be extracted for future matching. The fingerprint matching algorithm will further discuss in Section 3. If the input fingerprint matches with the template stored in the database, the LCD screen will display the user identity for shopkeeper to further verify with user. However, if the input fingerprint does not match any of the template stored in the database, the LCD will not display any user identity, and perhaps will show message "Not found in database". The whole fingerprint verification process is shown in Figure 9.

If the input fingerprint is successfully matched with the template stored in the fingerprint database, the user can carry out functions like topping up their debit account, paying for their meals, groceries, stationaries, services etc. and checking their top-up and purchase history. The whole process for the functions above is graphically illustrated in Figure 10, Figure 11 and Figure 12 respectively.

 DOI: https://doi.org/10.30564/aia.v1i2.1202

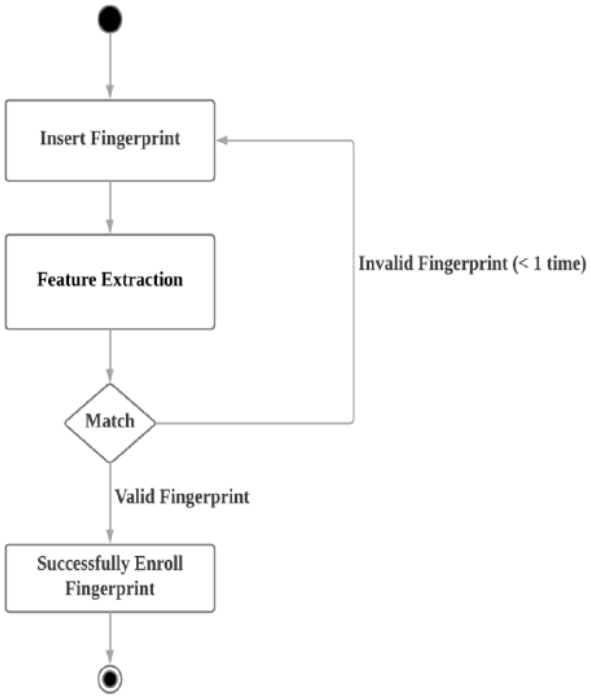


Figure 8. Activity diagram of fingerprint enrolment

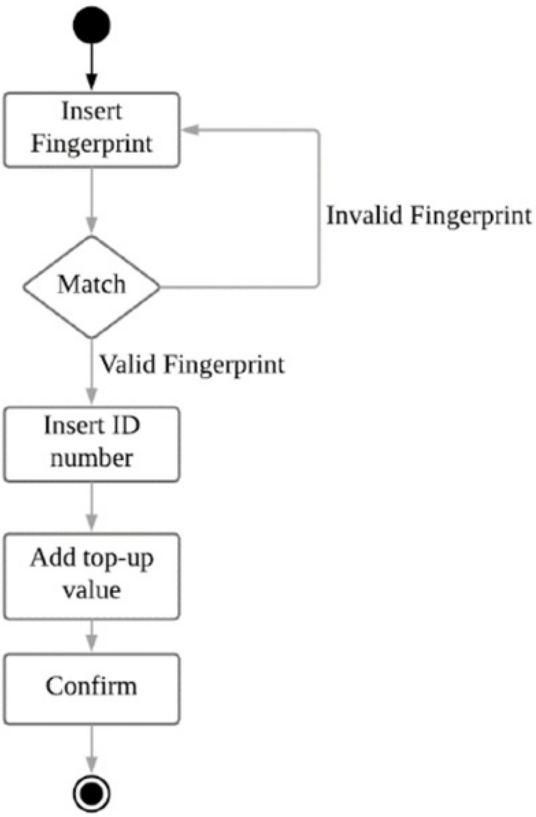


Figure 10. Activity diagram for top-up process

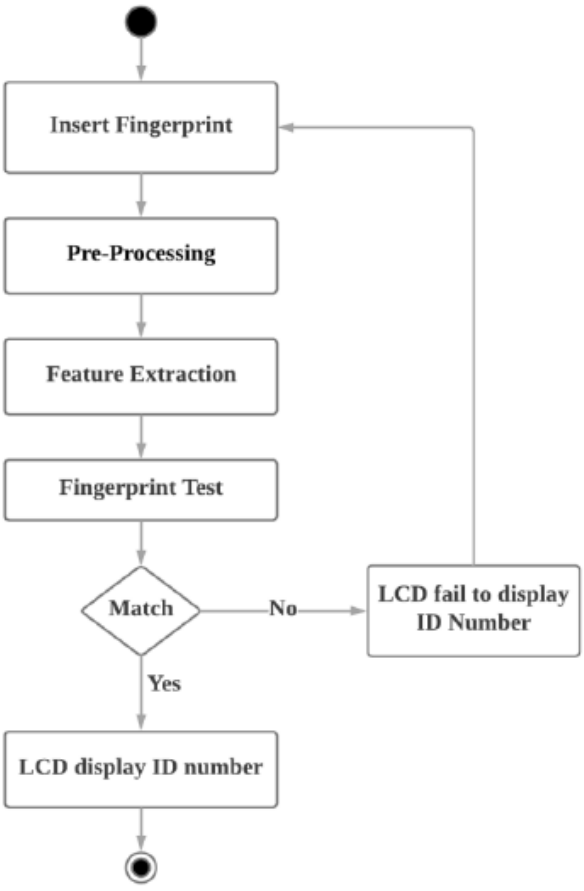


Figure 9. Activity diagram for fingerprint verification

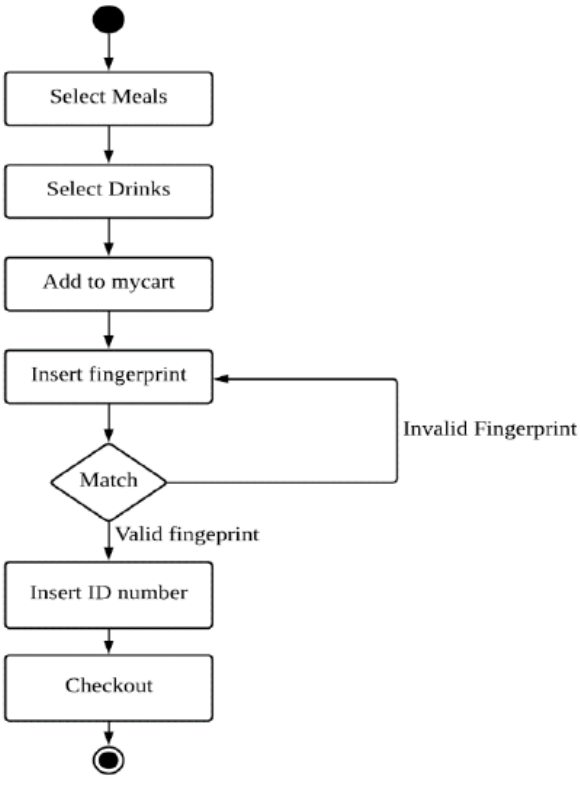


Figure 11. Activity diagram of transaction process

DOI: https://doi.org/10.30564/aia.v1i2.1202

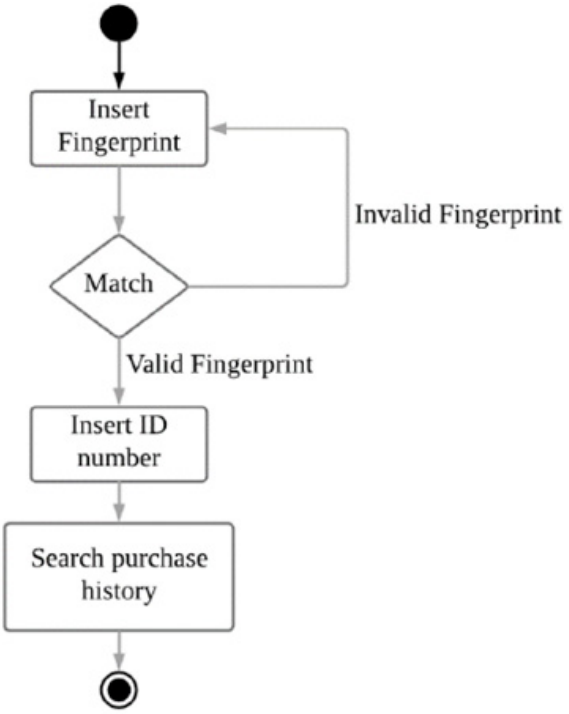
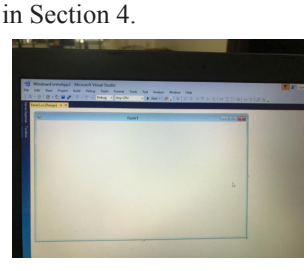


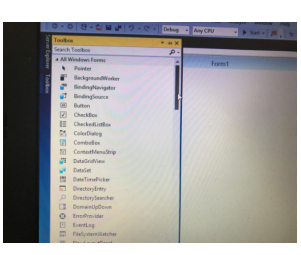
Figure 12. Activity diagram for checking purchase history

2.2.2 GUI Design and Database Software

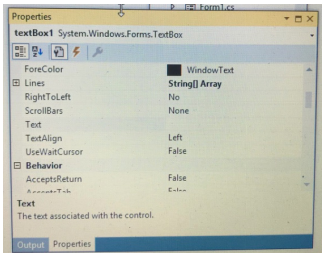
In this sub-section, the software implementation and procedures for designing a user interface is discussed. The Graphical User Interface (GUI) will be created on Microsoft Visual Studio 2017 as it can be easily created by clicking and dragging the desired components such as label, text box, buttons, check box and data grid into the GUI layout form. Figure 13 (a) shows a blank Microsoft Visual Studio 2017 GUI layout form and Figure 13 (b) shows its corresponding Toolbox. The component parameters and properties such as appearance, data and layout can be checked and changed by double clicking on the components. Furthermore, the database connection can be checked from the server explorer. This assures that all the data is entered into the database table. Figure 13 (c) shows the Microsoft Visual Studio 2017 Properties box and Figure 13 (d) shows the Microsoft Visual Studio 2017 Server Explorer. The completed design of the GUI will be shown in Section 4.



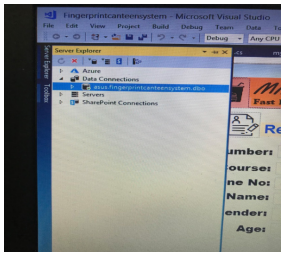
(a)



(b)



(c)



(d)

Figure 13. Microsoft Visual Studio 2017 (a) Blank template of GUI layout form (b) Toolbox (c) Properties box (d) Server Explorer

The database of the proposed fingerprint based school debit transaction system is built by Microsoft SQL Server Management Studio. The database of this project is to store and retrieving data such as personal information and the account balance. There will be total four tables of the product. Each of the tables is used to store and manage the collected data that are inserted from the GUI application, and it will be retrieved when it is requested by users. The connectivity of the database of the database is explained below. First, thee relational database management system is connected to the ASUS server host after the SQL Server Management Studio has been assessed. Then, a new database from the Object Explorer is created. The tables in the database can be used to assign and manage different input data directing from the GUI application. After a new table has been created, a name is assigned to each of the column in that table. Figure 14 shows an example of the created database.

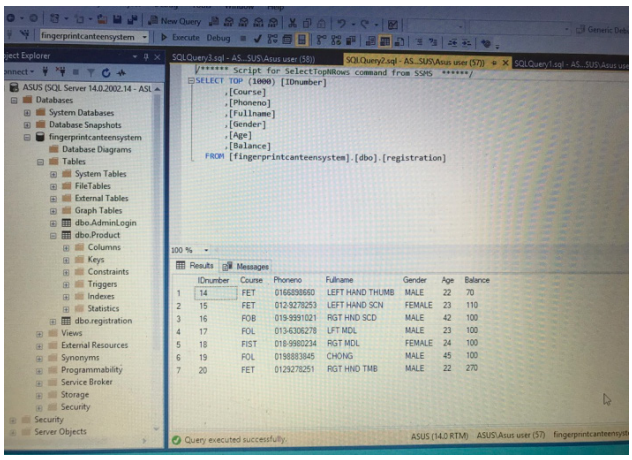


Figure 14. An example of database built by Microsoft SQL Server Management Studio

3. Hough Transform Minutiae Pairing Fingerprint Matching (HTMP) Technique

The Hough Transform Minutiae Pairing (HTMP) fin-

DOI: https://doi.org/10.30564/aia.v1i2.1202

gerprint matching technique is proposed to the develop fingerprint based school debit transaction system and it is run by the following six steps:

Step 1: Scan Live Fingerprint: Retrieve user's fingerprint image using R305-optical fingerprint module.

Step 2: Classify Fingerprint Image: Classify the fingerprint image into any of the below eight categories: (i) Plain Arch (ii) Tented Arch (iii) Ulnar Loop (iv) Radial Loop (v) Plain Whorl (vi) Central Pocket Loop Whorl (vii) Double Loop Whorl and (viii) Accidental Loop Whorl, as depicted in Figure 15.

Step 3: Identify Region of Interest: identify the essence point in the fingerprint image and crop the core region concentrated in the essence point.

Step 4: Enroll Fingerprint Minutiae: extract two minutiae spot sets M and N from two fingerprint images (database and inquiry) with undisclosed scale, rotation and translations by the following notations: $M = \left\{\left(m_x^1, m_y^1, \gamma^1\right),...,\left(m_x^P, m_y^P, \gamma^P\right)\right\}$, $N = \left\{\left(n_x^1, n_y^1, \delta^1\right),...,\left(n_x^Q, n_y^Q, \delta^Q\right)\right\}$ where P and Q are the total number of minutiaes in set M and set N respectively. $\left(m_x^i, m_y^i, \gamma^i\right)$ and $\left(n_x^i, n_y^i, \delta^i\right)$ are those three features (x-position, y-position, orientation) correlated with the i-th minutiae in set M and set N respectively.

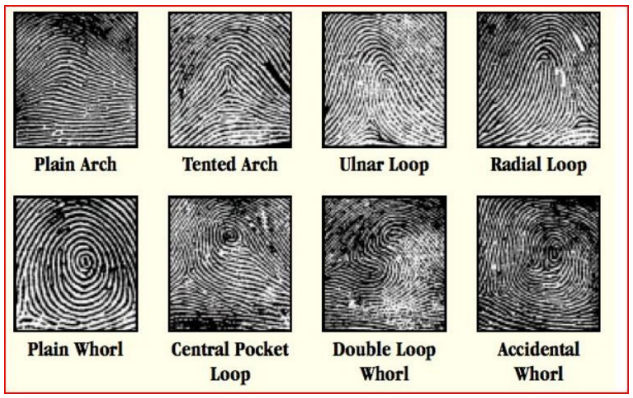


Figure 15. Fingerprint patterns [13]

Step 5: Determine Rotation and Translation Parameters: the transformation orientation function: $G_{s,\theta,\Delta x,\Delta y} : R^2 \rightarrow R^2$ is given by [14]:

$$G_{s,\theta,\Delta x,\Delta y}\begin{pmatrix} x \\ y \end{pmatrix} = s\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} \Delta x \\ \Delta y \end{pmatrix} \quad (1)$$

where s, θ, $(\Delta x, \Delta y)$ are the scale, rotation and translation parameters correspondingly. For fingerprint authentication/identification, the scaling factor s is set to unity, due to the reason that the same device is used to capture fingerprint images for both the offline processing stage and online authentication stage. The generalized Hough Transform [15] is applied to determine those parameters. The entry $E(l, p, q)$ sum up the verification of the orientation transformation $G_{\theta_l,\Delta x_p,\Delta y_p}$, where $(\theta_l, \Delta x_p, \Delta y_p)$ are the quantized values of $(\theta, \Delta x, \Delta y)$ correspondingly. The normalized $E(l, p, q)$ in the range from 0 to 1 is represented by $f(\theta, x, y)$ and is treated as the probability density function for θ, x, y transformation parameters. (θ, x, y) are independent from each other and can be estimated separately, hence $f(\theta, x, y)$ can be re-structured as:

$$f(\theta, x, y) = f_\theta(\theta) * f_x(x) * f_y(y) \quad (2)$$

(1) Rotation Parameter: Let $O_d = \left(O_d^1,...,O_d^{P_d}\right)$ be the orientation field from the database fingerprint image and $O_i = \left(O_i^1,...,O_i^{P_i}\right)$ be the orientation field from the inquiry fingerprint image, where P_d and P_i are the lengths of the O_d and O_i arrays respectively. The generalized Hough Transform based method to estimate the rotation parameter (θ) consists of following 2 main steps:

(a) Estimate the probability density function of the rotation parameter $f_\theta(\theta)$

(b) Search the correct rotation parameter of the two transformation among the two fingerprint images based on the results obtain in (a.)

An accumulator array $E(l)$ is used to gather the verification for each possible rotation by l degree, whereby $l = O_d^P - O_i^q$ degree which map O_i^q to O_d^p. The correct rotation transformation among two fingerprint images is computed by mass center [14]:

$$\mu_{\lambda(\theta)} = \frac{\sum_{l\in\lambda} l \times f_\theta(l)}{\sum_{l\in\lambda} f_\theta(l)} \quad (3)$$

where λ is the densest interval among the extracted minutiaes from the collected fingerprint images

(2) Translation Parameter: the computation of the translation parameters (t_x, t_y) can be done with the rotation parameter θ obtained above. Consider that the minutiae

DOI: https://doi.org/10.30564/aia.v1i2.1202

set M and N are extracted from the database and inquiry fingerprints correspondingly, utilizing the determined rotation transformation G_θ upon the minutiae in set N, a new rotated version of the N point set, N^r can be acquired. The following notation are in used:

$$N^r = \left\{\left(n_x^{r,1}, n_y^{r,1}, \delta^{r,1}\right),\ldots,\left(n_x^{r,Q}, n_y^{r,Q}, \delta^{r,Q}\right)\right\}$$

where $\left(n_x^{r,i}, n_y^{r,i}, \delta^{r,i}\right)$ are the three features (spatial, position, orientation) related to the i-th minutiae in set N^r. It can be calculated by [14]:

$$\begin{pmatrix} n_x^{r,i} \\ n_y^{r,i} \\ \delta^{r,i} \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} n_x^i \\ n_y^i \\ \delta^i \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \theta \end{pmatrix} \tag{4}$$

where $\left(n_x^i, n_y^i, \delta^i\right)$ is the i-th minutiae in set N, θ is the estimated rotation angle. Two minutiae points sets M and N^r are used to calculate the translation parameters $\left(t_x, t_y\right)$. The steps for calculating x-translation, t_x:

(a) Estimate the probability density function of the x-translation parameter $f_x(x)$

(b) Calculate the x-translation, t_x with $f_x(x)$.

An accumulator array $E(p)$ is used to gather the verification for each possible x-translation, whereby $p = m_x^i - n_x^{r,j}$ is the x-translation which map $n_x^{r,j}$ to m_x^i. m_x^i is the x-coordinate for the i-th minutiae in set M and $n_x^{r,j}$ is the x-coordinate for the j-th point in set N^r. The correct x-translation transformation among two fingerprint images is computed by mass center [14]:

$$\mu_{\lambda(x)} = \frac{\sum_{p\in\lambda} p \times f_x(p)}{\sum_{p\in\lambda} f_x(p)} \tag{5}$$

where λ is the densest interval among the extracted minutiaes from the collected fingerprint images.

The steps for calculating y-translation, t_y are identical with that of calculating x-translation, t_x. The correct y-translation transformation among two fingerprint images is computed by mass center [14]:

$$\mu_{\lambda(y)} = \frac{\sum_{q\in\lambda} q \times f_y(q)}{\sum_{q\in\lambda} f_y(q)} \tag{6}$$

whereby $q = m_y^i - n_y^{r,j}$ is the y-translation which map $n_y^{r,j}$ to m_y^i. m_y^i is the y-coordinate for the i-th minutiae in set M and $n_y^{r,j}$ is the y-coordinate for the j-th point in set N^r.

Step 6: Set Threshold to Compute Matching Score: Pair up the minutiae set if the two fingerprint images' features or components ($\mu_{\lambda(\theta)}, \mu_{\lambda(x)}, \mu_{\lambda(y)}$) are identical or within a range of tolerance. A tolerance box is generated throughout each minutiae feature for coping with the shifting in the minutiaes pairs. The minutiaes pairs are gathered among the pairs that fulfil the below geometric constraints [14]:

(a) The two minutiaes' Euclidean distance does not exceed a certain value Δd.

(b) The two minutiaes directions' angular difference below a certain tolerance $\Delta\theta$

(c) Supposing that in excess of one pairs situate in the same bounding box, the two minutiaes with the minimum Euclidean distance opt as the matched pair.

Concerning to weight out the similarity among two fingerprints, a similarity level measurement method applying the matching score ψ_s is adopted, with the below formula [14]:

$$\psi_s = \frac{N_{pair}}{\max\{P, Q\}} \tag{7}$$

where N_{pair} is the number of matched minutiae pairs, P and Q are the total number of minutiaes extracted from the database and inquiry fingerprint images correspondingly. ψ_s is with value ranging from 0 to 1. If ψ_s is tends to 0 implies that the two fingerprints are non-matching, else if ψ_s is tends to 1 implies that the two fingerprints are good match.

4. Experimental Results

In this section, the application of the proposed fingerprint school debit transaction system will be illustrated. It will cover the product overview, test run results and the product survey analysis. The fingerprint school debit transaction system was tested in an institution of higher learning within Malaysia, who wants to remain anonymous.

 DOI: https://doi.org/10.30564/aia.v1i2.1202

4.1 Product Overview

The final prototype of the fingerprint school debit transaction system is shown in Figure 16. The circuit board and Arduino UNO microcontroller module are stored inside an external custom made casing. The function of all the buttons are clearly labelled with laminated instruction signs. The LCD and LED will begin to operate once the USB cable is connected to PC/laptop/tablet. When the fingerprint verification process is successful, the green LED will light up, whereas if unsuccessful fingerprint verification process detected, the red LED will be light up.

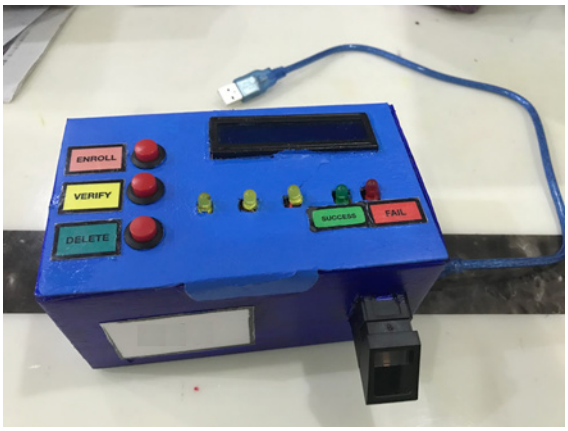


Figure 16. Final Prototype of the Fingerprint School Debit Transaction System (Fingerprint Collection Module)

The Admin Login GUI page is shown in Figure 17. This is the main page of the fingerprint school debit transaction system. Only the related school shopkeepers (Canteen, Cafeteria, Mini Mart, Printing shop, laundry shop, computer shop etc.) have their own username and password to login to the server to perform the business transaction (transfer students deposited money into their account). This is to ensure the privacy and confidentiality of every shopkeeper.

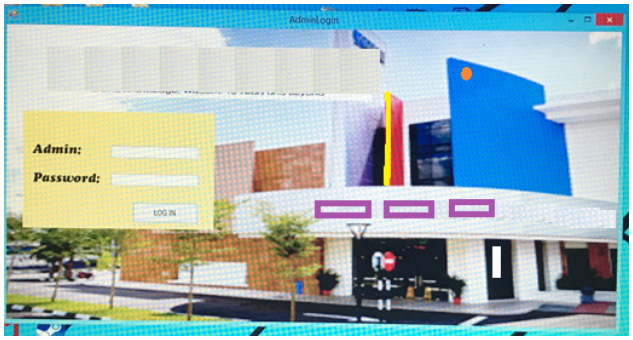


Figure 17. Admin Login GUI page

The first important step for the system to work is to enrol the students' (users') fingerprint and personal information into the system. The registration page is shown in Figure 18. The basic information to insert is course, phone number, full name, gender and age. After inserting all the relevant information, the "ADD" button is pressed to enrol in the system. In this case, the system will generate an ID number for that particular student. Moreover, the system can be used to update the latest information or delete the student's previous account.

Next, students are instructed to enrol their fingerprint with the assigned identification number in the fingerprint collection module. The "Enrol" button must press to enrol a fingerprint, the message "Please insert your ID" will be displayed on LCD screen, as shown in Figure 19(a). Once the ID number has been inserted, the student may place his/her finger on the fingerprint module to scan fingerprints. The student must place his/her finger twice in each registration process, because the second fingerprint input is required to compare and check with the initial template to ensure that both fingerprint inputs are matched. The system will then display "Print Matched, Enrol successful" to indicate a success case (as shown in Figure 19(c). Else it will display "Error" in the LCD screen for fail case. Students who have successfully enrolled their fingerprint into the database system may now start deposit /top up credit into the database. The top-up page is shown in Figure 19d.

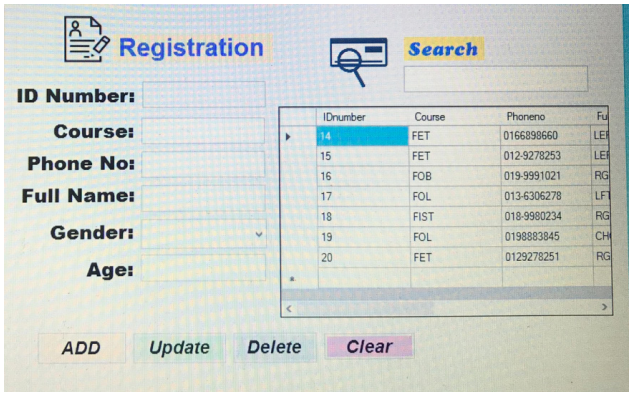
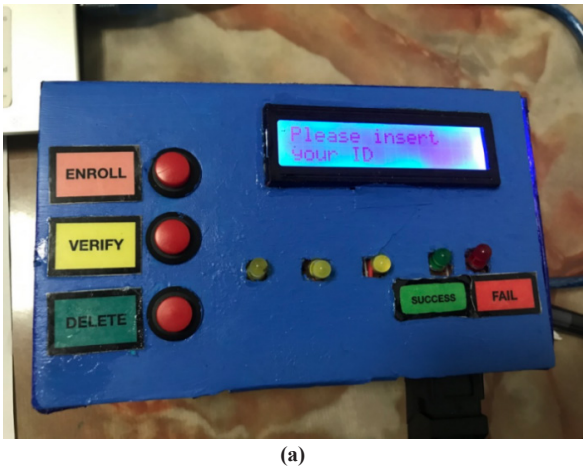
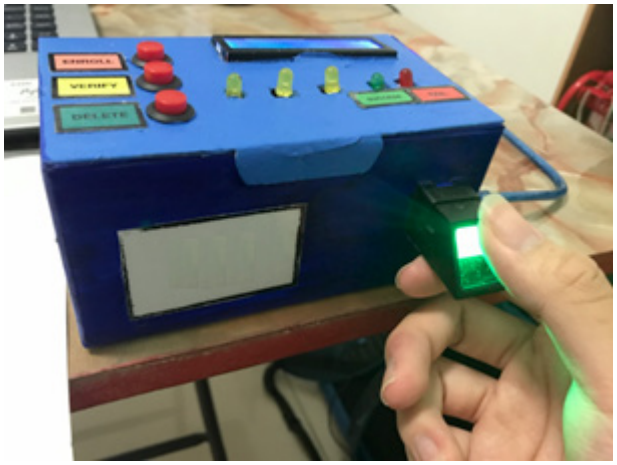


Figure 18. Registration Page at Server



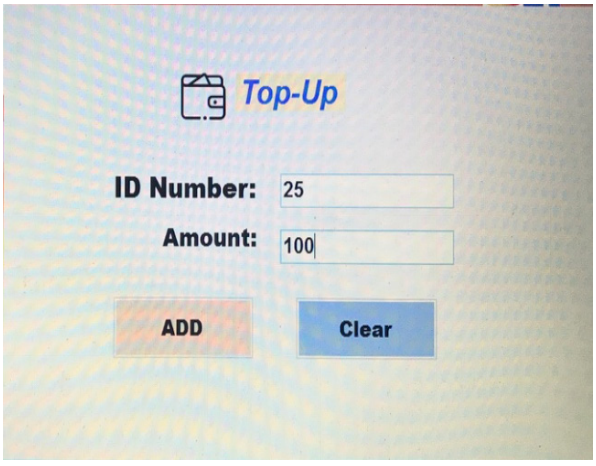
(a)

DOI: https://doi.org/10.30564/aia.v1i2.1202



(b)

(c)



(d)

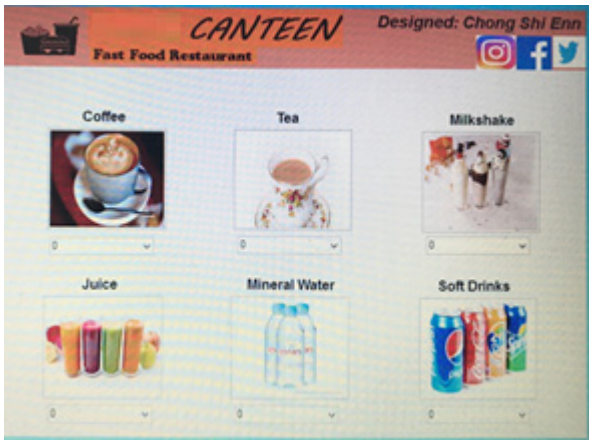
Figure 19. Enrolment (a) Message shown after Enrol Button Pressed (b) Scanning Fingerprint (c) Enrolment successful (d) Top-Up Credit page

Students may start purchasing meals, goods, services within the school after enrolled and deposited credit into the database. A canteen case is chosen for further studies. Figure 20a shows the Meal GUI page and Figure 20b shows the Drinks GUI page of the canteen menu page. The meals and drinks selected by the students are later added to their shopping list, under Mycart GUI page, as shown in Figure 20c. This page shows the price and quantity of items ordered by students.

In order to check out the items, students must authenticate their identity by evaluating their fingerprint for making payment. Students are required to press the "Verify" button on the fingerprint collection module, as shown in Figure 20d. After the "Verify" button pressed, the LCD screen will display the message "Waiting for valid fingerprint", as shown in Figure 20e, while processing the fingerprint to seek for the correct students' ID. The LCD screen will display the message "Found ID #.." for successful verification attempt, as shown in Figure 20f.

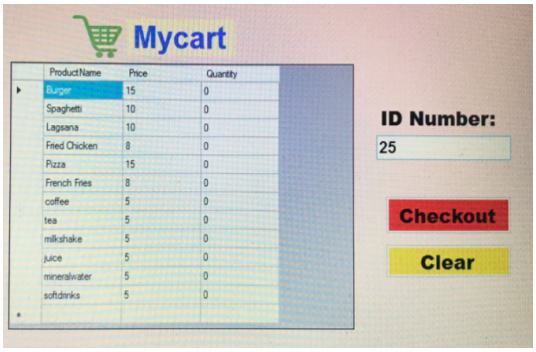
On the fingerprint collection module, the red LED will initially illuminate to indicate that there is no finger place on the sensor. The green LED will light up once the students' fingerprint had been identified. The LCD screen will display the students' identification number and the accuracy of the matching fingerprint. Only student who has successfully obtained his/her identification number can make transaction. The canteen operator will insert the students' identification number to complete the payment process.

(a)



(b)

 DOI: https://doi.org/10.30564/aia.v1i2.1202



(c)

(d)

(e)

(f)

Figure 20. Menu Selection and Authentication for Payment (a) Meals GUI page (b) Drinks GUI page (c) Mycart GUI page (d) Identity Verify Button Pressing (e) Identity Verify Process On-going (f) Results of Verification

4.2 Test Run Results

The fingerprint school debit transaction system was test run in the canteen of the institution of higher learning. The experiment tested between 1,000 different students and staff. Each person must contribute 2 fingerprint inputs, which are thumb and index finger during the experiment. Moreover, each fingerprint entry will be tested with total number of 5 times. There will be a total of 10,000 attempts in this experiment. The main experiment objective is to test the reliability of this fingerprint recognition system by calculating the successful authentication rate between 10,000 attempts. The rate of accuracy will be calculated with the below formula:

$$\text{Rate of Accuracy} = \left(\frac{\text{Successful Attempt}}{\text{Total Attempt}}\right)\times 100\% \quad (8)$$

Table 1 below shows the number of successful authentication in each of the thumb and index finger attempts. The total number of successful attempts in this authentication experiment is 9,090. Therefore, the accuracy rate for this system is 90.9% by using equation (8). Figure 21a shows the failure rate between the thumb and index finger and Figure 21b shows the failure rate between the (<2) attempts and (>2) attempts.

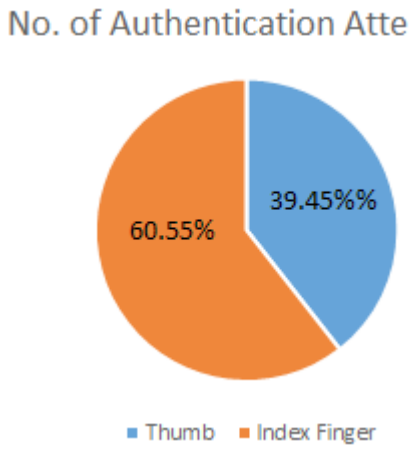
The pie chart in Figure 21a shows clearly that index finger has higher unsuccessful attempt rate (60.55%) compare to thumb finger (39.45%). The pie chart in Figure 21b shows that most of the unsuccessful attempts took place in the first two attempts of the experiment. It has failure rate up to 79.23% in the first two attempts of the authentication process. However, there is a drastic drop after the first two attempts (20.77%).

There are several reasons that could affect the accuracy of the authentication process such as the finger pressure exerted on the sensor and the immobility and fixed posture of finger during verification. Besides that, finger's skin conditions such as dry, moisture and dirt may also affect the authentication result. Thus, it can conclude that the initial failure rate was solely caused by human factor.

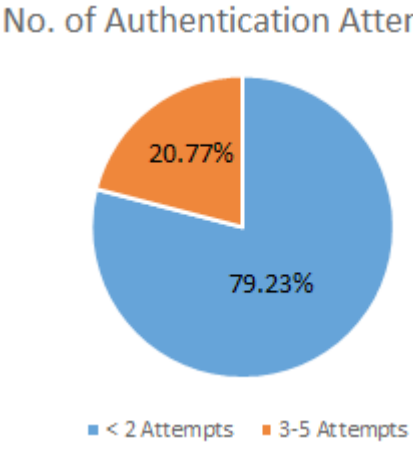
Table 1. Results of Fingerprint Authentication Attempts

Finger Types	No. of Authentication Attempts					
	1	2	3	4	5	Total
Thumb	761	960	979	971	970	4,641
Index Finger	679	879	972	960	959	4,449
Total Successful Attempts	1,440	1,839	1,951	1,931	1,929	9,090
Total Unsuccessful Attempts	560	161	49	69	71	910

DOI: https://doi.org/10.30564/aia.v1i2.1202



(a)

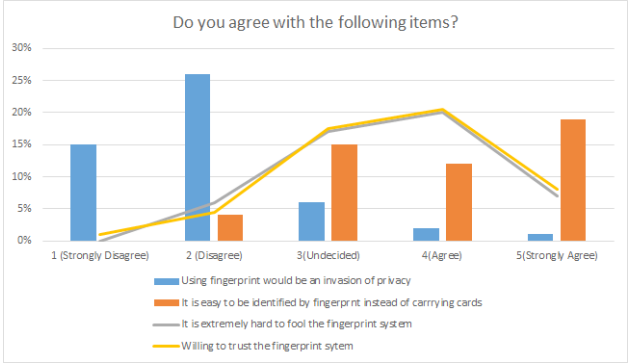


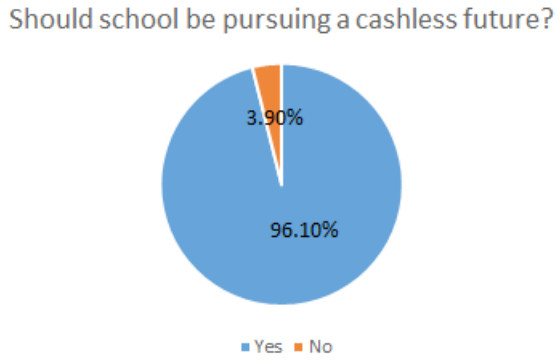
(b)

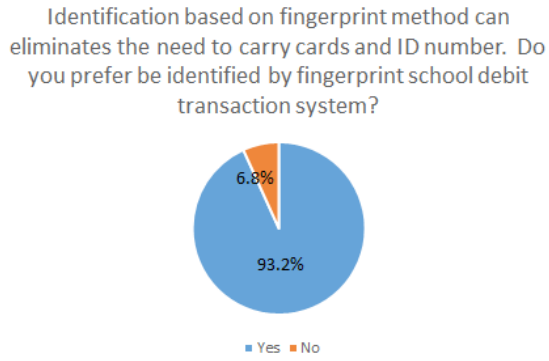
Figure 21. Pie Chart on Unsuccessful Attempt (a) Between Thumb and Index Finger (b) Number of attempts

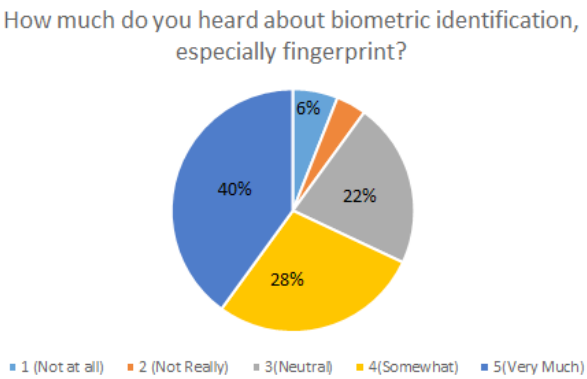
4.3 Product Survey Analysis

For the 1,000 participated students and staff in testing the fingerprint collection module, a survey was conducted onto them to determine the awareness and market value of the fingerprint based school debit transaction system. The questionnaire and the results are shown in Figure 22. Generally, majority of the respondents agreed that all schools should have a cashless future and 40% of them have heard about biometric identification, particularly in fingerprint technology. In addition, 98% of them agreed that a fingerprint based debit transaction system can eliminate the need for a student to carry cards and remember their password/identification numbers. Most of them are willing to replace the conventional payment method with this new fingerprint based debit transaction system. Furthermore, 82% of the respondents believe that the appropriate time taken to identify the fingerprints should be less than 1 minute (our proposed system current achievement is 30 second plus). Furthermore, most respondent do not believe that the use of fingerprints would be an invasion of privacy and are willing to trust the fingerprint based debit transaction system if it is introduced in the school business area.









 DOI: https://doi.org/10.30564/aia.v1i2.1202

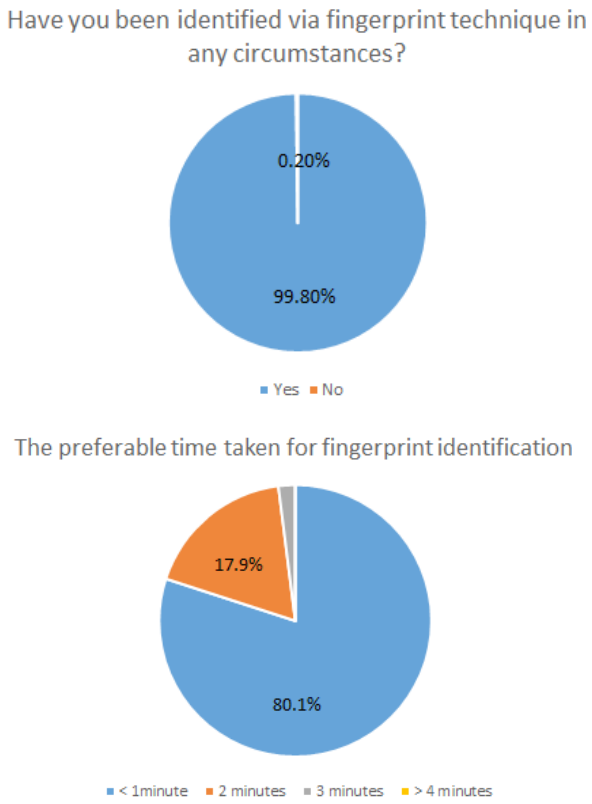


Figure 22. Questionnaire and the results surveying fingerprint based school debit transaction system

5. Conclusion

A fingerprint-based school debit transaction system is developed to promote a smooth flow and cashless transaction environment within the school. In this case, it makes all the procedures and step become more convenient and efficient. Furthermore, the implementation of fingerprint -based transaction system can totally avoid using cash money as well as prevent issues like debit card get lost or stolen. All of the transactions made within the school will be independent of PIN and cards. Therefore, with this cashless payment system, all the money can be safely secured in the student's account. Moreover, one of the highlights of this system is able to trace back all the purchase history. This function can help the parent to monitor and restrict their children from consuming any unhealthy diet and junk foods. Thus, parent can ensure that their children's money is being spent on the right intention. In addition, a survey was conducted with 1,000 students and staff in the corresponding institution of higher learning, and majority of them agreed that all schools should be pursuing a cashless future and willing to use fingerprint-based transaction system.

The proposed fingerprint-based school debit transaction system does have some limitation. It depends critically on the quality of the fingerprint's image. The resolution of the fingerprint's image has a vital influence on the accuracy of the matching system. The current optical fingerprint module might not be able to extract the important features from the fingerprint if the input is in extremely low quality (blur user's fingerprint surface). Therefor it can lead to rejection or acceptance. Furthermore, the pressure exerted and the finger's skin condition are also constraints to the current system.

The current fingerprint collection module is powered by electricity from the PC/laptop/tablet by each shop with the school. However, if there is a power failure occurs, the system will stop working. In this case, it will restrict the registration and verification process, and may stop other users from making payment with the system. An independent power source will be developed in future to prevent such incidents cause by power failure occurs. At this moment, the system only works in an offline mode within school. For instance, it does not allow parents to check the purchase history and credit balance via online. In addition, the proposed system does not support online banking yet. Parents have to come to the finance department to transfer or deposit funds to their children's debit account. In future, the debit transaction system will be integrated and corporates with several banks to allow online banking transaction.

References

[1] D. Thaktar. Biometric Solution for Schools- Fingerprint lunch line. Bayometric, 2018. From: https://www.bayometric.com/biometric-solution-schools-fingerprint-lunch-line/

[2] J. Trader. Why School Districts Should Implement Cashless Fingerprint Payment System, M2SYS Technology, 2016. From: http://www.m2sys.com/blog/education/why-school-districts-should-implement-cashless-fingerprint-payment-system/

[3] C. Kalyani. Various Biometric Authentication Technique: A Review. Journal of Biometrics & Biostatistics, 2017, 08(05).

[4] S. Hashemi, H. Tann, F. Buttafuoco and S. Reda. Approximate Computing for Biometric Security Systems: A Case Study on Iris Scanning. 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2018: 319-324.

[5] N. Charfi. Biometric recognition based on hand schape and palmprint modalities. Image Processing [eess.IV]. Ecole nationale supérieure Mines-Télécom Atlantique, 2017.

DOI: https://doi.org/10.30564/aia.v1i2.1202

[6] M. M. H. Ali, V. H. Mahale, P. Yannawar and A. T. Gaikwad. Overview of fingerprint recognition system. 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016: 1334-1338.

[7] R. Mansoor & B. Parisa. A Review Of Face Recognition Methods. International Journal of Pattern Recognition and Artificial Intelligence, 2013, 27(4): 1356005(1 -35).

[8] M. K. Sharma & O. Kumar. Speech Recognition: A Review. Special Conference Issue: National Conference on Cloud Computing & Big Data, 2014: 62-71.

[9] J. Choudhary. Survey of Different Biometric Techniques. International Journal of Modern Engineering Research (IJMER), 2012.

[10] M. N. Anjana Doshi. Biometric Recognition Techniques. International Journal of Advanced Research in Computer Networking, Wireless and Mobile Communications, 2015, 2(1): 143-152.

[11] D. Thaktar. Acceptance Rate (FAR) and Recognition Rate (FRR). Bayometric, 2017. From: https://www.bayometric.com/-acceptance-rate-far--recognition-rate-frr/

[12] W. Yang, S. Wang, J. Hu, G. Zheng and C. Valli. Security and Accuracy of Fingerprint-Based Biometrics: A Review. Symmetry, 2019, 11(141): 1-19.

[13] "Intergalactic Vault," [Online]. Available: http://www.intergalacticvault.com/if-you-have-a-spiral-whorl-fingerprint-pattern-this-iswhat-it-means/

[14] J. Qi, Z. Shi, X. Zhao and Y. Wang. A Novel Fingerprint Matching Method Based On The Hough Transform Without Quantization Of The Hough Space. Proceeding of the Third International Conference on Image and Graphics (ICIG' 04) Hong Kong, China, 2004: 262-265.

[15] N. Saroha and N. S. Gill. Hough Transform Based Fingerprint Matching Using Minutiae Extraction. International Journal of Advanced Research in Computer Science, 2013, 4(10): 117-120.

 DOI: https://doi.org/10.30564/aia.v1i2.1202