STUDENTS MONITOR FINGERPRINT BIOMETRIC SYSTEM

Supported by tetfund TERTIARY EDUCATION TRUST FUND

U. I. Oduah*, V. N. Nwaekwu and F. O. Anyadubalu
Department of Physics, Faculty of Science, University of Lagos, Nigeria
*Corresponding author: uoduah@unilag.edu.ng

Received: August 26, 2017 **Accepted:** January 28, 2018

Abstract: This research project developed a unique biometric fingerprint scanner applied in the monitoring of students attendance to class. The Students Monitor Fingerprint Biometric System (SMFBS) captures the fingerprint using a unique scanner, enrolls the image, stores the data, verifies the data, and uses it to authenticate the students. The fingerprint scanner used in this device implements the optical method to capture the fingerprint ridges and valleys. The enrolled fingerprint data is stored in micro secure digital (SD) cards. The stored fingerprint data is used to verify and authenticate a user. The SMFBS incorporates a digital counter which logs the student attendance to class using Arduino software. A printout of the students log presents each students attendance to class report indicating frequency of attendance, each attendance clock in and clock out time, and percentage attendance to class for each lecture. The developed device monitors the students' attendance to class for lectures and laboratory practical demonstrations. In line with the university regulations, students who did not meet the minimum required number of attendance to class will not be allowed to take the examination for the referenced course. The SMFBS eliminates the possibility of a student signing for other students, a habit very prevalent within the present school environment. The developed device precision and speed in enrolling and verifying a user is effective and efficient. This is an innovation that will compel students to attend lectures leading to an improvement in the standard of education in the higher institutions of learning.

Keywords: Biometric, fingerprint, optical scanner, Arduino software, digital counter

Introduction

A proper student attendance monitoring system is very important in educational institutes worldwide. The accuracy of the present attendance monitoring mechanism has been marred by challenging problems which ranges from the bulky nature of the conventional paper and pen method used in recording, manipulation of the attendance by fraudulent students, even to misplacement of the attendance register after it has been taken and so on (Subramaniam, 2013). It therefore becomes problematic task for the regular management and updating of such student records which were previously taken. Also the calculation of the percentage attendance to ascertain if a student qualifies to sit for a particular examination may not be achieved because of the unreliable records. The poor students' attendance to class in institutions of learning contributes to the deplorable standard of education (Kadry, 2010). Consequently, there is a need for a better method of monitoring students' attendance to class in order to improve on their participation during lectures.

In 1858, the first recorded methodical capture of hand and finger images for identification purposes was used by Sir William Herschel, Civil Service of India, who recorded a handprint on the back of a contract for each worker to distinguish employees (Jain, 2003). The biometric system is unique for identification, it is a technique currently used in areas such as criminal investigations, Automated Teller Machines (ATM) security services, passport control and credit cards. There are different types of biometric system for identification namely fingerprint, hand geometry, hand vein, iris, face, voice, signature, keystroke, gait, sometimes hand writing.

The use of fingerprint identification is one the most well-known and common biometric identification system because of its uniqueness and consistency over time. Fingerprints biometrics have been used for identification over many years, and more recently becoming common due to the advancement in computing capabilities and its application for authentication of users. Biometrics is implemented in some e-payment platforms. A comparison of fingerprint based biometrics authentication to traditional authentication methods for e-payments revealed a superiority of fingerprint biometrics as presented by (Ogbanufe, 2018). The reliability of fingerprint biometrics for identification purpose makes it very suitable for the development of this student monitoring device (Lee, 2017).

Materials and Methods

The SMFBS device process involves fingerprint enrollment, storage of captured data in a token, fingerprint verification, fingerprint authentication, and attendance logging. The operation is described in the block diagram in Fig. 1.

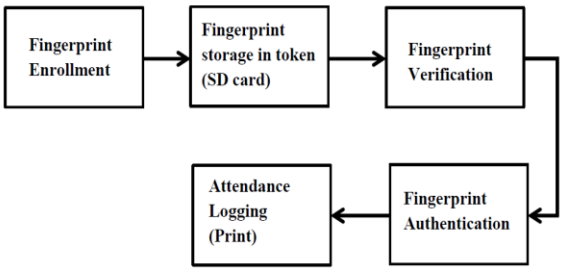

Fig. 1: Block diagram illustrating the operation of Students Monitor Fingerprint Biometric System (SMFBS)

In this research, the fingerprint identification system was used to achieve a reliable maintenance of the students' attendance to class record. The operation of this system requires students to enroll their fingerprints at the beginning of the semester for each course. At each lecture time, the students clock in through the scanning of their fingerprint which is verified and authenticated by the developed device. Also the students clock out after lectures. A printout of the students' attendance log can be made at any desired time. This system of monitoring attendance to class is error free and detailed, listing each student's time in class and percentage attendance. Other

reasons for the choice of fingerprint biometrics for the students monitoring device include:

- Accuracy and security: devices such as paper, magnetic strip cards can be lost, stolen or duplicated; passwords can be shared while on the other hand, biometric verification requires the physical presence of the user.
- Screening: in biometric verifications, users cannot assume multiple identities hence it ensures proper screening of students.
- Non- repudiation: with other security models, perpetrators of fraud can deny committing a particular action. Biometric completely eliminates the problem of repudiation.
- Universality: Everyone has a biometric feature and it is thus universal to everybody
- Environment friendly**:** It reduces paper and other resources requirements and does not cause any negative impact to the environment.
- Uniqueness**:** Since every**o**ne has an exclusive fingerprint identity (even Siamese twins), it makes it nearly impossible for fraudulent individuals to maneuver.

The shape and size of the SMFBS is about that of a Point of Sale (POS) machine with a small window for the fingerprint-scanner.

The fingerprint enrollment process begins with the capturing of the image of the finger. The finger scanner captures the image of the fingerprint applying optical method (Jianjiang, 2007). Some fingerprint scanners also uses capacitive method. The unique features of the fingerprint which includes the ridges and the valleys, and minutiae are properly captured by the scanner. The fingerprint ridges are described by the whorl, dot, and the bifurcation. These ridges differ for every individual enabling the comparator to match a saved fingerprint image with another for verification (Oduah, 2014).

The captured fingerprint image is stored in a micro secure digital card after enrollment. This storage device can store data up to 64 Gigabytes. The storage device is coded and blocked from access by any other device. It is possible to maintain a central server for all captured fingerprint images but this is not advisable because of the associated system link challenges leading to downtime (Peng, 2007). The micro storage device is as shown in Fig. 2.

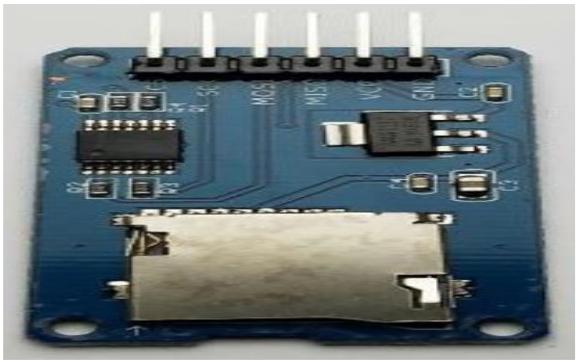

Fig. 2: Micro storage device card

The fingerprint verification unit deploys software to confirm a scanned fingerprint image after enrollment. The system compares the scanned fingerprint image with other existing images in the storage device and verifies the data ok if it does not exist. So, only verified captured fingerprint images will be stored in the device thereby preventing duplication of enrolment (Ashraf, 2014). The verification process is achieved with the aid of comparators.

The following software was used for the project: Adafruit-Fingerprint-Sensor-Library; Fingerprint sensor library for Arduino available at https://github.com/adafruit/Adafruit-Fingerprint-Sensor-Library. This library is host of codes that help in the controlling and successful usage of the fingerprint sensor (Ross, 2007). It feeds the microcontroller which in turn gives a feedback to other coupled components.

Table 1: Library properties of fingerprint sensor

Name	**adafruit fingerprint sensor library**
Version	1.0.2
Maintainer	info@adafruit.com
Category	Sensors
URL	https://github.com/adafruit/ Adafruit-Fingerprint-Sensor-Library
Architecture	*

The Arduino software used in programming of the comparator is open source software. It is very convenient to write and upload code to the Arduino board because it runs on windows mac and Linux operating system (Shehu, 2011). The environment is written in java and based on processing and other open source software. It is available at www.ardunio.cc

The fingerprint authentication process involves the matching of the fingerprint captured during clock in or out with the stored fingerprint image in the micro SD card. A student is authenticated if the saved detail corresponds with the scanned fingerprint. A description of the software is in Table 1.

The Attendance Log is generated and displayed through the output readout video display unit. A printout of the students' attendance log can be obtained via Bluetooth Module device to a local printer. The Bluetooth module is a hardware component that provides a wireless communication between the computer and Arduino and the finger print sensor (Brindha, 2013). It supports simple serial communication. The Bluetooth module device is as shown in Figure 3.

Fig. 3: Bluetooth Module

It follows that every time students attend a class for a course they have registered, they will need to scan their fingerprint through the SMFBS provided within the class. It would be imperative for every student to clock in by affixing the thumb on the finger-scanner to do fingerprint matching with the fingerprint record that had been stored in the system. Attendance will be verified automatically by the system once the student's fingerprint matches the fingerprint records in the system. If the fingerprint of the student does not exist in the system while clocking in, the system will display a message showing "Invalid fingerprint". However if the matching is successful, the system will display a message "Authenticated" validating the student's status.

The display screen used in this project is the 16 x 2 Liquid Crystal Display (LCD). It supports multiple serial connection ports and has a working voltage of 5v**.** During the enrollment exercise for the courses registered, the LCD screen serves as a visible means of determining if the student is successfully registered by displaying "Enrolled" or "Invalid" if unsuccessful. Figure 4 shows the LCD screen.

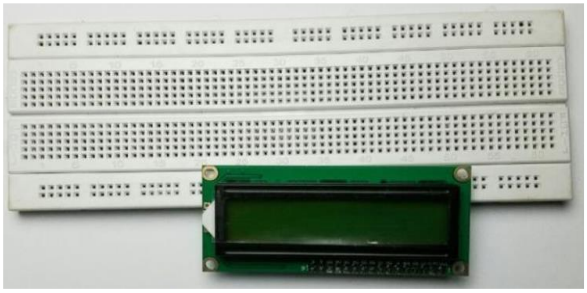

Fig. 4: Liquid crystal display screen

The fingerprint scanner on the breadboard is shown on Figure 5.

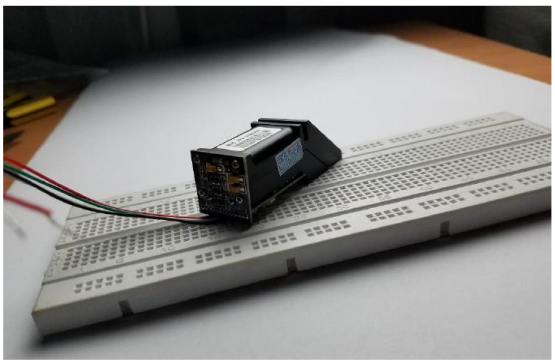

Fig. 5: Fingerprint scanner

The Arduino Uno Rev3 was used in the development of the SMFBS. The technical specification of the Arduino is presented in Table 2 below. The Arduino Uno r3 is a microcontroller board based on the ATmega328P (datasheet). It has 14 digital input/output pins (of which 6 can be used as Pulse Width Modulation output) 6 analog inputs, a 16 MHz quartz crystal, a Universal Serial Bus (USB) connection, a power jack, an In-Circuit Serial Programming (ICSP) header and a reset button.

Table 2: Technical specification of the Arduino

Microcontroller	ATmega328P
Operating voltage	5v
Input voltage	7-12v
Input voltage	6-12v
Digital input pins	14 (of which 6 provide PWM output
Pulse Width Modulation (PWM) digital input/output pin	6
Analog input pins	6
DC current per input/output	20mA
DC current for 3.3v pin	50mA
Flash Memory	32KB
Static Random Access Memory (SRAM)	2KB
Electrical Erasable Programmable Read Only Memory (EEPROM)	1KB
Clock speed	16MHz
LED_BUILTIN	13
Length	68.6
Width	53.4
Weight	25g

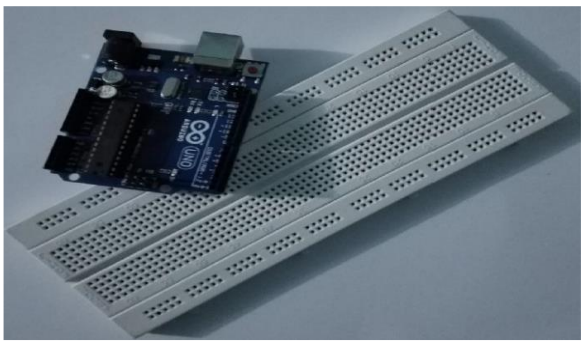

Fig. 6: Arduino Uno rev3

The Arduino board presented in Figure 6 above is a microcontroller that has a number of facilities for communicating with the computer and other microcontrollers. It acts as the link between the fingerprint module and the Bluetooth module. It converts the data received from the fingerprint scanner to a string that is transferred over the Bluetooth module. It also analyzes the data received from the fingerprint scanner and sends appropriate commands to the SD card storage device. It was used for this project because it has multiple serial ports available on the board making it easy to link with both Bluetooth module and the fingerprint scanner.

The operation of the SMFBS device is categorized into three units as follows:

- Administrative end
- Attendance system
- Report generation

The Administrative end involves each course lecturer as the resource officer to monitor the enrollment of only registered students for the course. The lecturer will therefore allow only students that have registered for the course to capture and verify their fingerprints using fields illustrated and presented on Figures 7(a) (b) (c) (d) (e) (f) and (g) below.

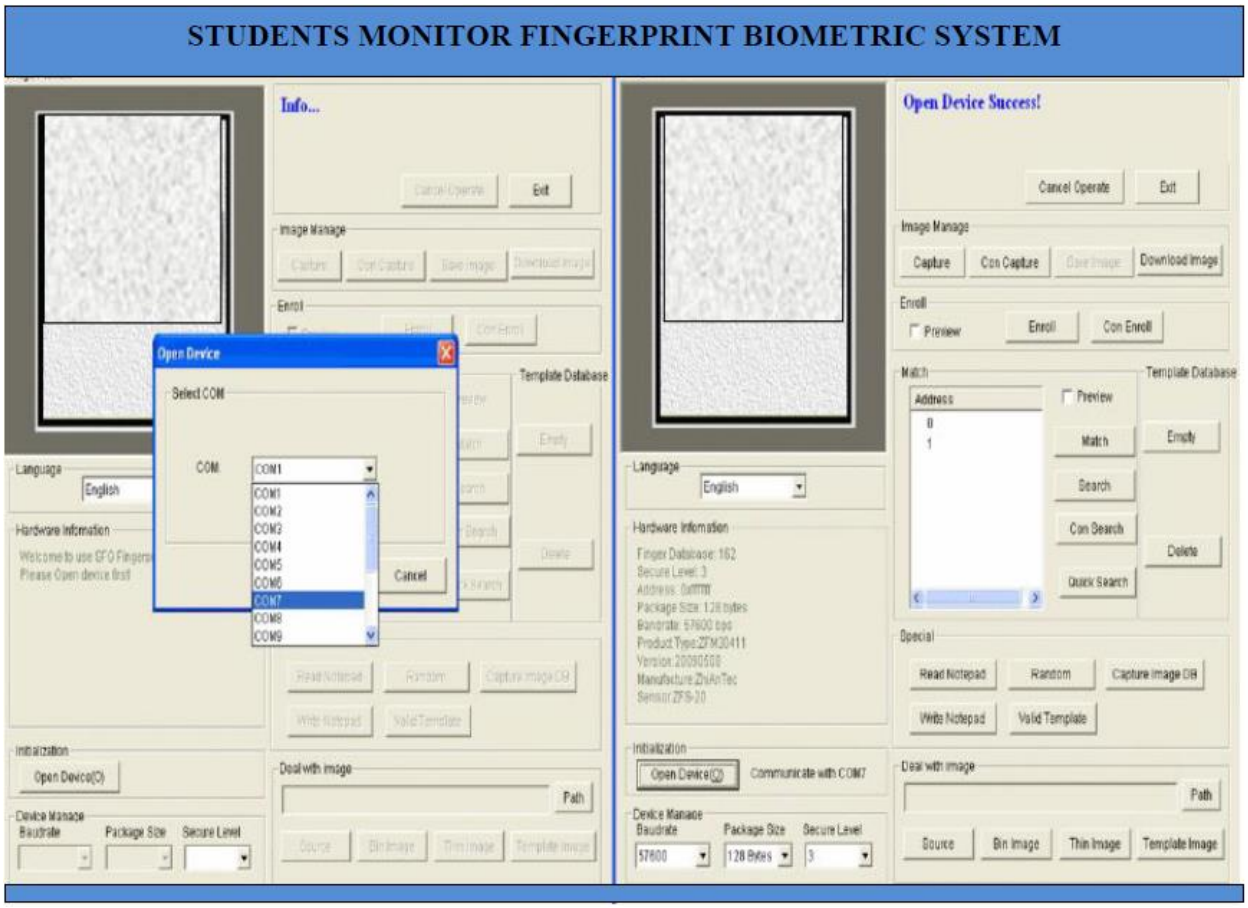

Fig. 7a: Device open successful

Next to enroll a new finger we start by clicking on the Preview checkbox and press the Enroll button next to it (Con Enroll means 'Continuous' enroll,). Another box would appear. Next is to assign an ID to the student by choosing the matriculation number.

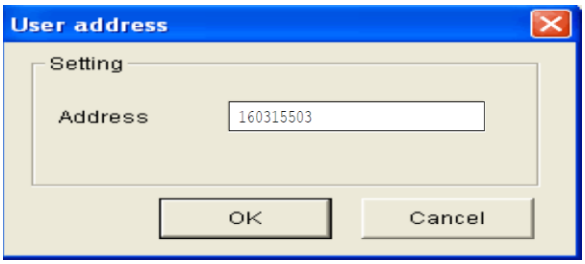

Fig. 7b: Approve the matriculation number

The software will pop up another box requesting the student to place the finger to the scanner.

Fig. 7c: Finger positioning

A preview would be developed.

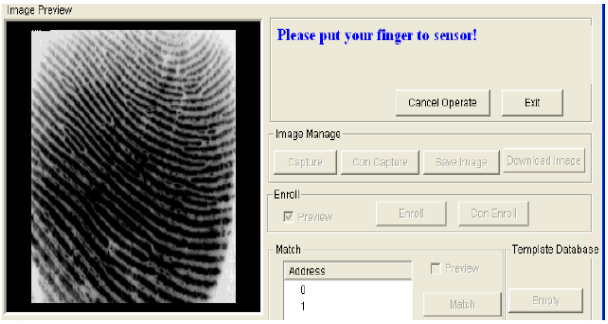

Fig. 7d: Fingerprint image

The student may need to re-insert his or her finger for a better capture before the specimen is verified.

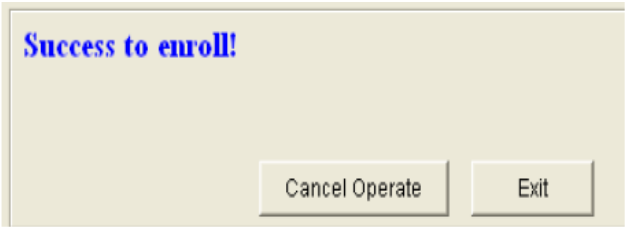

Fig. 7e: Fingerprint verified

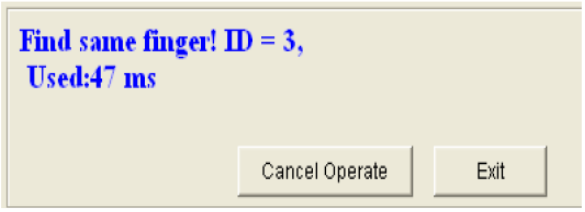

Fig. 7f: Reconfirm a fingerprint

However if the fingerprint is not in the database, a failure notice is displayed.

Fig. 7g: An invalid scan

Results

The SMFBS was tested using 80 students from year one Education Department, University of Lagos, Akoka Campus. Based on the survey carried out, 77 students enrolled successfully at first attempt, 3 students repeated their enrolment process before a successful validation. It took an average of 2 minutes to update each student details in the system and complete the enrolment. The clock in/out of each student took an average of 5 seconds. The developed device performed well and has the capacity to cover 5,000 students.

False Rejection Rate (FRR) = $\frac{number\ of\ false\ reject\ (FR)}{the\ total\ number\ of\ verification\ (N)} \times 100 = \frac{FR}{N} \times 100$

$\frac{3}{80} \times 100 = 3.75\%$

Conclusion

A Student Monitor Fingerprint Biometric System device has been developed in this research project. This device is projected to enforce student attendance to class which will boost their effective participation in class activities and translate to higher standards of education. The device will improve on the evaluation of students performance compared to their participation in class activities and form a realistic basis for the assessment of the quality of lectures presented to the students. It will also monitor the compliance of classes with the approved lecture time-table. Examination malpractice associated with impersonation will also be eliminated using this device. The generated class attendance log is a very important data which will be transformed into useful statistical information to be applied in various studies. This is a welcome development in all the institutions of learning.

References

Ashraf E 2014. *Design and implementation of biometric access control system using fingerprint for restricted area based on gabor filter.* Computer Science Department, Menofyia University, Egypt, pp. 81-83.

Brindha S & Rajalakshmi M 2013. Biometric based secured authentication in mobile web services. *College of Technology and Engineering, Pollachi, Tamilnadu,* 3: 71-74.

Jain AK, Maio D, Maltoni D & Prabhakar S 2003. *Handbook of Fingerprint Recognition*, Springer, New York, pp. 131-135.

Jianjiang F 2007. Combining minutiae descriptors for fingerprint matching. *Pattern Recognition*, 342-347

Kadry S & Smaili M 2010. Wireless attendance management system based on Iris Recognition. *Scientific Res. and Essays*, 5(12): 1428-1435.

Lee W, Cho S, Choi H & Kim J 2017. Partial fingerprint matching using minutiae and ridge shape features for small fingerprint scanners. *Elsevier Expert Systems with Applications*, 87: 183-198.

Oduah UI 2014. Application of the photorefractive effect of lithium niobate in the development of a fingerprint scanner with unique sensitivity. *Int. J. Comp. & Electrical Engr.*, l6(6): 824-829. DOI: 10.7763/IJCEE.2014.V6.829.

Ogbanufe O & Kim DJ 2018. Comparing fingerprint based biometrics authentication versus traditional authentication methods for e-payment. *Elsevier Decision Support Systems*, 106: 1-14.

Peng S, Jie T, Qi S & Xin Y 2007. A novel fingerprint matching algorithm based on minutiae and global statistical features. *IEEE Conference*, 27-29.

Ross A, Shah J & Jain AK 2007. From template to images reconstructing fingerprints from minutiae points. *IEEE Transactions*, 33: 72-77.

Shehu V & Dika A 2011. Using Real Time Computer Vision Algorithms in Automatic Attendance Management Systems. Proceedings of the ITI 2010 32nd Int. Conf. on Information Technology Interfaces, Cavtat, Croatia, pp. 21-24.

Subramaniam H, Hassan M & Widyarto S 2013. Bar Code Scanner Based Student Attendance System (SAS). *Jurnal TICOM.*, 1(3): 173-177.