

Stepwise Biometric Procedures for Managing Student Attendance in Higher Institutions of Learning

¹Kayode Adewole*, ²Rasheed Jimoh, ³Oluwakemi Abikoye, ⁴Adeleke Ajiboye

^{1,2,3,4}Department of Computer Science, University of Ilorin, Ilorin

Email: adewole.ks@gmail.com, jimoh_rasheed@unilorin.edu.ng, kemi_adeoye@yahoo.com,
ajibabdulraheem@gmail.com

ABSTRACT

Data and information security are very important issues in computing environment. Security of data prevents unauthorized users from accessing individual personal information. Biometric is one of the authentication methods used in a wide range of application domains such as airline and banking environment to secure confidential data. This technique is more reliable and capable of distinguishing between an authorized person and an impostor than traditional methods such as passwords. Large numbers of higher academic institutions in the developing countries are still using the process of manual attendance for both lecture and examination for students' authentication and authorization, hence, the need for automated system that can assist in this area. In this paper, stepwise biometric procedures for managing students' attendance for both lectures and examinations are presented. The various stages involved in student attendance management are discussed and simulated. These include enrollment, fingerprint matching and attendance management. The results show that the proposed system is able to identify those students who are qualified to sit for an examination.

Keywords: Data, Information Security, Biometric, Fingerprint, Minutiae

1.0 INTRODUCTION

Academic institutions have certain criteria for students regarding their attendance in class and during examination period. That is why keeping the accurate record of attendance is very important. In almost all institutions in the developing countries, attendance is usually taken manually using paper sheets and the old file system approach.

Lack of adequate attendance record keeping has indeed degenerated to a greater level most especially in Nigerian institutions. Examination malpractices have consistently remained a bane of Nigerian educational system. A common form of examination malpractices is the deliberate impersonation of the applicant. Part of the requirement of a credible examination is that the real applicants wrote the exams. An exam is credible if it possesses the following key elements: free and fair; devoid of partiality, cheating and all forms of examination malpractices. Candidate impersonation as mentioned earlier is one of the prominent forms of examination malpractices due to lack of adequate lecture attendance management by the lecturers. The idea is that a more knowledgeable personality is hired as machinery to write exam for the original candidate [1].

Biometric can be described as a measurable physical and/or behavioral trait that can be captured and used to verify the identity of a person [2]. Biometric is perceived as technologies as “automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic” [3]. In this modern age of electronically inter-connected society, reliable and user-friendly recognition and verification system is essential in many areas of our life most especially for attendance management. Individual physiological or behavioral characteristics, known as biometrics, are important and vital methods that can be used for verification and identification. Fingerprint recognition is one of the most popular biometric techniques used in automatic personal verification and identification [4]. This technique is the oldest method in biometric identification, which has been in existence since 2200 BC. In this period, ancient people from Assyria, Babylonia, China and Japan used this method. Since 1897, dactyloscopy, which involves manual fingerprint identification, was used in criminal investigation [5]. The discovery of Sir Edward Richard Henry in 1899 through Henry system of classification has significantly contributed to the advancement in fingerprint identification. By the early 20th century, researchers started understanding the fingerprint formations based on three biological principles: individual epidermal ridges and furrows have different characteristics for different fingerprints, the configuration types are individually varied within limits

which allow for a systematic classification, the configurations and minutiae details of individual ridges and furrows are permanent and unchanging [6] . Due to the inefficiency of traditional methods of attendance record keeping, a more secured and accurate biometric-based system is needed to be developed. In this paper, the various stages involved in attendance management using fingerprint biometric technology are discussed and simulated.

The main contributions of this paper are as follows:

- i. presents a biometric-based system framework for managing students attendance in higher institution of learning.
- ii. discusses the pseudo-codes for the various stages of attendance management.
- iii. simulates the different stages using MATLAB.

The remainder of this paper is organized as follows: Section 2 discusses enrolment, verification and identification processes in fingerprint biometric authentication. Section 3 presents related works on biometric attendance management. Section 4 describes the proposed system framework presented in this paper. Section 5 explains how the various stages were simulated in MATLAB environment and finally, overall conclusions are presented in Section 6.

2.0 ENROLLMENT, VERIFICATION AND IDENTIFICATION

2.1 Enrollment

Enrollment is the process by which information of the user both the biometric template and other user's information (biodata) are saved into the database for subsequent verification or identification. During this stage, the biometric data is processed and a set of significant discriminatory features are extracted to represent the underlying trait. This may involve extracting either the local or global features of the fingerprint. The local features deal with minutiae where the ridges of the fingerprint are used to obtain certain discriminatory features. This feature is referred to as template. During the enrollment process, the feature set extracted from the unrefined biometric sample is stored in the database (possibly) along with some biographic information such as name, matriculation number, sex, courses and so on which characterize the user. Figure 1 shows the process involved during enrollment stage.

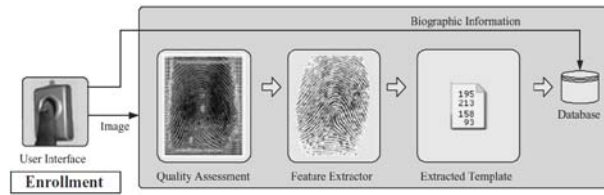


Figure 1: Enrollment stage [9].

2.2 Verification

During verification, the user claims an identity (e.g through provision of PIN, matriculation number, password etc) and the biometric system determines whether the user's claim is correct or not. After detecting that the user's claim is correct, then the biometric template recorded against the claim in the database is compared with the presented biometric template through computation of similarity score. If the score is above the set threshold, then access will be granted to the user, otherwise access will be denied [7] [8]. This method is also called one-to-one matching.

Biometric system's decision can be correct or false. The decision is correct in two cases [7]:

1. The biometric system has decided that the user's claim is correct and the claimed and the biometric identifier of the user belong to the same person. In this case, we say that a genuine individual has been correctly accepted or verified by the biometric system. The probability of making the correct verification is called the probability of correct verification or probability of verification (PV).
2. The biometric system has decided that the user's claim is not correct and the claimed and the biometric identifier of the user do not belong to the same person. We say that an impostor has been correctly rejected by the biometric system.

The decision is not correct in two cases:

1. The biometric system has decided that the user's claim is correct and the claimed and the biometric identifier of the user do not belong to same person. We say that an impostor has been falsely accepted as a genuine user. This error is called false acceptance, and the probability of making the false acceptance is called the false acceptance rate (FAR).
2. The biometric system has decided that the user's claim is not correct and the claimed and the biometric identifier of the user belong to the same person. We say that a genuine individual has been falsely rejected. This error is called false rejection, and the probability of making the false rejection is called the false rejection rate (FRR).

Figure 2: Verification stage [9].

2.3 Identification

During identification, biometric template of the user is presented to the biometric system, and the task of the biometric system is to establish the identity of the user. In the identification stage, the similarity scores between the user's biometric identifier and the biometric identifiers in the database are calculated. If the correct user has the highest similarity score, then we say that the biometric system has made correct identification [7]. This means that, the presented biometric feature of the user will be compared against all the biometric templates in the database in order to find a match.

3.0 RELATED WORK

An electronic card-based solution was presented to the lecture attendance problem in higher institutions in the developing countries [10]. This system was based on single-chip computer based subsystems interfaced serially to the serial port of the digital computer. However, not all computer systems possess serial port and the user can easily misplace the smart card. Student's attendance management system using Radio Frequency Identification (RFID) was previously presented as well [11]. The system is based on student card in order to allow or disallow the student from taking attendance. This technique did not identify individual based on biometric traits and can give room for impersonation. A new approach for fingerprint image enhancement was proposed based on Short Time Fourier Transform (STFT) analysis [12]. The proposed algorithm extracted several intrinsic properties of the fingerprint such as the foreground region mask, local ridge orientation and local frequency. In addition, the researcher also present a new feature extraction algorithm based on chain code contour processing which according to the researcher, provides a wide range of information about the contour such as curvature, direction, length and so on. A novel based fingerprint recognition algorithm that incorporates three new ideas was also presented. An embedded application for fingerprint verification system. An extensive study of fingerprint verification was presented [13]. This research was implemented on the ZF

Microsystems based single board computer with Cyrix Media GX based processor and coprocessor with a bus speed of 180MHz.

4.0 SYSTEM FRAMEWORK AND PROCEDURES

The proposed system framework consists of different modules as shown in Figure 3. The pseudo-codes for each of the modules are presented in this section.

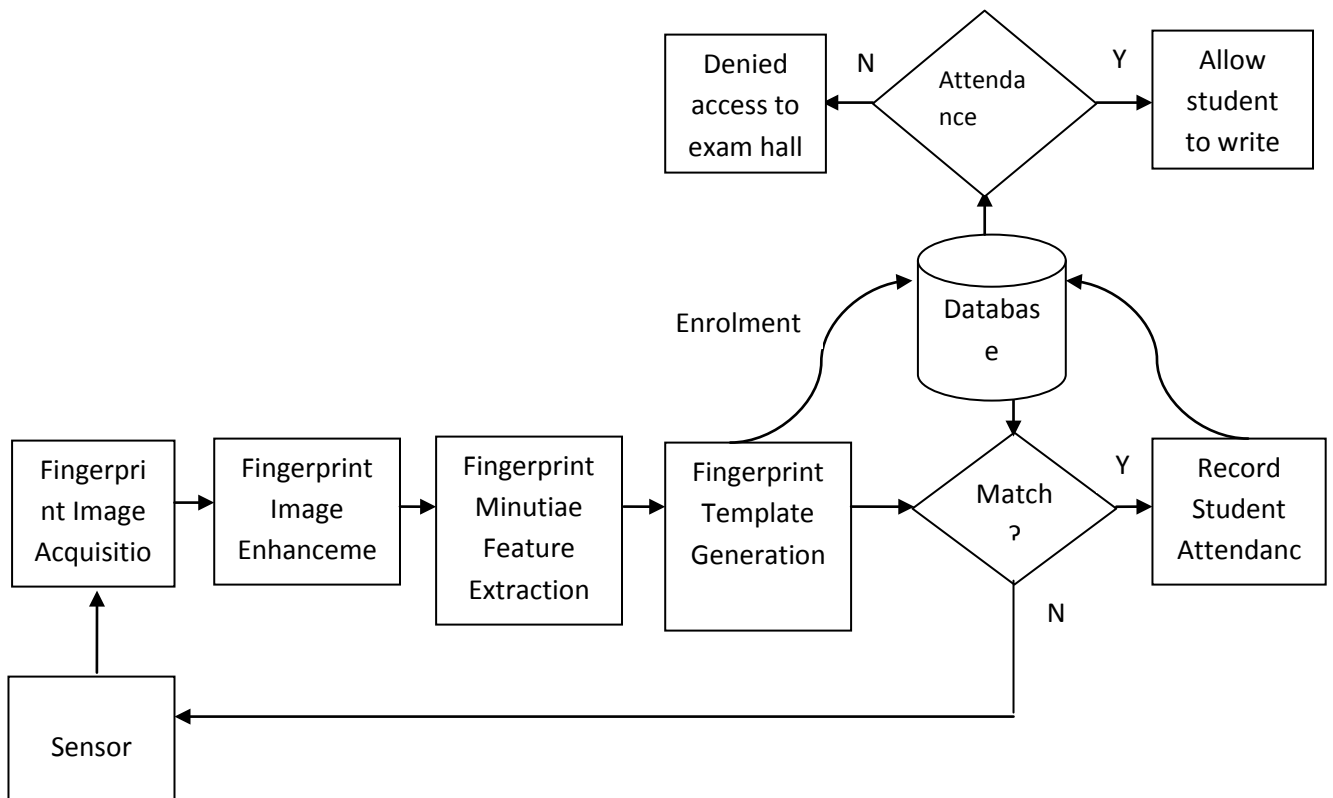


Figure 3: Proposed system framework

4.1 Fingerprint Sensors

Traditional fingerprints were acquired by transferring the inked impression onto the paper [12]. This process is termed as *off-line* acquisition. To authenticate the user, *live-scan* devices that capture the fingerprint image in real time is used. Fingerprint sensor is divided into the following:

Capacitive Sensor: Capacitive sensors use an array capacitor plates to image the fingerprint. Skin is conductive enough to provide a capacitive coupling with an individual capacitive element on the array. Ridges, being closer to the detector, have a higher capacitance and valleys have a lower capacitance. This variation is converted into an 8-bit gray scale digital image. Most of the electronic devices featuring fingerprint authentication use this form of solid state sensors due to its compactness. Some

capacitive sensors apply a small voltage to the finger to enhance the signal and create better image contrast. Capacitive sensors can be sensitive to electrostatic discharge (shock) but they are insensitive to ambient lighting and are more resistant to contamination issues than some optical designs.

Optical Sensor: Optical sensors are the oldest and most widely used of all the fingerprint sensors. In most devices, a charged coupled device (CCD) converts the image of the fingerprint, with dark ridges and light valleys, into a digital signal. They are fairly inexpensive and can provide resolutions up to 500 dpi. Most sensors are based on FTIR (Frustrated Total Internal Reflection) technique to acquire the image. Due to internal reflection phenomenon, most of the light is reflected back to the other side where it is recorded by a CCD camera. However, in regions where the fingerprint surface comes in contact with the prism, the light is diffused in all directions and therefore does not reach the sensor resulting in dark regions. The quality of the image depends on whether the fingerprint is dry or wet. Another problem faced by optical sensors is the residual patterns left by the previous fingers [12].

Thermal Sensor: Thermal sensors use the same pyro-electric material that is used in infrared cameras. When a finger is presented to the sensor, the fingerprint ridges make contact with the sensor surface and the contact temperature is measured, the valleys do not make contact and are not measured. A fingerprint image is created by the skin-temperature ridges and the ambient temperature measure for valleys. The biggest drawback of this technique is that the temperature change is dynamic and it only takes about a tenth of a second for the sensor surface touching ridges and valleys to come to the same temperature, erasing the fingerprint image. Additionally, this technology has many of the same contamination and wear issues as other sensors. While it can operate over a wide range of temperatures, if the ambient temperature is close to the finger surface temperature the sensor requires heating to create a temperature difference at least 1 degree Centigrade .

Pressure Sensor: Pressure sensing scanners can be made very thin and are often used in electronic devices. Early pressure sensing scanners had to make a tradeoff between durability and quality because any protective layer on the detector surface would diminish the contrast of the impression. There are two types of pressure sensing detectors available, conductive film detectors and micro electro-mechanical devices (MEMS). Conductive film sensors use a double-layer electrode on flexible films. MEMS is a newer technology that uses extremely tiny silicon switches on a silicon chip. When a fingerprint ridge touches a switch, it closes and is detected electronically.

RF Sensor: A low radio frequency (RF) signal is applied to the user's finger and then read by the detector array, with each pixel operating like a tiny antenna. The advantage of this detector is that it

reads the fingerprint from the dermal layer underneath the surface making it less susceptible to damaged or dry fingertips.

Ultra-sound Sensor: Ultrasound technology is perhaps the most accurate of the fingerprint sensing technologies. It uses ultrasound waves and measures the distance based on the impedance of the finger, the plate, and air. These sensors are capable of very high resolution. Sensors with 1000dpi or more are already available. However, these sensors tend to be very bulky and contain moving parts making them suitable only for law enforcement and access control applications [12].

4.2 Enrollment

This is the stage where the template of the student fingerprint will be saved into the database along with other student's details for subsequent authentication and attendance management. The pseudo-code is shown below:

Enrollment(Template T_p , array biodata[], array courses[])

{

Step 1: Connect to the database

Step 2: Create a new student record and save both the array element biodata[] and the student fingerprint template T_p

Step 3: Save the student registered courses in the database

Step 4: Close the database connection

Step 5: Stop

}

4.3 Fingerprint Matching and Attendance Management

At this stage, the student's fingerprint is captured and compare with the stored templates in the database. If the fingerprint corresponds to any of the enrolled fingerprint templates, attendance of the student in that particular course will be recorded, otherwise, the student will not have attendance for that course on that lecture day. The pseudo-code is described below:

FingerprintMatching(Template $T1$, Template Tp)

{

Step 1: Set $N = 1$, $S_{count} = 0$

Step 2: Obtain the minutiae sets $S1$ and $S2$ for each fingerprint template $T1$ and Tp^N respectively where $T1$ is the test template and Tp^N is the enrolled template at position N in the database.

Step 3: For each of the sets $S1$ and $S2$, obtain the minutiae type $e1$ and $e2$, coordinates $c1$ and $c2$ corresponding to the coordinate of the minutiae type, and the orientation angles $o1$ and $o2$ of the minutiae points for sets $S1$ and $S2 \in T1$ and Tp^N respectively.

Step 4: Compare if $S1$ and $S2$ are paired such that:

If (TYPE ($e1$) = TYPE ($e2$)) and (DIST ($c1$, $c2$) $\leq D_T$) and (ANGLE ($o1$, $o2$) $\leq A_T$) then

 Increase S_{count} by 1

 Goto Step 3 until no more sets to pair

Else

 Goto Step 3 until no more sets to pair

Endif

Here, D_T and A_T are the maximum tolerance for translation and rotation respectively.

Step 5: Obtain the total number of sets in $T1$ and call it $N1$

Step 6: Obtain the total number of sets in Tp^N and call it $N2$

Step 7: Compute the similarity measure M between $T1$ and Tp^N such that:

$$M = \sqrt{S_{count}} * S_{count} / (N1 * N2) \quad (1.1)$$

Step 8: Compare the source of the two fingerprint images such that:

If ($M \geq T$) then (where T is a threshold)

- The two fingerprint images $T1$ and Tp^N are from the same source

- Set Match = True

- Goto Label

Else

- The two fingerprint images are not from the same source

- Set Match = false

- Increase N by 1

- Goto Step 2 //this is necessary since identification method will be used

Endif

Exit

Label: Return Match

Step 9: Stop

}

RecordAttendance(Template $T1$, Template Tp , Course C)

{

Step 1: Test if the two fingerprint images $T1$ and Tp are from the same source i.e

If (FingerprintMatching(Template $T1$, Template Tp)) then

- Allow student access to the system

- Record student attendance for Course C

- Update the database

Else

- Deny student access to the system

Endif

Step 2: Stop

}

4.4 Test Attendance

At this stage, the student attendance in a particular course is tested in order to know if the 70% attendance criteria is satisfied or not. The student who meets this condition will be allowed entry into the examination hall, otherwise, access to the examination hall will be denied to such student. The pseudo-code is show below:

TestAttendance(Template *T1*, Template *Tp*, Course *C*)

{

Step 1: Set LectureTotalPeriod for Course C

Step 2: Test whether fingerprint images *T1* and *Tp* are from the same source i.e

If (FingerprintMatching(Template *T1*, Template *Tp*)) then

- Obtain StudentTotal attendance for Course C

- Obtain the Percentage of student attendance for Course C such that

Percentage = StudentTotal/LectureTotalPeriod * 100

If (Percentage < 70%) then

- Deny student access to the examination hall

Else

- Allow student access to the examination hall

Endif

Else

Deny student access to the system

Endif

Step 3: Stop

}

5.0 RESULTS AND DISCUSSION

In this section, the various results obtained from the proposed system are discussed. SecuGen fingerprint scanner was used to capture students' fingerprints. Fingerprint minutiae features of each student were extracted and template generated.

5.1 Enrollment and Template Generation

This section is used to enroll students at the beginning of academic session before the attendance is taken for any lecture. The interface is shown in Figure 4. In this interface, student biographic information are entered and the courses are selected from the list of available courses. The administrator will then click on 'Image Acquisition' in order to capture the student fingerprint image.

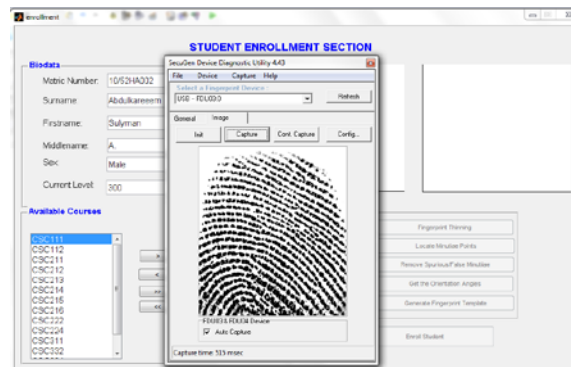


Figure 4: Image Acquisition Result

The next step is to load the image back onto the interface for processing. Figure 5 shows the image after clicking on 'Binarize' button.

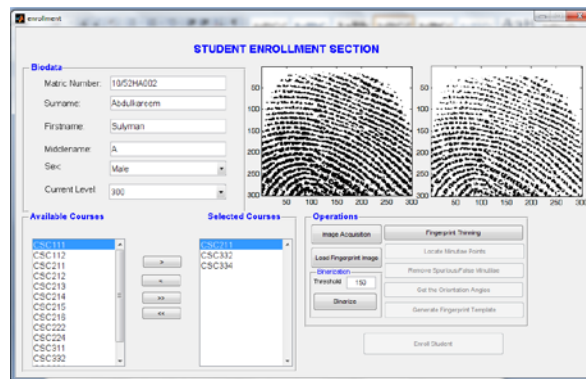


Figure 5: Image after clicking on Binarize button

The 'Fingerprint Thinning' button is clicked in order to perform the thinning operation on the image. The result is shown in Figure 6.

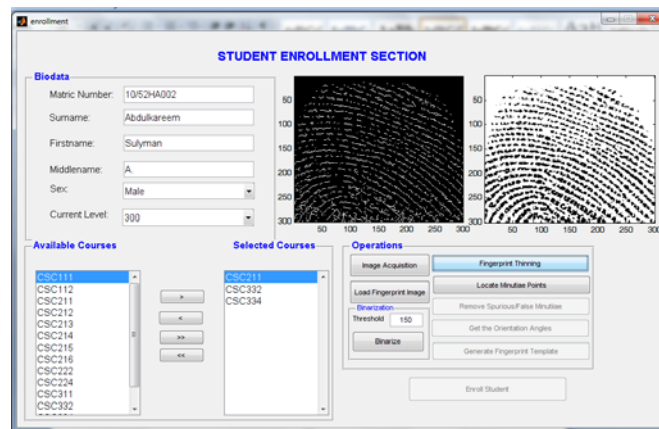


Figure 6: Image after performing thinning operation

Next is to locate all the minutiae points in the image. The extraction of minutiae features is done using the Crossing Number algorithm. The result of this stage is shown in Figure 7.

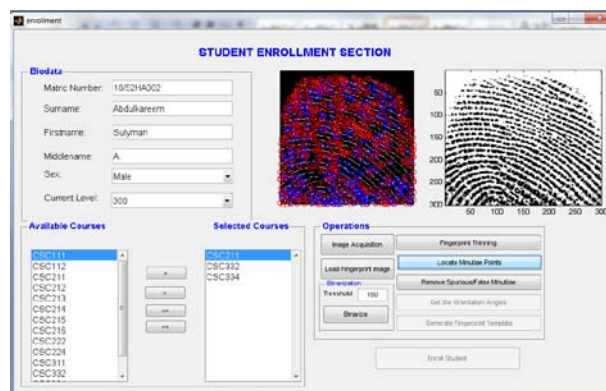


Figure 7: Locating the minutiae points in the fingerprint image

False minutiae can affect the process of good template generation. Therefore, there is need to remove false minutiae from the fingerprint image and define the region of interest (ROI). The interface in Figure 8 shows the result after removing the false minutiae.

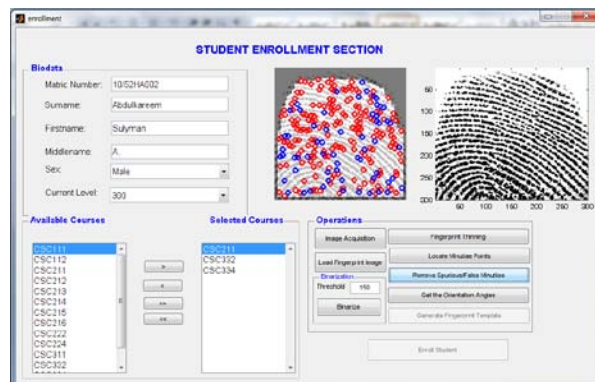


Figure 8: Removing false minutiae and defining ROI

After this operation, we need to compute the orientation angle of each minutiae point. This is done by clicking on 'Get Orientation Angles' button. Figure 8 shows the result of this operation:

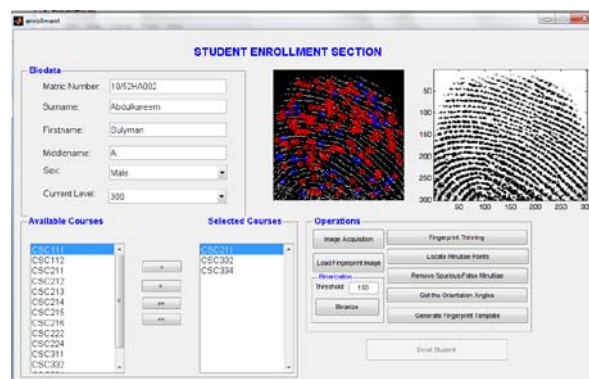


Figure 9: Calculating minutiae points orientation angles

The final step is to generate the template and save the data into the database for subsequent authentication.

5.2 Lecture and Examination Attendance Management

During attendance management, the student will be presented with the interface shown in Figure 10(a) and 10(b). It is the responsibility of the system to determine the type of attendance once the administrator has configured the current course. The major difference is that during lecture attendance, the test fingerprint template will be compared with the enrolled template and if a match is found, attendance of this student in the current course will be recorded. In the case of examination attendance,

the system first compares the test fingerprint template with the enrolled template and if a match is found, the system automatically computes the percentage of the lecture attendance and display a message based on the outcome of the computation. Figure 10(a) and 10(b) show sample attendance for a current course CSC332.

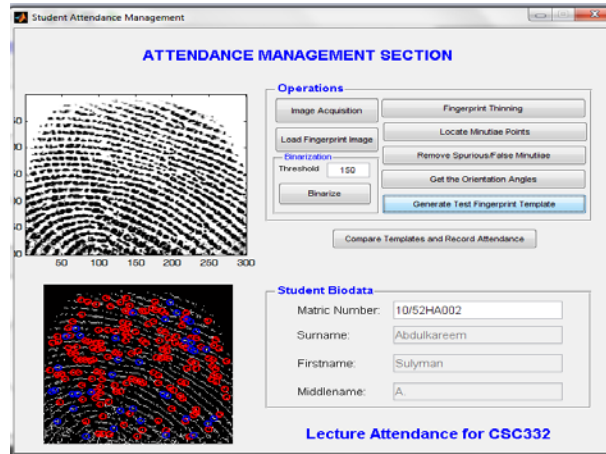


Figure 10(a): Lecture attendance result

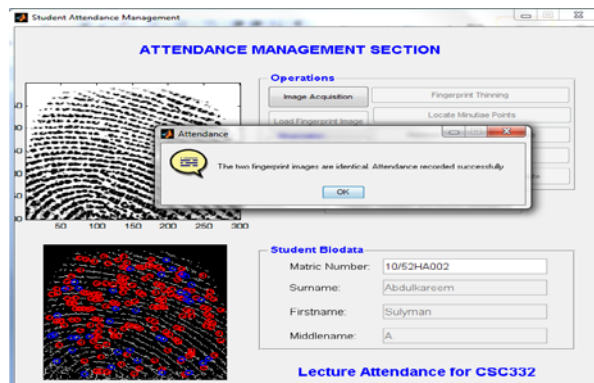


Figure 10(b): Output of a sample lecture attendance

5.3 Attendance Reports

The following figures show some of the outputs generated from the proposed system:

List of Courses

Course code	Title	Unit	Lecturer Name
CSC332	Mobile Computing	2	Mr. K. S. Adewole
CSC216	Assembly Language	2	Mr. K. S. Adewole
CSC111	Introduction to Computer Science I	2	Mrs. Akintola
CSC112	Introduction to Computer Science II	2	Mrs. Akintola
CSC211	Computer Programming I	3	Mr. K. S. Adewole
CSC212	Computer Programming II	3	Dr. P. B. Shola
CSC213	Object Oriented Programming	3	Mrs. Akintola
CSC214	Introduction to File Processing	2	Mr. A. O. Ameen

8

Figure 11: List of Courses

List of Students

MatricNo	Surname	Firstname	Middlename	Sex	Level
10/52HA002	Abdulkareem	Sulyman	A.	Male	300
10/52HA003	Abdulwahab	Muhammed	M.	Male	300
10/52HA005	Abikoye	Stephen		Male	300
10/52HA007	Ade-Lawal	Temitope		Male	300
10/52HA008	Adebayo	Michael		Male	300

5

Figure 12: List of Students

Lecture Attendance Report

MatricNo	Course code	Attendance Date	Attendance Time	Attendance Type	Session	Count
10/52HA002	CSC332	18/03/2013	9:00:40 AM	Lecture	2012/2013	1
10/52HA002	CSC332	25/03/2013	9:01:00 AM	Lecture	2012/2013	1
10/52HA002	CSC332	01/04/2013	9:04:20 AM	Lecture	2012/2013	1
10/52HA002	CSC332	08/04/2013	9:09:00 AM	Lecture	2012/2013	1
10/52HA002	CSC332	15/04/2013	9:11:00 AM	Lecture	2012/2013	1
10/52HA002	CSC332	22/04/2013	9:04:10 AM	Lecture	2012/2013	1
10/52HA002	CSC332	29/04/2013	9:15:10 AM	Lecture	2012/2013	1
10/52HA002	CSC332	06/05/2013	9:00:00 AM	Lecture	2012/2013	1
10/52HA002	CSC332	13/05/2013	9:50:00 AM	Lecture	2012/2013	1
10/52HA002	CSC332	20/05/2013	9:45:00 AM	Lecture	2012/2013	1
10/52HA002	CSC332	27/05/2013	9:20:00 AM	Lecture	2012/2013	1
10/52HA002	CSC332	03/06/2013	9:38:42 AM	Lecture	2012/2013	1
10/52HA002	CSC332	10/06/2013	9:44:30 AM	Lecture	2012/2013	1

Figure 13: Lecture Attendance Report

<u>Attendance Summary Report</u>					
MatricNo	Attendance Type	Course Code	Percentage(%)	Academic Session	Status
10/52HA002	Exam	CSC332	92.86	2012/2013	Qualified
10/52HA003	Exam	CSC332	78.57	2012/2013	Qualified
10/52HA005	Exam	CSC332	64.29	2012/2013	Not Qualify
10/52HA007	Exam	CSC332	64.29	2012/2013	Not Qualify
10/52HA008	Exam	CSC332	78.57	2012/2013	Qualified

5

Figure 14: Attendance Summary for Examination

6.0 CONCLUSION

Experience has shown that there are several problems attributed to the use of identity cards, paper sheets, and knowledge based techniques in uniquely identifying student. However, there is need for simplified, efficient and reliable procedures for managing students attendance based on biometric technology to be implemented. This however, is the focus of this paper. To achieve this, pseudo-codes for the various stages involved in attendance management were discussed and simulated. These include enrollment, fingerprint matching and attendance management. The naturalness in the use of fingerprint makes it a reliable access control technique. The fact that a student no longer needs to carry identity cards and other documents from one place to another for identification purpose explain the simplicity of the proposed system.

REFERENCES

- [1] Rufai, M. M., Adigun, J. O. and Yekini, N. A. (2012). A Biometric Model for Examination Screening and Attendance Monitoring in Yaba College of Technology. *World of Computer Science and Information Technology Journal (WCSIT)*. ISSN: 2221-0741, 2(4), pp. 120-124.
- [2] Erikson, M. (2001). *Biometrics Fingerprint based identity verification*. M.Sc. Thesis, Department of Computing Science, UMEA University.
- [3] Bowman, E. (2000). Everything you need to know about biometrics. Identix Corporation, Retrieved March 2nd, 2013 from <http://www.ibia.org/EverythingAboutBiometrics.pdf>
- [4] Naser, Z. (2011). *Minutiae-based Fingerprint Extraction and Recognition*. Kuwait: Arab Open University. ISBN: 978-953-307-618-8, InTech. Retrieved 18th May, 2013 from

<http://www.intechopen.com/books/biometrics/minutiae-based-fingerprint-extraction-and-recognition>.

- [5] Sunny, A. S. and Rudi, T. Y. (2012). Adaptable Fingerprint Minutiae Extraction Algorithm Based on Crossing Number Method for Hardware Implementation Using FPGA Device. *International Journal of Computer Science, Engineering and Information Technology*. 2(3), pp. 1-30.
- [6] Ghazali, B. S. (2005). Design and Development of an Automated Fingerprint Verification System. Retrieved February 3rd, 2013 from <http://www.eprints.utm.my/4348/1/74021.pdf>
- [7] Marijana, K. (2004). *Passport of the future: Biometrics against Identity Theft*. M.Sc. thesis in Information security. Norwegian Information Security Laboratory (NISlab).
- [8] Adewole, K. S., Abdulsalam, S. O. & Jimoh, R. G. (2011). Application of Voice Biometrics As An Ecological and Inexpensive Method of Authentication. *International Journal of Science and Advanced Technology*. 1(6), pp. 196-201.
- [9] Anil, K. J., Arun, A. R. and Patrick, F. (2008). *Handbook of Biometrics*. USA:Springer, ISBN 978-0-387-71040-2.
- [10] Shoewu, O., Olaniyi, O.M. and Lawson, A. (2011). Embedded Computer-Based Lecture Attendance Management System. *African Journal of Computing & ICT*. Vol 4, No. 3, pp. 27- 36.
- [11] Mahyidin, M. (2008). Student Attendance Using RFID System. Thesis, Electrical and Electronics Engineering Department, University of Malaysia Pahang. Retrieved March 2nd, 2013 from <http://umpir.ump.edu.my/345/1/3275Firdaus.pdf>.
- [12] Sharat, S. C. (2005). *Online Fingerprint Verification System*. M.Sc. Thesis, Department of Electrical Engineering, State University of New York, Buffalo.
- [13] Geetha, M. R. (2010). ZF Microsystem Based Embedded System Application for Fingerprint Verification. California: Department of Electrical and Electronic Engineering, California State University, Sacramento.