Scientia Africana, Vol. 13 (No.2), December 2014. Pp290-302
 ISSN 1118 - 1931

AN IDENTITY MANAGEMENT MONITORING SYSTEM

[1]F. A. U. Imouokhome and **A. O. Egwali [2]**

Department of Computer Science
University of Benin
Benin City, Nigeria

[1] ***Corresponding author:*** franmokome@yahoo.com. Phone: 07062289738;

[2]annie.egwali@yahoo.com Phone: 07033247730

Received: 06-05-14
Accepted: 18-06-14

ABSTRACT

As organizations/institutions grow the need for an efficient monitoring software tool that scrutinizes the true identity and the attendance behaviour of staff and students arises. In most organizations, the conventional method of keeping time books and attendance registers has failed to achieve the desired success and as a result there are regular occurrences of identity irregularities and identity theft. In Nigeria, the trends of employing identification systems using textual information or the conventional fingerprint biometrics for identification have not proved to be effective. An identification system, which employs the use of fingerprint biometric that conducts a one-to-many pattern-matching to authenticate the claimed identity of an individual (student), is proposed in this paper. The system is designed to comprise of a three-level process; namely, a system module, algorithm module, and a user module. The digital representations of the fingerprint biometric data are captured at the system module level. At the algorithm module level, the fingerprint features are extracted for comparison with features stored in the system database. The user interacts with the system at the user module level. The program of implementation of the system is the version 6.0 of the Visual Basic. Results from the implementation reveal that the system has an execution time of 3.01 seconds, making it preferable to the manual system with an execution time of 30 seconds.

Key Words: Biometrics, Pattern-matching Identification, Verification, Authentication, Fingerprints

INTRODUCTION

An organization is made up of a set of people that are gathered in order to accomplish some common goals that are of great importance for the organization itself **(**Rabuzin et al, 2007). Implicit in this characterization are the personal identity and behaviour of each member (i.e., staff and /or students) of the organization, and the rules and regulations that govern the operations of the organization within the official hours of work or lecture periods. In some organization, a user's identity which includes a set of attributes (e.g. name, national identity card number, e.t.c.) that are associated with a person, is concrete and is supported by legal documents. In the online world, a user's identity information may comprise of passwords, account names,

screen names, and login information (Paget, 2007; Egwali, 2011).

As educational institutions grow, the need to monitor the attendance behaviour of staff and students arises. In most of these institutions, one of the requirements is accurate student identification for lecture attendance, which in most cases is allocated 05% - 20% of the total required grade for a particular course. The conventional method of keeping time books and attendance registers has failed to achieve the desired success because it is usually fraught with fraud. The attendance registration system use paper-based methods for taking and calculating attendance; this manual method requires a lot of stationery material and sheets of papers on which students write their names. Registers are provided for students to tick or check a box or sign against their names, and/or a roll-call by the lecturer is done to check the names of students who are present for the lecture. The large population of students, who register for courses, makes it almost impossible for attendance to be taken by lecturers within the allotted lecture period. On some days only 60% of students would show up for class and yet the attendance would contain names for about 80%. This means that names of students who were absent from lectures were written down for them by their friends who were present for the lecture.

This manual system requires adequate supervision to forestall impersonation and wilful manipulations. Other disadvantages associated with these methods include: a lack of standard method of authentication and verification of students; proneness to human error due to fatigue, carelessness, etc. Other failures of the conventional approach could be attributed to the inaccurate data filled by staff and/or the inadequacy of the supervising officers or lecturers. For example, some members of staff in organizations who are late to work sign-in 'times' that do not reveal their 'late-coming'. When attempt is made to correct these irregularities, a good part of lecture or labour time is wasted. The need to check these evil practices by means of a biometric identity management system of attendance-taking, therefore, becomes imperative. Such a system will monitor the process by which the identities of individuals in a population are created (i.e. linking the attributes to a person), maintained and/or destroyed.

Presently biometric systems are used extensively by thousands of people on a daily basis to verify availability for access networks, telecommunication services, public services; access computer systems, access database, access devices, access banking and online account authorize transactions e.t.c. According to Dong-hun (2003), biometrics is an emerging technology for automatically identifying individuals by using their distinct physical or behavioural characteristics. In computer security, biometrics refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked.

Market trend shows that fingerprint biometrics is one of the most diffused biometric techniques used in automatic personal identification because of its strong reliability and its low implementation cost, thus we focused on fingerprint technology. Conventional fingerprint biometrics perform better that the textual manual approach at identifying users. However, the conventional fingerprint biometrics system

Scientia Africana, Vol. 13 (No.2), December 2014. Pp290-302
© College of Natural and Applied Sciences, University of Port Harcourt, Printed in Nigeria *ISSN 1118 - 1931*

has not proven to be very effective either. This paper therefore focuses on improving the conventional fingerprint biometrics system.

Several works have been done that applies the usage of several authenticating technologies including tokens and biometric technology methods and principles for effectively monitoring staff and students attendance. Gil et al (2003) proposed and designed an Access Control System that utilizes a fingerprint technology in a high level security environment to verify user access to some services. Zhang et al (2003) devised an online palmprint identification system for attendance keeping of employee attendance. Simao et al (2008) developed a time attendant system using biometric system that integrates with a multistation wireless communication. Kadry and Smaili (2007) proposed a wireless iris recognition attendance management system for employee identification in a highly secured environment. Shoewu et al (2011) developed an embedded computer based lecture attendance management system that employ the usage of electronic card and card-reader that serially interfaced with a computer system. Shoewu and Badejo (2006) proposed a student attendance system using Radio Frequency Identification Technology (RFID) in which each student is equipped with an RFID card.

Issues and Concerns with Fingerprint Biometric Identification Technique

Identification is the process of trying to find out a person's identity by examining a stored pattern derived initially from the person's identification features. A larger amount of identification data is collected, and the users of the system are identified based on previously collected profiles information of all users. Identifying a user with the conventional fingerprint biometrics means that the user has to be identified both with some textual information and his or her fingerprint. An identification system which uses only text information and fingerprints for identity authentication is designed for use in most organizations and tertiary institutions. In these cases, the method employed by a user to verify his identity depends on the application platform of the system. Some systems adopt a scale of *one: one* deployment (i.e. verification is provided for a single registered user), *one : few* deployment (i.e. verification is provided for several users who are matched against small size databases of about 10 to 100 registered users) and *one : N* deployment (i.e. a user is verified from a database containing about thousands or millions of registered users).

In the traditional fingerprint biometric system, first a user registers his/her textual information (i.e. name) and a fingerprint impression is acquired using any desired efficient fingerprint scanning device, which typically digitizes the fingerprint impression at 500 dots per inch per 256 gray levels per pixel. The digital image of the fingerprint acquired includes several unique patterns of ridge branches (or bifurcations) and ridge endings (or furrows) also called minutiae. Next, these features are identified in the fingerprint image by means of an automated feature extraction algorithm. Each feature is commonly represented by its location (x, y) and the ridge direction at that location (u) and stored in the database. For each individual, these features which are not evenly distributed are uniquely designed and peculiar to that individual alone. During the identification process, a legitimate user's textual and biometric data is matched by an expert (or an expert

computer system operating under threshold scoring rules) against the stored information in the template; the matcher subsystem compares the uploaded fingerprint details with the already stored information for that individual and attempts to arrive at a degree of similarity between the two sets of features after taking into consideration features translation, rotation and scale. This comparison often yields either a score or a distance describing the similarity between the new feature pattern and the template. Based on this score, a final decision of match or no-match is made and the system assigns the pattern to the person with the most similar biometric template. To prevent impostor patterns from being correctly identified, the similarity has to exceed a certain level (i.e. a decision threshold required by the system). If this threshold level is not reached, the pattern is rejected and the authenticating user is denied access or identified as illegitimate.

Although the entire traditional fingerprint method can enhance user's convenience, bolster security and involves a straightforward implementation, it is susceptible to various types of threats and so can easily be compromised (Uludag and Jain, 2004). Fingerprint biometric is susceptible to threats like *circumvention* which involves an intruder gaining access illegally in order to access or modify sensitive data; *coercion* in which at gun point a legitimate user is forced to use his print to log into a system improperly by an attacker; *collusion* wherein an administrator with more right into the system unlawfully fiddle with system parameters to permit an attack; *repudiation* which involves an illegitimate attack executed by a legitimate user who later denials it; *denial of service (DoS)* involves an attacker overwhelming a system's resources so that normal systems operations come to a standstill; and *covert acquisition* in which an attacker sneakily obtain the raw biometric data of a registered user for later criminal operations.

The following actions can disrupt the biometrics sequence of operation. Data in the communication channel between the various modules of the system can be modified; a *fake biometric trait* such as an artificial finger can be presented at the sensor; illegally *intercepted data* can be resubmitted to the biometric system; the feature extractor may be replaced by a Trojan horse program that produces pre-determined feature sets; *templates information* in the database can be altered, replaced or erased altered, replaced or erased and the matcher can be infected by virus (i.e. Trojan horse program) that alters the decision of the system thereby outputting scores that scores thereby flouting the system threshold scoring scale. Apart from the security state of the biometric technology, there are also issues relating to users.

One objection to fingerprinting in a tertiary environment is the issue of privacy. Many students and staffers fear that such stored database of fingerprints can be made available to law enforcement agents when needed by the school authority. Many also question the teachers' continuous good motive in securing such sensitive data since once a template is compromised it cannot by revoked. Many are afraid of inadequate security of the database which could be an attractive target for theft and consequently, the fingerprint images obtained from the templates could be used in other applications. Some just feel it is a privacy

Scientia Africana, Vol. 13 (No.2), December 2014. Pp290-302
© College of Natural and Applied Sciences, University of Port Harcourt, Printed in Nigeria *ISSN 1118 - 1931*

intrusion that is uncalled for. To erase the aforementioned fears, even though it is usually made known that the information will only be used for the purposes specified, a key software quality addressed is "interoperability" (i.e. the use of the fingerprint biometric information across different systems). Due to the fact that interoperable technologies could allow the database information to be used in another system platform when it is collected, the system was designed in such a way that there is no need for the issues of data protection.

The addition of these features made the system generally acceptable in terms of security and privacy. There is also the issue of the "fail to enroll" rate because some people have very faint fingerprints, or no fingerprints at all (about 20% of the general population), thereby making the system unusable for them **(**Dawson, 2001). A poor quality fingerprint input can be caused by a bad input scanners, improper finger insertion on the scanner, dirt on the finger, etc. Any of these can result in a fingerprint not being accepted by the system during Enrolment, which create problems during identification. To overcome these and other problems associated with the aforementioned conventional methods of identification, we designed a Biometric Students' Attendance Recording System called *BIO-REG*.

MATERIALS AND METHODS

BIO-REG Description

Design of Bio-Reg is in three levels, namely: System Module, Algorithm Module and User Module. Issues considered in the System Module include the process of capturing the digital representation of the biometric data, and the hardware to be used. The Algorithm Module involves two phases, the Feature Extraction Phase and the Feature Matching Phase. The Feature Extraction Phase is responsible for the extraction of fingerprint features and the Feature Matching Phase determines whether two sets of representative features are extracted from the same source by matching the minutiae pattern from the captured sample with those in the database to determine any correspondence between them (see figure 1). User interaction with Bio-Reg takes place at the User Module Level. It consists of three modules, namely: (i) the Enrolment Module, (ii) the Mark Attendance Module and the Administration Module. Each module consists of sequential feed-forward sub-phases which accept inputs from previous sub-phases and produce intermediate results that serve as inputs to activate the next sub-module.

Before using the system, each student first ensures that the following rules for enrolment and attendance registration are well absorbed:

i. Register only a particular finger of choice throughout a particular class.
ii. Insert finger and remove only after the red light emitter blinks.
iii. Attendance for a class starts at 30 minutes before class and stops at 15 minutes after class begins.
iv. A student marks attendance only once for a class.

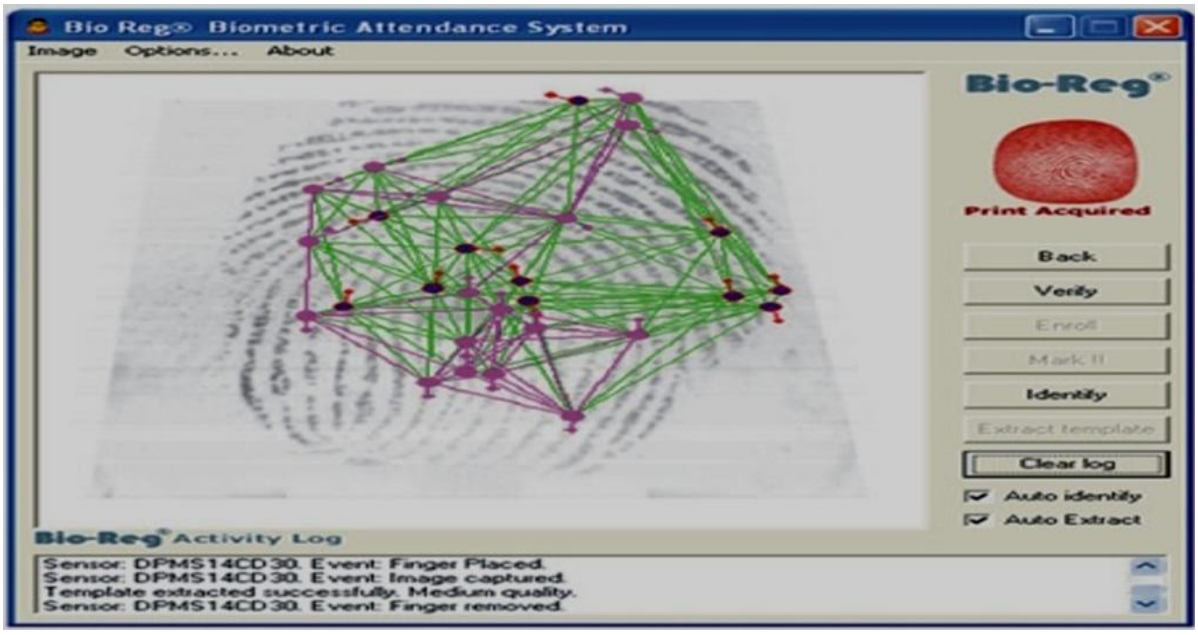

Figure 1: Digital Image of a Captured Finger

Enrolment / Registration Operations

The different available courses, lecturers and examinations are first registered into the database. There are provisions for different course codes and attendance-type to be selected by the individual lecturers. Next each student offering a particular course registers by filling in his/her bio-data which includes matriculation number, name, gender and date of birth and sends the form. Next the lecturer proofreads the student's data and then registers an eligible student by clicking the "Enrol Student" button at the "Administrative Tasks" interface (see figure 2); this activates the fingerprint scanner. Students can now enroll the desired finger. The task of the enrolment button is to register individual student's information into the system database. When the profile and the fingerprint of the user (student) to be enrolled are fed into the enrolment module, a minutiae extraction algorithm is first applied to the fingerprint images, and the minutiae patterns are extracted.

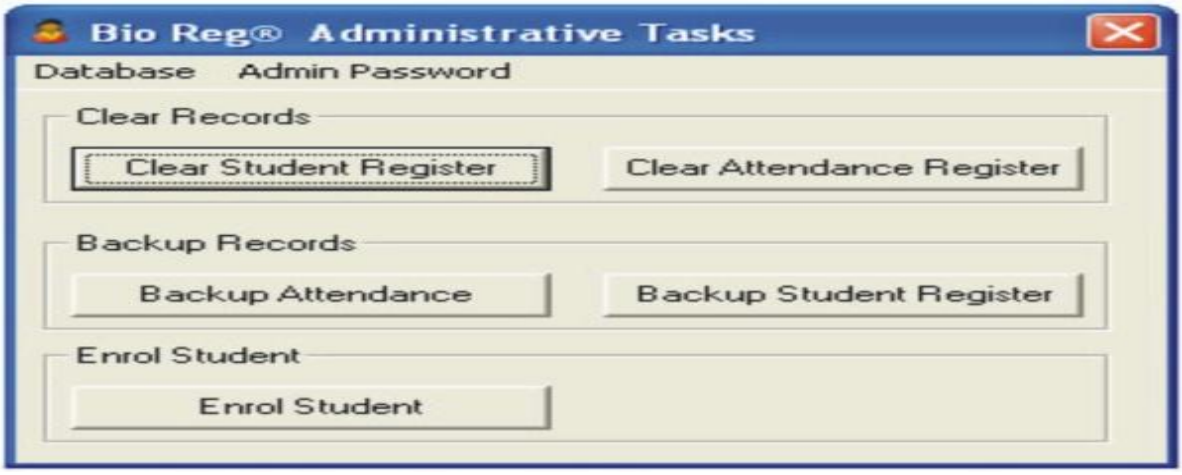

Figure 2: Administrative Task Form

Scientia Africana, Vol. 13 (No.2), December 2014. Pp290-302
© College of Natural and Applied Sciences, University of Port Harcourt, Printed in Nigeria *ISSN 1118 - 1931*

A quality checking algorithm is applied to ensure that high quality templates are stored in the database. If a fingerprint image quality is poor, the system tries to enhance it to clarify the ridge/valley (furrow) structures and drops all the regions that cannot be recognized or recovered. The enhanced (i.e., high quality) fingerprint image is then sent to the feature extractor. If the image is so poor that it cannot be clarified, a message is activated for the user to re-present the identity (fingerprint). This may continue until the algorithm is satisfied and the ID of the Enrolled template is displayed in the log text box. These information are then stored in the *BIO-REG* database.

Mark Attendance Operations

This module is meant to authenticate the identity of the student who intends to be marked present for a lecture. For this to be achieved, each student places his/her finger correctly on the fingerprint scanner for a digital image of the finger to be captured. The blinking of a red light emitter (i.e. between 1 to 2 seconds) denotes the fact that the finger image has been captured and the finger can then be removed from the capturing device. The student's minutiae pattern extracted from the image is sent to the matching program that matches the pattern against that stored in the database to identify and authenticate the user. If there is a match, the application automatically submits the corresponding matriculation number allocated to that fingerprint data to the current attendance database for that particular lecture (while also noting the time). The authenticated student is then prompted to click the "Mark Attendance" button to mark his/her presence for the lecture (see figure 3).

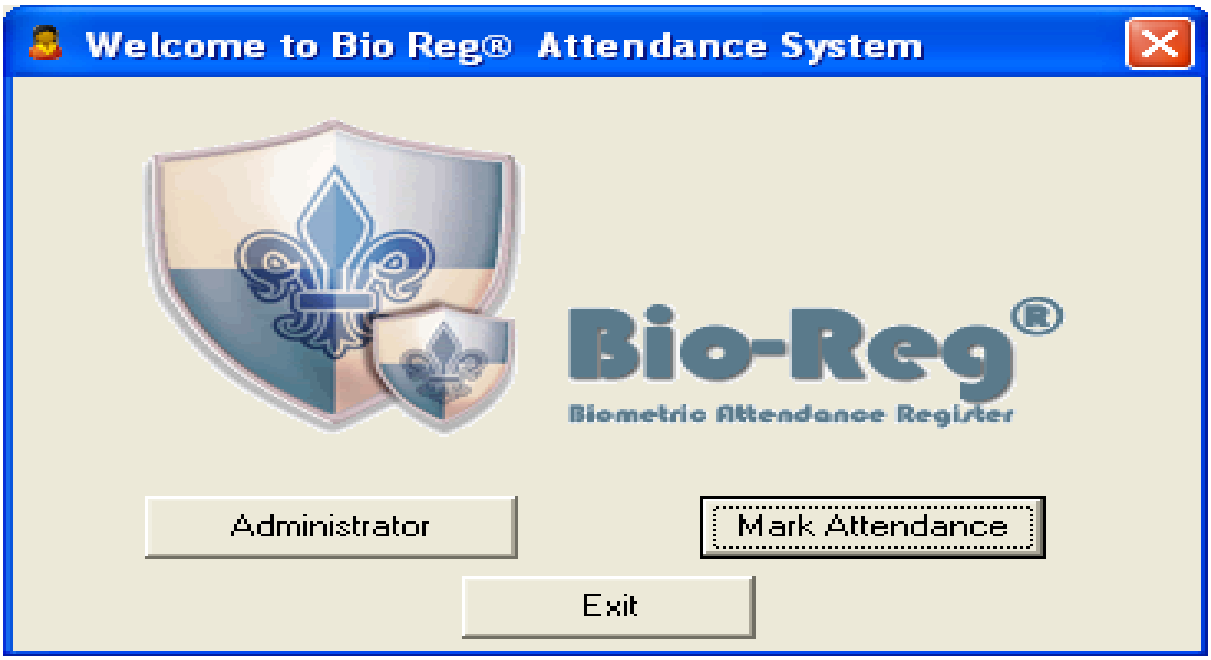

Figure 3: Attendance System screen

At the end of the semester, reports are generated from the attendance database by the Administrator who verifies the students that are eligible for exams and percentage of times the student attended lecture. The Administrator also has the authorization to clear students' previous records, backup records, and enrol student via the Administrative Task interface (see Figure 2).

Experimentation

The program of Bio-Reg, written in Visual Basic version 6.0, was in implemented on Pentium III computer with 750MHz processor, 512MB RAM, 500MB Hard Disk size and Microsoft Window XP service pack 2 Operating System. The choice of Visual Basic (VB) was informed by its flexibility and effectiveness in database manipulation, graphical interface handling, and its rich application development tools which enable programmers to create powerful applications within a relatively short period of time. Visual Basic, being an Object-Oriented programming language, has built-in support tools for implementation of Object-Oriented Design like that of Bio-Reg. Generally, programs developed in VB are more interactive since they respond to system events from mouse clicks, button clicks, and so on. It is also an event-driven programming language. Griaule Fingerprint Software Development Kit (SDK) 2007 that comes with the Software Development Kit (SDK) and allows integration with biometrics application was also installed along with a Microsoft Reader driver.

Bio-Reg was tested for use in keeping accurate lecture-attendance records of students within the University of Benin, Nigeria community. The test was carried out for two academic sessions using Computer Science students of the University of Benin, Nigeria, in respect of 300 Level CSC326 (Computer Architecture II) and 400 Level CSC 426 (Advance Digital Design) courses taught during the 2007/2008 and 2008/2009 academic sessions respectively. The students were randomly selected at each test-lecture. At the end of each enrolment, an aggregate of total number of students that registered was given, and the lecturer prints out a hard copy of such enrolment to ascertain the legitimate students for the class. This system was also tested by co-lecturers who taught some other courses and found it suitable for use. The bio-data and fingerprints of two hundred and ten (210) students were enrolled for CSC326 and one hundred and ninety-one (191) for CSC426. Figure 4 and 5 shows the students' Enrolment details for the courses, which are bio-data, department, matriculation number, course code, course title, etc.

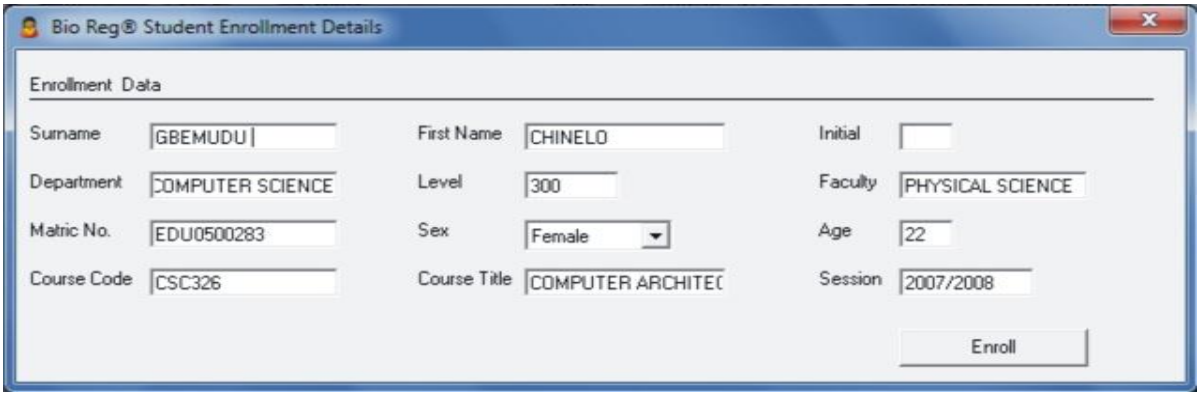

Figure 4: CSC 326 Enrolment details

Scientia Africana, Vol. 13 (No.2), December 2014. Pp290-302
© College of Natural and Applied Sciences, University of Port Harcourt, Printed in Nigeria *ISSN 1118 - 1931*

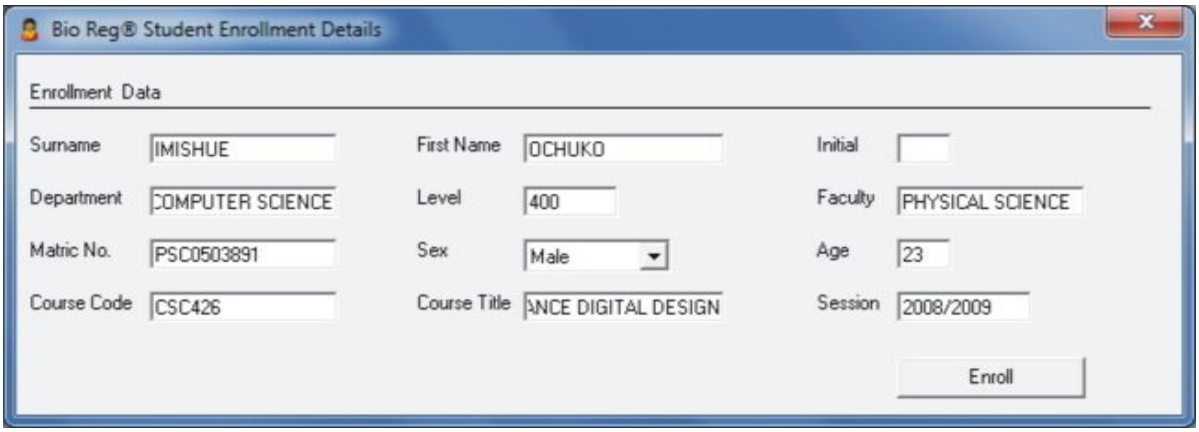

Figure 5: CSC 426 Enrolment details

Figures 6 and 7 which show student's identification number, lecture date and name, represent the attendance sheet for both courses. Figure 6 shows sample test results from the use of BIO-REG for taking attendance of students in respect of CSC326 course for the 2007/2008 academic session. Figure 7 shows sample test results from the use of BIO-REG in taking attendance of students in respect of CSC426 for the 2008/2009 academic session.

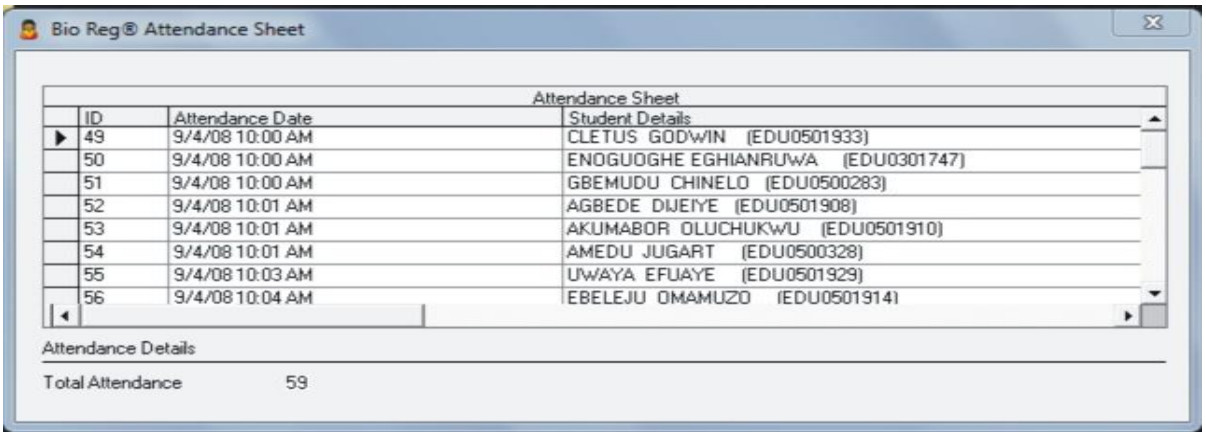

Figure 6: CSC 326 Attendance sheet

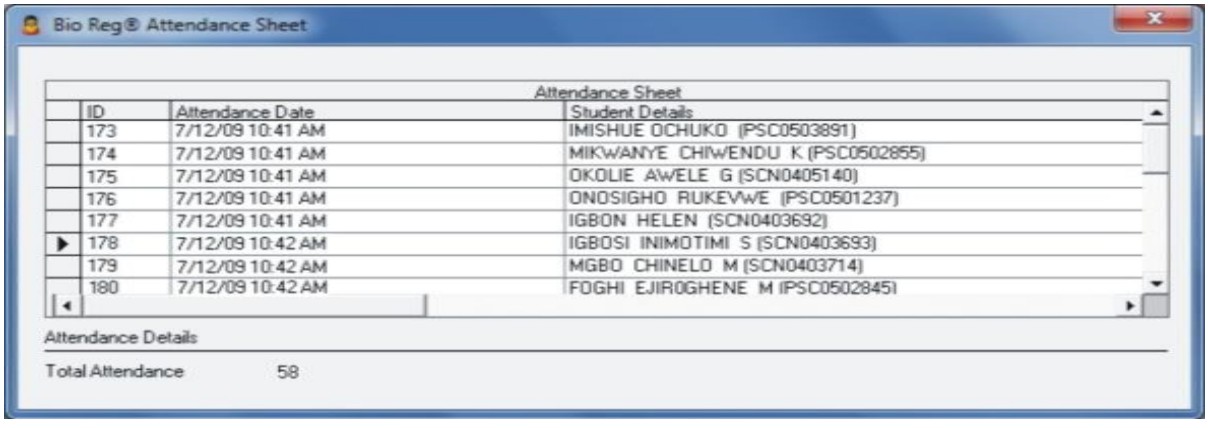

Figure 7: CSC 426 Attendance sheet

Figures 8 and 9 represent the attendance registers; each shows data in the enrolment form in addition to record key and template. The record key is unique for each student just as the template which represents the machine representation of each student's finger print. Contents of the 'template' columns are the ASCII code (American Standard Code for Information Interchange) representations of the fingerprints which are unique for each user.

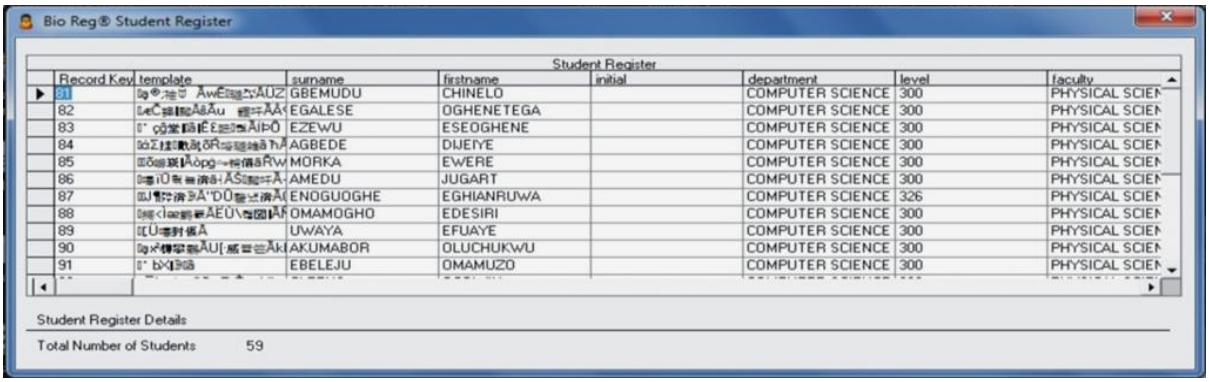

Figure 8: CSC 326 Attendance Register

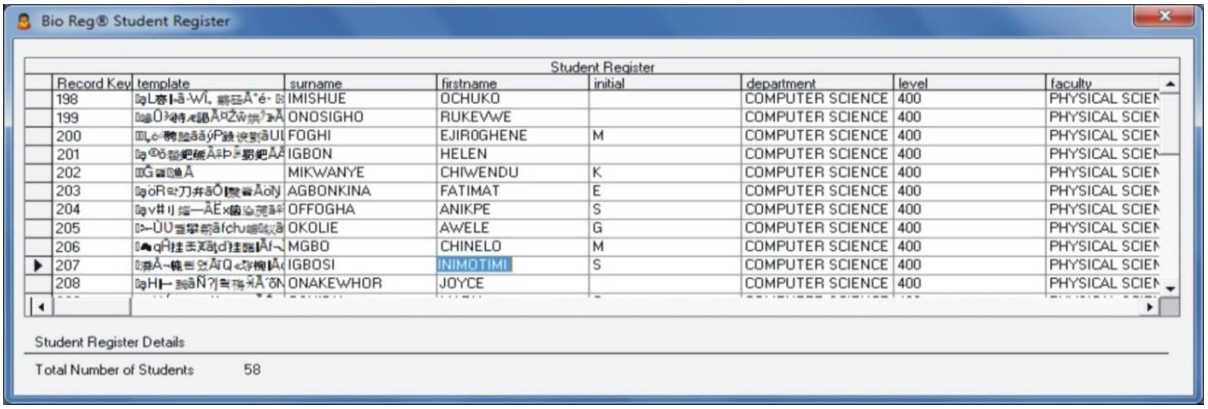

Figure 9: CSC 426 Attendance Register

RESULTS

Table 1: Result of fingerprint Identification

Class Size	Successful	Unsuccessful	success rate of
CSC326 = 210	207	03	over 98%
CSC426 = 191	189	02	over 98%

Scientia Africana, Vol. 13 (No.2), December 2014. Pp290-302
© College of Natural and Applied Sciences, University of Port Harcourt, Printed in Nigeria *ISSN 1118 - 1931*

Table 2: Execution Time Frame of Manual and Bio-Reg Students Registration

Student	Manual Registration	Bio-Reg Registration
Stu-1	20.12	04.11
Stu-2	18.29	02.45
Stu-3	18.34	02.13
Stu-4	17.22	03.23
Stu-5	13.49	02.43
Stu-6	18.52	02.57
Stu-7	19.56	04.32
Stu-8	20.10	03.08
Stu-9	15.23	03.44
Stu-10	16.47	02.10
Stu-11	17.50	04.13
Stu-12	18.93	03.10
Stu-13	13.56	03.23
Stu-14	16.50	03.18
Stu-15	20.11	03.13
Stu-16	16.57	04.10
Stu-17	17.43	04.23
Stu-18	19.33	03.11
Stu-19	17.55	02.13
Stu-20	17.38	04.10
Stu-21	18.20	02.23
Stu-22	19.17	04.13
Stu-23	16.28	04.55
Stu-24	17.43	02.33
Stu-25	18.55	03.13
Stu-26	21.49	04.21
Stu-27	18.12	02.17
Stu-28	19.15	03.45
Stu-29	14.36	04.11
Stu-30	15.57	03.27
Stu-31	20.16	03.43
Stu-32	17.11	02.36
Stu-33	19.13	02.34
Stu-34	18.29	03.56
Stu-35	13.13	02.47
Stu-36	15.17	02.13
Stu-37	21.33	03.46
Stu-38	17.21	02.18
Stu-39	16.59	02.44
Stu-40	19.51	02.28
Average Time Frame	**17.70375**	**3.01325**

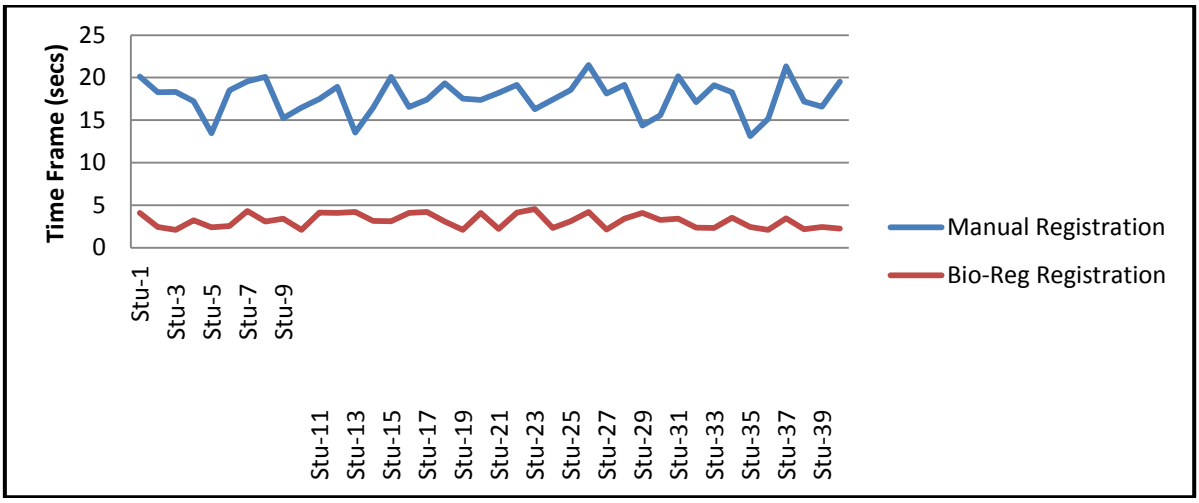

Figure 10: Execution Time Frame of Manual and Bio-Reg Students Registration

DISCUSSION

In the test, there was no false acceptance but there were a few false rejections. For instance, out of the 210 students who registered for CSC326, only 3 were rejected while for CSC436 only 2 were rejected as shown in Table 1. The false rejects could be as a result of improper placement of the finger on the scanner and some slightly scarred fingerprints due to injuries.

A comparison is also made on the execution time for the manual system against that of BIO-REG. Table 2 shows that the average execution time for the manual system for the students of CSC426 is about 17.70secs, while that of BIO-REG is 3.01secs. Reports generation for the attendance system takes approximately 30s. The table represents 40 students sample out of the 401 tests conducted. The values are plotted as a graph shown in Figure 10. The graph shows that the automatic attendance management system, using fingerprint authentication, is better and faster than the use of sheets of paper.

In this era when the population of students who enrol for courses in our tertiary institutions has exploded and is still on the increase, the conventional method of taking records of students who attend lectures for 75% of lecture periods per course per semester is no longer effective. Technological advancement has provided a new way of assisting all to get things done better, faster and in a more convenient and accurate manner. To this end, we recommend the use of Bio-Reg in all tertiary institutions as it would help in no small way to cub the evil activities of students who fail to meet the mandatory minimum number of lecture times per course per semester or rely on their friends to write down their names in absentia — to deceive lecturers that they were present for their lectures. It will also eradicate the practice of impersonation among students during examinations, whereby students who have passed a course, or who have even graduated from the institution come back to sit for examinations for their friends. Bio-Reg can be successfully used for attendance both at lectures and examinations. It is fast, efficient, reliable, reduces the workload of the lecturer, secure, and reduces cost, unlike the manual undependable system. For future work, we wish to establish the

Scientia Africana, Vol. 13 (No.2), December 2014. Pp290-302
© College of Natural and Applied Sciences, University of Port Harcourt, Printed in Nigeria *ISSN 1118 - 1931*

acceptance level of the use of biometric technology in educational institutions and ascertain some more room for improvement.

REFERENCES

Dawson, B. (2001); Vision-based Biometrics. Available online at: http://www.machinevisiononline.org/vision-basedbiometric.htm

Dong-hun, L. (2003); Biometrics as a new technology. Available online at: http://maincc.hufs.ac.kr/argus/detail

Egwali, A. O. (2011). "Appraising the Strength of Users Passwords in Computing Systems in Nigeria". *Journal of the Nigerian Association of Mathematical Physics,* 19: 483 – 486.

Gil, Y., Ahn, D., Pan, S., & Chung, Y. (2003). Access Control System with High Level Security Using Fingerprints. 32th Applied Imagery Pattern Recognition Workshop (AIPR'03), Washington DC, USA, 15-17.

Kadry, S., and Smaili, K. (2007). A Design and Implementation of a Wireless Iris Recognition Attendance Management System. Information Technology and Control, 36(3): 323 - 329.

Paget, F. (2007), Identity Theft. White Paper. Available at www.mcafee.com

Rabuzin, K., Baca, M. and Malekovic M. (2007). "A Multimodal Biometric System Implemented with an Active DBMS", Journal of Software, 2(4); Academy Publisher.

Shoewu O, Olaniyi O.M., and Lawson A. (2011). "Embedded Computer-Based Lecture Attendance Management System". *African Journal of Computing and ICT (Journal of IEEE Nigeria Computer Section)*. 4(3): 27 – 36.

Shoewu, O. and Badejo O. (2006). "Radio Frequency Identification Technology: Development, Application and Security Issues". *Pacific Journal of Science and Technology*, 7(2): 144-152.

Simao, P., Fonseca, J., & Santos, V. (2008). Time Attendance System with Multistation and Wireless Communications. IEEE International Symposium on Consumer Electronics. 14 -16.

Uludag U. and Jain A. K (2004). "Attacks on biometric systems: a case study in fingerprints," in *Proc. SPIE, Security, Seganography and Watermarking of Multimedia Contents VI*, (San Jose, CA), 5306: 622–633.

Zhang, D., Kong, W. K., You, J., & Wong, M. (2003). Online Palmprint Identification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(9), 1041-1050. www.intechopen.