International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Development of a Fingerprint Biometric Authentication Scheme in Electronic Examination

Mohammed Babatunde Ibrahim[1], Abubakar Usman Othman[1], Bukola Balogun Fatimah[2], Umar Musa[1], Ujah Chinalu Briget[3]

[1]Department of Computer Science, Federal University of Technology Minna, Nigeria
[2]Department of Computer Science, Kwara State University, Nigeria
[3]Department of Computer science, University of Ilorin, Nigeria

Abstract— *With the development of information communication technology (ICT) in the recent age, authentication has witnessed a drastic change in the way and manners it was done in the recent pass. The rapid growth in electronic examination (e-exams) has posed the need for a safer, faster, a more reliable and efficient method of user's verification than what passwords offered. Fingerprints are used as a form of biometric identification which is unique and does not change in a human's lifetime. The wide use of computer automations in the world has brought about changes in security at global institutions (banking, aviation, government, health) and deploying it in academic institutions would be a success. The most difficult challenges of biometric systems are evident in defining the right and accurate biometric system in solving specified problems. In this paper, we developed a Biometric authentication system for an image enhancement and incorporates SecuGen fingerprint. Minutiae points were extracted by the use of Crossing Number (CN) Concept. The system was developed using Java language for the applets and integrated PHP with a web server (XAMPP), using MySQL database as the backend. The experimental result shows that the developed system has an accuracy level of 97.5% for authentication of user fingerprint which shows that the system is well secured and reliable making it capable of preventing impersonation.*

Keywords— *Authentication: Biometric: Database: Electronic examination: Fingerprint: MySQL: Web server*.

I. Introduction

In many institutions and academic organisations, examination is a very important criterion which is used for students or employee's grading, assessing, and promotion. Today, many industries as well as schools are experiencing technological innovation and changes in the mode in which they carry out their operations.

E-learning has different application areas which include Electronic-examination (e-examination), which is employed to assess student's knowledge through recent computer technology that has no effect on the conventional institution of higher education course examination. Online (electronic) examinations are the most commonly adopted source for examinations in some universities, and the development of network technology polices has given the possibility to conduct the examinations online [1].

The locality of the examination most bat times are not secured enough, which made students to have access to unofficial domains [2]. Ref. [3], in their study conducted that 73.6% of students selected to partake in the exercise were of the opinion cheating is easy in an electronic examination.

Authentication is the mechanism used in identifying individuals, information or system and provides important roles (security) in our environment. Mechanisms include passwords, biometrics, access tokens, and watermarks. A process that requires a person's identity to be verified so as to know who is about to authenticate into the system is known as authentication. The conventional technique of identifying an individual is based on an object he/she possess (key, card) or alternatively, use of some alphanumeric characters known only to the individual. As this will only give the individual access to the system but does not determine if the individual is the rightful owner to the verified system [4].

The innovation and presence of information technology has led to the present day means of examining students using electronic systems which is bound to replace the paper or manual method characterised by impersonation, excessive examination leakages, bribing of lecturers, invigilators and supervisors of examinations. In Federal University of Technology, Minna, students' examinations can either be taking in two ways; pen-on-paper or electronic examination.

A biometric system is developed to solve a problem of matching an individual, through the behavioural and physiological body features of individuals. It works in two (2) ways; an individual must have registered in a system where the templates are saved in a database. The system then processes the output with an algorithm used in processing the templates during registration which is compared with what is in the database. Verification is considered successful, if a given threshold in the algorithm has been met, otherwise it is considered unsuccessful [5].

II. Page Layout

The authors in [6], defined electronic examinations as a system that conducts examination with the intranet or web with the use of a computer system. E-examination system is a software used to carry out the examination using the computer. The application may be a standalone (desktop) program optionally enriched with multimedia content and other features like time measurement or a choice of questions in a random manner. With the rapid development of internet technology, e-exams are much more often implemented as distributed applications that use public telecommunication network, with web browser based user interface (www service).

Ref. [7], proposed that biometric technologies can be given full evaluation and consideration if the following features are met;

i. *Uniqueness*: individuals must not have the same features.
ii. *Collectability*: The features must be easily measurable and collectible.
iii. *Universality*: All in individuals must have the required feature; those who do not have will have to be accommodated.
iv. *Permanence*: The specific features must not fade out with time.
v. *Circumvention*: There should be difficulty in trying to deceive the system.
vi. *Performance*: The technique should provide accurate outcome under diverse environmental circumstances.
vii. *Acceptability*: The entire populace must acknowledge the process used in collecting samples.

An extension to passwords and PIN codes which identifies and verifies a human through their typing mode where the system verifies he user at the point of logging in so as to monitor the biometric systems is known as keystroke dynamics and they are cheap to install as only the software package is needed [8].

A natural means of identification in biometrics is the face recognition [9]. The authors used face recognition through computers to identify or verify automatically an individual using a video frame form its source or a digital image. Facial metric and Eigen faces are the two areas where they have been deployed. Facial metric deals with specific facial features positioning (eyes, nose and mouth with its distances) with a fixed pre-defined size (150-100 points) in the face region. The facial metric is then computed and stored in a face template after canonical image has been normalized. The template size is mostly between 3KB and 5KB but a template also has a small size of 96 bytes.

Iris Scanning is used to identify an individual uniquely because it is the coloured part of the eye. During the baby's gestation period in the 8th week is when the iris is formed which does not change in life. Rings, freckles, furrows are the evident features of the iris which are scanned by video camera to generate a biometric template called Iris-Code. Ref. [10], presented work that uses the odd of two (2) irises returning identical Iris-Codes (1:1052), which makes it secure, and experts report a CER of 1 in 131,000 for iris verification. This machine also works for people who wear spectacles and not all part of the iris is captured as the top part is discarded because it might be covered by the eyelids. It is applicable in high security facilities, military formations and prison detentions.

Retina Scanning technique came about in 1935 when doctors who were on research on eye diseases came to a conclusion that vascular patterns are unique and relatively stable which led to a paper being published that retina photographs can also be used for identification. This made the leading company producing retina scanners increase productions in 1970s. Retina scanners are known to have low False Acceptance Rate (FAR) and are used for years in high security facilities. A Crossover Error Rate of 1 in 10,000,000 are reported in [11]. In scanning the retina, a low intensity light source is used at 360°. A template of 96 bytes is produced when a scan of 400 findings is reduced 192 reference points of vascular patterns which takes a time of 1.5 seconds of the whole verification process. Most of the retina scanners are not user-friendly in the sense that not all users will be comfortable using the device because of their heights when the device is wall-mounted. It also has its disadvantage as people are not comfortable with the laser emitted due to believe that it could damage their eyes.

Ref, [12], proposed phase correlation using a new minutiae-based fingerprint matching algorithm, which defined a new representation called Minutiae Direction Map (MDM) which is done by first converting the sets of minutiae into two-dimensional (2D) image spaces with transformation parameters calculated using their proposed phase correlation between the two MDMs to align the fingerprints so that they can be matched. The distance between the two minutiae sets determines the fingerprints similarity scores. The accuracy of their system was not available but they had an equal error rate of 2.44%.

In [13], the authors implemented a minutiae based fingerprint using crossing number concept. In their research, they proposed a three phase method for their algorithm consisting of image pre-processing, use of crossing number to extract minutiae and comparing the pre-processing with the extracted munitiae with the templates in the database. Their implemented system had an accuracy of 99.77% with a (FAR = 0% and FRR = 0.23%).

A minutiae extraction technique based on Gabor filter and Crossing Number concept for extraction was presented in [14], which had an accuracy rate of 92% with (FAR = 1% and FRR =7%) using the Fingerprint Verification Competition (FVC) 2000 database.

Verification is said to occur when the concerned person provides an identity. A one-to-one search is then performed by the system, which compares the biometric template stored in the database and the captured template (Am I whom I claim I am?). If a match is made the identity of the person is verified [15].

III. System Design

A. Fingerprint-Based System for E-Examination

After a study of the security challenges of electronic examination, a new fingerprint biometrics solution for electronic examination identification and verification was proposed.

B. Fingerprint Image Acquisition

For the purpose of this research, SecuGen fingerprint optical scanner was used for fingerprint image acquisition. This is because the pattern of the ridges and valleys of a person's fingerprint surface fingerprint is unique. A single curve segment on a fingerprint is known as ridge while a region between two adjacent ridges is known as valleys. Ridge endings and ridge bifurcations are the two major types of minutiae points which are used for uniqueness determination of an individual's fingerprint.

The proposed system uses the features of minutia fingerprint for extraction for students writing electronic examination. The algorithm considered for matching minutiae is a triplet m = {x, y, θ} which indicate x, y location coordinate of the minutiae (distance from the origin) and angle θ of the minutiae (destination between x and y). Minutia is gotten by the extraction of samples from same set of fingerprints and stored as a set of points in two-dimensional (2D) plane. For feature extraction, the description of its location (indicating x, y coordinates) and orientation (θ)is found based on the ridge endings and bifurcation of the input from the fingerprint images

C. *Fingerprint Image Enhancement*

One important characteristic is the ridge structures of a fingerprint image as this is what carries the information of the feature characteristics required for minutia extraction. The quality input of the fingerprint image for the performance of extracting the minutiae algorithms. Therefore, improving the clarity of the ridge structure is the purpose of the algorithm enhancement in the regions recoverable while the region unrecoverable is marked as too noisy for processing further. Figure 1 shows the stages of enhancement performed on the fingerprint image.

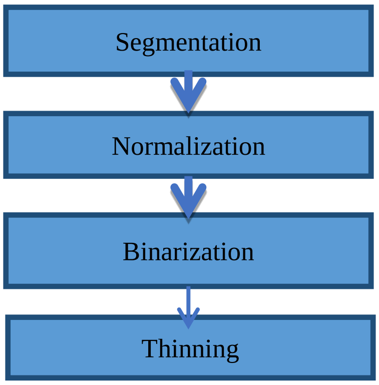


Fig. 1. Image enhancement process.

D. *Template Generation for Fingerprint*

At this stage, the minutiae feature of the fingerprint image is extracted and a template is generated after the student must have enrolled. This involves defining a 3 x 3 window size pixels centred at the black pixel. The algorithm then finds the number of pixels N, within the size which determines the minutia features which is shown in the algorithm section. The extracted template is stored along with the students other bio-information in the database.

E. *Electronic Examination System*

The proposed electronic examination system consists of primarily two parts:-

i. The Frontend Webpage
ii. The Backend Database

F. *The Frontend Webpage*

This application consists of an initial Login screen which request the students to present his/her enrolled fingerprint for verification before proceeding to write the examination, if a defined threshold has been met. For new students, there is an option for Signing Up by giving their details.

After Sign-Up, the details are stored in the database managed by MySQL. The Fingerprint is stored in "SHA1" Encryption Format, thereby adding to the security. Each time the student tries to Login using the biometric scanner, the scanned fingerprint is matched with the stored template in the Database, which if successful is allowed to continue to the Welcome Screen.

The Welcome Screen has Provisions for Log out as well as taking the Examination/ Test. If the option for the Examination/ Test is selected, the user is directed to the questionnaire which is connected to the Question Generator Database, from where random Questions are generated using random function. This page also has an embedded JavaScript code which maintains a timer, and redirects to the results page as soon as the time gets expired. The results are calculated comparing the input from user to the answer stored in the database. The Score is stored by a Server-side Counter which displays the results. The result is then stored in the Results Database, where the track of attempted and correct questions are kept. Then the User logs out from the session once he/she is done writing the examination.

G. *The Backend Database*

This is where the enrolled student's information is saved as well as the generated templates. Questions being uploaded, displayed, policy settings (time, date, number of questions, and mark per question) editing is done the administrator at the backend. This is developed using PHP and MySQL.

H. *Template Matching*

After the students must have filled the necessary information needed and fingerprints been enrolled, the algorithm attempts to find a match between the previously stored (S) templates and a new live (L) templates, before the students can proceed to write an examination. Therefore, in matching the sets of minutia, S is taken from the database and L is the test / live fingerprint. S and L are said to be paired if their minutia type are close in direction, and position and their minutia are the same.

Therefore If $M^1 \epsilon S$ and $M^2 \epsilon L$,

$$\text{TYPE } M^1 = \text{Type } M^1 \tag{1}$$
$$\text{their DIST } M^1, M^2 \underline{\leq} D_m \tag{2}$$
$$\text{and ANGLE} M^1, M^2 \underline{\leq} A_m \tag{3}$$

Here, (M^1, M^2) are set of minutia features that are matched. Their displacement (in x and y = D_m) and rotation (θ = A_m) are recovered respectively. Let S_m be a set of matched pairs of each element in S_m has the form ($M_{1,}^1 M_1^2$) whereM_1^1, is from S and M_1^2 is from L. There are two constrains to S_m.

All M_1^1, M_1^2should be different which implies that each minutia in S and L should not be matched more than once.

Therefore, the following condition must also be satisfied if(M_1^1, M_1^2) and(M_2^1, M_2^2) are two element in S_m

DIST $(M_1^1, M_1^2) - DIST\ (M_2^1, M_2^2)$ / <b, where b is a small value.

The next process involved therefore is to perform a similarity score Q by simply normalizing the matched minutiae element (representing k) with half the sum (m + n) / 2 of minutiae set in S and L.

$$\text{Score } (Q) = \frac{2k}{m+n} \qquad (4)$$

where m = number of minutia in S

n = number of minutia in L

IV. Results

The design requirements are met through the use of a fingerprint scanner which captures the fingerprint of the users and desirable results, some of which are highlighted below are achieved.

A. *Menu Design*

Menu provides a list of options or commands where a user can choose from. This is because most applications are now menu-driven component. Here, users can choose an item/option by using the mouse to click on the item. The work is implemented using a client server architecture where the server is the administrative end that manages various components such as database, fingerprint enrolment of students.

The client end serves basically as the platform for registering and writing examination. The proposed system consists of different menu as discussed;

Home: This menu allows students practice for their examination.

My Profile: This menu consists of students' bio-data such as Name, Matric number, School, Department, Level, Image

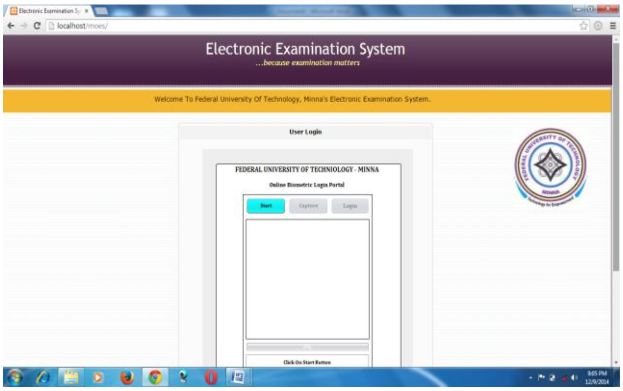
View Result: This menu allows students view their result after submitting their questions.

Log out Menu: The student can decide to log out of the system if they are through with their activities on the application.

B. *Form Interface Design*

This aspect involves the display of various forms used to interact with the fingerprint reader as well as the central database. The program was designed systematically to display key interfaces for users' interaction with ease. They include;

Login Page: This is the default page where the interface provides the entry point into the proposed system. This option is open for the student which allows them have access to the system. The student will have to register their details to be able to have access through the register menu below the biometric login interface. After registering, the student then proceeds to provide the required finger (left thumb) needed to be able to have full access to the system by clicking on the login button. The administrator also provides a user name and password, the system then authenticates theses parameters and if they are valid, the main menu interface will be displayed. The interface is shown in figure 2.



Electronic Examination System

...because examination matters

Welcome To Federal University Of Technology, Minna's Electronic Examination System.

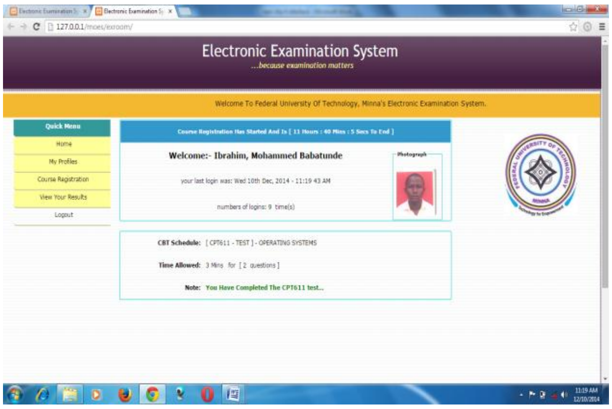
User Login

FEDERAL UNIVERSITY OF TECHNOLOGY - MINNA

Online Biometric Login Portal

Click On Start Button

Fig. 2. Biometric login page.



Electronic Examination System

...because examination matters

Welcome To Federal University Of Technology, Minna's Electronic Examination System.

Course Registration Has Started And Is [11 Hours : 40 Mins : 5 Secs To End]

Welcome:- Ibrahim, Mohammed Babatunde

your last login was: Wed 10th Dec, 2014 - 11:19 43 AM

numbers of logins: 9 time(s)

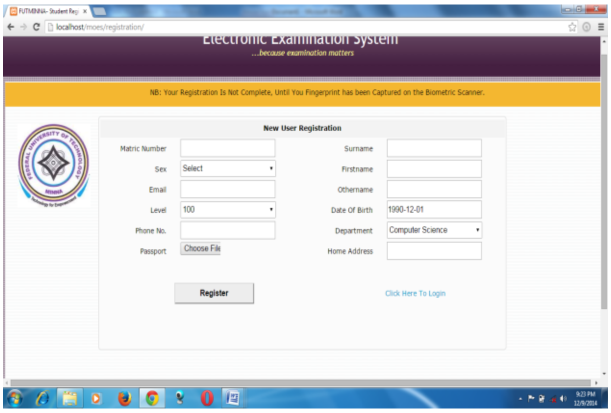
CBT Schedule: [CPT611 - TEST] - OPERATING SYSTEMS

Time Allowed: 3 Mins for [2 questions]

Note: You Have Completed The CPT611 test...

Homepage: Fig. 3. Student homepage.

Registration Page: This consists of student's information such as matric number, Names, email, phone no, home address, department, level and passport.



Electronic Examination System

...because examination matters

NB: Your Registration Is Not Complete, Until You Fingerprint has been Captured on the Biometric Scanner.

New User Registration

Matric Number		Surname	
Sex	Select	Firstname	
Email		Othername	
Level	100	Date Of Birth	1990-12-01
Phone No.		Department	Computer Science
Passport		Home Address	

Fig. 4. Student's registration page.

Biometric Enrolment Page: This page captures the students fingerprint after enrolling which is saved in the database.

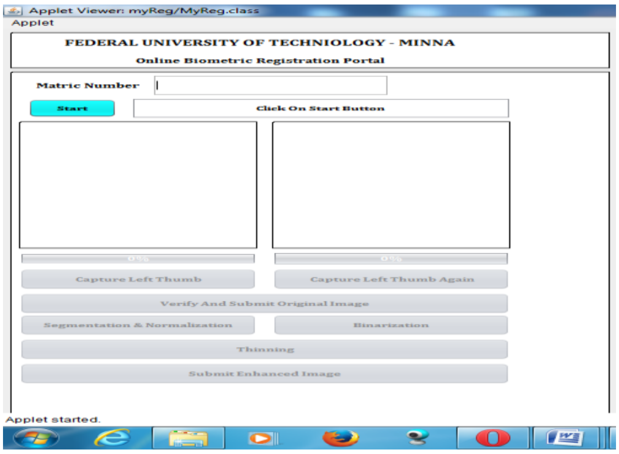
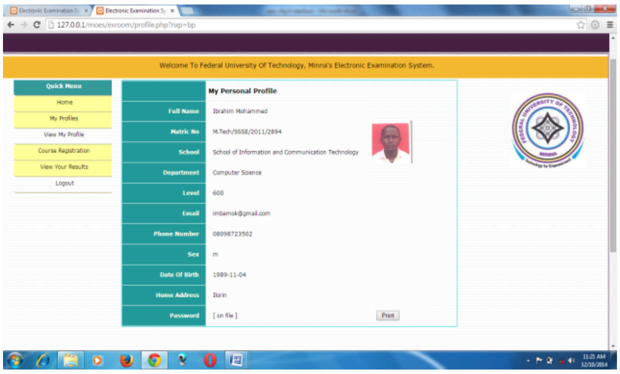

Applet Viewer: myReg/MyReg.class
Applet
FEDERAL UNIVERSITY OF TECHNIOLOGY - MINNA
Online Biometric Registration Portal
Matric Number
Start
Click On Start Button
0%
0%
Capture Left Thumb
Capture Left Thumb Again
Verify And Submit Original Image
Segmentation & Normalization
Binarization
Thinning
Submit Enhanced Image
Applet started.

Fig. 5. Biometric enrolment page.

Profile Page: This page contains the student's personal data and academic data.


127.0.0.1/moes/exroom/profile.php?nxp=bp
Welcome To Federal University Of Technology, Minna's Electronic Examination System.
Quick Menu
Home
My Profiles
View My Profile
Course Registration
View Your Results
Logout
Print

My Personal Profile

Full Name	Ibrahim Mohammed
Matric No	M.Tech/SSSE/2011/2894
School	School of Information and Communication Technology
Department	Computer Science
Level	600
Email	imbamok@gmail.com
Phone Number	08098723502
Sex	m
Date Of Birth	1989-11-04
Home Address	Ilorin
Password	[on file]

Fig. 6. Profile page.

Admin Homepage: This is the admin homepage which consists of manage users, Manage questions, Schools and Courses and Schedule exams and log out.

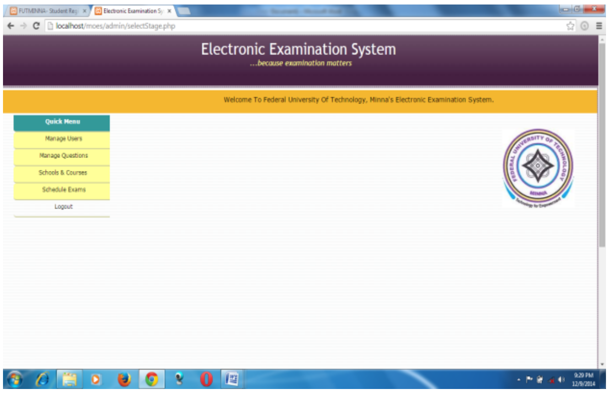
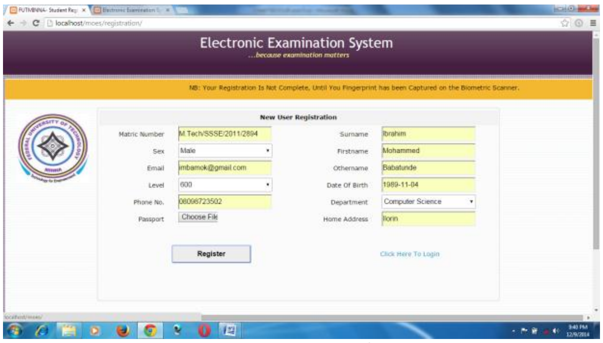

localhost/moes/admin/selectStage.php
Electronic Examination System
...because examination matters
Welcome To Federal University Of Technology, Minna's Electronic Examination System.
Quick Menu
Manage Users
Manage Questions
Schools & Courses
Schedule Exams
Logout

Fig. 7. Administrative page.

C. Input Design

This involves the registration of eligible candidates of the university. This is necessary to uniquely identify each of the students. In this phase, each student is required to register personal information such as matriculation number, name, email, phone no, home address, school, department. The system is able to register students who are registering for the first time. This is shown in figures 7 and 8. Also the system is able to avoid multiple registrations which are also an important aspect of the work thereby preventing duplication of student's data.

Registration form


localhost/moes/registration/
Electronic Examination System
...because examination matters
Choose File
Register
Click Here To Login

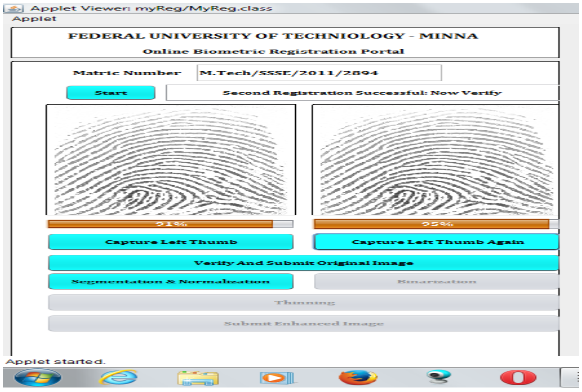
NB: Your Registration Is Not Complete, Until You Fingerprint has been Captured on the Biometric Scanner.

New User Registration

Matric Number	M.Tech/SSSE/2011/2894	Surname	Ibrahim
Sex	Male	Firstname	Mohammed
Email	imbamok@gmail.com	Othername	Babatunde
Level	600	Date Of Birth	1989-11-04
Phone No.	08098723502	Department	Computer Science
Passport		Home Address	Ilorin

Fig. 8. Registration form.

Fingerprint Template Captured: This is the page where the students' presents his/her fingerprint for enrolment

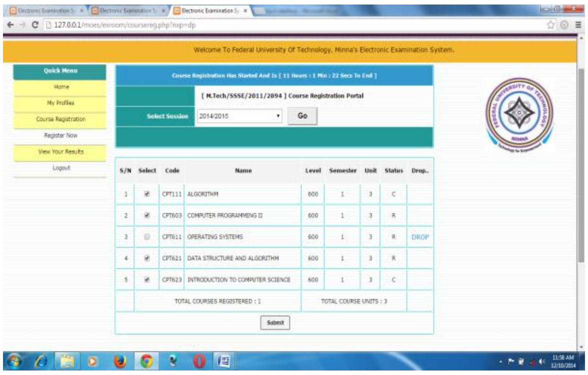

Applet Viewer: myReg/MyReg.class
Applet
FEDERAL UNIVERSITY OF TECHNIOLOGY - MINNA
Online Biometric Registration Portal
Start
91%
95%
Capture Left Thumb
Capture Left Thumb Again
Verify And Submit Original Image
Segmentation & Normalization
Binarization
Thinning
Submit Enhanced Image
Applet started.

Matric Number: M.Tech/SSSE/2011/2894

Second Registration Successful: Now Verify

Fig. 9. Fingerprint enrolment page.

Course Registration Profile: This interface allows students register courses for the semester.


127.0.0.1/moes/exroom/coursereg.php?nxp=dp
Welcome To Federal University Of Technology, Minna's Electronic Examination System.
Quick Menu
Home
My Profiles
Course Registration
Register Now
View Your Results
Logout
Go
Submit

Course Registration Has Started And Is [11 Hours : 1 Min : 22 Secs To End]

[M.Tech/SSSE/2011/2894] Course Registration Portal

Select Session: 2014/2015

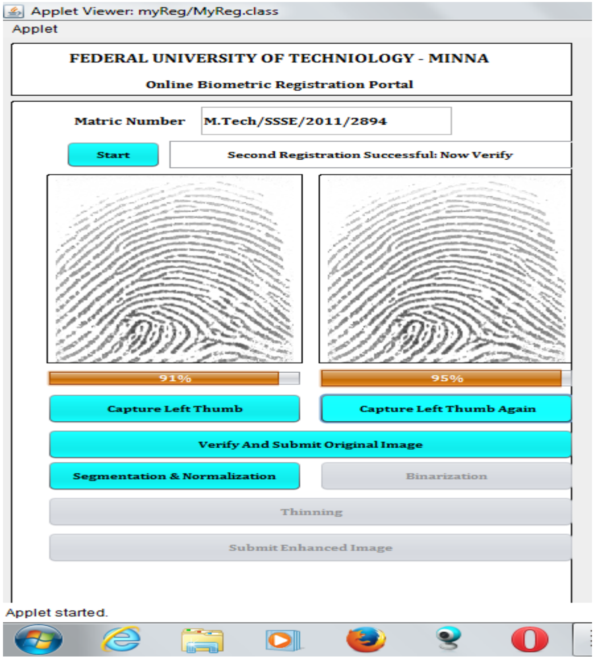
S/N	Select	Code	Name	Level	Semester	Unit	Status	Drop..
1	☑	CPT111	ALGORITHM	600	1	3	C	
2	☑	CPT603	COMPUTER PROGRAMMING II	600	1	3	R	
3	□	CPT611	OPERATING SYSTEMS	600	1	3	R	DROP
4	☑	CPT621	DATA STRUCTURE AND ALGORITHM	600	1	3	R	
5	☑	CPT623	INTRODUCTION TO COMPUTER SCIENCE	600	1	3	C	
	TOTAL COURSES REGISTERED : 1			TOTAL COURSE UNITS : 3				

Fig. 10. Course registration page.

D. Output Design

This is a crucial component of the system design since it produces result of processing carried out on the input data. It should be noted that only needed data is allowed on the system. For the purpose of this work, the application is expected to generate a set of output for the users.

Figure 11 shows a student's fingerprint enrolled after filling the required bio-data and presenting his/her fingerprint. Figure 11 shows the captured fingerprint of a student after segmentation and normalization



FEDERAL UNIVERSITY OF TECHNOLOGY - MINNA

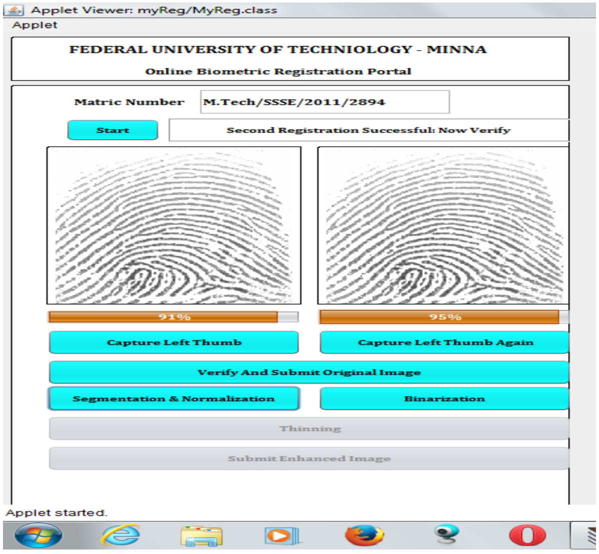
Online Biometric Registration Portal

Matric Number: M.Tech/SSSE/2011/2894

Second Registration Successful: Now Verify

Fig. 11. Fingerprint captured.

Segmentation and Normalization template



FEDERAL UNIVERSITY OF TECHNOLOGY - MINNA

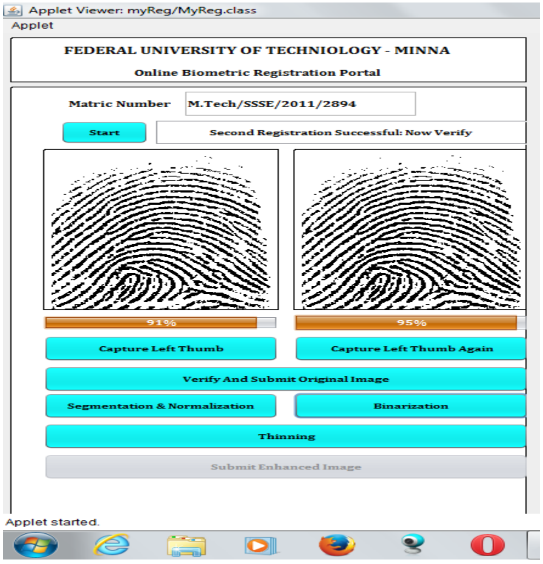
Online Biometric Registration Portal

Matric Number: M.Tech/SSSE/2011/2894

Second Registration Successful: Now Verify

Fig. 12. Segmentation and normalization captured.

Binarised Image: This is the next step have the segmentation and normalization process has been performed.



FEDERAL UNIVERSITY OF TECHNOLOGY - MINNA

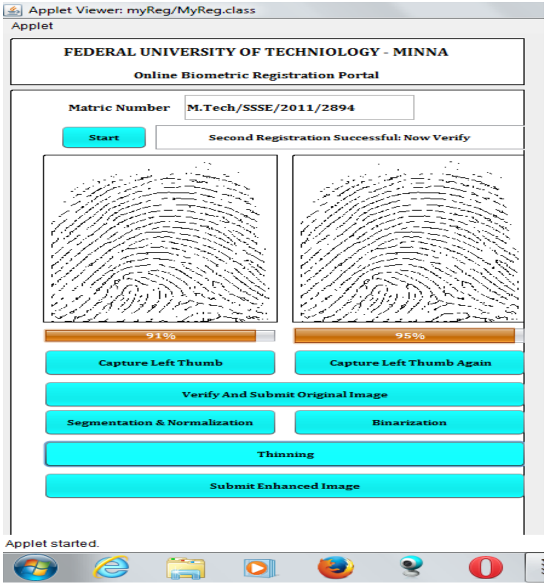
Online Biometric Registration Portal

Matric Number: M.Tech/SSSE/2011/2894

Second Registration Successful: Now Verify

Fig. 13. Binarised image.

Thinned Image: This is the last stage involved in image enhancement process, where the extracted template is thinned to get a better template for enrolment.



FEDERAL UNIVERSITY OF TECHNOLOGY - MINNA

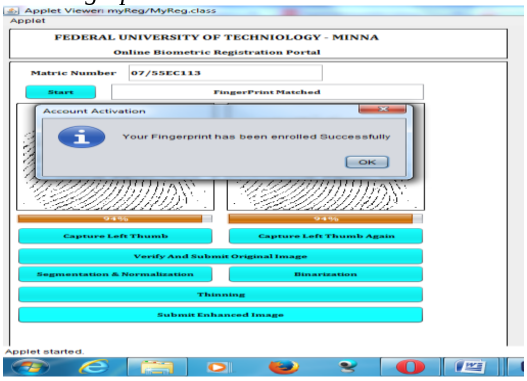
Online Biometric Registration Portal

Matric Number: M.Tech/SSSE/2011/2894

Second Registration Successful: Now Verify

Fig. 14. Thinned image.

Registered Fingerprint



FEDERAL UNIVERSITY OF TECHNIOLOGY - MINNA

Online Biometric Registration Portal

Matric Number: 07/55EC113

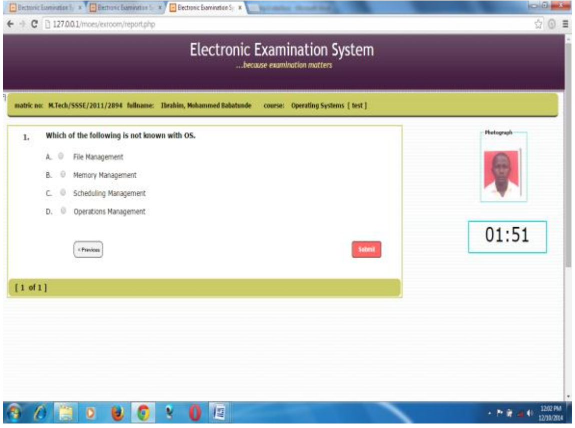
FingerPrint Matched

Account Activation

Your Fingerprint has been enrolled Successfully

Fig. 15. Fingerprint successfully registered.

Interface of Multiple Questions E-Exams System



127.0.0.1/moes/exroom/report.php

Electronic Examination System
...because examination matters

matric no: M.Tech/SSSE/2011/2894 fullname: Ibrahim, Mohammed Babatunde course: Operating Systems [test]

1. Which of the following is not known with OS.

A. ○ File Management
B. ○ Memory Management
C. ○ Scheduling Management
D. ○ Operations Management

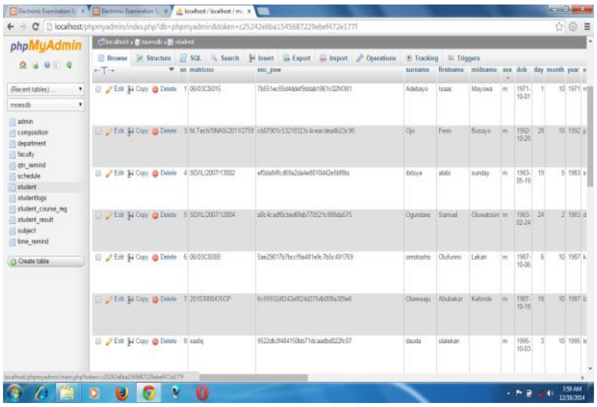
[1 of 1]

Fig. 16. Interface of multiple questions E-Exams system.

The test result shows that the system is effective and has a very fast response. There was no false identification of students, there were few cases of false rejection which were later accepted and only pre-registered students were authenticated. The system was tested using bio-data and fingerprints collected from students. During the test, there was no false acceptance that is a person not pre-registered was not falsely enrolled to take examination. There were few rejections during the test in which the system failed to authenticate some pre-registered users. This could be as a result of improper placement of finger on the reader.

E. Database Design

For convenience, compatibility and flexibility, MySQL was used to design the database of the proposed system. After every successful registration of students, the administrator is able to access the stored data from the database. The system is able to view and retrieve records of all registered students. The figure below shows the number of registered students.



localhost/phpmyadmin/index.php?db=phpmyadmin&token=c25242e6ba1545687229ebef472e177f

sn	matricno	enc_psw	surname	firstname	midname	sex	dob	day	month	year	e
1	06/03CS015	7b551ec65d4ddef9ddab1861c02f4381	Adebayo	Isaac	Mayowa	m	1971-10-01	1	10	1971	m
3	M.Tech/SNAS/2011/2758	cb07901c53218323c4ceacdea4b23c98	Ojo	Femi	Busayo	m	1992-10-28	28	10	1992	jc
4	SD/IL/2007/13002	ef0da84fcd69a2da4e8010d42e5bf6bc	ibitoye	alabi	sunday	m	1983-05-19	19	5	1983	s
5	SD/IL/2007/12004	a0c4cadf0cbed6feb770521c888da575	Ogundare	Samuel	Oluwatosin	m	1983-02-24	24	2	1983	d
6	06/03CS005	5ae29817b7bccf9a481e9c7b5c491769	omotosho	Olufunmi	Lekan	m	1987-10-06	6	10	1987	k
7	20103000435CP	6c65932df242e8f24d275db008a309e6	Olawaju	Abubakar	Kehinde	m	1987-10-18	18	10	1987	k
8	sadiq	9522db3f484150bb71dcaadbd022fc07	dauda	olalekan		m	1995-10-03	3	10	1995	k

Fig. 17. Table showing number of registered students.

F. Software Requirement

One more important subsystem of a computer system, without it, the system cannot function and it is a predefined logical set of instruction for achieving a task on the computer system. Therefore, the following software is needed;

i. Microsoft Operating systems (Windows XP, Windows Vista, Windows 7) to boot the computer
ii. XAMPP (X-OS Apache MySQL PHP Perl) server
iii. MySQL database Management system
iv. Fingerprint SDK software
v. PHP (Hypertext Preprocessor) programming language
vi. Java Runtime version 8
vii. Netbeans (IDE for java)

G. Programming Language Used

In this work, codes used for the design are in PHP (Hypertext preprocessor) programming language which will function with the use of a server called XAMPP (X-OS Apache MySQL PHP Perl). XAMPP is a server that can run on almost any Windows Operating System as well as other Operating Systems. XAMPP includes Apache, MySQL, PHP, and Perl. PHP is an open-source, HTML (Hypertext Markup Language) embedded Web-scripting language that is compatible with Web servers. PHP enables you to embed code fragments in normal HTML pages code that is interpreted as your pages are served up to Users. Java language was used to develop the applets used for capturing fingerprint image.

H. Performance Evaluation

In evaluating the performance of the proposed system, FAR (False Acceptance Rate) and FRR (False Rejection Rate) are calculated. Table I shows the FAR and FRR of proposed fingerprint identification system. Firstly, we enrolled 122 fingerprint images of students in database, and then to calculate FRR of the proposed system we have tested the system by giving 122 input fingerprint images for identification. During the process of enrolment, problems were encountered as they were some failure to enrol. This was as a result of prolonged usage of the scanner, hard thumbs and moisture effect on the scanner surface. We solved the moisture effect by unplugging the scanner and resetting it on the system and making new attempts to enrol. We had to suspend the process of enrolment until the scanner was ready to perform again, for the hard thumb we made use of spirit to soften it.

False Accept: If an imposter's template is within a given threshold of a genuine user, the imposter may be accepted. The FAR is normally stated, in either fraction or in percentage, the probability of someone else matching as you. FAR is defined by the formula:

$$\text{FAR} = \frac{\text{FA}}{\text{N}} \text{ x } 100 \qquad (5)$$

Where FA is the number of false accept and N is the total number of verification.

False Reject: At authentication, a genuine user may be rejected if an acquired biometric template is of poor quality. This error is known as "false reject", if a user fails to match against his/her own template. This events probability is known as false rejection rate, or FRR. FRR is defined by the formula:

$$\text{FRR} = \frac{FR}{N}\, x\ 100 \qquad (6)$$

Where FR is the number of false reject and N is the total number of verification.

For the performance analysis, the developed system was tested using the bio-data and templates collected from One hundred and twenty-two (122) students of which 90 are students of computer science and computer engineering, while the remaining 32 were from other departments of the institutions. The fingerprints taken were the thumb and fore fingers for the purpose of identification. From the fingerprint image, the minutiae data was extracted and stored in the database to be known as template for the user along with user's ID. At the authentication stage, the user biometric is captured again and minutiae extracted which forms the test template to be matched with what we already have in the database. Here, if the matching score is less than the given threshold, the student is rejected otherwise accepted. From equation 5 –6, Table I gives us the values needed for FAR and FRR carried out from the test.

TABLE I. Test values for FAR and FRR.

False Acceptance Rae (FAR)	False Rejection Rate (FRR)
0.0%	2.46%

Our false acceptance rate was zero (0) percent, which shows that there was no false acceptance rate (no pre-registered person was accepted). We had some cases of false rejection rate (2.46%) from pre-registered students which could be attributed to improper placement of the finger or because the scanner was used for a long time.

TABLE II. Evaluation details.

	Successful Authentication	Unsuccessful Authentication
Student	119	3
Total	119	3

Table II shows the total number of students registered in the system that had successful authentication (119) while of the pre-registered students three (3) had unsuccessful authentication.

TABLE III. Evaluation details.

Number of enrolee	Successful Authentication	Unsuccessful Authentication	Accuracy
122	119	3	97.5%

An accuracy of 97.5% was recorded due to its genuine acceptance rate.

Based on the result evaluation of the study, the developed fingerprint biometric authentication technique for electronic examination has an accuracy of 97.5% and when compared with the existing work in [13], had an accuracy of 99.77%, which was higher than the accuracy obtained in this study. In [14], had an accuracy of 92%, lower than that of this study. Though, in the literature they did not incorporate their techniques with an electronic examination platform and that is what the researcher has done in this study. From the results obtained from the implementation of the work, the fingerprint biometric authentication technique for electronic examination has proven to be reliable in terms of avoiding impersonation, ease problems encountered when using the old method and does not allow unregistered students take part in the examination. The student data is retrieved almost immediately on request, assessed and analysed, easy to understand by the intended users and efficient.

I. System Testing

This is the test that is carried out on the system as a whole. The output of this system testing determines the reliability of the whole system and testing of sub-system is made easier by separate testing of each modular program. After the sub-programs have been tested thoroughly without error, then the system as a whole is tested to ensure that it does the entire task assigned as expected.

Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary units (in parentheses). This applies to papers in data storage**.** For example, write "15 Gb/cm^2 (100 Gb/in^2)." An exception is when English units are used as identifiers in trade, such as "3½-in disk drive." Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity in an equation.

The SI unit for magnetic field strength H is A/m. However, if you wish to use units of T, either refer to magnetic flux density B or magnetic field strength symbolized as $\mu_0 H$. Use the center dot to separate compound units, e.g., "A·m^2."

V. CONCLUSION

This system provides both the students and administrators with ease of access to information needed as well as monitoring of the students by the administrators. This will increase the productivity of institutions and organizations. Results have shown that this system can be implemented in academic institutions and other organization offering similar activities for better results.

Experiments were conducted using SecuGen fingerprint reader to capture live image of students and image enhancement was performed using crossing number concept to extract the enhanced images so as to improve the image quality. It was coded using Java (NetBeans IDE 7.4) to implement algorithms for enhancement, minutiae extraction and matching processing, where the resulting minutiae information was used as a method for identifying and matching fingerprints. The naturalness in the use of fingerprint makes it a better method for access control as this will dissuade students from carrying identity cards or other known documents for identification and authentication during electronic examinations explains the ease of use. Hence, a system with expected results have been developed, however there is still room for improvement of the system. The performance of the system was acceptable and everyone who tested the system was pleased and interested in the product being developed for use in schools.

REFERENCES

[1] S. Mohammed and M. Ilyas, "Challenges of online exam, performances and problems for online university examination." *International Journal of Computer Science Issues*, 10(1-1), 2013, pp. 439-443.

[2] E. Marais D. Argles, "Security issues specific to E-assessments". *8th Annual Conference on www Applications. Conference proceedings, Bloemfontein, South Africa, 2006.*

[3] C. G, King, R. W. Guyette, and C. Piotrowski, "Online exams and cheating: An empirical analysis of business students' views". *The*

Journal of Educators Online, 6(1). Available at: http://www.thejeo.com/Archives/Volume6Number1/Kingetalpaper.pdf, 2009. Retrieved on March 6th, 2013

[4] C. C. Philippe, "Biometric authentication system using human Gait," Unpublished PhD Dissertation submitted to the Swiss Federal Institute of Technology, ETH Zurich, 2002.

[5] G. Qinghai, "Online teaching: Do you know who is taking the final exam"? *Fall 2010 Mid-Atlantic ASEE Conference, Villanova University, United State of America (USA), 2010.*

[6] C. K. Ayo, I. O. Akinyemi, A. A. Adebiyi and U. O. Ekong, "The prospects of e-examination implementation in Nigeria". *Turkish Online Journal of Distance Education,* 8 (4), 2007, pp. 125-135.

[7] A. K. Jain, "Biometric Recognition: How do I know Who You Are"? *Signal Processing and Communications Applications Conference, Proceedings of the IEEE*, 2004, pp. 3– 5.

[8] S. Hocquet, J. Ramel and H. Cardot, "Fusion of methods for keystroke dynamic authentication," *Proceedings of 4th IEEE Workshop on Automatic Identification Advanced Technologies,* USA, 2005, pp. 224 – 229.

[9] M. A. Dabbah, W. L. Woo and S. S. Dlay, "Secure authentication for face recognition," *Proceedings of IEEE Symposium on Computational Intelligence in Image and Signal Processing,* USA, 2007, pp. 121-126.

[10] J. Daugman, "Iris Recognition": The Technology, 2010. Available at http://www.irisscan.com/iris_technology.htm. Retrieved on March 6th, 2013.

[11] T. Ruggles, "Comparison of Biometric Techniques". Available at: http://www.biometric-consulting.com/bio.htm, 2001. Retrieved on March, 6th, 2013

[12] W. Chen, and Y. Gao, "A Minutiae-based fingerprint matching algorithm using phase correlation," *Digital Image Computing Techniques and Applications, IEEE,* 2007, pp. 233-238. Retrieved 23rd July, 2014.

[13] A. S. Chaudhari, G. K. Patnaik, and S. S. Patil, "Implementation of minutiae based fingerprint identification system using crossing number concept," *Informatica Economică*, 18(1), 2014, pp. 17-26.

[14] F. A. Afsar, M. Arif and M. Hussain, "Fingerprint identification and verification system using minutiae matching," *National Conference on Engineering Technologies*, 2004.

[15] S. Prabhakar, S. Pankanti,and A. K. Jain, "Biometrics recognition: Security and privacy concerns," *IEEE Security & Privacy Magazine*, 1(2), 2003, pp. 33-42.