

Development of a Microcontroller Based Fingerprint Examination Access Control System

O. A. Akinola¹, A. Abayomi-Alli² & R. A. Adeniyi³

^{1,3}Department of Electrical and Electronic Engineering

²Department of Computer Science

Federal University of Agriculture Abeokuta

Abeokuta, Ogun State, Nigeria.

¹akinolaoa@funaab.edu.ng, ²abayomiattia@funaab.edu.ng

ABSTRACT

The common access control method for candidates into examination halls in higher institutions is the paper based examination pass. This method is prone to irregularities and human manipulations leading to examination malpractices. This paper presents the development of fingerprint system with an application interface for the integration of the peripherals required for the smooth running of the system. The system algorithm was based on Euclidean distance method and the program codes developed using C-Sharp computer programming language while the user interface was designed using Microsoft Visual studio for the links within the system. The acceptance of fingerprint images was achieved using a Futronic fingerprint scanner which detect and accept fingerprints both in the identification and verification modes of the system. The interconnection of the system and the designed application was done through the integration of the scanner's system development kit. Analyses were carried out using the False Acceptance and False Rejection for 75 candidates. The system testing showed a convenience score of 98.67 % and Security value of 100 % at the threshold value of 25 %.

Keywords: Microcontroller, Fingerprint, Examination, Access Control System.

African Journal of Computing & ICT Reference Format:

O. A. Akinola, A. Abayomi-Alli & R. A. Adeniyi (2015): Development of a Microcontroller Based Fingerprint Examination Access Control System. Afr J. of Comp & ICTs. Vol 8, No. 2, Issue 2. Pp 145-152.

1. INTRODUCTION

Verifying the identity of a person has become a critical and important task in a globally connected society like Nigeria. Cash terminals, access control, examination pass identity, internet transactions are basic examples of security issues where the identities of the users are important and useful [1]. Most universities in Nigeria adopt the use of the paper means of authentication for eligibility of candidates for examinations. This is issued by the university's examinations and record units. This contains vital information needed in identifying candidates. These may include the student's name, the registered courses, matriculation number, passport photographs and school's authentication stamps. This is known as 'examination pass'. It is the method devised by the institution's authorities in identifying eligible candidates for various examinations.

However, it is imperative to note that with the level of information provided in these examination passes, they are still open to students' manipulations as some of the information displayed by this pass can still be tampered with for the sole purpose of impersonation and other examination fraud as the case may be.

Some of these irregularities attached to this paper means of identification include students making several copies of this examination pass and using this as a means of bringing papers to the examination hall, presenting the clean one to the invigilators on the verge of entering the hall and the ones with written substances hidden somewhere in their body to perpetrate examination fraud. Some of these passes as the case may be are sometimes duplicated and then stamped with fake ones fabricated for the purpose of impersonation. Even, the passport photographs are sometimes removed and replaced with another one and in addition, it is not a viable enough to distinguish between two identical twins.

In view of these irregularities and fraud that may arise from the use of the paper based examination pass issuance to students for examination identities, the fingerprints as a form of biometrics (which measures physiological and behavioral characteristics is viable to provide reliable identification system [1] [2] is a better alternative since it is a widely accepted fact that every human being has a unique set of fingerprints. This may be adopted for the sole purpose of proving the eligibility of students for examinations.

The aim of the paper is to design and develop a fingerprint based examination pass system through the design and implementation using C# programming language with a Futronic FS80 scanner. The scanner was integrated using the Standard Development Kit (SDK) from Futronic and the system and its interface was developed with Microsoft Visual Studio 2010.

The system is designed to work basically in three principles, these are:

- The image acquisition stage
- The feature extraction stage
- The pattern matching stage

The image acquisition stage is the most essential part of the project. This involves the acquisition of the images using the fingerprint user interface [3]. The fingerprint user interface of the system is the Futronic FS80 fingerprint scanner through which the images are acquired and stored in the database. The feature extraction stage involves the extraction of the minutiae points in fingerprints. This involves extracting important minutiae of the fingerprints and then forwarding it for storage in the database. This is as important stage and a depending factor in which the matching stage depends on.

The main task of the matching stage is to compare and verify the template fingerprints (the one already stored in the database) and the input pattern (the one to be verified) based on a chosen threshold value set for the matching of the images.

The general model of the system is shown in Figure 1:

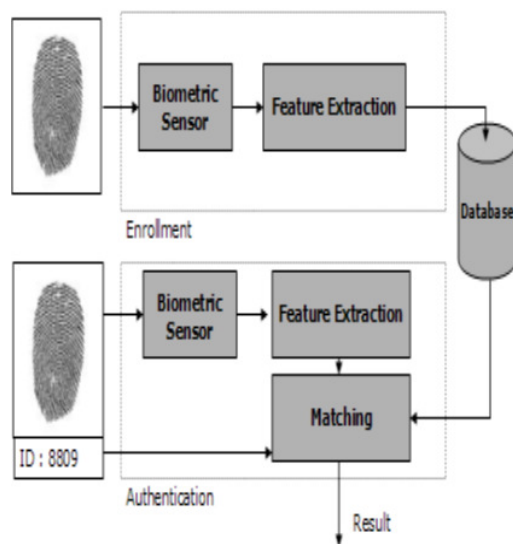


Figure 1: General architecture of the system [4].

2. LITERATURE REVIEW

[4] Proposed a method of fingerprint identification based on minutiae matching. This was achieved through the classification of fingerprints into ridges and valleys. The dark areas of the fingerprints were classified as the ridges while the white areas were referred to as the valleys. These various points are called Minutiae. It is on this that the system designed was based on. The system works based on the recognition of distance of a particular template patterns relative to other minutiae which is to be verified.

The matching of the minutiae is premised on finding enough minutiae in one image with that having corresponding minutiae in another image and then comparing them to know the level of similarity that exist between them. This is then matched together based on the relative distance to other minutiae around it.

[5] Proposed and developed algorithms on fingerprint identification. The study is based on enrolment and authentication. In the enrolment exercise, biometric features are captured and then stored in a database.

The biometric features were detected and then compared with the existing data in the database through some techniques that involve a feature extractor and a biometric matcher cascaded effectively. This research work went further to categorize the sets of algorithms used in the implementation of the system. These are the minutiae, the correlation and the Euclidean based algorithms.

The minutiae algorithm involves extraction of the finger minutiae. This has some constraints as it depends on the image acquired. The correlation algorithm devised a technique which aligns two fingerprint images and subtracts the input image from the template image to see if the ridges correspond. The final algorithm which is the Euclidean distance model involves measuring relative distances between the corresponding features extracted.

[5] Concluded their research work by making reference to two important parameters that are used to determine the reliability of the system built. These are the False Acceptance (FA) and False Rejection (FR). These were used respectively in determining the Security and Convenience of the system.

Another interesting research work which illuminates the world of fingerprint identification is the work of [3]. This work identifies the flaws in minutiae based fingerprint system. The study proposed the Singular Value Decomposition system (SVD) for the acquisition of images, extraction of features and matching of patterns. The first involves acquiring of images through a fingerprint user interface while the feature extraction stage involves the extraction of the features from the images through the Singular Value Decomposition algorithm by splitting it into vectors and taking into consideration, their vectorial positions. The matching stage was achieved through the Euclidean distance algorithm.

[3] Tested for the accuracy and reliability of the system employing the False Acceptance (FA) and False Rejection (FR) in making judgment on the performance of the system built.

3. METHODOLOGY

The system designed works based on three stages;

- The image acquisition stage
- The feature extraction stage
- The pattern matching stage

The image acquisition stage is the most important and a critical section of the fingerprint system. This is because the quality of the fingerprint image captured will go a long way in determining the end output of the system [3]. Thus, the system depends on what is acquired in this stage. The acquisition of the images was achieved through the use of a Futronic FS80 USB 2.0 fingerprint scanner. This as a device makes use of advanced Complementary metal-oxide semiconductor (CMOS) sensor technique and clear optical system to deliver high quality fingerprint image [6]. The feature extraction involves the extraction of the minutiae points for storage into the database which will be used for the matching stage. It is called template pattern. The extraction of the fingerprints is done by the integration of the System Development Kit (SDK) of the scanner (Futronic) into the algorithm. The fingerprint SDK is a software kit that allows synergizing of biometric fingerprints recognition into designed applications [7]. This helps in the extraction of the unique minutiae which is the focal point of the operation of the system.

The matching stage which may be seen as the authentication stage involves comparing the minutiae points from the input patterns (impressed fingerprint) and the template fingerprint (fingerprints in the database) through the use of the Euclidean distance algorithm. The Euclidean distance algorithm involves measuring the distance between any two points that are represented in a two dimensional axes [3]. The axes are the location of the feature vector of the images obtained through the scanner i.e. the fingerprints.

$$\text{Test } X_v = \{x_1, x_2, x_3, \dots, x_n\} \quad (1)$$

and the extracted vectors of the corresponding fingerprint which is stored in the database and then retrieved using the equation;

$$\text{Db } Y_v = \{y_1, y_2, y_3, \dots, y_n\} \quad (2)$$

Then, the Euclidean distance between the two extracted features in representations is calculated as shown below:

$$Ed^2 = (x_1 - y_1)^2 + (x_2 - y_2)^2 + \dots + (x_n - y_n)^2 \quad (3)$$

After the Euclidean distance has been established, a reference threshold of alignment is set in the algorithm for verification such that this set threshold must be reached as matching score between the template and the input pattern for authentication to be granted to the user.

The modes of operation of the system are basically in two ways. These are;

- The Enrolment/Registration mode
- The Authentication mode

The registration mode is the section where the students get themselves registered. The registration mode will capture the name of students, the registered courses, the student's passport photograph through the webcam and the fingerprint of the candidates. This is then saved in the database for proper accessibility when needed. This is shown in the flow chart Figure 2.

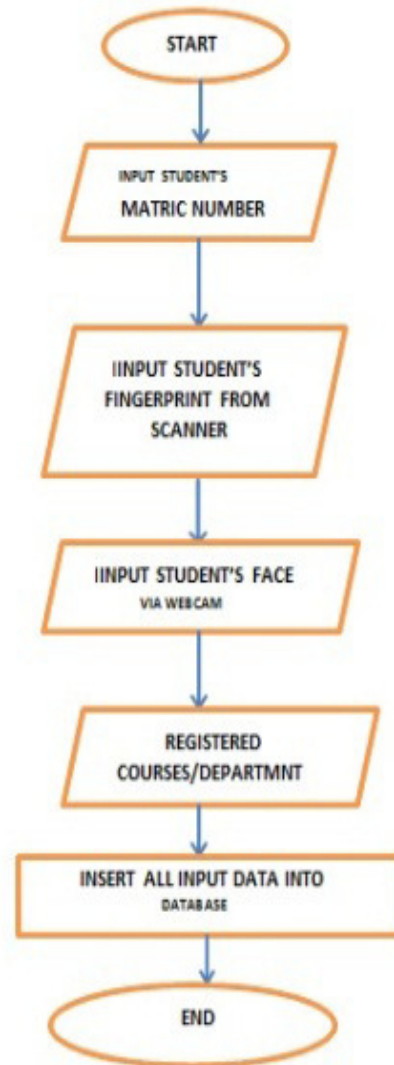


Figure 2: Flow of chart for registration.

The other mode which is the authentication mode involves the students getting themselves verified prior to the start of an examination. Thus, it comes up at the verge of writing an examination. This includes accepting the students once the database of the students captures the name and the course to be written and reject the student if the course is not found in the database of the student. Thus, for the fingerprint system to authenticate, it must have properly enrolled the student into the database. This is shown in the flow chart Figure 3. The procedures followed in the construction of the system were carried out in two phases. These are the software and hardware construction. The hardware construction involves connecting the fingerprint scanner to the PC for proper input of the images.

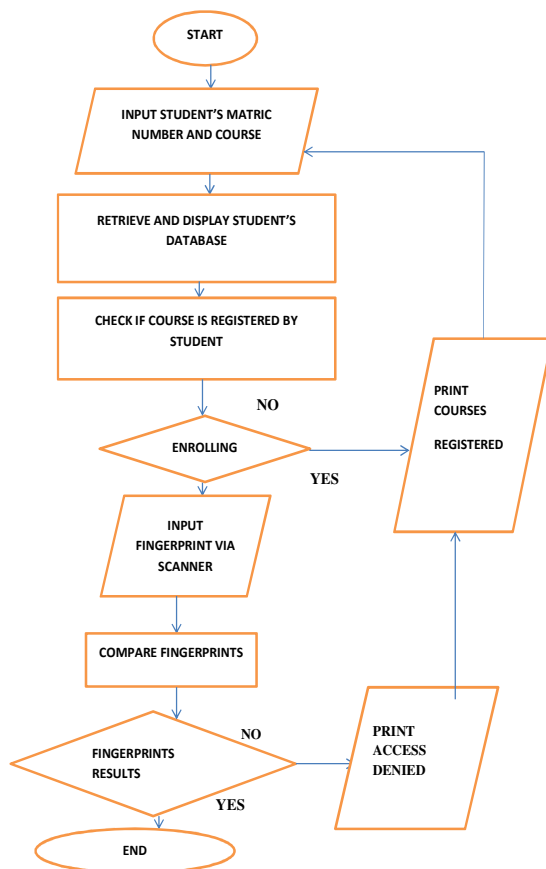


Figure 3: Flow of chart for authentication.

The software construction was achieved through a C# sharp computer programming and the interface was developed using Microsoft visual studio 2010. Four forms were developed (this includes the interface for the enrolment and the verification stages). The database of the system was designed using Microsoft access 2010. The whole software works in line with the System Development Kit (SDK) of the Futronic FS80 scanner.

4. RESULTS AND DISCUSSION

The procedures on how the fingerprint security system is used are in two categories. These are the registration and authentication categories.

The procedures for the registration modes are;

- Open the device interface on the PC.
- Click on 'register' for the registration mode of the system as shown in Figure 4.

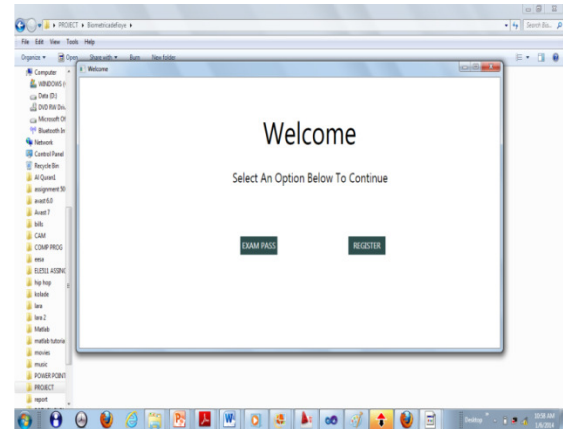


Figure 4: Registration homepage.

- Enter the student's name, matriculation number and the courses for the semester as shown in Figure 5.
- Click on open webcam for the student's passport photograph and once satisfaction of the picture is done, 'capture picture' is then clicked for the passport photograph.
- Then, click on 'select finger' to load in the fingerprint which must have been captured by the fingerprint scanner and then loaded into the interface as shown in Figure 6.
- After the inputs of the data have been satisfactorily done, then, 'register button' is then clicked for the registration and saving of the data into the database of the system.
- A confirmatory message "REGISTRATION IS SUCCESSFUL" is displayed to show that the data has been successfully registered. See Figure 7.

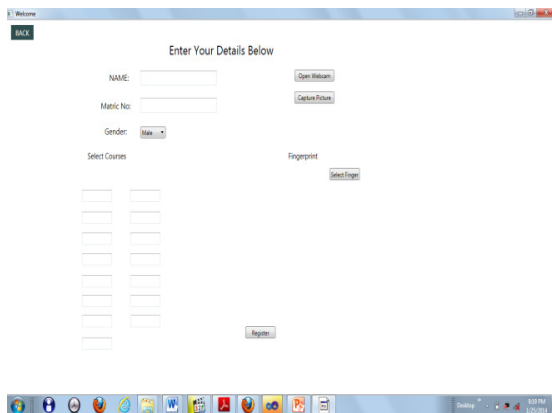


Figure 5: Candidate's information input stage.

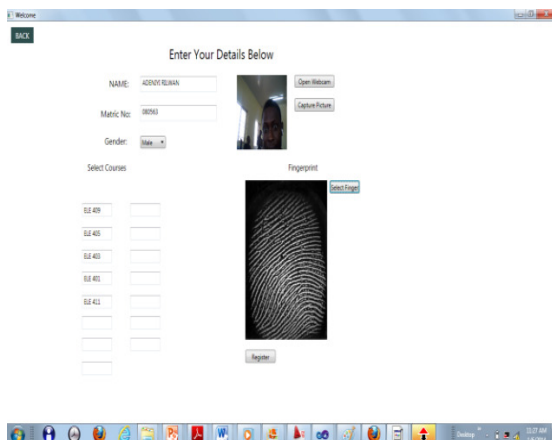


Figure 6: Fingerprint authentication stage.

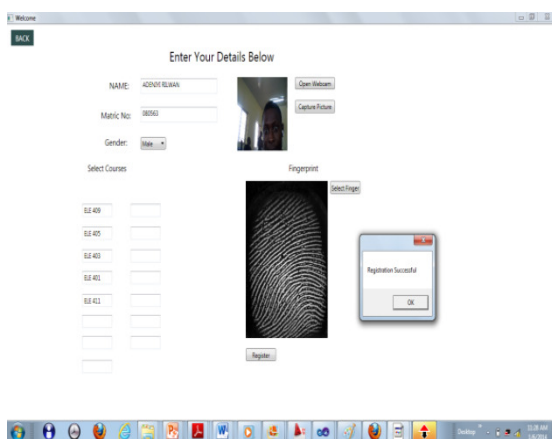


Figure 7: Fingerprint registration stage.

To use the application for the authentication of candidates, the following procedures are followed.

- Click on “Exam Pass” for the verification mode. This is displayed in the welcome interface in Figure 4.
- Enter Matriculation number and the course which is to be written in the examination hall. The interface is shown in Figure 8.

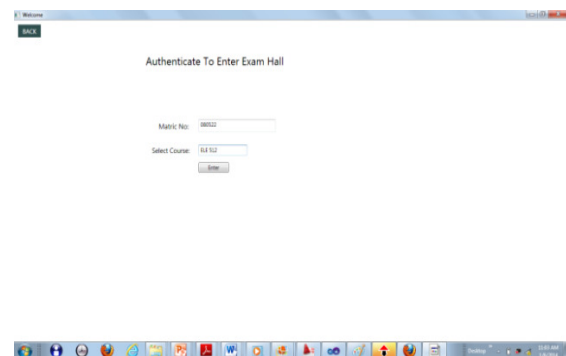


Figure 8: Confirmation of candidate's eligibility into hall.

- Click “enter” to confirm to verify if the student actually register for the course. This is verified through a message which is displayed. The confirmation message along with the interface is shown in Figure 9.
- The passport photograph of the candidate is displayed as a delivery message and the fingerprint stored on the system database. This is clearly shown in Figure 10.
- The fingerprint of the student is then loaded to confirm the eligibility of the student. This is shown in Figure 11.
- To prevent impersonation, the matching score of the fingerprints is displayed along with the fingerprints. It is the final authentication stage. This is clearly shown in Figure 12.

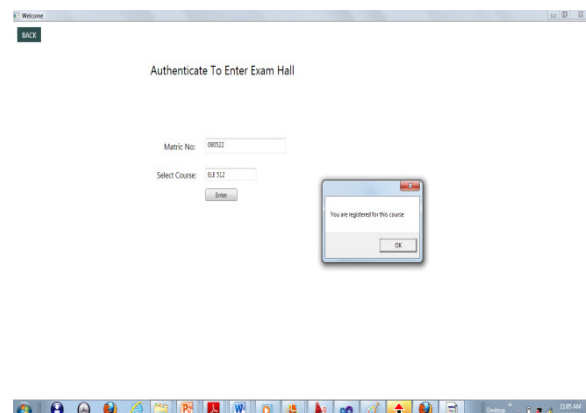


Figure 9: Confirmation of registration of course stage

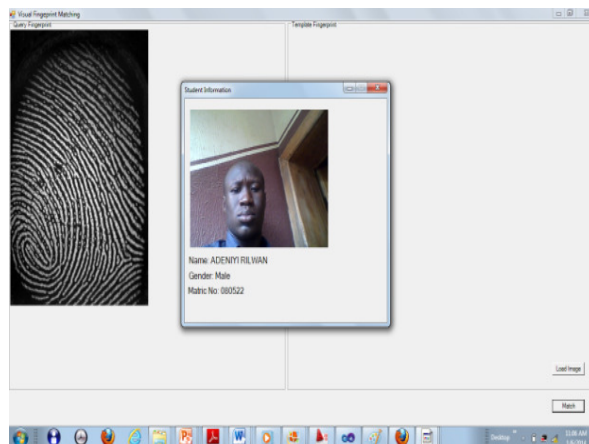


Figure 10: Candidate's fingerprint validation stage.

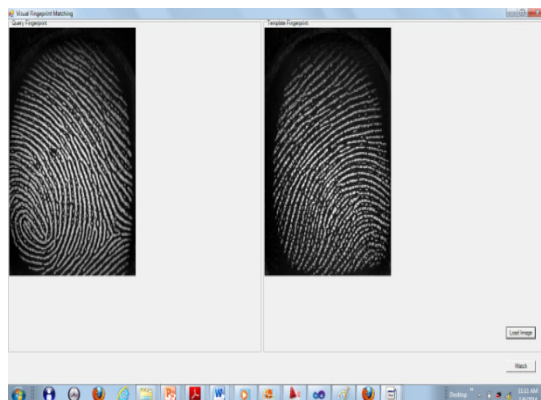


Figure 11: Candidate's fingerprint confirmation stage.

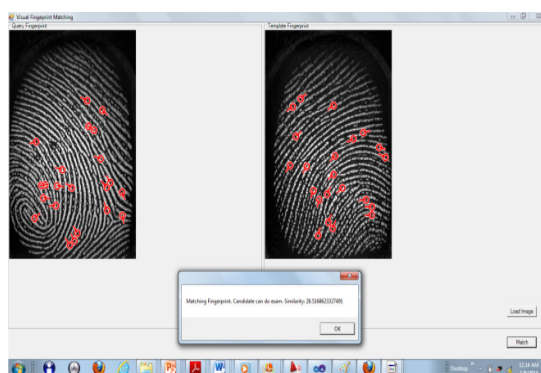


Figure 12: Candidate's fingerprint authentication stage.

4.1 Result Analysis

In testing for the reliability and accuracy of the system (this was done to measure its correctness), two parameters were used. They are the False Rejection (FR) and False Acceptance (FA).

4.1.1 False Rejection (FR)

False rejection is defined as the scenario or instance in which a biometric system is unable or denies authentication of an authorized person [8, 9]. This depends on the image acquired and the threshold value set for the matching of the template pattern and the input pattern.

4.1.2 False Rejection Rate (FRR)

The False Rejection Rate (FRR) is the probability or the measure of the possibility that the fingerprint security system will wrongly or incorrectly reject an attempt to access the system by an authorized user [17]. This is shown mathematically as;

$$FRR = \frac{\text{Number of False Attempt} \times 100}{\text{Number of Identification}} \quad (4)$$

It does not denote a flaw in the biometric system [10]; rather, it shows convenience since it is a function of the threshold value set for the matching of the images.

In testing for the false rejection, candidates were selected and registered and were then authenticated three different times to check if FR may occur.

Table 1: Result of the test carried out on the system.

Total Sample	Threshold Value (%)	FR	FRR (%)
75	25	1	1.333

FR = False Rejection.

FRR = False Rejection Rate.

4.1.3 False Acceptance (FA)

This refers to an instance or scenario in which a security system incorrectly authenticates or verifies an unauthorized person [11, 12]. This is the most important of all biometric security errors since it gives access to an unauthorized user.

4.1.4 False Acceptance Rate (FAR)

This is the probability of a biometric system incorrectly matches the input pattern to a non-matching template in the system's database [10]. This is possible if the impostor's matching score is higher than the threshold set for the matching of the system.

For the determination of FAR, the candidates were registered and after that, three different candidates were asked to impersonate a registered candidate. This was done by trying to break through the system by impressing their fingerprints and then comparing it with the template in the database of the system.

Table 2: Summary of the test.

Total Sample	Threshold Value (%)	FA	FAR (%)
75	25	-	-

FA = False Acceptance

FAR = False Acceptance Rate.

4.2 Convenience

The convenience shows how conducive it is to use the fingerprint system i.e. how the security system analyses the template and the input pattern. The fingerprint system may be designed to have a very high threshold value thus, making the matching score of the pattern (template and input) to be very high for authorized users to authenticate and also, reducing the threshold will also make the matching score so low for authentication.

The convenience of a biometric system depends on the False Rejection Rate (FRR). This is mathematically shows as;

$$\text{Convenience} = 1 - \text{FRR} \quad (5)$$

Using table 1, then we

$$\text{Convenience} = 1 - 0.0133 = 0.9867$$

4.3 Security

This shows how reliable and secured the fingerprint system. This depends on the False Acceptance Rate (FAR) that may occur during the testing of the system. This is shown mathematically as;

$$\text{Security} = 1 - \text{FAR} \quad (6)$$

Since no FAR occur while testing the system, then, it may be concluded that the system 100% is secured and accurate.

5. CONCLUSION

The fingerprint system was developed in two practical modes; the registration and the verification mode. The registration mode was designed to capture the following data; students' name, matriculation number, passport photographs, registered courses and fingerprints which were properly and correctly saved into the database of the system. The authentication mode was designed to confirm the eligibility of candidates for the courses to be taken in the examination from the database. The acceptance of fingerprints was designed with the use of Futronic FS80 scanner while that of passport photographs was designed using the Webcam of the computer system. Hence, the Futronic scanner and webcam are peripherals that work alongside with the computer system in the smooth operation of the system.

The system designed works basically on three criteria. These are the image acquisition stage which involves capturing the image (fingerprint) via the FS80 Futronic scanner. The feature extraction stage is the second stage which involves extracting the important minutiae for the purpose of the matching stage which is the authentication stage. The matching stage then tends to compare the template image and that of the input image based on a 25% threshold value set for the operation of the system.

The system was tested using 75 students in rating its performance. This was premised on the occurrence of False Acceptance (FA) and False Rejection (FR) during the sampling. False Rejection occurred once while False Acceptance did not occur during this exercise. The False Rejection Rate (FRR) gave a Convenience value of 98.67% while False Acceptance Rate (FAR) gave a Security value of 100% making it very reliable and effective biometric system to use in Institutional environments as examination pass. For wider proliferation, the system is coded as a setup and can be installed in computer system for use.

REFERENCES

- [1] www.upcommons.upc.edu/bitstream/2099/1604/1/hardware-software-co-design-fingerprint-biometric-identification.pdf. Data retrieved on 17/11/2014.
- [2] en.m.wikipedia.org/wiki/biometrics. Data retrieved 4/7/2015.
- [3] James Stephen, Prasad Reddy (2012). Implementation of Easy Fingerprint Authentication with Euclidean and Singular Value Decomposition Algorithm. International Journal of Software Computer Application, 3(2), 1-15.
- [4] Andrew Ackerman, Rafail Ostrovsky (2003). Fingerprint Recognition. Available from: <http://www.cs.ucla.edu/honors/thesis.pdf> [Accessed August 2015].
- [5] Lourde M.R., Dushyant K. (2010). Fingerprint Identification in Biometric Security System. Journal of Computer and Electrical Engineering, 2(5), 852-855.
- [6] www.futronic-tech.com/fs80_brochure.pdf. Data retrieved 20/7/2015.
- [7] en.m.wikipedia.org/wiki/fingerprint_SDK. Data retrieved 15/04/2015.
- [8] NSTC Subcommittee on Biometrics (2006). Fingerprint Recognition. National Science and Technology Council.
- [9] Parul Sindha (2012). Minutiae Based Fingerprint Recognition System, Indian Journal of Research, 1(12), 88-90.
- [10] Jain, A. K. (2004). Biometric recognition: how do I know who you are?, 12th IEEE Proceeding on Signal Processing and Communications Applications Conference, 2004, pp.3-5.
- [11] Sri Shimal Das, Jhunu Debbarma (2011). Measure for Enhancing Automated Teller Machine Security in Indian E-banking System. International Journal of Information and Communication Technology Research, 1(5), 197-201.
- [12] Anthony J Bertino (2012). Forensic Science: Fundamentals and Investigation, 2012 Update, Capstone Edition. [Online] Centage Learning Publishers. Available from <http://www.cengage.com/forensicscience> [Accessed 01/06/2015].