IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 4, Ver. I (Jul - Aug 2017), PP 20-25
www.iosrjournals.org

An Automated Door Control System using Biometric Technology

J. O. Odiete, A. O. Agbeyangi & O. Olatinwo
(Department of Computer Engineering, Moshood Abiola Polytechnic, Abeokuta, Ogun State, Nigeria)

Abstract: *Biometric technology has been seen as one of the most effective technology for human secured identification systems. In this paper, we present the development of an automated fingerprint-based door control system to address the shortcomings of the manual door control systems. The developed system used fingerprint sensing device and an application to control the whole system. The fingerprint sensing device controls user identification, enrollment and verification while the application provides access to the system. The control application was implemented using C# programming language. The result shows that the system works as expected and scored 89% from the testing metrics used. There are other issues which can be taken as further research.*

Keywords: *Biometric technology, fingerprint, door automation.*

I. Introduction

Biometric technology is a valuable tool in various fields such as computer security, military, pharmacy, education, etc. The technology has enjoyed widespread acceptance in recent years due to its numerous advantages. It can be classified based on several techniques such as iris recognition, retina scan, vein recognition, fingerprint recognition, and so on. Based on these techniques, a number of solution systems have been developed and investigated to solve different problems, viz. attendance management system, door security management system, etc. Among these techniques, fingerprint recognition is regarded as a reliable approach for automatic personal identification. Over the years, it has received increasingly more attention [1][2]. In [3], fingerprint simply describes the pattern of ridges and valleys on the surface of a fingertip. In Figure 1 (a), a fingerprint pattern is presented. In the figure, the ridges are black and the valleys are white. Its orientation field, defined as the local orientation of the ridge valley structures, is shown in Figure 1 (b). The minutiae, ridge endings and bifurcations, and the singular points, are also shown in Figure 1 (a). Singular points can be viewed as points where the orientation field is discontinuous. Fingerprints are usually partitioned into six classes according to their macro-singularities that include an arch, a tented arch, a left loop, a right loop, a twin loop and a whorl, as shown in Figure 2. Most classical fingerprint recognition algorithms take the minutiae and the singular points, including their coordinates and direction, as the distinctive features to represent the fingerprint in the matching process [4]. According to [5], there are several techniques used for fingerprint matching in biometrics. Examples of fingerprint matching techniques are graph based, minutiae based and pattern matching. For modern embedded fingerprint recognition systems, the minutiae-based matching is often used, simply because the minutiae of the fingerprint are widely believed to be more discriminating and reliable features, and that the template size of the biometric information based on minutiae is much smaller and the processing speed is higher than that of graph-based fingerprint matching. These characteristics are very important for saving memory and energy on the embedded devices.

A variety of sensor types, such as optical, capacitive, ultrasound, and thermal, are used for collecting the digital image of a fingerprint surface. Optical sensors take an image of the fingerprint, and are the most common sensor today. The capacitive sensor determines each pixel value based on the capacitance measured, made possible because an area of air (valley) has significantly less capacitance than an area of finger (friction ridge skin) [6]. Other fingerprint sensors capture images by employing high frequency ultrasound or optical devices that use prisms to detect the change in light reflectance related to the fingerprint. Thermal scanners require a swipe of a finger across a surface to measure the difference in temperature over time to create a digital image [7].

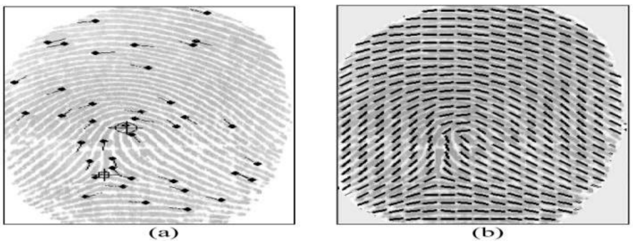


Fig. 1: Fingerprint images
(source: ([3]))

Manual door systems are designed with sub-standard components, and this makes them to be prone to several challenges. Thus, they are inefficient. Therefore, there is need for efficient automated door system to overcome these challenges.

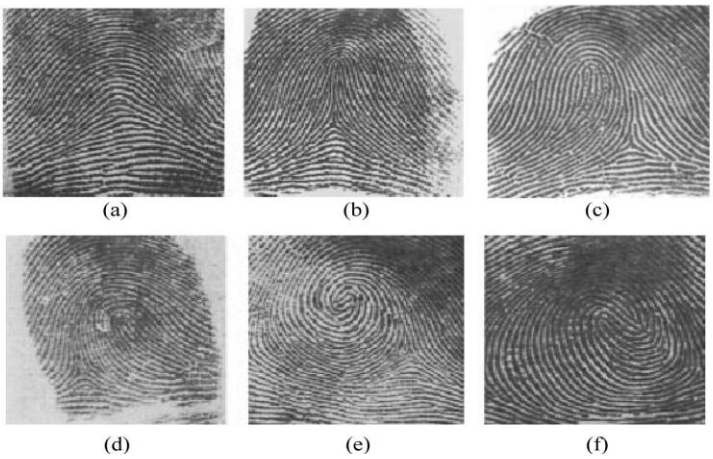


Fig. 2: Fingerprint images types
(source: ([4]))

The rest of the paper is organized as follows: section 2 discusses related works; section 3 examines material and methods used for the research; section 4 discusses the results, while section 5 concludes the paper.

II. Related Works

A number of works have been done on minutiae-based fingerprint matching. Some of them use the local structure of the minutiae to describe the characteristics of the minutiae set [8]. This approach has high processing speed and robustness to rotation and partial prints. However, the local structure usually has less distinct features because it only represents some parts of the whole minutiae set. Prints from different fingers may have quite a few similar local structures by coincidence while prints from the same finger may only have very few similar structures due to the presence of false minutiae and the absence of genuine minutiae. As used in [8], Alignment-based matching algorithms take use of the shape of the ridge connected to minutiae. This might improve system accuracy. However, this approach results in a larger template size because the associated ridges for each minutia must be saved. Research in [9], combines the local and global structures. The local structure is used to find the correspondence of two minutiae sets and increase the reliability of the global matching. The global structure of minutiae reliably determines the uniqueness of a fingerprint miniature.

In [10], a locker system based on biometric and short message service technologies was developed. This study made use of biometric technology for data enrolment, and short message service for passcode generation and authentication. In [11], an office automation system using RFID and GSM technology was developed. This study made use of both RFID and GSM technology to electronically control the opening and closing of door.

Also in [12], a biometrically-controlled door system using iris recognition with power backup to gain access to a place or resource developed. All these works were used as a theoretical tool in the development of our system.

III. Material And Methods

The developed fingerprint-based door control system consists of a number of subsystems, namely, a door with a lock, an interfacing control system, a thumbprint reader and a control program written in C#. The developed control program application which operation depends on sensing of the matched fingerprint with the database template controls the operation of the interfacing control circuit, while the interfacing control circuit controls the operation of the door lock for opening and closing operations.

The framework for the developed system is shown in Figure 3. The stepwise procedures followed in for the system development are:

- Fingerprint acquisition: The acquisition of fingerprint was obtained from the fingerprint sensor hardware and few information about authorized person were also collected through the software interface,
- Feature extraction: Features were extracted from each of the individual fingerprint by using a feature extraction algorithm,
- Template generator: A template was generated for each of the features extracted and finally stored.

- Stored templates: The extracted features were stored as a template in the system database
- Matching: A matching algorithm was applied by the control program
- Evaluation: The performance of the system was evaluated based on time of recognition.

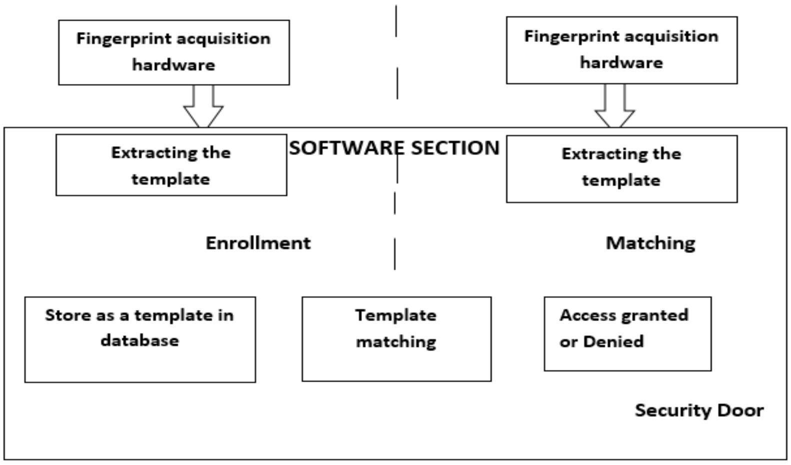


Fig. 3: The System Development framework

An interfacing technique was used to integrate the two important parts of this study, namely the hardware part and the software part.

Hardware Part

The hardware part entails the interconnection of components with the sensor through buses that are compatible with the sensor. It consists of the electrical components connected together on the circuit board serving as a source of power for the lock on the door, the circuit acquires energy from the computer system after the authentication and verification has been done. Figure 4 shows the circuit diagram used. It shows the interfacing of electronic devices with PC using either serial or parallel COM port. The serial port requires DB-9 connector while the parallel port requires a female DB-25 and a special male DB-25p to a centronic male which has 36 pins. The signals from the parallel are TTL compatible with 0v representing logic low and 5v representing logic high and no line driver required. The data line DO (pin2) is used to send signal to the interfacing circuit while pin 25 is used as the ground.

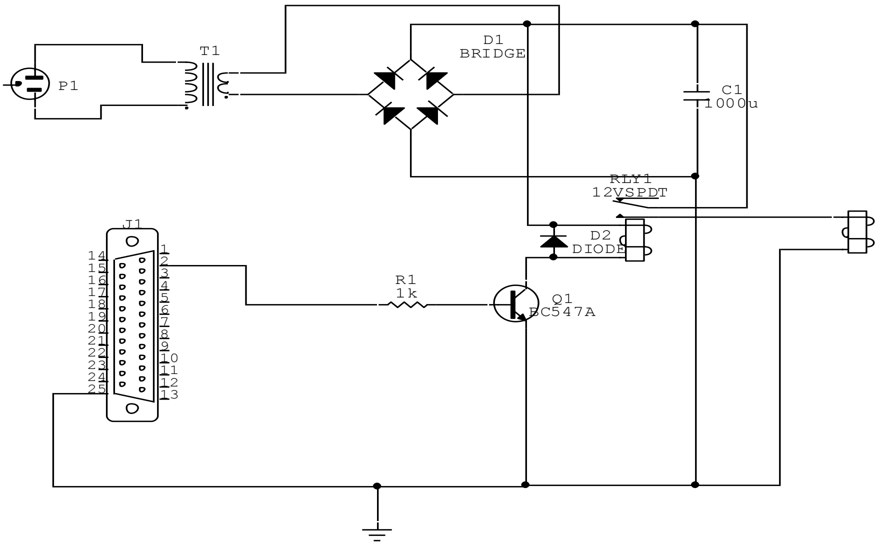


Fig. 4: The System Circuit Diagram

The fingerprint acquisition device used is a fingerprint sensor that detects the patterns on the finger of each person to be saved in the database for verification purpose. The fingerprint sensor used was Gr fingerprint sensor. It is a USB device that is connected to the PC via the USB port. Once the individual places his or her finger on the sensor, the acquired fingerprint is converted into electric signals which are analog in nature. These analog signals are then converted into digital signals via an analog to digital converter (ADC). The digital signals are then fed into the PC via the USB connection through the USB port of the PC. The efficiency of the entire system depends, to a large extent, on the quality of the sensor array. A generic block diagram of the fingerprint acquisition hardware is shown in Figure 5.

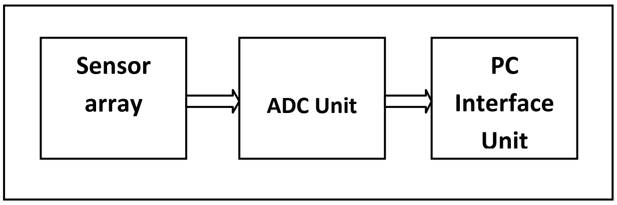


Fig. 5: Data Acquisition Model

Software Part

The software sub-system is the part where most of the functions of the system are implemented. These include the control hardware interfaces, minutiae extraction, database and the template matching process. Its main function is basically the extraction of template from the scanned fingerprint, storing of the acquired template in the database and also the matching of acquired template with the stored template in the database.

As shown in Figure 6, the template is first extracted in the enrollment part and secondly in the matching part. At the enrollment part, the template is extracted from each user to be stored in the database of the system while in the matching part; the template is extracted from each user to be verified with the already stored template of the user during enrollment. The entire fingerprint templates extracted from each person are stored during the enrollment process. Each acquired fingerprint is then compared with the stored template in the database for verification. A matching algorithm was applied by the control program to match the template with the previously stored template in the database. The flowchart of the fingerprint acquisition control process is shown in Figure 7a while the flowchart for the matching and verification process is shown in Figure 7b.

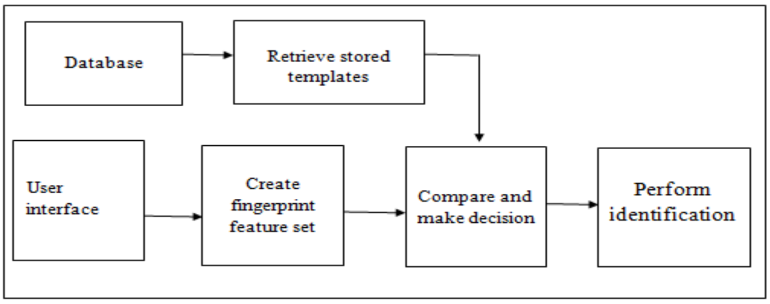
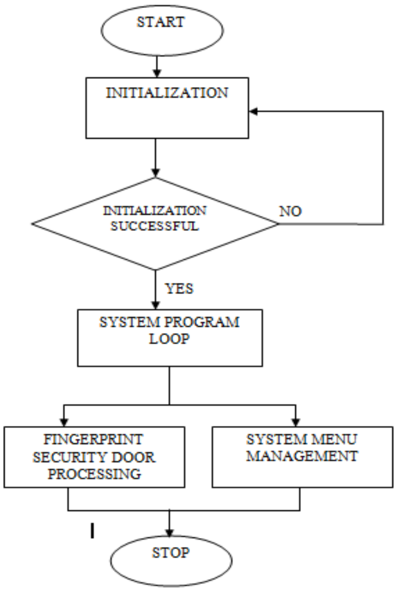

Database
Retrieve stored templates
User interface
Create fingerprint feature set
Compare and make decision
Perform identification

Fig. 6: The System Software Identification Process.



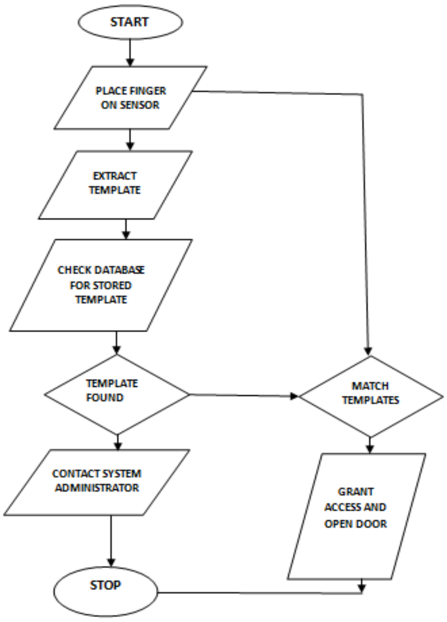
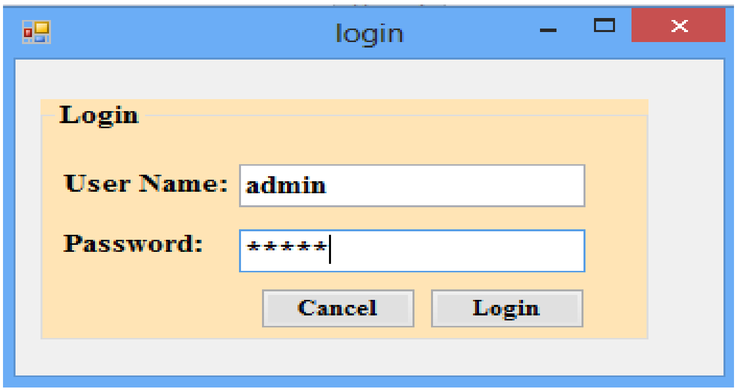

START
PLACE FINGER ON SENSOR
EXTRACT TEMPLATE
CHECK DATABASE FOR STORED TEMPLATE
TEMPLATE FOUND
MATCH TEMPLATES
CONTACT SYSTEM ADMINISTRATOR
GRANT ACCESS AND OPEN DOOR
STOP

Fig. 7a: The System Control Program Process **Fig. 7b:** The Matching and Verification Process

IV. Results And Discussion

The first interface on launching the application is the “Login Page”. The login page gives the administrator access the application. The administrator “username” determines who can access or enable pages like the registration page, admin page and print page. The login display dialog box is shown in Figure 8.



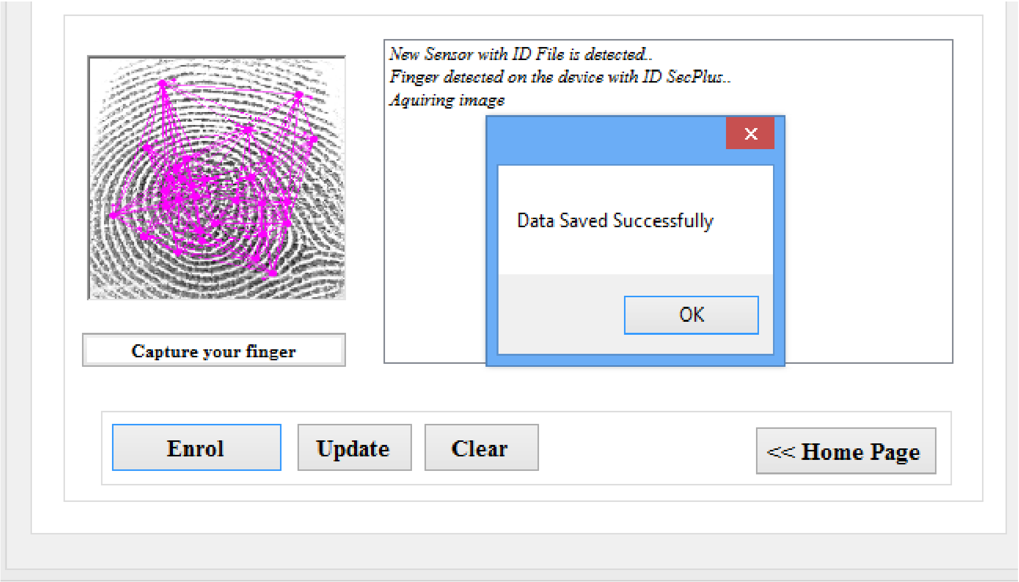
User Name: admin

Password: *****

Fig. 8: The System Application Login Interface

The administrator is the person managing the security features of the system and is responsible for monitoring the various activities of registration and accessibility of individual to gaining access to the door at all-time either to grant access or denied.

The registration page enable individual authorized to access the security door system ability to register via the fingerprint sensor. After supplying the information including the scanned fingerprint, the administrator enrolls such person as one of the authorized user. The page keeps the record of the time and date of registration, which helps in monitoring the actual time and date of registration of individual in case of any emergency. In case of any status update of individual that had accessed, the biodata of such individual can be retrieved by the form number or tag number and finally updated by clicking the “update button”. The registration page interface is shown in Figure 9.

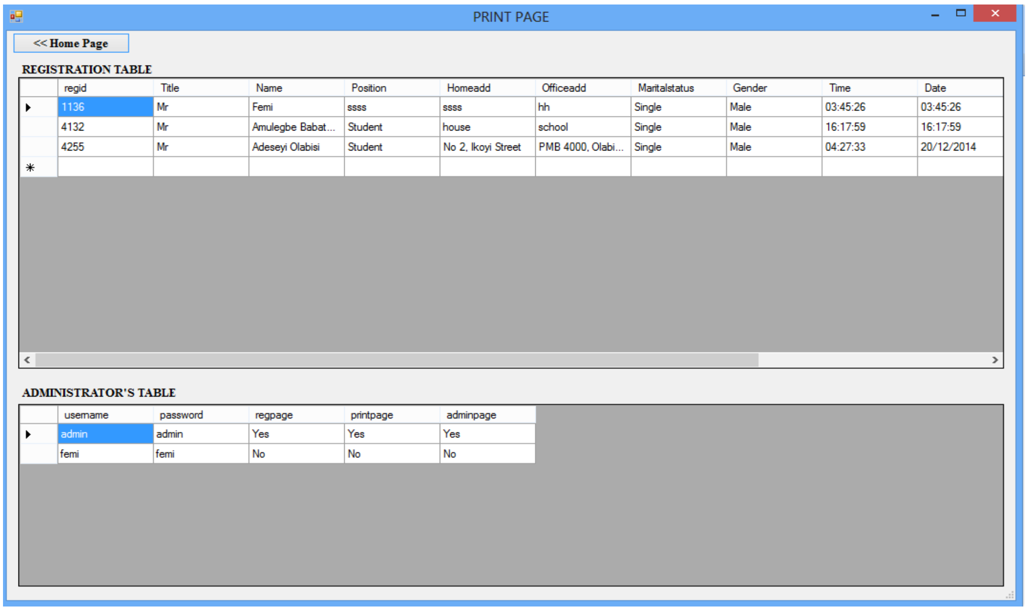


```
New Sensor with ID File is detected..
Finger detected on the device with ID SecPlus..
Aquiring image
```

Data Saved Successfully

Fig. 9: Registration Page Interface

The enrollment tasks can be classified into three steps: image capture, signature extraction and storage. The enrollment list page is shown in Figure 10. It gives a glance into the number of registered individual. The list of authorized users, having access through the security door system and the number of administrator that can login, navigate through the pages of the application and finally monitor the work flow of the whole system are all captured.



REGISTRATION TABLE

	regid	Title	Name	Position	Homeadd	Officeadd	Maritalstatus	Gender	Time	Date
▸	1136	Mr	Femi	ssss	ssss	hh	Single	Male	03:45:26	03:45:26
	4132	Mr	Amulegbe Babat...	Student	house	school	Single	Male	16:17:59	16:17:59
	4255	Mr	Adeseyi Olabisi	Student	No 2, Ikoyi Street	PMB 4000, Olabi...	Single	Male	04:27:33	20/12/2014
*										

ADMINISTRATOR'S TABLE

	username	password	regpage	printpage	adminpage
▸	admin	admin	Yes	Yes	Yes
	femi	femi	No	No	No

Fig. 10: Enrollment List Page

V. Conclusion

The fingerprint-based security door control system development in this study enables door to be electronically operated. It eliminates the challenges attributed to reliance on human security. It requires little or no human intervention in opening and closing the door; thus, a greater level of security and efficiency. The performance of this system in terms of time to recognize user has made it more effective as compared to other existing system.

References

[1] A. Jain, R. Bolle and S. Pankanti, *Biometrics: personal identification in networked society* (Boston: Kluwer Academic Publishers, 1999).

[2] J. D. Woodward, M. Nicholas and P. T. Higgins, *Biometrics* (Osborne, New York: McGraw Hill, 2003).

[3] H. Kang, Biometric identification system by extracting hand vein patterns, *Journal of the Korean Physical Society*, 38(3), 2001, 268-272.

[4] S. Crisan, I. G. Tarnovan and T. E. Crisan , A low cost vein detection system using near infrared radiation, *Proc. IEEE Sensors Applications Symposium*, San Diego, California, 2007.

[5] S. Pankanti and A. K. Jain, Biometric recognition: security and privacy concerns, IEEE Security and Privacy, 1(2), 2003, pp. 33-42.

[6] J. R. Young and H. W. Hammon, Automatic palmprint verification study, *Rome Air Development Center Final Technical Report*, 1981.

[7] J. L.Wayman, Biometric systems technology, design and performance evaluation (London: Springer, 2005)

[8] C. Jain and P. Prabhakar, Handbook of fingerprint recognition (Springer: New York, 2005).

[9] G. Jiang, X. Song, F. Zheng and A. M. Omer, Facial expression recognition using thermal, *Proc. 27th Annual Conference on IEEE Engineering in Medicine and Biology*, 2005.

[10] C. D. Cortez, J. S. Badwal, J. R. Hipolito and J. C. Inalao, Development of microcontroller-based biometric locker system with short message service. *Lecture Notes on Software Engineering*, 4(2), 2016.

[11] M. Patil, and S. Reddy, Design and implementation of home/office automation system based on wireless technologies, *International Journal of Computer Applications*. 79(6), 2013.

[12] A. S. Falohun, E. O. Omidiora, O. A. Fakolujo, O. A. Afolabi, A. O. Oke and F. A. Ajala, Development of a biometrically-controlled door system (using iris), with power backup, *Am. J. Sci. Ind. Res*., 3(4), 2012, 203-207