International Journal of Mechanical Engineering and Technology (IJMET)
Volume 9, Issue 9, Sep 2018, pp. 596-607, Article ID: IJMET_09_09_065
Available online at http://www.iaeme.com/ijmet/issues.asp?JType=IJMET&VType=9&IType=9
ISSN Print: 0976-6340 and ISSN Online: 0976-6359

A BIMODAL BIOMETRIC BANK VAULT ACCESS CONTROL SYSTEM

Kennedy Okokpujie, Odusami Modupe, Etinosa Noma-Osaghae, Olusola Abayomi-Alli, Esther Oluwawemimo

Department of Electrical and Information Engineering,
Covenant University, Ogun State, Nigeria.

ABSTRACT

The bank vault system has security as its most important aim. Banks could go bankrupt if the vault's security system becomes compromised. In this paper, the use of bimodal biometrics (fingerprint and iris) is proposed as a means of ensuring the full integrity of the bank's vault system, thus, further reducing the rate of compromise and theft within the bank's vault system. A scanner captures the fingerprint and the iris of authorized users. The images of the fingerprint and iris captured by the scanner are segmented, normalized and made into templates that are stored in a database along with the particulars of the users. The accuracy of the system is measured in terms of sample acquisition error and recognition performance using False Accept Rate (FAR), False Identification Rate (FIR) and False Reject Rate (FRR). The result shows that the proposed system is very effective.

Keyword: Access Control, Bank Vault, Biometrics, Biometrics, Fingerprints, Security.

Cite this Article: Kennedy Okokpujie, Odusami Modupe, Etinosa Noma-Osaghae, Olusola Abayomi-Alli, Esther Oluwawemimo, A Bimodal Biometric Bank Vault Access Control System, International Journal of Mechanical Engineering and Technology (IJMET), 9(9), 2018, pp. 596-607.
http://www.iaeme.com/ijmet/issues.asp?JType=IJMET&VType=9&IType=9

1. INTRODUCTION

The bank vault is the most important aspect of the banking sector, this is where treasures, valuables, money, records and documents are kept, and any compromise to this section of the bank can lead to the fold up of the bank. Bank vaults are an integral part of the building within which they are constructed using armored walls and a firmly designed door closed with a complex lock. The security of the vault is the single most important aspect of the vault system [1]. The bank vault usually consist of locks that involves a right combination for it to unlock and then two specially designed keys are also used together with the lock combination, these keys are given to two different personnel in the bank to keep and whenever there's a need for anything to be taken out of the vault or to be put inside the vault the two personnel are always required to be around to both unlock and lock the vault system. Despite the security level involved in the bank vault system, there is still the lingering probability of compromise. A

wrongly handled key, a divulged password, a malicious hacker and organized criminal groups can almost easily make a vault system vulnerable.

To prevent the possibility of internal compromise by the staffs of the banks that have been given the duty to keep the keys to the vault and the passcodes of the vault higher level of security such as the use of biometrics has to be implemented. Biometrics technology now has a very wide range of applications in virtually all industries [2].

According to [3] biometric based authentication system has good accuracy for authentication. There were various existing studies about bank-vaults system as far as securing the bank-vaults in which most of the studies had mainly aimed to develop an improved prototype [4]. The work in this paper focus on designing an improved biometric bank vault system using fingerprint and iris recognition. The operational stage of the system is into two stages: the biometric enrollment stage where the fingerprint and the iris of two different individuals will be taken. Templates of the images acquired were stored along with the particulars of the authorized users, in a database. These stored templates were used to identify and authenticate users of the bank's vault system.

2. TECHNICAL BACKGROUND

2.1. Banking Vault System

A bank vault is usually built with respect to the banks specifications and requirements; it has to be built first before the rest of the banks design can be started. The size and shape of the vault is determined by the owners of the bank before the manufacturers of the vault can commence building. The position of the door is also another important aspect of building a vault that will be determined by the bank owners. A bank vault is to be a single unit including floors, walls, ceilings, doors and locks, constructed to be structurally independent of the building where it is sited [5].

2.2. Biometric System

Biometrics is used for automated person recognition. The science of recognizing individuals based on their unique behavioral or physical traits such as iris, fingerprints, face, voice, gait etc. is referred to as biometrics [6]. Sensors are usually used to acquire biometric traits. Biometric systems acquire the unique traits peculiar to it for the first time via a process called enrollment [7]. The unique features of biometric traits are acquired during enrollment. To verify the authenticity of a user, the biometric system makes a comparison between enrolled biometric trait and the query trait. This comparison usually returns a match or mismatch. Biometric traits are unique. Biometric systems utilize the uniqueness of biometric traits to prevent impersonation. Most biometric systems are either Unimodal or Multimodal [8]. The Unimodal biometric system, as the name implies, uses only one biometric trait while the Multimodal system uses more than one biometric trait. According to [9] the use of multimodal method enhances the efficiency of biometric system.

2.3. Fingerprint Recognition

Fingerprints are the most established and most generally utilized type of biometric identification. Every individual's fingerprint is unique. The structure of the ridges and valley on the surface of the fingers is responsible for this uniqueness. Specific points, called minutiae points are used to differentiate fingerprints [10]. In Fingerprint recognition, the distinct ridges on the fingertips produced the impressions from which features are being extracted [11]. Fingerprint image is captured using optical scanner, is enhanced and converted into a template. Algorithms are responsible for determining the level of similarity or otherwise of fingerprints

[12]. There are a few factor that make fingerprint matching an exceptionally difficult issue [13] such as image noise, skin condition, distortions, rotations, displacement, Researchers such as [14] [15] , implemented a fingerprint minutiae-based authentication system. It is mandatory to acquire the optimal displacement and rotation alignment of fingerprints to maximize the quantity of minutiae matched. The most widely used biometric trait is the fingerprint [16]. It is quite accurate and reliable as a biometric identifier. However, fingerprint biometric systems can return a false match or mismatch whenever users fingers were too dry, too wet etc. [17].

2.4. Iris Recognition System

The unique pattern of the iris can be used as a biometric trait for verification and authentication [18]. The Iris has a feature that can be used to accurately differentiate one individual from another. This unique feature of the iris remains the same throughout the lifetime of an individual. According to [19] iris has been accepted as a reliable biometric ever since it was introduced. There are five major steps in iris recognition process: the image of the individual's eye is first acquired through a process called enrollment, segmented to extract the part of the eye image that represents the iris, the unique features are extracted from the iris, normalized, the template of the normalized image is filtered and changed into an iris code that can be used for comparison purposes [20]. These steps are shown schematically in Figure 1. [21] [22] used iris as the biometric identifier to improve security access control. The iris has a very high level of extractable unique features that are genetically independent, stable, and protected by the cornea. Implementation of either iris recognition system or fingerprint recognition system is categorized as a unimodal based biometrics system. The inherent challenges of unimodal biometric systems, such as spoof attack and noise can be overcome by using the multimodal biometric system. The use of more than one biometric trait can solve this problem conveniently [17], [23-25] employed a bimodal biometric identification system in achieving a better accuracy and production output [26-31].

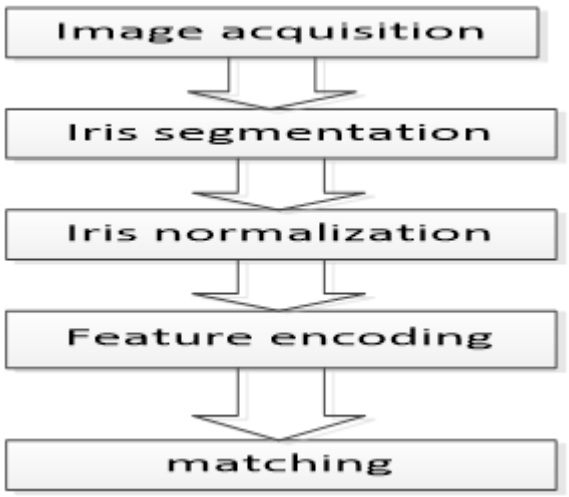

Figure 1 Major Steps of an Iris Recognition System

3. DEVELOPED SYSTEM ARCHITECTURE

This system is centered on two biometric traits of authorized users using the same passcode to improve security and reduce the possibility of compromise within the bank. The system design consists of hardware design and software design, implemented together to actualize a well secure bank vault access control. Figure 2 depicts the block diagram of the system. The system has several hardware components such as the Microcontroller, the Iris Scanner, the fingerprint Sensor, Keypad, LCD, Power Supply Unit and Door mechanism. The microcontroller

PIC18f452 is an 8 bit microcontroller. The fingerprint Scanner is used for the acquisition of an individual fingerprint image for use at the enrollment stage and also to confirm the authentication of individuals claimed identity. The fingerprint sensor has a self-adaptive adjustment mechanism that improves the quality of both dry and wet fingers, one of the advantages of this fingerprint sensor is the low cost and ease of use. The iris scanner is used to capture of iris image acquisition at enrollment and verification of identity. As a feedback to the user on operations of the system, an alphanumeric 20x4 LCD display is used. As an input device to the system, a multiplexed 4x4 matrix keypad is used to communicate with the device. The system's hardware design is shown in Figure 3.

3.1. Description of the Proposed Bank Vault Access System's Software

The complier used during development is the GNU complier. The GNU support various programming languages. The GCC is a major tool in the GNU tool-chain. Eclipse is an Integrated Development Environment (IDE) that was used in this project; it has a lot of unique features that gives the operator a very interactive environment. The ability of the IDE to integrate various plugins makes the IDE a choice for many applications such as C++, C, PHP, VHDL, Java, etc. The needed plugin was CDT (c/CPP Development Tool). The CDT provides a fully functional C based on the Eclipse.

3.2. Operational Principle of the Proposed System

The operation of this system will involve two stages: the biometric enrollment stage where the fingerprint and the iris of two different individuals will be taken to be stored in a database and the identification or authentication stage where the already registered fingerprint and iris will be checked for a match in the database with the new input to grant access into the vault. The system is designed to follow a predefined sequence of steps in an orderly fashion. These steps are: Idle state, Request state, Registration state and authentication state. At the idle state, the system is not being operated upon or used. This is the initial state of the system at start up; it can be changed from this state to another and back. Request state involves the users to press the enter key on the keypad and the state of the machine transit to the request state, where the fingerprint and the iris of the user is requested for, In the case where only the fingerprint is presented without the iris for scanning the system returns to idle state. Registration state occurs only once, and it is the stage where the authorized personnel fingerprint and iris are scanned and stored in the database. At the authentication state, the individual presents his fingerprint or iris to be scanned depending on the biometric trait registered for the individual, the scanner then extracts the features and runs a check with the registered features that are in the database for a match. When match is found the system moves to the authenticated state, if a match is not found then the system returns to the request state.

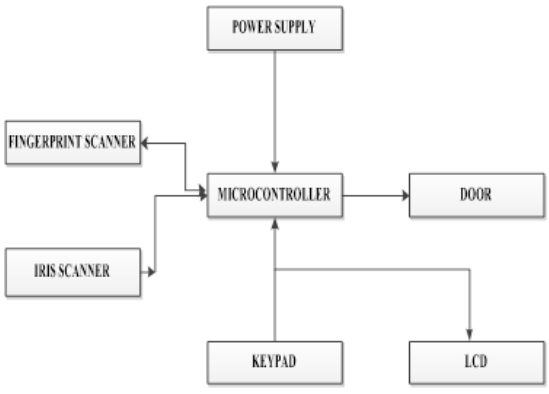

Figure 2 Block Diagram for the Bank Vault's Access System

3.3. Enrolment Stage

Every individual that wants to get authenticated to access what a biometric system protects must first of all enroll. The process involves the use of special scanners to acquire the fingerprint and iris of the user, creating templates of the images after segmenting, extracting the unique features and normalizing the images. Enrollment also gives room for the creation of profiles for users of the biometric system. The flowchart for the enrollment stage is shown in Figure 4.

3.4. Identification and Authentication Stage

Once the individual has been enrolled into the system the user is then given access to the vault. Identification simple means a one to many matches requiring the user to provide either his fingerprint or his iris as a means of identification. The just acquired biometric sample presented for identification is compared to the previously stored sample in the database if there is a match with the fingerprint or iris pattern enrolled, access is provided to the vault door, and otherwise it is declined. The flowchart for the Identification stage is shown in Figure 5.

3.5. The System's Database

A database was created for the different users with the users' information after testing the functionality of the system with different users. The database contained the Admin passcode where after access, creation of users IDs was done with the acquisition of their passcode, their fingerprint and iris details which were later stored in the database for when authentication would be required. The database was developed as shown in the Table 1.

4. PERFORMANCE EVALUATION

The designed and implemented system was tested by carrying out The performance metrics that were used include False Acceptance Rate (FAR), False Rejection Rate (FRR), False Identification Rate (FIR), Enrollment Time (ET), and Response Time (RT). A measure of the frequency of occurrence over all verification attempts expressed as a percentage is the error rate. The system permits several input per attempt. An input is the query biometric trait presented to the biometric system for further processing. The number of valid inputs for which the biometric system returns a mismatch is known as the "False Rejection" rate. The number of invalid inputs for which the biometric system returns a match is known as the "False Acceptance" rate. Twenty individuals were enrolled in the designed system.

Figure 3 The Bank Vault Access System's Hardware

4.1. False Rejection Rate

In order to evaluate false rejection rate, Equation 1 was used. Table 2 shows the parameters for the calculation.

FRR= $NFR/NEIA$ (1)

Where;

NFR is the number of false rejection rates.

NEIA is the number of enrollee identification attempts.

From equation 1, and using the parameters in table 1

FRR =$\frac{5}{200}$ =0.025= 2.5% (2)

Figure 6 depicts the graphs of false rejection rate The graphs shows that the number of authentication system false rejection rate is significantly small compare to the number of times the users try . It is also noticed that the performance of the system is accurate with the false rejection rate of 2.5%.

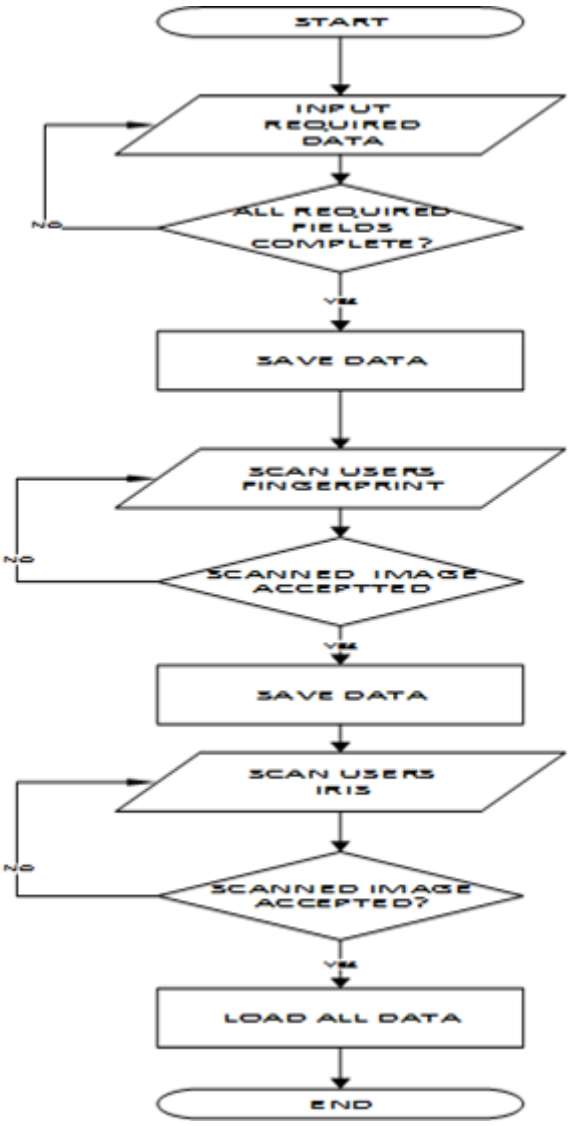

Figure 4 The Flowchart for Enrollment Stage

4.2. Enrolment Stage

FAR= $NFA/NIIA$ (3)

Where;

NFA is number of false acceptance.

NIIA is number of imposter identification attempts

The false acceptance test was conducted on impostors with ten inputs. Each volunteer presents their thumb and iris against his/her biometric. The results of the test are shown in Table 3. From equation 4. FAR is calculated as

FAR= 0/200 = 0 (4)

Figure 7 shows the graph of false acceptance rate at ten inputs . The graphs shows that the authentication system false acceptance error rate is very low.

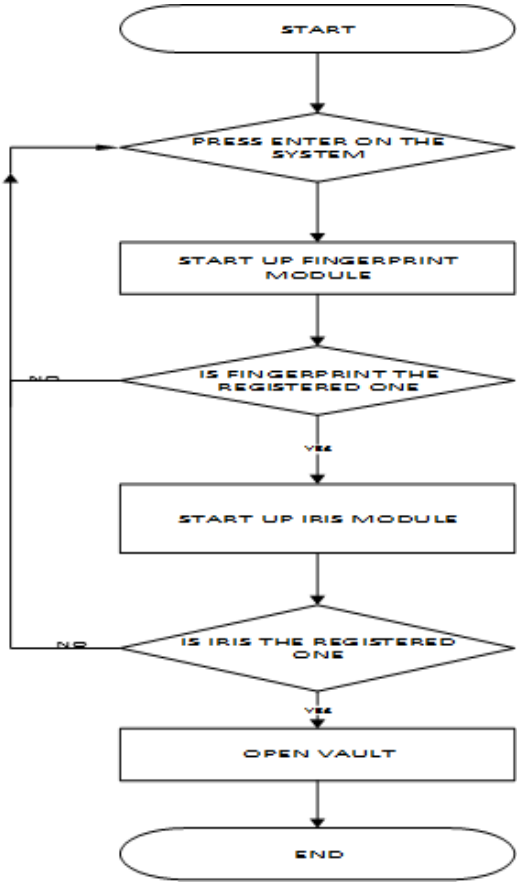

Figure 5 The Flowchart for Identification Stage

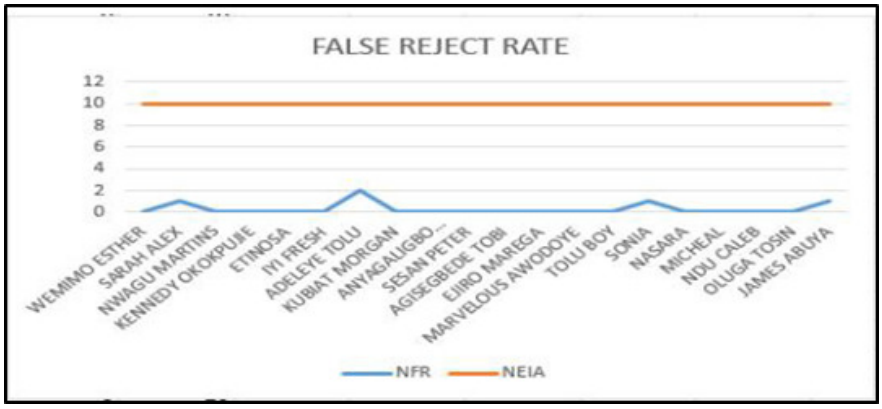

Figure 6 False Rejection Rate

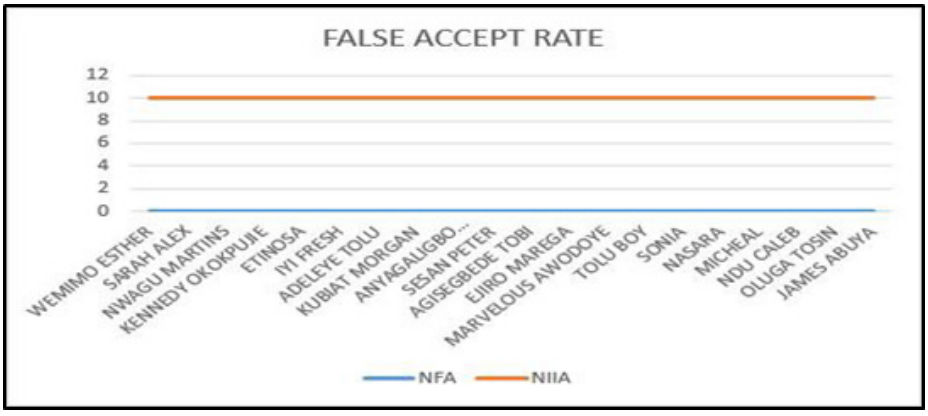

Figure 7 False Acceptance Rate

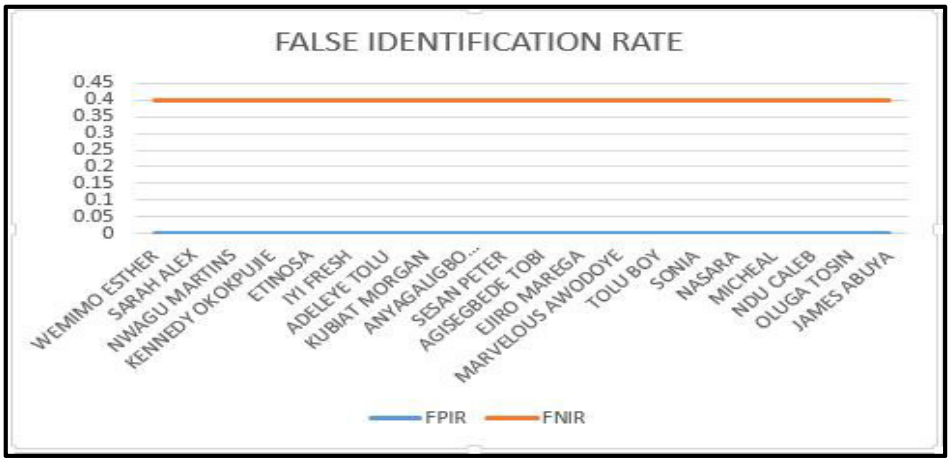

Figure 8 False Identification Rate

4.3. False Identification Rate Error (FIR)

FIR is the probability of marking as identified, candidates that are not on the reference list. This would be the false acceptance rate in the case of verification. The False Positive Identification Rate (FPIR) and the False Negative Identification Rate (FNIR) were used to find the measure of the false identification rate for the implemented bimodal biometric system. These are indicated in equation 5, 6. 7 and 8

FPIR=$1-(1-FAR)^N$ (5)

Table 1 User Database Generated by the Designed System

Name	User ID	Enrollment Pin
Wemimo Esther	USERID 0	1230
Sarah Alex	USERID 1	1231
Nwagu Martins	USERID 2	1232
Kennedy Okokpujie	USERID 3	1233
Etinosa Power	USERID 4	1234
Iyi Fresh	USERID 5	1235
Adeloye Tolu	USERID 6	1236
Kubiat Morgan	USERID 7	1237
Anyagaligbo Precious	USERID 8	1238
Sesan Peter	USERID 9	1239
Agisegbede Tobi	USERID 10	1240
Ejiro Marega	USERID 11	1241
Marvelous Awodoye	USERID 12	1242
Tolu Boy	USERID 13	1243
Sonia Dimukoro	USERID 14	1244
Nasara Belfast	USERID 15	1245
Michael Jordan	USERID 16	1246
Ndu Caleb	USERID 17	1247
Oluga Tosin	USERID 18	1248
James Abuya	USERID 19	1249

Table 2 Mathematical Calculation Parameters

Name	NFR	NEIA
Wemimo Esther	0	10
Sarah Alex	1	10
Nwagu Martins	0	10
Kennedy Okokpujie	0	10
Etinosa Power	0	10
Iyi Fresh	0	10
Adeloye Tolu	2	10
Kubiat Morgan	0	10
Anyagaligbo Precious	0	10
Sesan Peter	0	10
Agisegbede Tobi	0	10
Ejiro Marega	0	10
Marvelous Awodoye	0	10
Tolu Boy	0	10
Sonia Dimukoro	1	10
Nasara Belfast	0	10
Michael Jordan	0	10
Ndu Caleb	0	10
Oluga Tosin	0	10
James Abuya	1	10

FAR= 0, N= 20

FPIR $= 1 - (1 - 0)^{20} = 0$ (6)

FNIR $= 1 - (1 - FRR)^{N}$ (7)

FRR= 0.4, N=20

FNIR $= 1 - (1 - 0.025)^{20} = 0.4$ (8)

Figure 7 indicates the False Identification Rate Graph.

Table 3 False Acceptance Rate

Name	NFR	NEIA
Wemimo Esther	0	10
Sarah Alex	0	10
Nwagu Martins	0	10
Kennedy Okokpujie	0	10
Etinosa Power	0	10
Iyi Fresh	0	10
Adeloye Tolu	2	10
Kubiat Morgan	0	10
Anyagaligbo Precious	0	10
Sesan Peter	0	10
Agisegbede Tobi	0	10
Ejiro Marega	0	10
Marvelous Awodoye	0	10
Tolu Boy	0	10
Sonia Dimukoro	0	10
Nasara Belfast	0	10
Michael Jordan	0	10
Ndu Caleb	0	10
Oluga Tosin	0	10
James Abuya	0	10

4.4. Enrollment Time

This is the time it takes a person to have his or her biometric reference template successfully created. The enrollment time of the system is fifteen seconds because it takes a longer time for the iris scanner to enroll a person.

4.5. Response Time

This is the time required by a biometric system to return a decision on identification of a sample. The response time of the system is twenty five seconds.

5. CONCLUSION

This paper has presented the hardware and software of the design and implementation of a bimodal biometric bank vault access control system based on fingerprint and iris biometric traits. The hardware was implemented using commercial off-the-shelf components with low cost to enable cheap and simple installation. The developed system provides an alternative method that is more accurate and eliminates fraud and compromise as oppose to replace the usual methods of keys and password combinations. The results for FRR and FAR is 2.5% and 0% respectively. The enrollment time of the developed system takes longer time which is a tradeoff for the accuracy of the system. The developed system is comparatively faster than the traditional method of accessing the bank vault. Generally, the developed system has proven the possibility of implementing an automatic access control system based on bimodal biometrics for bank vault. An enhanced multimodal biometrics can be implemented in the future. Also biometrics is vulnerable to errors and can be spoofed, fraudulent reproduction of biometric data is possible, it is recommended to design sensors that can detect liveness in order to prevent spoofing.

ACKNOWLEDGEMENT

The paper is sponsored by Covenant University, Ota Ogun State, Nigeria.

REFERENCES

[1] K. O. Okokpujie, N.-O. Etinosa, O. J. Okesola, J. N. Samuel, and O. Robert, "Design and Implementation of a Student Attendance System Using Iris Biometric Recognition," in Computational Science and Computational Intelligence (CSCI), 2017, Las Vegas, USA, 2017.

[2] N.-O. Etinosa, C. Okereke, O. Robert, O. J. Okesola, and K. O. Okokpujie, "Design and Implementation of an Iris Biometric Door Access Control System," in Computational Science and Computational Intelligence (CSCI), 2017, Las Vegas, USA, 2017.

[3] C. Atuegwu, K. O. Okokpujie, and E. Noma-Osaghae, "A Bimodal Biometric Student Attendance System," 2017.

[4] K. Okokpujie, N.-O. Etinosa, S. John, and E. Joy, "Comparative Analysis of Fingerprint Preprocessing Algorithms for Electronic Voting Processes," in International Conference on Information Theoretic Security, 2017, pp. 212-219.

[5] K.O. Okokpujie, O.O. Uduehi, and F. O. Edeko, "An Innovative Technique in ATM Security: An Enhanced Biometric ATM with GSM Feedback Mechanism," Journal of Electrical and Electronics Engineering (JEEE), vol. 12, pp. Pages 68-81, 2016.

[6] K. Okokpujie, E. Noma-Osaghae, S. John, and A. Ajulibe, "An Improved Iris Segmentation Technique Using Circular Hough Transform," in International Conference on Information Theoretic Security, 2017, pp. 203-211.

[7] K. Okokpujie, E. Noma-Osaghae, S. John, and P. C. Jumbo, "Automatic home appliance switching using speech recognition software and embedded system," in Computing Networking and Informatics (ICCNI), 2017 International Conference on, 2017, pp. 1-4.

[8] K. Okokpujie, E. Noma-Osaghae, S. John, and R. Oputa, "Development of a facial recognition system with email identification message relay mechanism," in Computing Networking and Informatics (ICCNI), 2017 International Conference on, 2017, pp. 1-6.

[9] K. Okokpujie, F. Olajide, S. John, and C. G. Kennedy, "Implementation of the Enhanced Fingerprint Authentication in the ATM System Using ATmega128," in Proceedings of the International Conference on Security and Management (SAM), 2016, p. 258.

[10] K. Okokpujie, O. Uduehi, and F. Edeko, "An Enhanced Biometric ATM with GSM Feedback Mechanism," Journal of Electrical and Electronics Engineering, vol. 12, pp. 68-81, 2015.

[11] K. O. Okokpujie, E. Noma-Osaghae, G. Kalu-Anyah, and I. P. Okokpujie, "A Face Recognition Attendance System with GSM Notification," 2017.

[12] M. S. Sayemul Islam, "<Design-of-a-Bank-Vault-Security-System-with-Password-Thermal-Physical-Interrupt-Alarm.pdf>," vol. 4, 2013

[13] Ogbanufe, O. and Kim, D.J., 2017. Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. Decision Support Systems.

[14] Belguechi, R., Cherrier, E., Rosenberger, C. and Ait-Aoudia, S., 2013. An integrated framework combining Bio-Hashed minutiae template and PKCS15 compliant card for a better secure management of fingerprint cancelable templates. computers & security, 39, pp.325-339.

[15] Addy, D. and Bala, P., 2016, September. Physical access control based on biometrics and GSM. In Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on (pp. 1995-2001). IEEE.

[16] Kihal, N., Chitroub, S., Polette, A., Brunette, I. and Meunier, J., 2017. Efficient multimodal ocular biometric system for person authentication based on iris texture and corneal shape. IET Biometrics, 6(6), pp.379-386.

[17] A. Jain, A. Ross, K. Nandakumar, "Introduction to Biometrics", Springer Science & Business Media, 2011.

[18] Oluwadamilola, K.O., Ayodeji, A.O., Martins, O.O., Olufunmi, I.S. and Rapheal, O.A., 2017, November. An improved authentication system using hybrid of biometrics and cryptography. In Electro-Technology for National Development (NIGERCON), 2017 IEEE 3rd International Conference on (pp. 457-463). IEEE.

[19] S. Shukla and P. Mishra, "A Hybrid Model of Multimodal Biometrics System using Fingerprint and Face as Traits," no. 1, pp. 406–410, 2012.

[20] D. P. S. Roli Bansal, Dr. Punam Bedi "Minutiae Extraction from Fingerprint Images - a Review," vol. 8, 2011.

[21] Jagadiswary, D. and Saraswady, D., 2016. Biometric authentication using fused multimodal biometric. Procedia Computer Science, 85, pp.109-116.

[22] F. Besbes, H. Trichili, and B. Solaiman, "Multimodal biometric system based on Fingerprint identification and Iris recognition," in Proc. 3rd Int. IEEE Conf. Inf. Commun. Technol.: From Theory to Applications, ICTTA pp. 1–5. 2008.

[23] D. Maltoni, D. Maio, A.k. jain, S. Prabhakar, Handbook of Fingerprint Recognition, second ed, Springer Publishing Company, Incorporated, 2009.

[24] Li, P., Yang, X., Cao, K., Tao, X., Wang, R. and Tian, J., 2010. An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. Journal of Network and Computer Applications, 33(3), pp.207-220.

[25] Benhammadi, F. and Bey, K.B., 2014. Password hardened fuzzy vault for fingerprint authentication system. Image and vision computing, 32(8), pp.487-496.

[26] K Okokpujie, E Noma-Osaghae, O Okesola, O Omoruyi, C Okereke, S John, IP Okokpujie. Integration of Iris Biometrics in Automated Teller Machines for Enhanced User Authentication. InInternational Conference on Information Science and Applications 2018 Jun 25 (pp. 219-228). Springer, Singapore.

[27] K Okokpujie, E Noma-Osaghae, O Okesola, O Omoruyi, C Okereke, S John, IP Okokpujie. Fingerprint Biometric Authentication Based Point of Sale Terminal. InInternational Conference on Information Science and Applications 2018 Jun 25 (pp. 229-237). Springer, Singapore.

[28] KO Okokpujie, EC Chukwu, E Noma-Osaghae, IP Okokpujie. Novel Active Queue Management Scheme for Routers in Wireless Networks. International Journal on Communications Antenna and Propagation (I. Re. CAP). 2018;8(1):53-61.

[29] KO Okokpujie, M Odusami, IP Okokpujie, O Abayomi-Alli. A Model for Automatic Control of Home Appliances using DTMF Technique. International Journal of Scientific & Engineering Research. 2017 Jan 26;8(1):266-72.

[30] KO Okokpujie, A Abayomi-Alli, O Abayomi-Alli, M Odusami, IP Okokpujie, OA Akinola. An automated energy meter reading system using GSM technology

[31] SE YEKINI, IP Okokpujie, SA Afolalu, OO Ajayi, J Azeta. Investigation of production output for improvement. International Journal of Mechanical and Production Engineering Research and Development. 2018;8(1):915-22.