BOOK OF PROCEEDINGS

Series 9 Vol. 1

ISTEAMS

Cross-Border Multidisciplinary Conference 2016

Theme:

Addressing Human-Centred **Challenges**

Through Multidisciplinary Innovations & Inter-tertiary Collaborations.

Date: 21st - 23rd March, 2016.

Venue: University of Professional Studies, Accra Ghana

Editors:

PROF. LONGE O.B.
Adeleke University, Ede, Nigeria.

Dr. Ibrahim Mohammed
University of Professional Studies, Accra, Ghana.

PROF. ADEKUNLE OKUNOYE
Xavier University, Cincinati, Ohio USA

Dr. Jimoh Rasheed
University of Ilorin, Nigeria.

Secure Fingerprint Authentication System for Electronic Examination Using Enhanced Advance Encryption Standard

[1]Uhunamure, O. H., [2]Inyiama, H. C.,[3]Olaniyi, O. M., [4]Ameh, I. A.
[2,2]Department of Computer Science
[3,4]Department of Computer Engineering
Federal University of Technology, Minna, Nigeria
E-mail: harryuhunamure@gmail.com
Phone: 08037833722

ABSTRACT

The emergence of biometric technology has provided a more secure approach to tackle the inherent deficiencies in the traditional authentication methods. As technology advanced, data intrusion became common and cheap attack can be carried out on stored data, like electronic examination scenario. This data intrusion and attack renders the information insecure and prone to intruders, hence, candidates can be impersonated without the fingerprint authentication system detecting the fraud. In this work, a secured fingerprint authentication system was designed using enhanced Advanced Encryption Standard for the administration of electronic examination. This was achieved by designing a prototype of the model and evaluating the performance of the prototype system using False Matching Rate, (FMR), False Non Matching Rate (FNMR) and Average Matching Time (AMT) performance metrics. The result obtained shows that at a scanner sensitivity rate of 0.8000, there is a certainty of the same FMR and FNMR (0.0064). This implies that about 6 out of every 1000 impostors attempts would be falsely accepted and same number genuine attempts would be falsely rejected. The large scale implementation of the developed prototype could be used to curb the activities of malicious candidate and improve the integrity of result awarding institution through validation of candidates during electronic–examination.

Key words: Key words: *False Acceptance Rate, False Rejection Rate, Equal Error Rate, Correct Recognition Advanced Encryption Standard, Threshold, Examination.*

1. BACKGROUND OF THE STUDY

Biometric Technology uses computerized methods to identify a person by their unique physical or behavioural characteristics. The biometric recognition of an individual is the use of certain physiological or behavioural features to determine the identity of a person. Traditionally knowledge-based security such as passwords and token-based security such as Identity cards are used for access control to restricted systems or places, (Shashi, Chhotaray, Raja & Sabyasachi, 2010). However, these systems are prone to fraud when a password is divulged to an unauthorized user or a card is stolen. Furthermore, simple passwords are easy to guess by an impostor, while difficult passwords may be hard to recall by a legitimate user.

The biometric technology is based on several parts of human body such as face, fingerprint, palm print, iris, retina, and behavioural characteristics such as signature, voice. The biometric validation of a person has several advantages compared to other validation systems such as the use of smart cards, Personal Identification Number (PIN), password, credit cards and debit cards. This is because it obviates the need to remember a password/PIN which may be forgotten, or the need to carry the tokens like passports and driver's licenses which may be stolen, forged or lost. Biometrics has the capability to distinguish between an authorized user and imposter. The emergence of biometric technology has provided an attractive alternative to solve the problems present in traditional verification methods. Finger scan Technology is a biometric science which uses unique features of the fingerprint to identify or verify the identity of individuals (Senthil & Vijayaragavan, 2014). From security perspective, fingerprint consists of sensitive information that has to be protected. Towards this direction, the method discussed in this research isolates the fingerprint of the candidate which is stored for future reference. Fingerprint is the impression of the minute ridge (called dermal) of the finger. Fingerprint ridges are unique and unalterable, (Ravi & Dattatreya, 2013). Individuals, schools or agencies can access this information for the purpose of verification in order to authenticate candidates' results.

Fingerprint has been the most practical and widely used biometric technique in personal identification for several centuries. Among all the other kinds of popular personal identification methods; knowledge-based security such as passwords and token-based such as identity cards, fingerprint identification is the most matured and reliable technique (Shashi*et al.*, 2010; Hartwig& Klaus, 2008). Uniqueness and permanence are the two properties of fingerprint identification. With the exception of permanent scare and or significant injury to the finger, it is believed that no two individuals including identical twins have the same fingerprints and a fingerprint does not change throughout the lifetime (Ravi &Dattatreya, 2013). Fingerprint recognition takes advantage of the fact that the fingerprint has some unique characteristics such as minutiae and the ridges.

The minutiae points are the ridge endings or the bifurcation branches of the finger image. The relative position of these minutiae is used for comparison, and according to empirical studies carried out, two individuals (including twins) will not have eight or more common minutiae (Shiv and Anshul, 2012). Usually, live-scan finger print contains between 30 and 40 minutiae. Fingerprint technology is used by hundreds of thousands of people daily to access network Personal Computers (PCs), Physical Security/Time, Attendance and Civil Identity (ID). Many military bases, Banks and Government buildings use computers to check fingerprints of employees before they are admitted to secure areas.

In forensic applications, fingerprints are used for criminal investigation, terrorist identification, parenthood determination, missing children. In Government applications, it is used for. In this paper secure biometric fingerprint authentication system is developed for electronic examination application.

This system is meant to verify and validate that examination candidates for‘‘who’’ they claimed to be using the developed enhanced Advanced Encryption Standard (AES). This will eliminate the incidences of impersonation in electronic examination. Biometric technology is used as a means to stem the increasing rate of examination malpractice resulting from impersonation of candidates in the conduct of examinations. The use of secure fingerprint authentication system for electronic examination using enhanced AES ensures that the person who registers for an examination is the same person who sits for specific examination.

National Identity Cards, correction facility, driving license, passport control, signing-in signing-out in offices, election process. Considering commercial applications, fingerprints are useful in computer network logic, electronic data security and identification at banks, e-commerce, internet access, Automated Teller Machine (ATM), credit cards, cellular phones, medical record management and access to allocated rooms in hotels. One of the most transformative technologies of our time is perhaps the Internet. This has opened doors to so many innovations.

2. STATEMENT OF THE PROBLEM

In today’s digital age, database intrusion is common and cheap attacks are carried out by various kinds of intruders. This causes a potential risk of data theft, as well as real-time biometric data manipulation in the database by vicious intruders. For example, an impersonator’s biometric data can be used by an intruder to over-write the original biometric data collected of the candidate during registration. This renders the information insecure as a candidate can be impersonated without the Fingerprint authentication system detecting the fraud. As a result of this, the aim of using fingerprint for authentication and verification will be defeated. With respect to aforementioned problem, this work seeks to authenticate duly registered candidates for e-examination.

3. AIM AND OBJECTIVES OF THE STUDY

The major aim of the study is to develop a secured Fingerprint Authentication System using Enhanced-AES cryptography. While the objectives are to design fingerprint authentication system using enhanced AES, to implement a prototype of the designed model and to evaluate the performance of the system using FMR, FNMR and AMT performance metrics

4. METHODOLOGY

4.1 SYSTEM OVERVIEW

The system design is made up of four modules which are database module, encryption module, matching module and decision module. The data module consists basically of a fingerprint sensor for capturing live fingerprint scans and the candidate’s registration application through which student’s data are captured. Fingerprint images from this module are transferred to the feature extraction module where the extraction is done. After extraction, the features are then stored in the database module in the form of templates. The database module contains all enrolled students data along with their respective biometric templates. The matching module comprises of the pattern matching algorithm necessary for the measurement of resemblance between two biometric samples. The process of pattern matching involves the comparison of the biometric data of an unknown user to a biometric template in the database. The decision module uses the result of the matching process to either grant access or deny access.

4.2 SYSTEM ARCHITECTURE

The System architecture of the proposed fingerprint Authentication System Using AES cryptographic technique which is composed of four modules is shown in Figure 1.

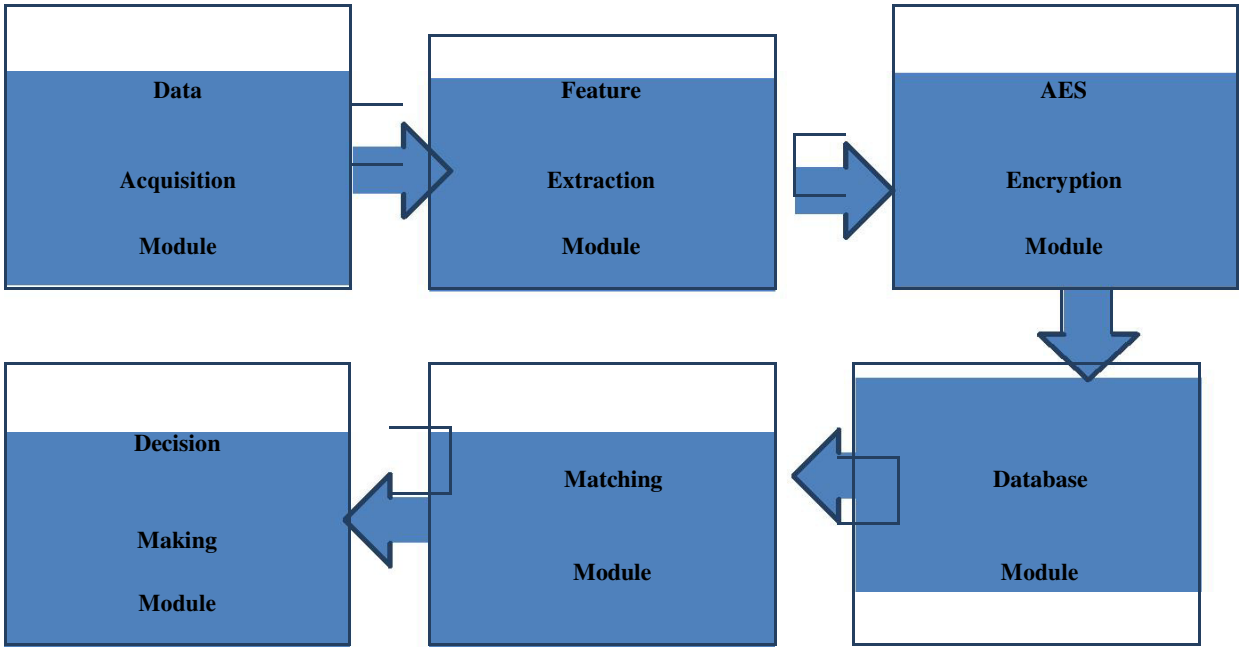

Figure 1: Block Diagram of the Fingerprint Authentication System

Candidates' enrollment at registration centres where their registration data and biometric data are taken occurs in the data acquisition module. The minutiae features are extracted in the feature extraction module by the feature extraction algorithm. The fingerprint matching algorithm makes up the matching algorithm and the decision making module grants or denies access to the examination hall.

4.2.1 The Data Acquisition Module

A fingerprint verification system constitutes of two processes, one at the point of enrolment or registration for the examination and another at the point of authenticating the features acquired during registration. The two processes involve the use of a fingerprint acquiring device (sensor) and feature extractor. At registration point after features are extracted they are stored for future reference (fingerprint information database).

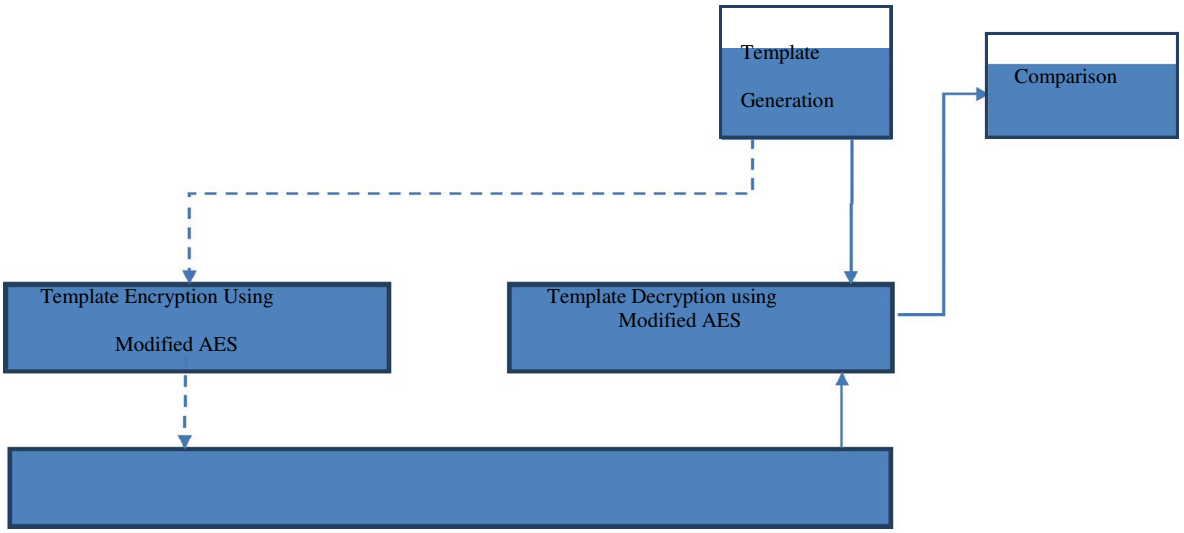

Figure 2: Modified Typical Structure of Fingerprint Authentication System

For the acquisition of fingerprint, optical or semi-conduct sensors are used. They are very high efficient and have acceptable accuracy except for some cases that the user's finger is too dirty, injured or dry. However, the template in database for this thesis will isolate bad cases. The minutia extractor and minutia matcher shall be explained in detail in the next part for algorithm design and other subsequent sections. At verification point, there is comparison between the stored information and the newly introduced fingerprint. Thereafter the result is generated accordingly.

4.2.2 Candidates Enrollment

At the point of registration, biometric and non-biometric data of Candidates are collected. The followings are the non-biometric data: age, sex, state of origin, Address and Subject Combination. The candidates' age is necessary information captured during the registration process. It reflects how old they are. For the purpose of this research, the candidates were grouped by age for easy evaluation as presented in Table 1. The candidates subject combination gives an insight into the groupings of different subjects which they intend to write in the examination. The subject group include: Core, Science, Humanity, Technology, Trade, Language and Business as shown in Table 1.

Table 1: Classification of subjects into different groups

Subject Group	Subjects
Core	Mathematics, English, Civic & one of the Trade Subjects
Science	Physics, Biology, Chemistry, Agric Science
Humanity	Geography, Economics, Arts, Government
Trade/Entrepreneurship	Photography, Word Work, Metal-Work
Business	Financial Accounting, Commerce
Technology	Technical Drawing, ICT
Languages	Edo, Efik, Hausa, Ibibio, Igbo, Yoruba

The biometric, fingerprint images are obtained through the fingerprint sensor. These set of images are only accepted when they all have the same pixel resolutions.

4.2.3. Candidate Authentication

Candidate Authentication process begins at the point of entry during examination. The Candidate is asked to place any of the four fingers used during registration on the sensor. The sensor captures a probe and compares it with the templates in the database as shown in Figure 3.

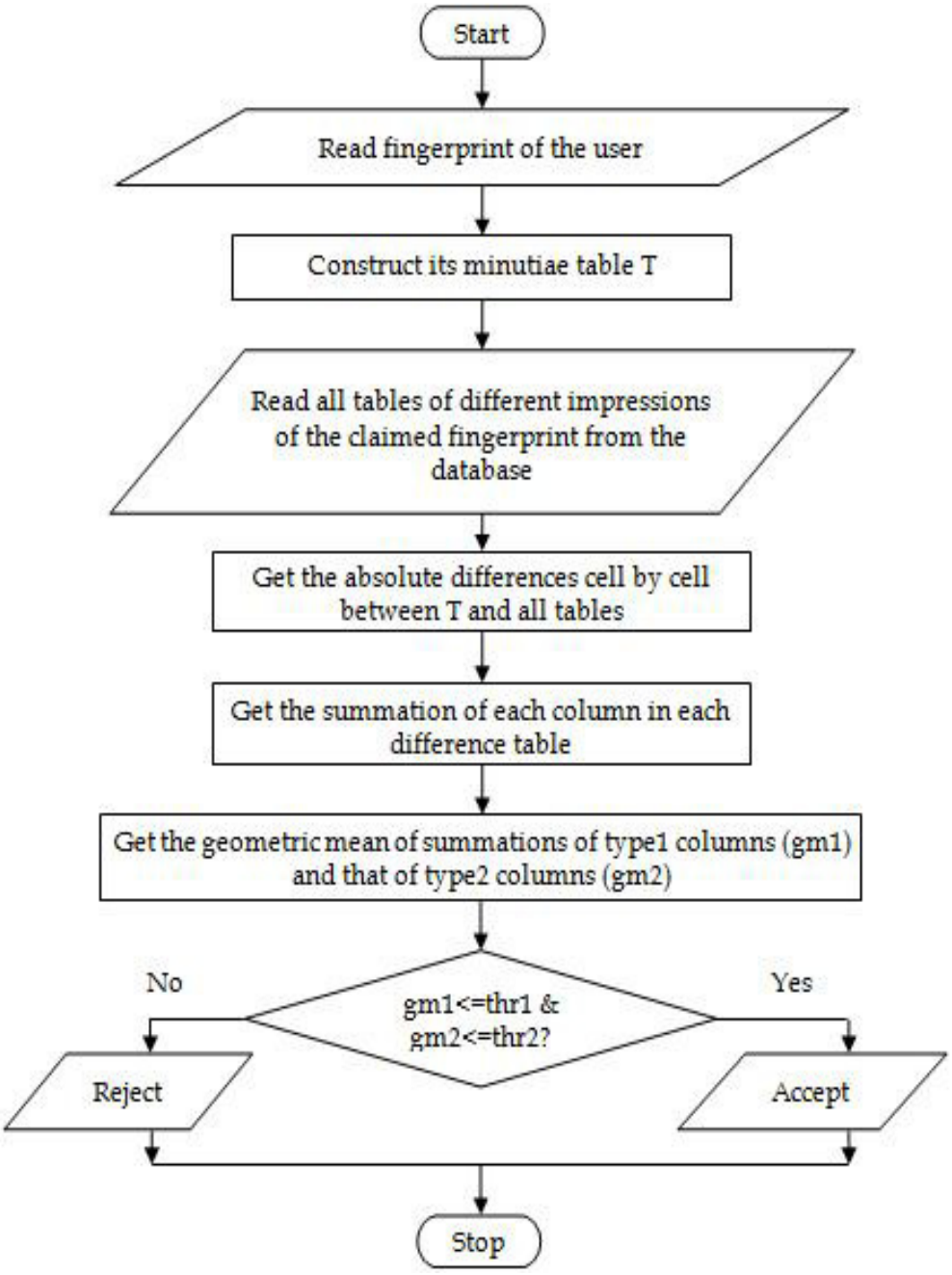

Figure 3: Flow Chart for fingerprint Authentication Process

4.2.4 THE DATABASE MODULE

This is the module where all the biometric and non-biometric data resides in storage for later retrieval. The database module was designed using MySQL Database System which is a Robust Relational Database Management System (RDBMS)

4.3 ENHANCED AES ALGORITHM

The flows of model development, a secured Fingerprint Authentication System using Enhanced-AES cryptograph include:

1. 128 bits key length is used for the modified AES algorithm.
2. The proposed system's encryption and decryption is the same as normal AES algorithm.
3. The round function of encryption process is also similar as the normal AES algorithm. IV. There is additional phase of making S-box mobile as shown in Figure 4.
4. Before sub byte stage, the static S-box is converted into mobile using cipher key. VI. The round structure of AES is used as shown in Figure 4.
5. Mobile S-box is applied in the round structure of AES as shown in Figure 4, 256 bit data is taken as Input to the system.
6. Here the Input Data is split into two blocks of 128 bits each. IX. One Block is given as Input to the AES section of the System.
7. The other Block is given as Input to the AES sections of the System in the next round as regard the round structure.
8. This is done for I, II, IV and X rounds respectively.
9. These outputs are then combined together to form 256 bit block of encrypted data.

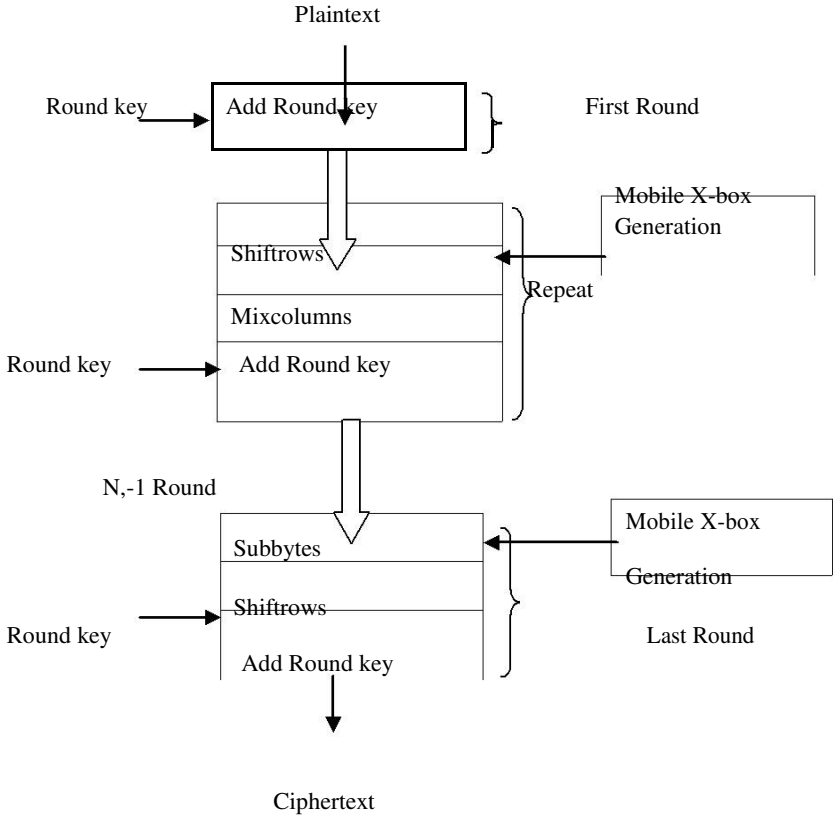

Figure 4: Enhanced AES Mobile S-box

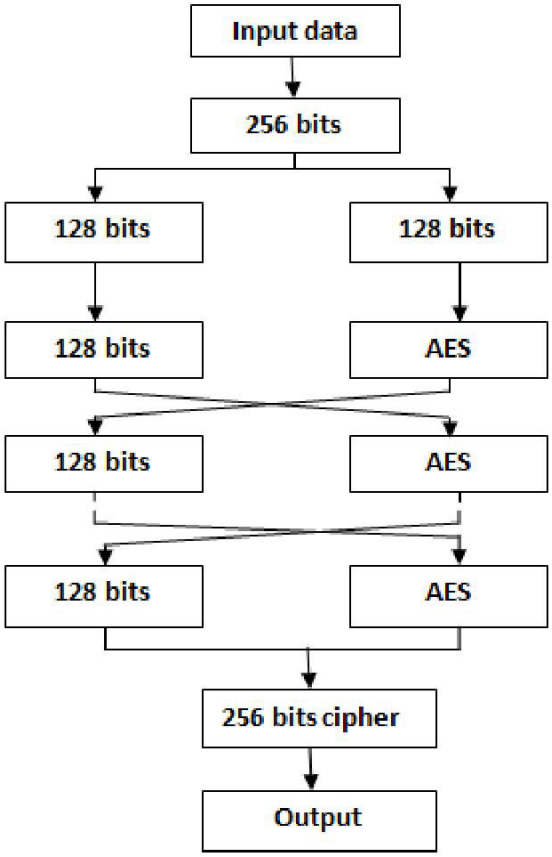

Figure 5: Round AES (Adapted from Prerna & Abhishek, 2013)

4.3 SYSTEM DESIGN AND IMPLEMENTATION

The architectural design of the system comprises of the fingerprint sensor and the Biometric application software. The Enhanced AES cryptography was used to raise the security level of the candidate's data. When the fingerprint sensor captures a fingerprint image it relays the data to the matching algorithm, this image is then compared to a decrypted version of fingerprint templates within the database. If a match is found the necessary records of the candidates will be displayed for further verification and if no match is found, an error message will be displayed to the screen to indicate no record of the candidate in the database.

4.3.1 THE FINGERPRINT SCANNER

The fingerprint scanner of choice used for the successful implementation of this work is the Digital Persona UareU family of fingerprint scanners. The choice was carefully made after several tests and consultations were made to ascertain the speed of processing, the durability of the scanner sensors. This scanner comes with a USB cable for PC interconnection along with a device driver attached to the PC including the scanner and a software development kit which enables the software developer adapt the fingerprint scanner to custom made software applications.

4.4 THE BIOMETRIC APPLICATION

The Biometric Application incorporates several technologies to ensure a correct, secure and robust implementation of the system. The application was written in java programming language using swing technology for the front-end or user interface development. The language is a high level object oriented programming language which pays for its data security and robustness. The back-end is accomplished using MySQL Database Server which is a relational database management system. The database server enables persisting of candidate's records for later use.

4.4.1 OPERATION OF THE ENHANCED-AES AUTHENTICATION SYSTEM

When a candidate gets to the Examination centre and places a finger on the sensor, the candidates fingerprint image is captured and sent to the Biometric application. The Biometric application then retrieves the stored biometric templates and decrypts them for the matching process. The captured fingerprint image is then compared with the decrypted fingerprint templates, if a match is found the necessary candidate's information is then pulled from the database and displayed and then the candidate can be allowed into the examination hall. If no match is found an error message will be displayed to the user, the verification process restarts again while the unverified candidate is denied access to the examination hall.

5. DISCUSSION OF FINDINGS

The data obtained during biometric authentication of Students just before sitting for the examination were presented by applying performance metrics. The standard metrics used for this evaluation include the False None Matching Rate (FNMR), False Matching Rate (FMR), Cross-over Error Rate (CER) and Average Matching Time (AMT)

5.1 EXPERIMENTAL RESULTS AND PERFORMANCE EVALUATION OF THE SYSTEM

The evaluation of the secure fingerprint authentication system for e-examination using our proposed technique was carried out with data obtained from one hundred randomly selected students out of one hundred and fifty students of Sacred Heart Catholic College, Abeokuta, Ogun State, Nigeria. The analysis of the data obtained from the students revealed that sixty were male, while forty were female. The distribution of these one hundred randomly selected students is shown in Table 2.

Table 2: Age Distribution of Students

No of students	8	25	30	25	12
Age Distribution	0-12	13-15	16-18	19-21	> = 22

During registration process, students enroll for different subject combinations. The selected 100 Students were distributed around 6 different subject combinations and assigned 1 to 6 includes:

1 - Languages

2 - Trade/Entrepreneur

3 - Science

4 - Technologies

5 - Humanity

6 - Business

Data in Table 3 shows that 6 of the Students registered for Languages while 12, 20, 10, 36 and 16 students registered for Trade/Entrepreneurial, Sciences, Technology, Humanity and Business subject combinations respectively.

Table 3: Subject Combination Distribution of selected Students

No of Students	6	12	20	10	36	16
Subject Combination	1	2	3	4	5	6

At the point of registration, Students biometric data are collected (Fingerprints). The sampled 100 Students did fingerprint enrolment 4 times each amounting to 400 fingerprint data. This consists of 2 impressions from the right and left thumb and 2 from the right and left of the fore-finger. The whole enrolment was done within 6 hours with image size of 202 x 258 pixel and resolution 450 dots per

inch (dpi).There were few cases of Failure Enroll Error during the enrolment. The error emanated from defaced thumbs and hard textured fore-finger. Lotion was robbed on the hard textured fore-finger and carefully wiped off hence the finger was soft and usable.

5.1.1 EXPERIMENT AND RESULT

The False None Matching Rate (FNMR) test was conducted by matching each thumbprint with the other three thumbprints from the same thumb using the implemented fingerprint matching algorithm at various thresholds (matching score) as shown in Table 4.

Table 4: False None Matching Rate (FNMR) Test on Data

Threshold	Matching Attempts (N)	False Non Matches (FNM)	FNMR= ____)	FNMR= ___ (%)	Genuine Acceptance (1-FNMR)%
1.000	1200	16	0.013333	1.333333	98.666700
0.800	1200	10	0.010000	0.833300	99.166700
0.600	1200	8	0.006667	0.666700	99.330000
0.400	1200	0	0.000000	0.000000	100.00000

Figure 7 shows the obtained Receiver Operation Characteristics (ROC) for the Results. The Genuine Acceptance Rate (1-FNMR) is represented on the X-axis while the FNMR (%) is represented on the Y-axis of the curve

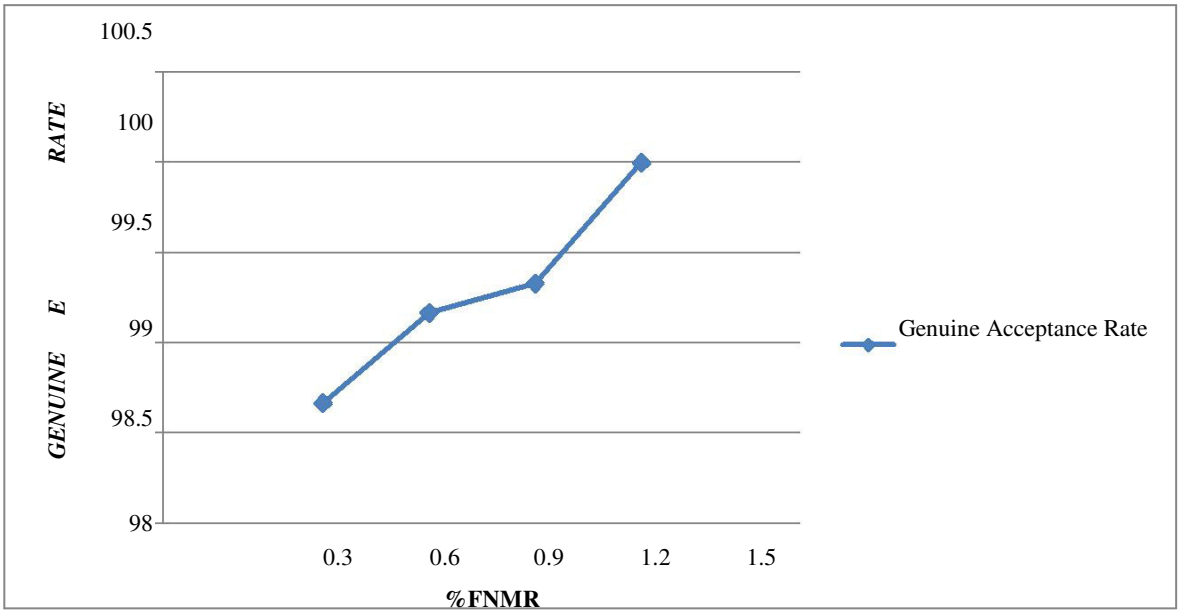

Figure 6: Receiver Operation Characteristics

The False Marching Rate (FMR) was implemented by matching four thumbprints of one of the thumbs in the data group with the 396 thumbprints from the other 99 thumbs at different thresholds. The threshold depicts the level of sensitivity of the sensor. When set on 1, it termed to be highly sensitive but when reduced to 0.4, the level of sensitivity reduces; hence false non match cases are high.

Table 5: False Matching Rate Test on data

Threshold	Match Attempts (N)	False Matching (FM)	FMR =()	FMR=( ) (%)	GMR (1-FMR)
1.000	1584	0	0.000000	0.000000	100.0000
0.800	1584	8	0.005051	0.505100	49.4950
0.600	1584	10	0.006313	0.631300	36.8687
0.400	1584	14	0.008838	0.883838	11.6162

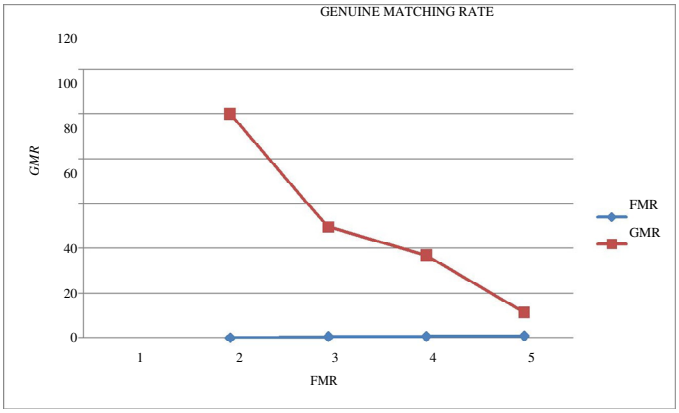

Figure 8: Genuine Matching Rates

Where, FMR stands for False Matching Rate and GMR represent Genuine Matching Rate

5.1.2 EQUAL ERROR RATE (EER)

Equal Error Rate was generated from the experiments. EER is the best description of the Error Rate of an algorithm and the lower its value, the lower the error rate and adequacy of the algorithm. For each matching threshold, EER is the value at which FNMR and FMR are equal. A graphical representation of FNMR and FMR functions against different thresholds are shown in Figure 6.

Table 6: Equal Error Rate

Thresholds	FMR Equal Error Rate	FNMR Equal Error Rate
1.0000	0.000000	0.013333
0.8000	0.005051	0.008333
0.6000	0.006313	0.006667
0.4000	0.008838	0.000000

The result obtained EER (FMR = FNMR) occurred at (0.6000, 0.0064), meaning that at a scanner sensitivity (threshold) of 0.6000, there is a certainty of the same FMR and FNMR of 0.0064 for the algorithm. This implies that about 6 out of every 1000 impostor's attempts would be falsely accepted and same number genuine attempts would be falsely rejected or genuine attempts would succeed.

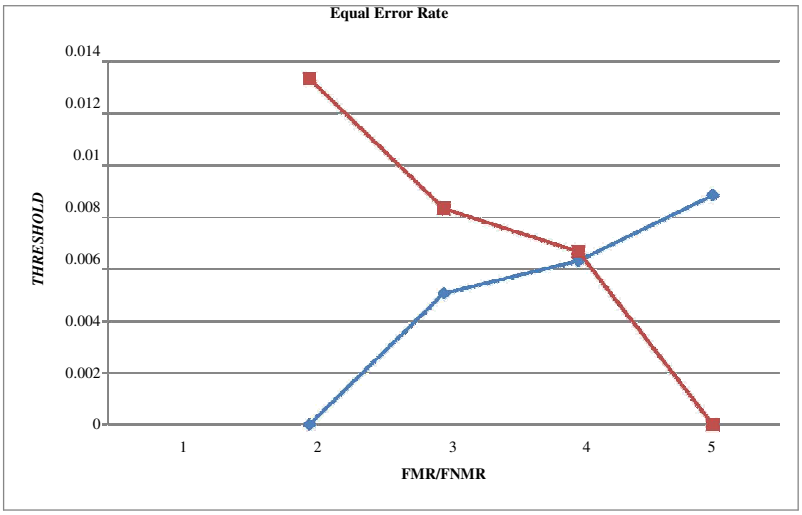

Figure 9: Graphical Representations of Equal Error Rate

5.2 SECURITY TEST USING BRUTE FORCE ATTACK

Even though the modifications are performed on the original AES algorithm, the security of the original algorithm remains intact. The cipher key in AES is of 128bits. Therefore to break the cipher key it requires 2128 possibilities and tests to be carried out. This is theoretically almost impossible. Therefore, the Brute-force Attack fails on the AES algorithm. The modifications made to the existing AES have made sure that there is no fixed pattern in any of the steps of the algorithm. The modification has provided the algorithm with strong diffusion and confusion. Hence, statistical analysis of the ciphertext fails. The most important security advantage is that no differential or linear attacks on AES have been able to break the algorithm.

The modifications proposed can be implemented without increasing the size of the key block. Though the original algorithm is secured, the proposed changes in the processing of the algorithm will help to encrypt the data by making stronger diffusion and confusion.

6. CONCLUSION AND RECOMMENDATION FOR FUTURE RESEARCH WORK

6.1 CONCLUSION

This work has successfully presented a secure fingerprint biometric authentication system for validating near and remote candidates in electronic examination scenario. The results obtained showed that an attempt by malicious candidates to impersonate and commit examination fraud can be detected with the proposed enhanced Advanced Encryption Standard Cryptographic Technique.

This was demonstrated from the ROC curve and EER value which indicates that the proposed technique can curb the activities of erring candidates and thus, improves the integrity of electronic examination in future.

6.2 RECOMMENDATION AND SCOPE FOR FUTURE WORK

It is hereby recommended that the work should be adopted for the administration of electronic examination to check incidences of impersonation. This security mechanism will enhance the credibility of certification of the electronic examination. The implementation of a multifactor biometric system could be addressed by future researcher in similar electronic examination scenario, to reduce error rate and increase overall security of the system.

6.3 CONTRIBUTION TO KNOWLEGDE

This work improved on the existing architecture of AES, which made it more difficult to compromise the security of electronic examination authentication system.

REFERENCES

Akinsanmi O., Agbaji O.T., &Soroyewun M.B. (2010).Development of an E-Assessment Platform for Nigerian Universities.*Research Journal Applied Sciences, Engineering and Technology* 2(2), 170-175

Ashish M., &Madhu S., Fingerprint Core Point Detection using Gradient Field Mask. *International Journal of Computer Applications,* 2, 19-23.

Fingerprint Verification Competition (2004), Database http://bias.csr.unibo.it/fvc. Retrieved May 2014

FIPS 197, Advanced Encryption Standard (AES)*http://www.ratchkov.com/vpn/aes/aes.html*

RIJNDAEL http://www.cs.mcgill.ca/~kaleigh/computers/crypto_rijndael.html

The Laws of Cryptography *http://www.cs.utsa. edu/~wagner/laws/.* Retrieved May 2014

Hartwig F. & Klaus K., (2008).Local Features for Enhancement and Minutiae Extraction in Fingerprints. *IEEE Transactions on Image Processing,* 3(17), 354-363.

Huszti A. &Petho A., (2008).A Secure Electronic Exam System.*Informatika a felsőoktatásban.* 2(1),1-7.

Iwasokun G. B., Akinyokun O. C., Alese B. K. &Olabode O., (2012). Fingerprint Image Enhancement: Segmentation to Thinning. *International Journal of Advanced Computer Science and Applications (IJACSA), Indian*, 3(1).

Jannik D., Rosario G., Ali K., & Pascal L., (2014). Formal Analysis of electronic examination https://orbilu.uni.lu/bitstream/10993/18586/1/main.pdf. *702-710*

Levy Y. Michelle M. Ramim (2007). A Theoretical Approach for BiometricsAuthentication of e-Exams, *Nova Southeastern University, USA*.93-101.

Maltoni D., Maio D., Cappelli R., Wayman J. L. & Jain A. K., (2002). FVC2002: Second Fingerprint Verification Competition. *16th International Conference on Pattern Recognition*. 811 - 814.

Olawale A., &Shafi'i M. Examinations, (2008) System for Nigerian Universities with emphasis on Security and result integrity. *International Journal of the Computer, the Internet and Management*18(2), 6-9

Onyeizu M.N., &Ejiofor N.E., (2013).Distribution of Architecture for post UTME Assessment.*Unpublished Master's Thesis, NnamdiAzikiwe University, Awka, Nigeria,* 054-060

Prerna M., &Abhishek S., (2013) A Study of Encryption Algorithms AES, DES AND RSA for Security.Global Journal of Computer Science and Technology Network, Web and Security. 13(15), 0975-4350

Rashad M.Z., Mahmoud S. K., Ahmed E. H., & Mahmoud A. Z., (2010). An Arabic Web-Based Exam Management System.*International Journal of Electrical & Computer Sciences IJECS-IJENS.* 10(1), 48-55.

Ravi, S., &Dattatreya, P. M. (2013).A study of Biometric Approach Using Fingerprint Recognition.*Lecture note on Software Engineering,* 1(2) 075-89

SentilK.,&Vijayaragavan S. (2014). New secured Architecture for Authentication in Banking Application, *International Journal of Innovative Research and Science,EngineeringandTechnology*, 2(3)

Seung-Hoon C., & Jong K., (2009).Ridge-Based Fingerprint Verification forEnhancedSecurity.*Digest ofTechnical Papers International Conference on ConsumerElectronics,* 1-2.

Shashi K. D. R., Chhotaray R. K., Raja K. B., &Sabyasachi, (2010). FingerprintVerificationbasedon Fusion of Minutiae on ridges using strength factor. *InternationalJournal of ComputerApplication,* 4(1), 79- 88

Shiv K., T., &Anshul M. (2012). Secured Internet Verification Based on Image Processing Segmentation. *International Journal of Scientific Research Engineering and Technology, 6(3),* 91-95

Sunitha K., &Prashanth K.S, (2013). Enhancing Privacy in Cloud Service Provider Using Cryptographic Algorithm. *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278- 8727* 12(5), 64.