Available Online at http://www.journalajst.com

ISSN: 0976-3376

ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

Asian Journal of Science and Technology
Vol. 10, Issue, 03, pp.9550-9558, March, 2019

RESEARCH ARTICLE

ENHANCED PLATFORM FOR THE APPLICATION OF BIOMETRICS SECURITY IN ELECTRONIC BANKING - A CASE STUDY OF NIGERIA

***Eneji Samuel Eneji, Ekwegh Kelechukwu Chimdike, Onyenweuwa Basil Onyeogaziri and Ajie Gospel Ozioma**

Department Of Computer Science, Federal College of Education, Obudu, Cross River State, Nigeria

ARTICLE INFO

Article History:
Received 18th December, 2018
Received in revised form
29th January, 2019
Accepted 18th February, 2019
Published online 30th March, 2019

Key words:

Electronic, Banking,
Biometrics, Security.

Corresponding author:
Eneji Samuel Eneji

ABSTRACT

Electronic banking is the modern trend in the banking industry. It has provides banking services to customers with satisfaction and enthusiasm. Irrespective of the delight in the electronic banking, many customers detest its introduction in the banking system due to the new frauds associated with it which is devastating. A lots of security measures have been put in place to combat the challenges, but this has not satisfactorily solve the problems. The introduction of biometric security offers a better alternative to combating security issues associated with electronic banking, but the application of biometrics in real time processing with heavy databases slows the processing speed. This does not suit banking operations. This paper discuses electronic banking, biometrics security, application of biometric security in real time processing, challenges with the application of biometrics security in real time systems, as well design an algorithm using Divide-And-Conquer algorithm technique with Merg Sort method that provides enhanced platform for smart application of biometrics security in electronic banking. The system so designed employs two databases, two servers, which are used in keeping bank customer's biometrics records only in a database and the other records without the biometrics in another database. Bothe databases are run separately in different servers, while the sorted data are collated and presented as a customer's page for authentication of customers as well as other banking services if authenticated.

***Citation: Eneji Samuel Eneji, Ekwegh Kelechukwu Chimdike, Onyenweuwa Basil Onyeogaziri and Ajie Gospel Ozioma,* 2019.** "Enhanced platform for the application of biometrics security in electronic banking - A case study of Nigeria", *Asian Journal of Science and Technology*, 09, (03), 9550-9558.

INTRODUCTION

The banking industry houses monies and other valuables for safe keeping pending when such monies or valuables would be needed by their owners. The banking system provides consistent and dependable banking services to customers accordingly. To improve on service delivery by the banking sector was the introduction of internet banking which began in the 1990s. Internet or electronic banking is simply online banking which mean, banking using communication gadgets such as the computer, phones, Automated Teller Machine (ATM), etc. Internet banking improves greatly on banking services to customers and makes transactions more of fun (Onu *et al.,* 2017). With internet banking, one can buy and sell without physical cash, make deposits, transfer, pay bills, etc. with ease (Adewale *et al.,* 2014). The electronic banking with its numerous benefits to the banking system, introduced great security threats to banks, and their customers (Adewale *et al.,* 2014). Fraudsters use the electronic banking platforms to divulge or steel customers secret access codes which they personalize, and use the opportunity to impersonate and rob their victims of their valuables from the bank. Some robbers confiscate ATM cards from owners with their PINs; seize tokens and other electronic banking applications access codes; which they use in defrauding their victims (Onu *et al.,* 2017). Many banking customers resist electronic banking for fear of being defrauded. Some internet thieves text touching lies at random to phone numbers requesting personal electronic bank access codes (phishing and spooling). Bank customers who do not seek verification from their banks will easily fall prey. Notwithstanding, the introduction of electronic banking has come alongside with its challenges. Worst of the challenges is electronic banking fraud. Ref, "(Jadhav *et al.,* 2015)" posited that, in recent past, there has been upward movement of bank frauds; they further stated that bank frauds figure rose to ₦8, 309.83 billion in 2004 as against ₦3, 399.39 billion in 1994 with the increase of over 380%. The recent increase is believed to be as a result of the introduction of electronic banking. Ref "(Taiwo *et al.,* 2016)" noted that, the Nigeria banking system is failing to adequately live up to expectations and fulfil their roles, due to several risks that they are exposed to. Ref, "(Jadhav *et al.,* 2015)" and, Ref, "(Taiwo *et al.,* 2016)" observed that one of the risks which is increasingly becoming a source of worry, is the banking risk associated with incessant frauds and accounting scandals. One of the security aspects that have proven over times to be reliable and dependable is the biometric security (Adewale *et al.,* 2014). Biometric security measures the physical patterns of human features or behaviour, to ensure that in any transaction, the owner is verified in person (Imiefoh, 2012). Application of biometrics in electronic transactions is challenge due to the weight of the banking database (Onu *et al.,* 2016). Being a real time system, it becomes difficult to sort heavy pool of data for biometric authentication within an insignificant time interval.

Objective of the study

The aim of this research work is to design a model that enhances the application of biometric security in electronic banking.

The specific objectives of the research work are as follows;

1. To develop an algorithm that suits the application of biometrics in real-time electronic banking with less time slack.
2. To enhance flexibility in the application of biometrics authentication in the banking industries.
3. To reduce significantly, or eliminate frauds associated with electronic banking.

Literature review

A. Electronic Banking: Electronic banking is the application of Information and Communication Technology (ICT) in banking transactions.

Ref, "(Onu *et al.,* 2016)" opines that, electronic banking allows banking transactions such that transactions are not limited to the physical environments of the bank. Global and local bank customers can do banking transactions without barrier of distance or location. Today due to electronic banking, the barriers between the bank and customers has been removed, as a customer can access banking services comfortably inside his bed room.

Ref, "(Adewale, *et al.,* 2014)" states that, electronic banking services include; bill payments, account inquiries, cash withdrawal and deposits, fund transfer, payment for goods and services, airtime purchase, etc.

Ref, "(Onodugo, 2015)" defined electronic banking as the application of computer technology to banking, especially in payment aspects of banking. He further defines electronic banking as a system of banking that made used of communication network that permits online processing of credit, and debit transfer of funds, within member of clearing institutions at the same day.

Ref, "(Das, 2016)" defined electronic banking as, a banking system in which funds are transferred through exchange of electronic signals between financial institutions, rather than exchanging cash, cheques or other banking instruments.

Ref, "(Omotayo, 2007)" looked at electronic banking as, a system of banking where funds are moved between different accounts, using computerized real time system without involvement of cheques.

Ref, "(Ibidapo *et al.,* 2010)" is of the view that, electronic banking is a system, in which financial transactions are settled electronically with the use of electronic gadgets such as; ATM, POS terminals, GSM phones, V-Cards, etc handled by e-holders, bank customers and stake holders.

Ref, "(Ikpetan *et al.,* 2006)" is of the opinion that, electronic banking is an umbrella term for the process which customers performs banking transactions electronically, without visiting a physical bank building.

Electronic banking makes use of the following ICT gadgets to effect it transactions; cell phones, tablets, Point-Of-Sale (POS) device, notes, PCs, ATM, etc. ATM and POS are customized electronic banking devices. Others make use of electronic banking applications such as first money, easy money, U-mobile, etc, to drive home electronic banking. ATM is the fastest growing electronic banking system in Africa financial market rising from 83% in 2006 to 89% in 2007 with over 900 ATM deployed and over 26 million ATM cards issued by 16 commercial banks and 14 micro finance banks [1]. Electronic banking has been able to reduce drastically many of the problems associated with traditional banking system, by providing a more convenient and comfortable ways in banking.

B. **Biometric Security:** Biometric is a measure of physical features of the human bodies such as fingerprint, face, DNA, iris, etc used to give unique identity of different individuals. Biometrics is a combination of two Greek words; "bios" meaning life and "metrikos" meaning measuring [24]. By the Greek description, it implies that Biometrics is the measure of stable or fixed human characteristics. Each individual has unique biometric features different from any other individuals. This becomes a yardstick for the design and implementation of a secured security system. Biometric is the scan of the patterns of human features, which is translated by algorithm into stream of bits that can be analyzed, stored and use as a medium to recognize the person's identity in subsequent times, using the current scan of the individual biometrics. The current scan is equally converted to stream of bits, and then pattern matching is analyzed to determine of the two data (past and present) collected if identical. Primarily, Biometrics is used to identify and authenticate individuals before granting access to him or her (Edet, 2008) Biometric pre-dates to the 14th century when the Chinese merchants stamp children palm prints and footprints on paper with ink to differentiate between children. In late 18th century, Paris anthropologies and police Desk clerk Alphones Bertillon looked at photographic memory, and decided to study the use of biometrics in identifying convicted criminals. Multiple body measurement techniques were developed by Bertillon (Bertillonage) which was used all over the world until when it was uncovered that more than one person can have similar measurements. Richard Edward Henry of Scotland Yard developed a finger printing system which was used by the police after the failure of Bertillonage. In recent times, Biometrics has included more biometric features such as face, iris, DNA, etc and incorporate a more sophisticated gadgets for biometrics application (Biometric history – How did it start?)

Ref, "(NSTC, 2006)" outlined physical biometrics to includes;

i) Bertillonage: This has to do with the measure of body lengths. This feature is no longer in used today
ii) Fingerprint: this analyzes fingertip patterns of individuals

iii) Facial recognition: the measurement of facial characteristics
iv) Hand geometry: measurement of the shape of the hand
v) DNA: Analysis of the genetic features of the individual
vi) Retinal scan: analyzing the blood vessels in the eye
vii) Iris scan: analysis of coloured ring features of the eye
viii) Vascular patterns: vein patterns analysis.

Widely used physical biometric feature is the fingerprint which has also proven overtimes to be reliable with high degree of accuracy. The united states in 2006 through the National Science and Technology Council (NSTC) formed subcommittee on Biometrics to look into the following (Biometrics. *et al.,* 2016);

(1) To develop and implement multi-agency investment strategies that advance biometrics sciences to meet public and private needs.
(2) Facilitate the inclusion of privacy-protecting principles in biometrics system design
(3) Coordinate biometric related activity that are of inter agency relevance
(4) Ensure a consistent report about biometrics and government initiatives, when agencies interact with congress, the press and the public.
(5) Strengthen international and public sector partnerships, to foster the advancement of biometrics technologies.

This was aimed at providing a stronger and more reliable security in government and business transactions. According to NSTC (Biometrics. *et al.,* 2016), the common challenge by government and industry in today's global society is how to provide more robust identity management tools, and identify governance principles on how to deploy the tools to intelligently meet national and international needs. They further emphasis that biometrics are the most definitive, real time identity management tools currently available. From the analysis on how to embark on large scale use of biometric identity, it was discovered that there was need to;

i) Improve on collection device (i.e. biometric sensors)
ii) Develop more efficient and effective large-scale operational capabilities (biometric systems)
iii) Establish standards for plug-and-play performance (biometrics systems interoperability)
iv) Enable informed debate on why, how and when biometric should and can be used (biometrics communication and privacy).

Today, a number of biometrics systems have been developed and in used both nationally and internationally. Application of biometrics in real-time applications though feasible, it has been faced with problem of time slack especially when the database is dynamic. With the advancement in technology, miniaturized devices with very high processing speed has been invented to tackle this challenge, yet, one of the world problems today is information management which has to do majorly with storage and access to information. Real time applications need immediate response. In a situation whereby the weight of data stored in the storage medium is so large, the access time will be affected, and this does not suit real time transactions. Biometrics are graphical in nature, as such, its integration with records in a dynamic database will create a database that will be difficult to implement in real-time. The question here is what do we need to do in order to effectively and efficiently integrate and manage biometrics security in real-time applications? The Federal Bureau of Investigation's (FBI's) integrated Automated Fingerprint Identification System (IAFIS), which provides automatic fingerprint search capabilities, latent search capability, electronic image storage and electronic exchange of fingerprints; this takes a whole of 24 hours response (Rhodes, 2003). It follows that to verify and authenticate an individual; it takes about 24 hours to scan through a collection of biometrics. This actually will not suit operations such as electronic banking (Rhodes, 2003). The other issue with the application of Biometrics security is the high false rejection rate due to placement adjustment of the face and finger scan during registration and verification. Based on this, Ref, "(Bobde and Satange, 2013)" in their work biometric in secure e-transaction suggested a multi-biometrics which is the integration of various biometric models that can handle different physical features of the individual simultaneously to avoid elution of verification and authentication. The multi-biometrics security system pre-mapping fusion information was classified into two levels: sensor level or feature level.

The sensor level was organized into three classes:

i) Single sensor-multiple instances
ii) Intra-class multiple sensors
iii) Inter-class multiple sensors

The feature level was organized into two categories;

i) Intra-class and
ii) Inter-class: the intra-class was further categorized into;
iii) Same sensor, same features
iv) Same sensor, different features
v) Different sensors, same features
vi) Different sensors, different features (Bobde and Satange 2013)

C. Fingerprint Recognition Algorithm

The algorithm for fingerprint recognition consists of two technologies (Image processing and matching algorithm) which are required to verify the identity of a user, by automatically extracting the fingerprint image minutiae. Fig 1 gives detail of the overall block map, for the fingerprint recognition algorithm application.

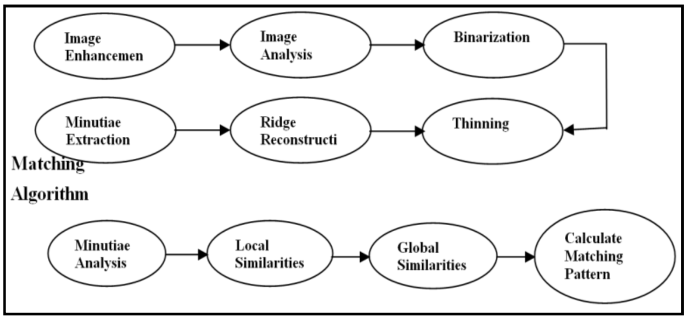

Figure1. Fingerprint Recognition Algorithm

Image Processing: Image processing consists of six stages which are

a. Enhancement Stage where noise on the input fingerprint image is eliminated, as well as fortification of contrast for successive stages.

b. Image Analysis Stage which prevents fingerprint recognition against its corruption.
c. Binarization Stage is to binarize the gray-level in fingerprint captured image.
d. Thinning Stage thins the binarized image
e. Ridge Construction Stage Constructs the ridge by removing pseudo minutiae
f. Minutiae Extraction Stage extracts minutiae from the reconstructed ridge image.

Matching Algorithm: the geometric characteristics such as distance and angle between standard minutiae and its neighbouring minutiae based on the analysis of the image processed features data is analyzed. From the analysis, all the minutiae pairs have some kind of geometric relationships with their neighbouring minutiae which is used as the basic information for the local similarity measurement.

The Process: the user placed his fingerprint against a biometric fingerprint scan reader's interface. The scanner transmits the scanned fingerprint to a database in the computer which is compared to the one stored in the database for matching.

Review of electronic transaction systems with biometrics security

The application of Biometric security in real time application has taken various dimensions by scholars. It is the current trend proposed to manage ill fates with electronic applications/systems. Ref, "(NSTC, 2006)" stated that, the emergence of biometrics has addressed the problems that plaque traditional verification method. They further explained that biometric culture plays more vital role in authentication or verification of a person.

A. **Biometric ATM:** Bioenable Technology Organization developed Automatic Teller Machine (ATM) that utilizes biometrics for verification and authentication of users. The machine integrates different forms of biometrics such as fingerprint, iris, face recognition and retina. The machine was called multi-Biometric ATM do to the integration of multi-biometric features.

Features of the Multi-Biometrics ATM

The feature of the multi-Biometrics ATM includes;

- The system possesses large CPU and memory that provides, sufficient processing capabilities that supports high-end biometric identification and verification.
- The point of controlling was designed with touch screen multilingual interface for easy interaction and reduction in manpower cost.
- The system was designed such that, it is easy to maintain and repair (Bioenable, 2017).

Achievement of the ATM machine

The following were achieved with the ATM system (Bioenable, 2017).

- Single/multi teller Biometric authentication using fingerprint, iris, face, palm vein
- Multi factor authentication using card, pin and Biometrics
- Cardless authentication

Application of the Multi-Biometrics ATM

The multi-biometrics ATM can be applied as follows (Bioenable, 2017)

- Banking and finance
- Food coupon/tickets/canteen ATM
- Membership verification ATM
- Transaction/check deposit ATM
- Self service ATM and
- Retail ATM

Challenges of the Multi-Biometrics ATM

The system developed, achieved the objectives as stated above, but the following are areas the system was not able to address.

- The system is not portable as it requires a large CPU and a large memory for efficient operation. Electronic transaction has growing database- what will happen when the database becomes too large? It is expected that there should be a more convenient methodology to manage the transactions even with a smaller CPU and memory.

B. Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-banking System

Ref, "(Imiefoh, 2012)" proposed and designed a prototype of ATM that uses PIN, and finger print to verify and authenticate electronic banking customer in the cause of using the ATM for banking transaction. The work was basically an enhancement on the existing ATM systems' security by introducing fingerprint.

Challenges

- The system does not take into consideration the weight of fingerprint in real time application. As such do not make provision for the efficient management of large volume of biometrics.
- The system only addresses the issue of verification and authentication.

C. A Real-Time Biometric System for Person Authentication Using Embedded Processor

Ref, "(NSTC, 2006)", proposed a concept which was on the inclusion of biometrics system in real-time system for persons' authentic (Imiefoh, 2012). Notwithstanding, (NSTC, 2006) considers the weight of biometrics and what could be done to guarantee efficiency. They then introduced embedded processor to effect high speed processing. Still the inclusion of embedded processor will help, but the system so proposed will be cost ineffective because of high purchasing and maintenance cost. The system as well can only verify a person.

D. Biometrics in Secure e-Transaction

Biometric in secure e-transaction was proposed by (Bobde and Satange, 2013). The proposed system introduced the inclusion of biometrics in electronic transactions. The emphasis was based on the use of portable mobile devices. They went ahead and design a cell phone that has a video camera to capture face images, fingerprint scanner to scan finger and build in-microphone to capture voice sample. The system designed would be able to guarantee a reliable verification and authentication of the user, but the system does not consider the challenge of time slack to the application of biometrics in real-time systems.

E. Facial verification technology for use in ATM Transactions

Facial verification has to do with the use of technology, to capture the facial features of a person as a biometric input requirement for the person's verification and authentication. The facial features are captured and digitized with appropriate technology, using the mathematical algorithmic design, for its representation, and stored in the database against the persons' records. The stored biometrics served a better means for user's identity. Ref, "(Aru and Ihekweaba, 2013)" proposed the design of ATM that uses facial biometric for the verification and the authenticity of an ATM user. The logic of the proposed design is represented in the flowchart diagram (Fig 2) below.

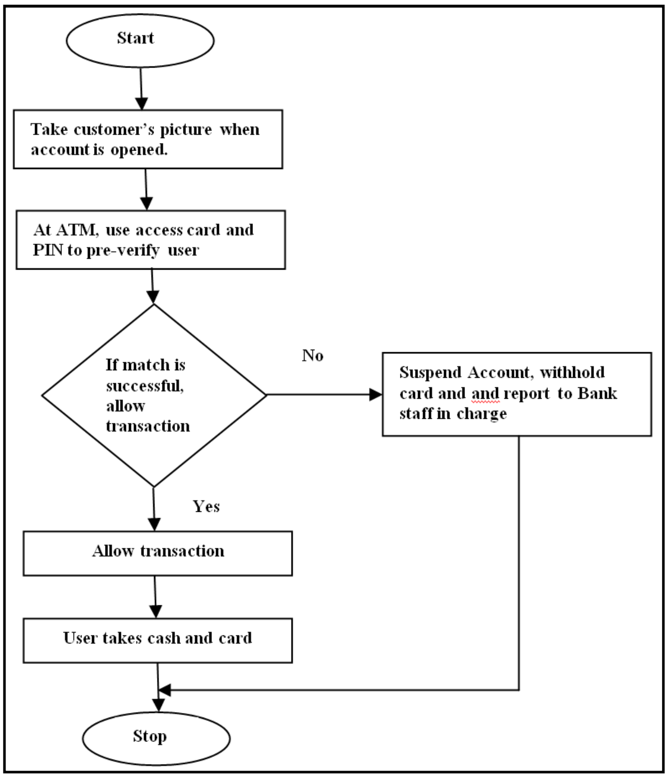
Start
Take customer's picture when account is opened.
At ATM, use access card and PIN to pre-verify user
If match is successful, allow transaction
No
Suspend Account, withhold card and and report to Bank staff in charge
Yes
Allow transaction
User takes cash and card
Stop

Fig. 2. Flowchart of Electronic Banking Transaction Using Facial Biometric

The proposed system like the earlier ones discussed above, focus on the use of PIN and facial biometrics as a means of verifying ATM users. The authors did not consider the challenges of effective and efficient application of biometrics in real time application with growing database, knowing too well that biometric data is graphical in nature and requires high processing speed technology, large RAM and large secondary storage unit.

F. Proposed E-Payment System Using Biometrics

The work of (Marimuthu and Nagartnam, 2011) proposed the use of biometric feature in e-payment. In their work, they compare performance, acceptability and circumvention of the various biometrics (face, finger, hand geometry, hand vein, iris, retinal scan, signature and voice) and came up with the following comparison.

1. That fingerprint is best in performance to all other biometrics, while the retina and iris has a higher circumvention to the fingerprint.
2. That the retina scanner is a burden to the customer in the cause of transaction
3. That plastic card and fingerprint has mobility advantage. Ref, "(Marimuthu and Nagartnam, 2011)" used their biometrics analysis, and propose a system design which uses biometrics security to implement e-payment. The designed system is shown in Figure 3.

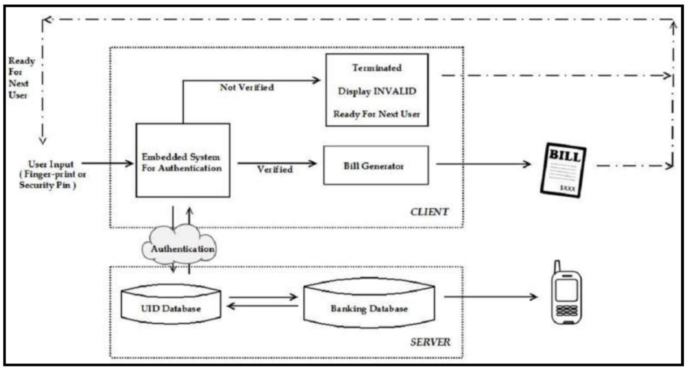

Figure 3. Finger Print Verification and Identification

The proposed system lacks provision for efficient application of heavy graphic data like biometrics in online applications.

G. A Model of Cyber Crime Detection and Control System: Ref, "(Agana, 2016)" proposed a control measure of mitigating cyber crime using biometric identification and geo-referencing. He used his postulations to design cyber crime detection and control system. The system was such that before a user gains access to the net either to surf or use the net for whatsoever transaction, his identity should be verified and authenticated using his biometrics saved on the database during registration. The system was also incorporated with GPS system that can always locate the position of the net user wherever he is accessing the net. The system has some level of security sensitivity that can monitor and detect suspicious internet practices. Using GPS and security reports generated continuously about any user whose activities are declared by the system suspicious (criminal activity), and make it possible to quickly track and interrogate such a suspected criminal.

The system was able to achieve identity verification, show some level of security sensitivity by monitoring and reporting practices suspected to be malicious or criminal in nature, and provide efficient means to track and apprehend criminals. The system lacks consideration for effective application of heavy graphic like biometrics in online application with growing database.

System analysis, Design and Mythology

A. System Analysis: The study observed that the introduction of electronic banking in Nigeria has led to increase in banking fraud with considerable percentage on electronic banking fraud. In further analysis, it was observed that electronic banking make use of personal identification such as user name and password, tokens or transaction pins as means of identification and authentication. With the level of technological advancement today, both in hardware and software, the existing identification and authentication methods are vulnerable. The vulnerability has given opportunity to intelligent and smart individuals to take advantage and hack into banks and bank customers' accounts defrauding them. This is one of the reasons why most bank customers are afraid to use electronic banking applications or integrate ATM with their personal accounts. Also due to the vulnerability of the identification process in electronic banking, armed robbers and thieves can forcefully collect bank customers ATM cards and their personal banking identities which they use to defraud their victims. It was also observed that ATMs have biometric capturing device which is use as a mere documentary for third party witness. The biometrics is not integrated as a means of identity and authentication for electronic banking transactions. The ATM machine designed by Bioenable technology made use of biometrics though lacks the technology that will sustain the system in future. Also, the machine is expensive both to purchase and to maintain due to large CPU and large memory.

B. System Design

The proposed design is as follows;

Design of Enhanced Platform for the Application of Biometrics Security in Real Time Processing

Figures 4 and 5 illustrate the enhanced biometrics application in real time processing

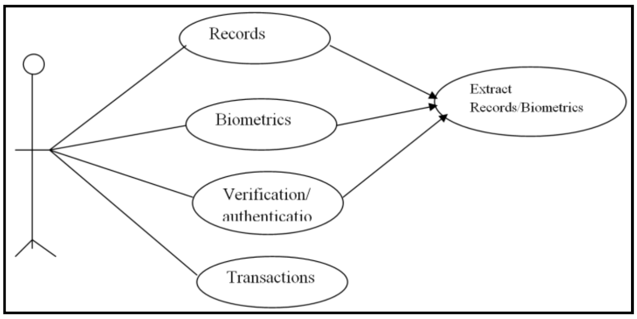

Figure 4. A Single Use Case Diagram for Enhanced Biometrics Application in Real-Time Processing Transaction

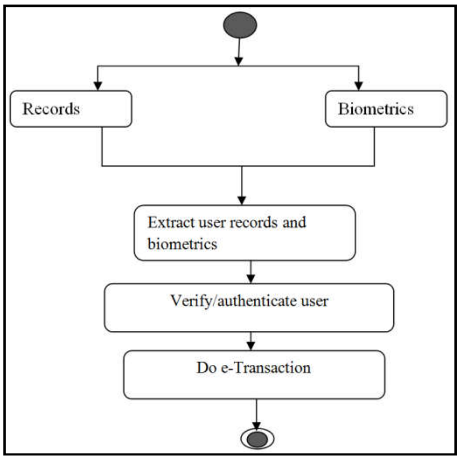

Figure 5. Activity Diagram of Smart Biometric Security in Real-Time Transactions

From Figure 4 and 5, the following was achieved;

- In the cause of registration as an online user, both personal records with biometrics of the user are collected and separated into two databases run by two servers; the customers' record database without the biometrics, and the customers' biometrics only database. Both databases are treated as object components of the class (electronic banking database).
- Each individual's biometrics in the biometric database table is linked dynamically to his personal records in the record database table.
- In the course of accessing online services, the record is uploaded from the record database table by server 1, while the biometrics is equally called from the biometric database table dynamically by server 2.
- The user is then verified and authenticated
- Access is granted if user is authentic

Design of an Algorithm for Enhanced Application of Biometrics Security in Real-Time Transactions: The algorithm for real-time biometric application consists of three technologies (the record, biometrics and matching algorithm) which are required to verify the identity of a user, by automatically loading the stored records of the user, edit the biometric minutiae, extract a fresh minutiae from the user's new biometrics enrolment on point of transaction, and then perform a matching. The algorithm analyses the following features;

i. The customer's record is created which is divided into his bio-data and the other records without biometrics data.
ii. Both data exist as object kept as separate databases in two different servers, but with a dynamic link to each other.
iii. The concurrence attributes of objects allow the two objects compete and cooperate with each other.
iv. Divide-and-Conquer Algorithm is applied to the objects using mergsort technique to sort the customer data from the two servers in the cause of customer login request.
v. The customer's sorted data (bio-data and the other data) are loaded to the ram for matching and authentication.

The algorithm for real-time biometric application consists of three technologies (the record, biometrics and matching algorithm) which are required to verify the identity of a user, by automatically loading the stored records of the user, edit the biometric minutiae, extract a fresh minutiae from the user's new biometrics enrolment on point of transaction, and then perform a matching. Figure 6 give details of the overall block map for the enhanced biometrics application for real-time processing consisting of the three technologies.

Record loading algorithm

Record loading consists of six stages. At pin analyzer's stage, the user's pin is analyzed for inclusion. The address locator picks the addresses of the user's record and the biometrics from their dynamic storage. At record extractor's and Biometric dialler stages, the record of the user and the biometrics are loaded as extracts from the dynamic storage. At Editor's stage, the records are made editable for further transaction. The edit minutiae will edit the minutiae of the user's biometrics extracted and saved during registration, and wait for matching with the enrolled biometrics extracted from the user at the point of transaction.

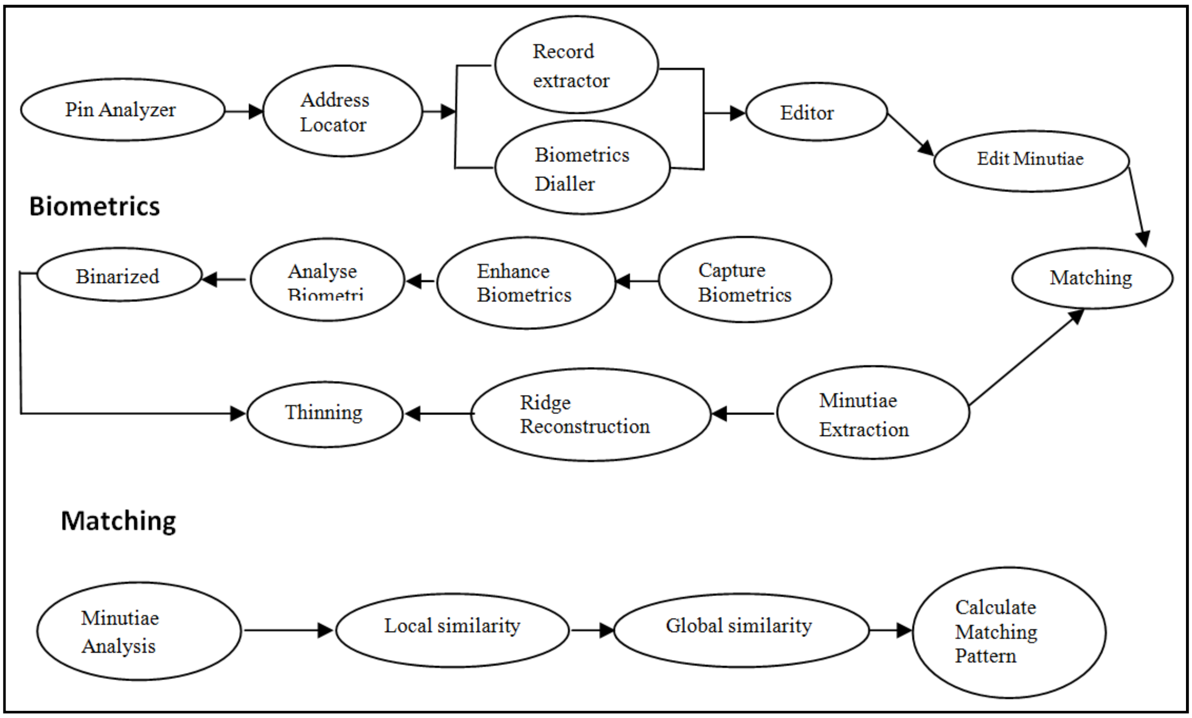

Fig. 6. Algorithm for Enhanced Application of Biometrics in Real Time Systems

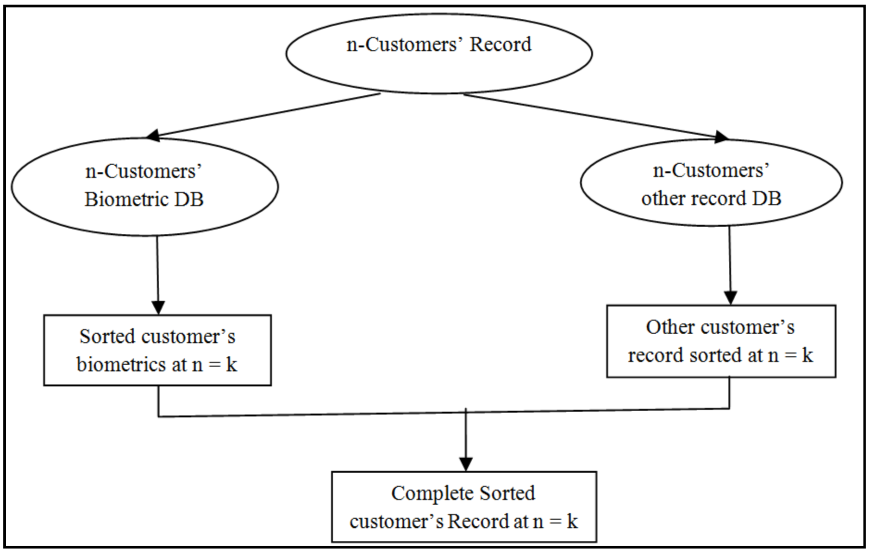
n-Customers' Record
n-Customers' Biometric DB
n-Customers' other record DB
Sorted customer's biometrics at n = k
Other customer's record sorted at n = k
Complete Sorted customer's Record at n = k

Fig. 7. Algorithm for Enhanced Application of Biometrics Security in Real Time Applications using Divide-And-Conquer Technique

Biometrics processing algorithm

Biometrics processing algorithm also consists of six stages. Noise on the input biometrics scanned is eliminated at the enhancement stages, while contrast is fortified for the sake of successive stages. Image analysis stage prevents biometrics corruption to prevent adverse effects on recognition. The gray-level of the biometrics is binarized at the binarization stage. The binarized biometrics is thin at the thinning stage. The biometric ridges are reconstructed by removing pseudo minutiae at the Ridge reconstruction stage. Minutiae are extracted from the reconstructed ridge biometric which is used to do matching calculation with the edited minutiae from the dynamic database.

Matching algorithm

The matching algorithm consists of four stages. The minutiae analysis stage analyses the geometric characteristics (distance and angle) between the edited stored minutiae and scanned, and, or captured processed minutiae based on the analysis of image-processed data. In the cause of the analysis, if all the minutiae edited have geometric relationship with the scanned and, or captured minutiae, the similarities will form the bases for local similarity measurement.

The process

It is expected that the user was enrolled in an online transactions, as such, has a records that includes his biometrics in the web storage. The user now in the cause of real-time transaction will need to place his finger and face against a small fingerprint reader or a webcam camera. Such a reader is connected to the computer where the scanned and, or captured biometrics is matched with the existing biometrics for similarity check. Where there is a perfect match, access is granted. The key achievement in this algorithm is the separation of data and biometrics of the same user saved in different tables, but with competitive and cooperative features of OOP, which allow both data to be processed with high speed. To achieve the above, we employ the divide-and-conquer algorithm design technique as represented in Figure 7. The algorithm in figure 7 separates customer's record into biometrics record stored on a separate table, and the other records without the biometrics also stored in a separate table of a database. The two records are dynamically linked together with a link-list. At the point of transaction, both records are sorted with Mergsort sort using divide-and-conquer algorithm technique.

The equations below, analyzes the algorithm and the time sequence.

$$f_n = n/2(f_a . f_b) \qquad (1)$$

Where;

f_n = Verified User (expected bank customer) at point of login
f_a = User's Records only without biometrics filtered from the stored other record database in the database during login.
fb = User's Biometrics Records only filtered from the stored biometrics table in the database during login.
n/2 = Divide-And-Conquer factor
n = the numerical sizes of each record of customer stored on tables.

$$(I . f_n) \acute{\varepsilon} \begin{cases} y_1 = F_p \text{ if } (F_p . F_a) = \mathrm{T} \\ Y_2 \; Otherwise\ suspect\ user \end{cases} \qquad (2)$$

Where;

I = User's Identity at the point of transaction (verification/ authentication).
f_n = Analyzed pin and biometrics of user captured from user at the point of transaction.
f_p = Pin verification at the point of transaction
f_b = Biometrics authentication during transaction

$$T_{(n)} = (n) T_{(n/z)} + f_{(n)} \qquad (3)$$

Where;

$T_{(n)}$ = the general divide-and-conquer recurrence time spent in sorting customer's records from the database
n = instances of size n/z composed by the process, and their possible solutions.
y and z = the divide-and-conquer constant, and the order of growth of the $f_{(n)}$
$f_{(n)}$ = the function equation.

At y = z =2, $f_{(n)} = 1$, equ (3) can further be decomposed into;

$$T_{(n)} \acute{\varepsilon} \begin{cases} \mathrm{n}^{\mathrm{d\ if\ y<}\, z^d} \\ (\mathrm{n}^{\mathrm{d}} log_n) \; if \; y = z^d \\ (\mathrm{n}^{log_2 \mathrm{y}}) \; if \; y > \; z^d \end{cases} \qquad (4)$$

Where;

d = integer value ≥ 0.

Eqn(1) above is the function that sorts and merge customer's biometrics and other data from the their different tables in the database. The function produces the complete record of customer filtered from the database presented for further verification and authentication in the cause of login. Eqn(2) authenticates customer's pin and biometric inputs, with the existing ones in the database for fraud analysis. Eqn(3) is the time function which estimates, the time taken to completely sort customer's biometrics and the other data from the database. Eqn(4) is the instances of time computed when the recurrence d ≥ 0 in eqn(3). For instance, if y = z = 2, and d = 0, it follows that;

$$\mathrm{K(n)} \; \acute{\varepsilon} \; (\mathrm{n}^{\mathrm{log}_{\mathrm{z}}{}^{\mathrm{y}}}) = (\mathrm{n}^{\mathrm{log}_{2}{}^{2}}) = (\mathrm{n})$$

MATERIALS AND METHODS

The proposed system was designed using Divide-and-conquer algorithm technique with mergsort technique. It was analyzed with Structured System Analysis and Design methodology and Object Oriented Methodology (OOM) using waterfall technique. SSADM suits in analyzing large systems. It gives the designer and analyst the opportunity to break down large and complex systems into smaller manageable but independent units, modules and sub-systems. The subsystems can be managed independently, which makes it easy to code and implement. OOM has the features which can be used to break down components into objects. OOM also suits in designing online applications. Related objects are classified into classes. A class is equivalent to a unit, module or subsystem in SSADM. Properties of objects and classes can be shared and inherited such that duplication of codes is eliminated. With these properties of OOM and others such as data abstraction, polymorphism, etc, OOM suits for the development of a portable system with unimaginable performance.

Conclusion

It has been enormous task to combat electronic banking fraud in the Nigeria banking systems due to the difficulty of preventing frauds associated with electronic banking. This has become one of the major challenges with the electronic banking system over times. The application f biometrics security in banking has been challenging due to the heavy graphics associated with biometrics data. This research work deems it fit to come up with an enhanced biometrics security models that is homogeneously integrated with the electronic banking application, to aid fraud investigation and mitigation. This design if developed and implement, it is hoped to improve the efficiency of the application of biometrics security not only in electronic banking, but in real time systems as a whole. The system so design has smart application of biometrics with less time slack. The proposed design was able to achieve the development of an enhanced platform for the application of biometrics security in electronic banking. This was achieved by the design of an algorithm that supports smart application of biometrics in real time systems using Divide-and-Conquer algorithm on the concurrence feature of OOP. The design is for now only a model, which if accepted as an international standard for electronic banking, then the application of biometrics security on electronic banking would no longer be that tedious.

REFERENCES

Adewale, A., A., Ibunni, A., S., Badejo, J., and Odu, T. 2014. Biometric Enable E-Banking in Nigeria Management and

Customers' Perspectives. *Journal of Information and Knowledge Management,* 4(11), 23-28.

Agana, M.A. 2016. A Model of Cyber Crime Detection and Control System. A PhD Thesis presented to Department of Computer, Faculty of Physical Sciences, Ebonyi State University, Abakaliki.

Akazue, M., and Efozia, N., F. 2010. A Review of Biometric Technique for Securing Corporate Stored Data, 1(1), 329-342.

Aru, O., E., and Ihekweaba, C. 2013. Facial Verification Technology for Use in ATM Transactions. *American Journal of Engineering Research (AJER),* 2(5), 188-193.

Bioenable, 2017. Biometric ATM. Accessed from http://www.bioenable.com/biometrics.atm on 10th April, 2017.

Biometric Solution, 2016. Biometric Solution: Classification of Biometric Technologies on Physical Threats Accessed from http://www.questbiometrics.com.biometrics-solution.html on 12th August, 2016.

Bobde, S. and Satange, D.N. 2013. Biometrics in Secure e-Transaction. *International Journal of Emerging Trends and Technology in Computer Science (IJETTCS),* 2(2), 243-248.

Boulgouris, N., V. *et al,* 2009. Biometrics: Theory, Methods, and Applications. Wiley-IEEE Press. Clive, W. 2007. Academics Dictionary of Banking. New Delhi, India: Arrangement Academic.

Das, R. 2016. Adopting Biometric Technology: Challenges and Solutions. March 9th, 2016 CRC Press, page 242. Accessed from http://www.crcpress.com/Adopting-Biometric-Technology-challenges-and-olutions/Das/p/book/9781498717441 on 12th August, 2016.

Edet, O. 2008. Electronic Banking in Banking Industries and its Effects. *International Journal of Investment and Finance,* (3) 10 – 16.

Ibidapo, O. A., Zaccheous, O. and Olufemi, M.O. 2010. Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-Banking System. *International of Electrical and Computer Sciences IJECS-IJENS,* 10(6), 68-73.

Imiefoh, P. 2012. Towards Effectively Implementation of Electronic Banking in Nigeria. *International Multidisciplinary Journal, Ethiopia,* 6 (2), 25 – 31.

Ikpetan, O., A., Mba, A., and Aca, F. 2006. Growth of Bank Frauds and the Impact on the Nigerian Banking

Industry. Ota, Department of Banking and Finance.

Jadhav, V., V., Patil, R. R., Jadhav, R., C., and Magikar, A., N. 2015. Proposed E-Payment System Using Biometrics. *International Journal of Computer Sciences and Information Technologies (IJCSIT),* 6(6), 4957-4960.

Marimuthu, P. and Nagartnam, R. 2011. A Real-Time Biometric System for Person Authentication Using Embedded Processor. A paper presented in the 3rd National Conference in Signal Processing, Communication and ULSI Design (NCSCV'II) on the 6th and 7th May; Department of ECE, Anna University of Technology, Coimbatore.

NSTC, 2006. The National Biometrics Challenge. National Science and Technology Council Sub Committee on

Biometrics. Access from http://www.biometrics.gov on 12th August, 2016.

Omotayo, G. 2007. A Dictionary of Finance, West Bourne, England: West Bourme Business School.

Onodugo, F. C. 2015. Overview of Electronic Banking in Nigeria. *International Journal of Multidisciplinary Research and Development,* 2 (7), 336 – 342.

Onu, F., U., Eneji, S., E., and Anigbogu, G. 2016. The Effect of Object Oriented Programming on the Implementation of Biometric Security System for Electronic Banking Transactions. *International Journal of Science and Research (IJSR),* 5(2), 935-941.

Onu, F.u, Umeakuka, C., V., Eneji, S., E. 2017. Computer Based Forecasting in Managing Risks Associated with Electronic Banking in Nigeria. *Journal of Innovative Research and Advanced Studies (IJIRAS);* 4(3), 390-396.

Rhodes, K. A. 2003. Information Security Challenges in Using Biometrics. Testimony before the subcommittee on Technology, information policy, intergovernmental relations, and census. Accessed from http:///www.gao.gov/new.items/d031137t.pdf on 12th August, 2016.

Taiwo, J., N., Agwu, M., E., Babajide, A., A., Okafor, T., C., and Isibor, A., A. 2016. Growth of Bank Frauds and the Impact on the Nigerian Banking Industry; *Journal of Business Management and Economies (JBME),* 4(12), 1-10.

Vasiliki, A., Dionysios, D., and Theodor, V. 2007. Biometric Implementation and the Implications for Security and Privacy. Information accessed from http://www.fidis.net/fileadmin/journal/issues/1-2007/Biometric Implementation and the forsecurity and privacy.pdf on the 12th, August, 2016.

****