Towards Implementing An Efficient Biometric Authentication Framework For Nigeria Customer Banking Systems

by
Imuetinyan Bernadette Iyawe

Abstract
With the rapidly increasing number of break-in reports on traditional Personal Identification Number (PIN) and password security systems, there is a high demand for greater security for access to sensitive or personal information in the Nigerian Banking System. This paper reviews the current practices in Nigeria's customer banking services; reveals the results of a survey and suggests a more efficient biometric framework for a more secured Nigeria Customer Banking System. Customer banking, which includes a wide spectrum of banking services, must be carried out with proper authentication to ensure not only the security of transactions, customers' information and funds, but also the protection of the Banks' global image and brand. It is clear that Information Security and Information Management tend to interrelate in innovative systems thereby triggering the need for sustainability. The uses of traditional forms of authentication such as signatures, Identity cards and PIN have not adequately met this security need. In recent times, biometric technologies have been typically used to analyze human characteristics for security purposes as biometric-based authentication serves as a solidified form of authentication for real-time security processes.

Introduction
The quest for information security in today's world of solutions is one that involves a wide range of activities ranging from encrypted passwords and usernames (used in online systems) to biometric authentication (various methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits). Various sectors make extensive use of the different data security methods available today. Banks have sought for newer and more efficient methods to improve the security of data or assets so as to satisfy their customers and also avoid unnecessary loss. Biometric authentication, one of such efficient methods, has gained a lot of acceptance in various sectors of global human activities. For instance, the 'go cashless' campaign presently raising awareness in the Nigeria banking sector has opened doors for biometric authentication of customer transactions.
Generally, banking sectors requests that a high sense of security be observed due to the nature of its activities - cash withdrawal, cash deposit, fund transfer - and owing to the high value attached to money and the things it can buy. Fraudsters tend to hinge their fraudulent activities on the security lapses and weaknesses in the banking systems, especially in developing countries as Nigeria. In view of this, a more efficient biometric framework is required to bridge the gap between efficient information security and the Nigeria banking system.

The Nigeria Banking System
In the Nigeria Banking System, the major authentication technique used to render customer banking services include **Online Authentication** (the use of usernames, passwords and PIN's for online banking transactions and Automated Teller Machine (ATM)) and **Manual Authentication** (the recurrent use of ID cards, driver's license, utility bills and signature for branch banking transactions), which are challenged in performing effectively with respect to the three major customer activities - **account opening, cash deposit** and **cash withdrawal**. This research paper addresses the low effectiveness of current authentication systems in the Nigeria Banking System in context with four activities - **Branch Banking, ATM Banking, Internet Banking** and **Mobile Banking**.
Branch Banking- A customers' bank account is accessed by interacting with a cashier/teller through deposit slip, withdrawal slip, cheque or bank form for customer activities such as fund transfer, transaction check and account balance checking. Prior to these activities the customer's signature or valid documents are checked for customer authentication against the intended account name and number in the banks' database. Recently, Guaranty Trust Bank Plc. commenced the utilization of Fasttrack PIN Pad device, which is a portable electronic device with a card reader connected to the cashiers' or tellers' computer for customer card transactions (http://www.bellanaija.com/2011/10/06/gtbank-introduces-fasttrack/). This device can be accessed by a customer by inserting his or her ATM card into the device card slot, after which transaction can take place and receipt issued to customer by the cashier. Security Issues-Facial masks have been used by fraudsters who must have mastered an account holder's signature to impersonate the true customer. Also a cashier may not be able to tell the difference between a forged signature and a genuine one when under job pressure or may not have the eye to perceive pressure and depth of the signature in the database, which is judged only by the flow pattern of the signature.
ATM Banking- A customer who applies for an ATM card for his or her bank account is issued one with a PIN and can use any bank's ATM machine to carry

out transactions for cash withdrawal, balance check, mini statement issue, PIN change and mobile phone airtime recharge. On insertion of the ATM card into the machine there is a request for the PIN and when entered wrongly a number of times the card is withheld by the bank's machine. Security Issues- Once an unauthorized person gets a hold of a rightful customer's ATM card along with the PIN, an unauthorized access is granted. Basically, fraudsters carry out ATM scam by inserting a thin, clear, rigid plastic sleeve into the ATM card slot prior to when the customer inserts the ATM card. At the time the customer visits the ATM machine, the machine is unable to read the strip, keeps requesting for a re-enter of PIN, and with extra careless of the customer the perpetrator watches as the PIN is keyed in. After several attempts the customer unknowingly gives up thinking the machine has retrieved the card and walks away after which the perpetrator removes the plastic sleeve along with the card and accesses the customer's funds.

Internet Banking- Customers who request for internet banking services can perform online transactions with their bank accounts. Basically, with the obstacles possessed by online transaction security, the use of a singular password is not considered effective. Hence, the integration of the Transaction Authentication Number (TAN) System is used as an additional security to authorize financial transactions. Security Issues- Though Internet banking incorporates the use of two authentication method, the fact still remains that it provides no security solution when a customers' password or other personal details is used by an unauthorized third party to access the customer's online bank account.

Mobile Banking- With the mobile banking service a customer can carry out transactions such as balance inquiry, mini statement, funds transfer, airtime purchase and payments of bills. For this mobile service, the customer's smart card is tied to his/her phone number along with the PIN for validation. Instead of relying on traditional memorized passwords, singular passwords are requested by consumers each time they want to perform transactions using the online or mobile banking interface. When the request is received the password is sent to the consumer's phone via SMS. The password is expired once it has been used. Security Issues- In Mobile Banking Authentication System the security provided by OTPs is quite reliable but is better if enhanced with biometric authentication.

Recently, the Central Bank of Nigeria (CBN) set a deadline for all ATMs to incorporate biometric features for non-numerate customers. In February 2011, the First Bank of Nigeria Plc., in addition to PIN selection, unveiled the pioneering Biometric ATM (fingerprint authentication) to improve security of its customers' transactions and to explore the unbanked segments of the economy, thereby welcoming the uneducated customers to its benefit and eliminate fear in their minds of being victims of fraud (www.firstbanknigeria.com). These notwithstanding, an early exploration of multi-biometric systems for today's Nigeria banking system would pose a better step for its future financial economy.

Biometric Technologies

Biometrics is the science of identifying, or verifying the identity of, a person based on physiological or behavioral characteristics (Bolle et al., 2003). Biometric technology is a way of automatically recognizing a person by traits such as fingerprints, hand geometry, signature, retina, iris, voice, thermal imaging etc. (Capoor, 2006). Recent advances in reliability and performance and cost drops make these technologies attractive solutions for many computer and network access, protection of digital content and physical access control problems. Biometric systems are used for verifying or recognizing the identity of a living person based on a physiological or behavioural characteristic (Ruud et al. 2003).This method of authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample such as a fingerprint captured during a login. During Enrollment, a sample of the biometric trait is captured, processed by a computer, and stored for later comparison. There are various methods of biometrics recognition currently available - Fingerprint, Face, Voice, Iris, Hand Geometry, Vein Pattern, Retina, Signature and DNA Recognitions. Among these the fingerprint based identification is one of the most mature and proven authentication techniques (Jain et al., 2000). Sitalakshmi and Indika's (2008) SWOT analysis of biometric techniques used commercially reveals that fingerprint, face, voice and signature recognitions form the cheapest biometrics systems to implement. Most importantly, it is the opinion of this paper that the integration of any biometric technology be significant to each customer banking service and in context is able to provide security business solutions beyond measure before cost consideration.

Over the years, biometric technology explored by several banks majorly aims at providing business solutions and best customer services. **Bank of Central Asia, Indonesia** incorporates **fingerprint systems** to secure the processing of high-value electronic fund transactions. If a large transfer is initiated, the teller and possibly a supervisor need to be authenticated by the system before the teller can finalize the

transaction. The teller cannot deny performing the transaction. If under duress, the teller can authenticate with a duress finger (alerting the police) (Krawczyk and Michaud, 2005). **Chase Manhattan Bank** utilizes **voice recognition** for bank transactions where customers enroll with a standard phrase and when entering the bank they go to a podium housing a modified telephone, swipe the bank card (identification), speak the standard phrase (verification) and then receive a receipt to present to the teller. One advantage of this is that the cashier is able to pull the customer's file before they get to the teller, hence conserving time (Krawczyk and Michaud, 2005). The Javelin Strategy and Research's Report (2009) on Multi-Channel Authentication via Mobile Banking, the fingerprint, vein pattern and voice authentications are easy to use formats for biometric identification. The framework suggested in this paper employs three biometric recognition types- Fingerprint, Face and Voice recognitions- and works in conjunction with the traditional authentication systems widely in use today.

Fingerprint Recognition

Finger print recognition involves taking an image of a person's finger tips and recording its characteristics like whorls, arches and loops along with the patterns of ridges, furrows and minutiae. Finger print matching is achieved in three ways (David and Durio, 2002):

i. *Minutiae Based Matching*: stores minutiae as a set of points in a plane and the points are matched in the template and the input minutiae.
ii. *Correlation Based Matching*: superimposes two fingerprint images and correlation between corresponding pixels is computed.
iii. *Ridge Feature Based Matching*: is an advanced method that captures ridges, as minutiae capturing are different in low quality fingerprint images.

To capture the fingerprints, current techniques employ optical sensors that use a Charge-coupled Device (CCD) or Complimentary metal-oxide semiconductor (CMOS) image sensor which are solid state sensors that work on the transducer technology using capacitive, thermal, electric field or piezoelectric sensors, or ultra sound sensors that work on echography in which the sensor sends acoustic signals through the transmitter towards the finger and captures the echo signals with the receiver (David and Durio, 2002). The significant factor in fingerprint recognition is that no two persons have the same fingerprint. Fingerprint scanning has a high patronage due to its consistency and is applied for security and logistics measure in the bank, and other areas such as electronic voters' registration and student registration.

Face Recognition

This biometric technique records face images through a digital video camera and analyses facial characteristics like the distance between eyes, nose, mouth, and jaw edges. These measurements are broken into facial planes and retained in a database, which will later be used for comparison. Face recognition can be done in two ways (Ruud et al., 2003):

i. Face Appearance: employs Fourier transformation of the face image into its fundamental frequencies and formation of eigenfaces, consisting of Eigen vectors of the covariance matrix of a set of training images.
ii. Face Geometry: models a human face created in terms of particular facial features like eyes, mouth, etc. and layout of geometry of these features is computed. Face recognition is then a matter of matching constellations.

Zhao et al. (2003) splits face feature extraction into three forms: generic methods based on edges, lines, and curves; feature-template-based on methods that are used to detect facial features such as eyes; and structural matching methods that take into consideration geometrical constraints on the features.

As a commercial face recognition system, it has advanced technicality and is applied in areas such as information security, law enforcement and surveillance, smart cards and access control (Zhao et al. 2003).

Voice Recognition

Voice or speaker verification combines physiological and behavioral factors to produce speech patterns that can be captured by speech processing technology (Mir, Rubab and Jhat 2011). Voice recognition techniques can be divided into categories depending on the type of authentication domain (Ruud et al., 2003):

i. Fixed Text Method: is a technique where the speaker is required to say a predetermined word that is recorded during registration on the system.
ii. Text Dependent Method: Here, the system prompts the user to say a specific word or phrase, which is then computed on the basis of the user's fundamental voice pattern.
iii. Text Independent Method: This is an advanced technique where the user need not articulate any specific word or phrase. The matching is done by the system on the basis of the fundamental voice patterns irrespective of the language and the text used.
iv. Conversational Technique: verifies identity of the speaker by inquiring about the knowledge that is secret or unlikely to be known or guessed by someone else.

In voice recognition systems, inherent properties of the speaker like fundamental frequency, nasal tone, cadence, inflection etc. are used for speech authentication. The text-dependent systems (fixed text) generally perform better than text-independent systems (free text) because of the foreknowledge of what is said can be exploited to align speech signals into more discriminant classes (Mir, Rubab and Jhat 2011).

Methodology

A survey was conducted for this research and targeted 100 respondents based on random selection. Data was collected via interview and questionnaire. The questions sought to determine:

a. The banking services utilized by the respondents.
b. The method of authentication employed by each respondent's bank for account access.
c. The respondent's level of experience of biometric authentication systems.
d. The method of banking authentication preference.

Findings and Discussions

The results of the survey are depicted in Tables 1-5:

Table 1: Banking Services

Banking Services	Percentage (%)
Branch Banking	100.0
ATM Banking	94.0
Internet Banking	04.0
Mobile Banking	00.0

Table 2: Banking Authentication Technique

Banking Authentication Technique	Percentage (%)
Signature	100.0
ID	00.0
Biometric	00.0

Table 3: Bank Account Authentication Technique Rating

Bank Account Authentication Technique Rating	Percentage (%)
Poor	06.0
Fair	20.0
Good	50.0
Very Good	20.0
Excellent	04.0

Table 4: Biometric Experience

Biometric Experience Technique	Percentage (%)
Fingerprint Recognition	96.9
Voice Recognition	00.0
Face Recognition	03.1
Iris Recognition	00.0
Retina Recognition	00.0
Signature Recognition	00.0
Hand Geometry Recognition	00.0
Vein Pattern Recognition	00.0

Table 5: Biometric Banking Recommendation

Biometric Banking Recommendation	Percentage (%)
Yes	93.8
No	06.2
TOTAL	100.0

Table 1 reveals that most respondents engage in Branch banking and ATM banking with internet banking rarely patronized and no mobile banking services at all. Table 2 shows that 100.0% of the respondents are authenticated in branch banking with signature technique, which is rated fairly in Table 3. From Table 4, 96.9% of respondents have experienced fingerprint recognition system while 93.8% respondents gave high preference to biometric banking authentication as depicted in Table 5. Though there is a low level of respondents with no biometric experience, various factors come into play with regards to access, knowledge of use and general individual perception.

Multi-Biobanking Framework

The Multi-BioBanking framework tries to depict a multimodal biometric system, which is a system that combines more than one source of information for establishing human identity (Mir, Rubab and Jhat, 2011). However, the framework is in no way rigid and can be designed to fit the requirement of the bank.

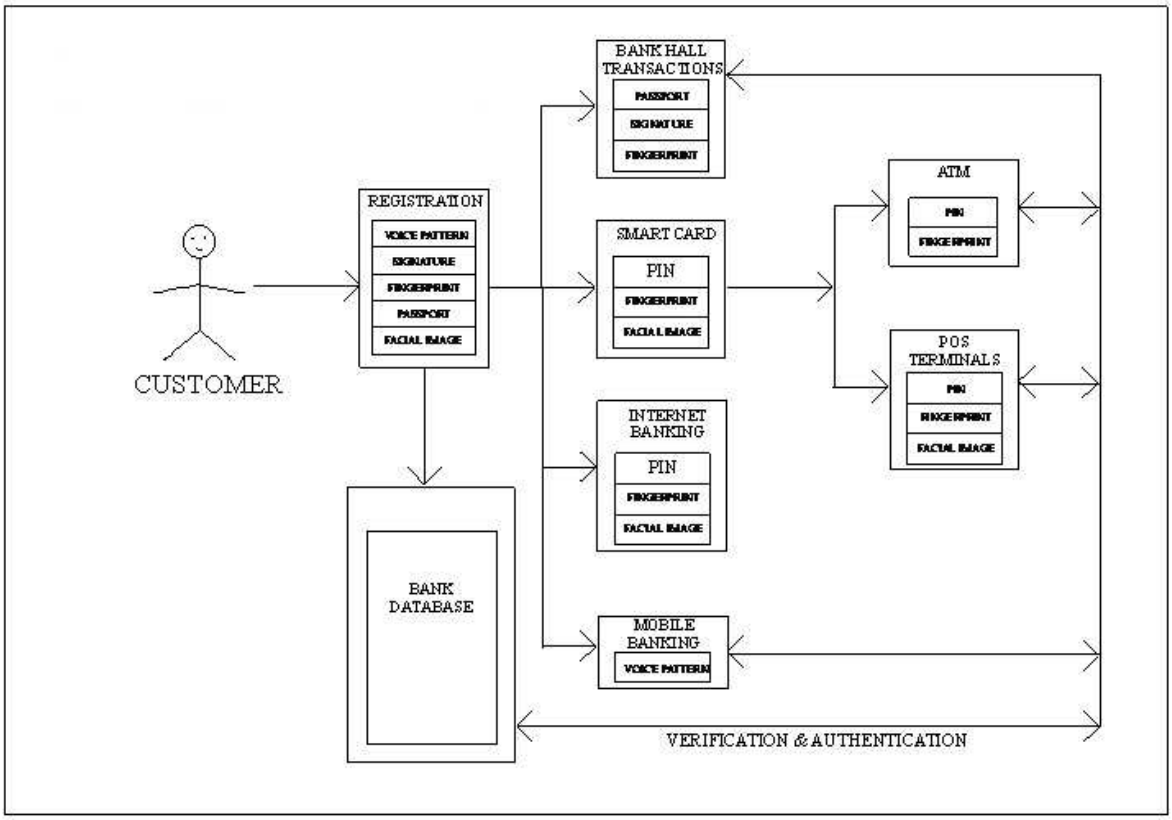

Fig.1 Multi-BioBanking Framework

Registration:

Customers biometric traits required should be collected at the point of opening accounts, which is stored in the bank's database. The form of transaction the customer wishes to carry out with the bank determines what would be embedded in the chip of the smart card that will be assigned. This starts at the initial time the customer comes to open an account with the bank. At the point of registering a new account a biometric trait of the customer such as the fingerprint should be read as part of the requirements for opening a new account. This scan is stored in the customer's record in database. The data is then embedded on the smart card that will be given to the customer, hence utilizing a Smartcard based fingerprint authentication. (Lee et al., 2002; Clancy, Kiyavash and Lin, 2003; Waldmann, Scheuermann and Eckert, 2004).

Bank Hall Transactions:

In addition to the use of signature and passports, transactions within the banking hall, the customer should be authenticated with Fingerprint Recognition. This is achieved using a finger print scanner positioned at each teller's counter to authenticate the customer before any transaction is carried out. Even if the signature can be forged, the fingerprint remains unique to every individual. We provide two case scenarios showing how the biometric authentication will be implemented in addition to the traditional use of signature and passport photograph.

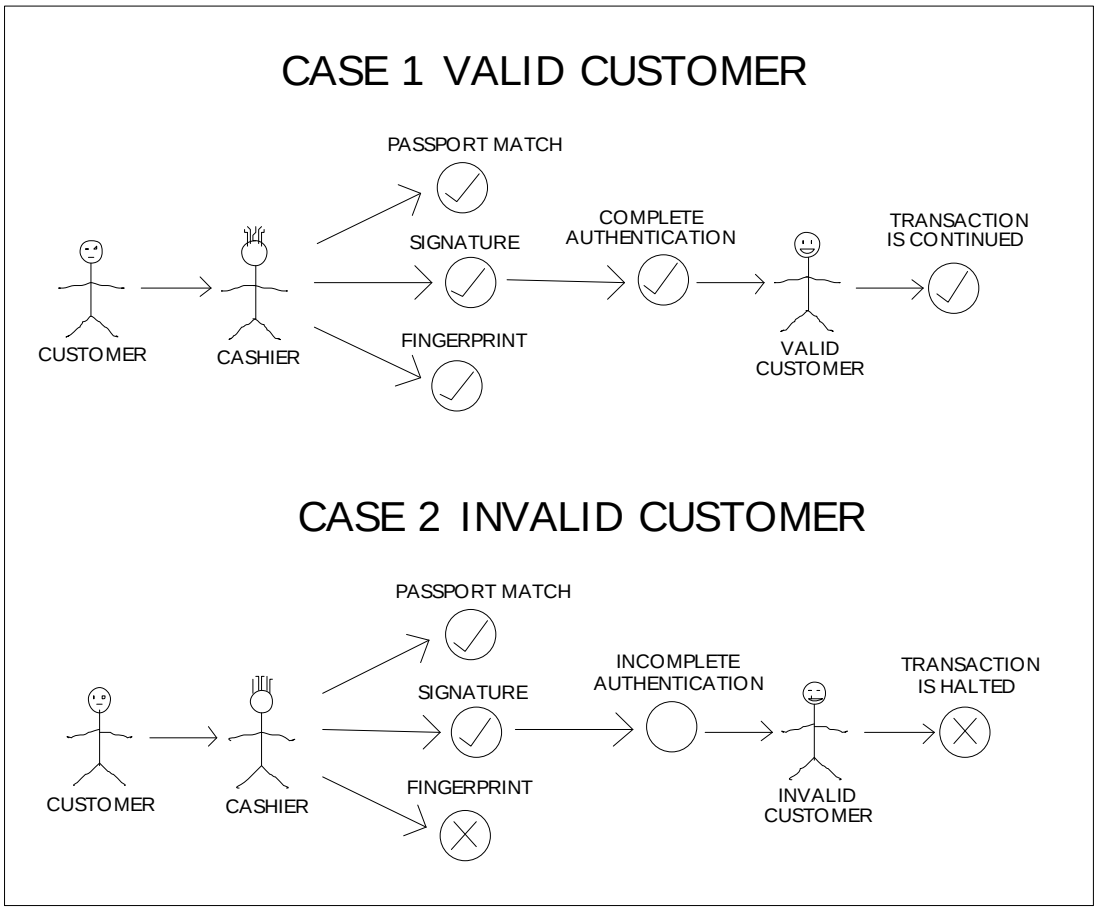

Fig. 2 Illustration of fingerprint recognition used alongside traditional branch banking

Case 1- If on verification, the fingerprint of the customer in front of the counter is a match with that stored in the bank database, the customer is a valid customer.

Case 2- If on verification, the fingerprint is not a match with the fingerprint in the bank database, the transaction is terminated or halted until the customer is able to be authenticated. Else the customer is considered a fraud and security measures will be taken.

Fingerprint Authentication with Fasttrack PIN Pad:

The Fasttrack PIN Pad is an electronic device that basically automates what the cashier or teller does behind the counter and makes the process faster. In terms of security, it implements the security used with the smart card's chip and PIN system. Implementation of fingerprint authentication in addition to the use of PIN on the Fasttrack device will eliminate the possibility of impersonating a customer and the customer's PIN being accessed by a third party.

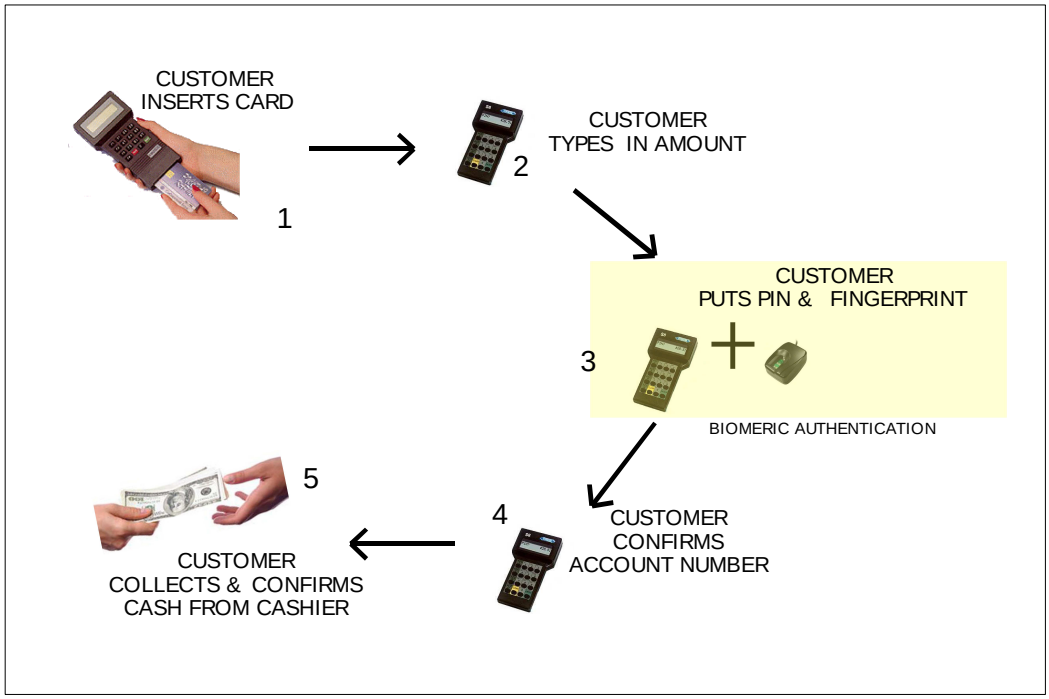

Fig. 3 Illustration showing fingerprint authentication used with the Fasttrack PIN Pad

If at the point of opening an account, every customer's fingerprint is read and stored in the bank database for later authentication, the PIN Pad can then work with a fingerprint scanner, which will in addition to the use of PIN authenticate the customer before the cashier completes the transaction as a valid one.

Smart Cards – ATM and PoS:

If a customer wishes to carry out ATM or PoS transactions may incorporate either or both fingerprint and facial pattern authentication in addition to the PIN, which will be enrolled as part of the customer's identification information in the bank and embedded in the chip. The security feature for enhancing the ATM utilizes the client/server approach. There is a link between the customer's identification information, customer's accounts and records in the bank (server). The network is designed to support a large number of users and uses a dedicated server to accomplish this.

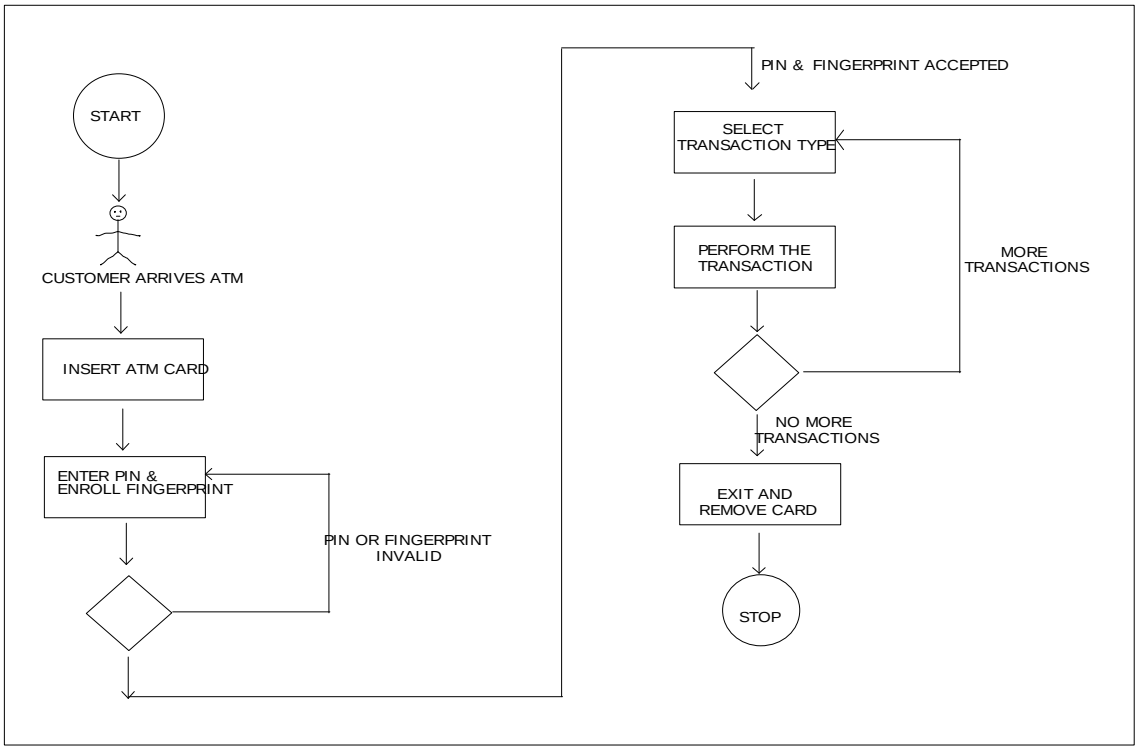

Fig. 4 Combined PIN and fingerprint recognition in ATM

When a customer goes to the ATM to perform any transaction, the customer is asked to provide his PIN and in addition his fingerprint. This will require that ATMs have a fingerprint scanner. Once the card has been verified as authentic, the customer enters a 4-digit PIN, which is submitted to the chip on the smartcard; if the two are a match, the chip tells the terminal the PIN was correct, otherwise it informs it that the PIN is incorrect. Once PIN verification is completed, the ATM tells the customer to provide a fingerprint, which is checked against that in the bank's database for verification and authenticated. Biometric ATM utilization of the customers' fingerprint in addition to PIN implies stronger security and makes it almost impossible for any other person to use the smart card in case of misplacement or theft making it difficult for fraudsters to perpetrate their fraudulent practices.

Internet Banking:

A leading technology in use today with Internet banking is the Face Expert Bank Identification System for Internet Banking (FEBIS-INTERNET BANKING) developed by Asia Software Ltd. It is a biometric identification system for bank clients who conduct their financial operations through the Internet. It enables secure management of clients' financial resources (accounts, deposits) and bank financial operations that are being conducted through the Internet. This special software doesn't require the installation of any additional specific equipment and is easily integrated with information systems used by banks. In order to use this system, the user's PC has to be equipped with a standard web camera. A database of the bank's clients and people who had been previously served by the bank is formed as a normal part of the system operation. A personal biometric card of the client is created when opening an account and contains the customer's personal data and facial image. Each person who applies to the bank to open an account or receive a card is checked through the database with the aim of registering as a new bank client or for identification. The database search is conducted quickly and accurately. In servicing accounts after the registration of a new customer has been accomplished, the customer sets his personal settings (name, password, photo image) to manage the account via the Internet. Personal settings data and web camera photo images are sent to the bank's central server where an automatic comparison is made between the user's biometric image and the biometric data of the client registered in the FEBIS-INTERNET BANKING system. Access to the account and other confidential information is granted only if the biometric and personal data are an absolute match. (http://www.asia-soft.com/en/prod_febis_ib.asp). If a customer wishes to carry out online transactions,

facial pattern and fingerprint will be embedded in the smart card chip. Internet transactions should involve Face Recognition or Fingerprint Recognition for authentication depending on which will be easier to implement by the bank as it fits the customer .

FEBIS-INTERNET BANKING uses a human facial image that serves as a reliable tool against unauthorized access. It easily integrates with other banking systems and doesn't require expenditure for additional special equipment; can present statistical data on accomplished financial operations and form an event journal with facial images; and can be adapted to the organization requirements in any given country (http://www.asia-soft.com/en/prod_febis_ib.asp)

.

Mobile Banking:

Mobile transactions should be authenticated using Voice recognition. Mobile banking is a feature that serves as a backup and gives customers more options in banking. Voice recognition seems to be the most promising area of biometric application in mobile banking (www.javelinstrategy.com). In this case, customers have their voice pattern registered and whenever a transaction has to be carried out via mobile phone, the voice pattern is verified and authenticated.

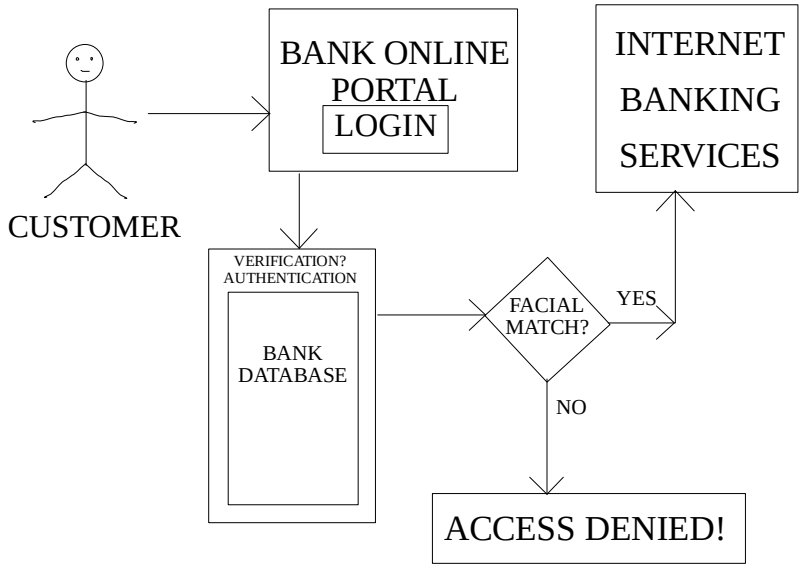

Fig. 5 Facial Recognition in Internet banking

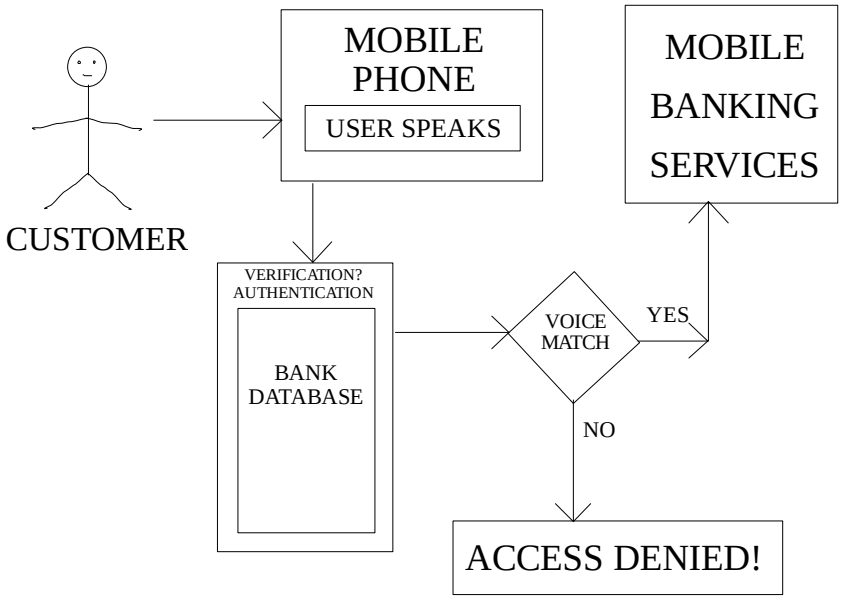

Fig. 6 Voice Recognition in Mobile banking

Though voice can be affected by outside noise (Krawczyk and Michaud, 2005), voice recognition in mobile banking is easy and reliable to use as voice patterns cannot be faked by an impersonator.

Conclusion

The superiority in extended biometric authentication cannot be overlooked. This system when applied would help in ensuring efficient transaction security. The banking industry in Nigeria has been very responsive to better technology as individuals (customers) that depend on banking institutions for various financial transactions tend to increase constantly. Regardless of context, customers need assurance of security for their information or assets in the bank. As biometric authentication takes effect in Nigerian banks a more positive response would be to implement a biometric framework in the customer banking system that incorporates several biometric authentication systems such as the one in this paper.

Recommendation

a. The multi-biobanking framework suggests the following recommendations:
b. Implementation of a multi-biometric system in customer banking authentication should be applied in all banking activities and services, not just ATMs or PoS. This extension would eventually improve the security state of the country and enhance the standard of services rendered to customers.
c. Banks should partner with computer companies to manufacture special computers or machines with in-built multi-biometric recognition devices such as fingerprint and face pattern scanners.
d. Erratic power supply could make implementation of biometric authentication systems handicapped. The government should look into the problem of power if biometric authentication in customer banking is to survive and function properly.

References

Akanbi, F. and Agbo, M. (2012), "Nigeria: Cashless Lagos to Cost CBN, Banks Over N2.5 billion", This Day Live, Published in Microfinance Africa. Retrieved on 05/02/2012 from http://microfinanceafrica.net/technology-and-mobile-money/nigeria-cashless-lagos-to-cost-cbn-banks-over-n2-5-billion/

Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K. and Senior, A. W. (2003), "Guide to Biometrics", Springer, New York.

Capoor, S. (2006), "Biometrics as a Convenience", Security: For Buyers of Products, Systems & Services, Vol. 43 Issue 12, p48-50, 2p.

Clancy, T.C., Kiyavash, N., Lin, D.J. (2003), "Secure smartcard-based fingerprint authentication", ACM workshop on Biometric Methods and Applications, Berkeley, California, pp 45-52.

First Bank Nigeria Plc., "First Bank Launches Nigeria's First Biometric ATM". Retrieved on 05/02/2012 from ttp://www.firstbanknigeria.com/MediaCentre/PressReleases/FirstBankLaunchesNigeriasFirstBiometricATM/tabid/550/Default.aspx

Jain, A.K., Prabhakar, S., Hong, L. and Pankanti, S. (2000), "Filterbank-based fingerprint matching" IEEE Trans. on Image Processing, pp.846-859.

Javelin Strategy & Research's Report (2009), "Multi-Channel Authentication via Mobile Banking: Assessing the Technologies, Vendors, and Solution Providers", Retrieved on 05/02/2012 from https://www.javelinstrategy.com/uploads/files/923.R_MultiChannelAuthenticationViaMobileBankingSampleReport.pdf

Kaushal, N. (2010), "Fingerprints: Historical Background and Future Trends", The Internet Journal of Forensic Science, Vol. 4 No. 2. Retrieved on 04/02/2012 from http://www.ispub.com/journal/the-internet-journal-of-forensic-science/volume-4-number-2/fingerprints-historical-background-and-future-trends.html

Krawczyk, S. and Michaud, C. (2005), "Biometrics in the Banking Industry", CSE 891.

Lee, J. K., Ryu, S. R. and Yoo, K. Y. (2002), "Fingerprint-based remote user authentication scheme using smart cards" Electronics Lett., pp. 554-555.

Maltoni, D., Maio, D., Jain, A. K. and Prabhakar, S. (2003), "Handbook of Fingerprint Recognition", Springer, New York, NY, USA.

Mir, A. H., Rubab, S. and Jhat, Z. A. (2011), "Biometrics Verification: a Literature Survey", **J**ournal of Computing and ICT Research, Vol. 5, Issue 2, pp 67-80.

Nanni, L. and Maio, D. (2006), "Combination of different fingerprint systems: a case study FVC2004", Sensor Review, Vol. 26 No. 1, pp. 51-55.

Owens, J. and Bantug-Herrera, A. (2006), "The Catching the Technology Wave: Mobile Phone Banking and Text-A-Payment in the Philippines". Retrieved on 05/02/2012 from http://www.bwtp.org/asiamicrofinance/documents/JohnOwensCatchingtheTechnologyWave_000.pdf

Venkatraman, S. and Delpachitra, I. (2008), "Biometrics in Banking Security: a case study", Information Management & Computer Security, Emerald Group Publishing Limited Vol. 16 Iss: 4, pp.415 – 430.

Waldmann, U., Scheuermann, D. and Eckert, C. (2004), "Protected transmission of biometric user authentication data for oncard - matching", In *P*roceedings of the 2004 ACM Symposium on Applied Computing (Nicosia, Cyprus), Association for Computing Machinery -ACM-, Special Interest Group on Applied Computing - SIGAPP, pp 425-430.

Zhao, W., Chellappa, R., Phillips, P. J. and Rosenfeld, A. (2003), "Face Recognition: A Literature Survey", ACM Computing urveys, Vol. 35, No. 4, pp. 399–458.