A Framework for the Integration of Biometric Into Nigerian Banking ATM System

Emuoyibofarhe O.J
Department of Computer Science and Engineering Ladoke Akintola University of Technology, Ogbomoso, Nigeria

Fajuyigbe O.
Department of Computer Science and Information Technology Bowen University, Iwo, Nigeria

Emuoyibofarhe O·N
Department of Computer Science and Information Technology Bowen University, Iwo, Nigeria

Alamu F.O.
Department of Computer Science and Engineering Ladoke Akintola University of Technology, Ogbomoso, Nigeria

ABSTRACT
The use of ATMs is a good innovation but the current use of Personal Identification Numbers (PINs) for verifying the customer is plagued with several limiting factors and security flaw.
There is therefore the need to employ more secured verification/authentication technique which is uniquely different for every customer. In this paper, we propose the use of biometrics; a technology that identifies individuals uniquely based on their physiological or behavioural traits to improve the authentication of legitimate account holders. The actual (commercial) implementation of the pseudo model will go a long way in enhancing security while gearing the nation to explore a vital technology (biometrics) that obviously would be useful in order sector of the economy in relation to issues of national identification databases in the nearest future apart from the financial sector.

1. INTRODUCTION
An automated teller machine (ATM) is a computerized telecommunications device that provides the customers of a financial institution with access to financial transactions in a public space without the need for a human clerk or bank teller at any time of the day at the nearest location (Zdene, 2000). On Nigeria's ATMs (powered by Inter-switch Ltd), the customer is identified by inserting a plastic ATM card with a magnetic stripe or a smartcard with a chip (valve card), that contains a unique card number and some security information. Security (authentication) is provided by the customer entering a personal identification number (PIN).

There are various security issues surrounding the operation of ATM, such issues vary from physical attack on the machine, customer's security transaction process secrecy and customer identity integrity (Gary, 2001)
. Considering physical attack on machine and customer's security, measures like assigning a security man to the machine, enclosing the machine in a secured /fenced compound have been employed although this form of insecurity is infinitesimal. Another security issue is the integrity of transaction processes which is concerned with the shielding of vital information as data is being transmitted and processed, this also is catered for by encrypting data to avoid unauthorized knowledge in case of interference (Gary, 2001)

Finally and most commonly, security issue of customer identity integrity is about the most challenging aspect although personal identification numbers (PINs) are used to authenticate and verify users' identity, there are still ways where such measures are rendered ineffective(Stefano, 2002).

The term "Biometrics" is derived from the Greek words bio meaning life and metric meaning to measure. A biometric is a measurable physiological attribute and/or a behavioural characteristic that can be used to identify an individual. The term 'biometrics' is commonly used to mean the automated or computerized recognition of a person through use of such attributes as the individual's fingerprint, voice, or eye structure (Jim, 2007).

Physiological attributes are those attributes unique to your human features; they include fingerprints, face, hand and vein geometry, iris and retinal scan etc. Behavioural attributes on the other hand are concerned with the way you carry out some tasks, they include key strokes (way you type), voice, signature etc. some other features being brought up include gait (the way you walk), ear recognition, odour etc (Jalaynea, 2007)
.

Biometric technologies vary in complexity, capabilities, and performance, but all share several elements. Biometric identification systems are essentially pattern recognition systems. They use acquisition devices such as cameras and scanning devices to capture images, recordings, or measurements of an individual's characteristics and computer hardware and software to extract, encode, store, and compare these characteristics.
Because the process is automated, biometric decision-making is generally very fast, in most cases taking only a few seconds in real time. Depending on the application, biometric systems can be used in one of two modes: verification or identification. Verification, also called authentication, is used to verify a person's identity, that is, to authenticate that individuals are who they say they are. Identification is used to establish a person's identity; that is, to determine who a person is. Although biometric

technologies measure different characteristics in substantially different ways, all biometric systems involve similar processes that can be divided into two distinct stages: enrolment and verification or identification

2. ATM: ELECTRONIC TRANSACTION

Typical ATMs have two input devices (a card reader and keypad) and four output devices (display screen, cash dispenser, receipt printer, and speaker). Not visible to the client is a communications mechanism that links the ATM directly to an ATM host network. The ATM functions much like a PC; it comes with an operating system (the platform for Nigeria's ATM is windows) and specific application software for the user interface and communications.

Whereas most ATMs use magnetic strip cards and personal identification numbers (PINs) to identify account holders, other systems may use smart cards with fingerprint validation.

The ATM forwards information read from the client's card and the client's request to a host processor, which routes the request to the client's financial institution. If the cardholder is requesting cash, the host processor signals for an electronic funds transfer (EFT) from the customer's bank account to the host processor's account. Once the funds have been transferred, the ATM receives an approval code authorizing it to dispense the cash. This communication, verification, and authorization can be delivered in several ways. Leased line, dial-up, or wireless data links may be used to connect to the host system,

3. PHYSIOLOGICAL BIOMETRICS

Physiological biometrics is related to specific and unique frames or shapes of some part of the body which could basically one of the following; fingerprint, hand geometry, vein geometry, iris, or voice. Other physiological biometrics are retina, ear recognition, facial thermogram, DNA, odour and palm prints. However, several survey studies revealed that fingerprint is most preferred biometric feature by most people (Cooper, 2007) and hence this study concentrates on fingerprint.

FINGERPRINT

The fingerprint biometric identification scheme is the analysis of an individual's unique fingerprints. Fingerprints are made up of ridges and valleys on the surface of the finger. Segments on the upper skin layer are the ridges and the lower skin layers are the valleys. Minutia points are formed by ridges. The fingerprint is uniquely determined by the pattern of the ridges and minutiae points. A fingerprint pattern can be split into 5 categories: arch, tented arch, left loop, right loop, and whorl. In order of percentages, the loops make up most of the fingerprint with 60%, whorls make up 30%, and arches make up 10% as shown in figure 1 below

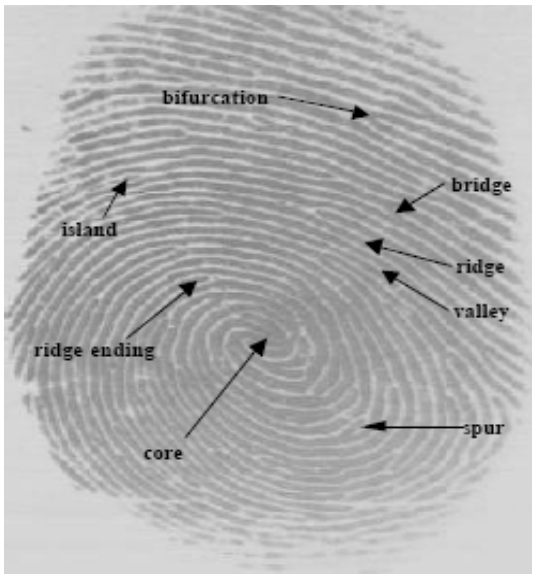

Fig 1: Fingerprint showing different pattern factor

4. BIOMETRIC DATA FORMAT AND PROCESSING LEVELS

Since the computerised systems are known to accept input data, process the data and produce an output data or information as the case may be. Whenever the biometric data must be stored, they must be stored in computerized coded format that are compliant with the standardized formats as in [ISO19794].

4.1 Limitations of Pin

Cards and Personal identification numbers (PINs) are the first and only authentication method in use on Nigeria's ATMs and in agreement with Gary Ross (2001) that there are many reasons why PINs are not good enough: Some of these reasons include:

➔ PIN does not prove the identity of the card holder – just that the user knows the PIN

➔PINs can be forgotten leading to user frustration and cost of card/PIN replacement.

➔PINs can be mistakenly used with incorrect cards due to proliferation of cards/PINs.

➔4 digit PINs only provide a variability of 1 in 10000.

➔People write down PINs as memory aid but risk fraud

➔PINs are easily transferred or distributed

➔PINs can be "stolen" by observation or fraud measures

Biometrics could provide a more secure, easier to use alternative.

Ideally biometrics:

- Proves the claimed identity of the card holder
- Cannot be forgotten
- Has very high variability
- Cannot be transferred or stolen (surgery, 2D and 3D copies and severed body parts should not work *ideally*)

With the correct choices and application of a biometrics system, all of this can be valid. As mentioned, biometric systems have replaced card/PIN in many physical access

security systems, but do not have widespread use in self-service terminals, particularly ATMs (Pat et al 2000)

Cooper (2007), compares the drawbacks with the advantages of different biometric types. Tables 1 and 2 show results of the comparison for fingerprint and hand

Table 1: Fingerprints

Advantages	Disadvantages
Can be placed on a smart card for an added degree of Authentication	Higher risk of false rejection (a rate that authentic users are denied or prevented access to authorized areas, as a result of a failure in the biometric device)
Low instances of false acceptance (a rate that fraudulent users or non –users are allowed access to systems or areas, as a result of failure in the biometric device)	The degradation of the fingerprint caused by occupation, age or even trauma.
Low cost	
Integration is easier	
Fingerprint readers are small in size.	

Table 2: Hand

Advantages	Disadvantages
Easy to use	Injury or trauma degradation can make the print hard to read
Easy to integrate	The hand itself is not unique. It is the parameters that makes it unique
Does not significantly change after ageing	Does not work well for people with arthritis
Used to improve security, accuracy and convenience for access control time and attendance	Accuracy is low
Can work with dirty hands	Fairly expensive

Apart from the physiological biometric type comparism, Cooper also did comparism for behavioural biometric types:
Considering the analysis by Cooper, one could see that the fingerprint poses a better balance between ease of use, ease of integrating into pre-existing structures and cost. Although there are other equally good biometric types but they do not fit into the uniqueness of ATM transactions since ATMs are much in number, one need to consider how many people will be comfortable using strenuous authentication method.

However, in the case of assistive technology, one could put physically challenged individuals into consideration, for instance, people with damaged fingers could have the opportunity to use voice or biometrics and since it will be extremely weird to have damaged fingers and at the same time be dumb and blind.

4.2 Authentication: Totally Different From Identification

Whenever a biometric system is employed, it is either for authentication/verification or identification. According to the report submitted by Keith A. Rhodes (September, 2003) of the General Accounting Office (GAO) of the United State, biometric systems can be used in one of two modes: verification or identification. Verification—also called authentication—is used to verify a person's identity—that is, to authenticate that individuals are who they say they are. Identification is used to establish a person's identity—that is, to determine who a person is.

4.3 Fingerprint Matching

According to Zdene, íha and Václav (November, 2000) they affirmed that fingerprint matching techniques can be placed into two categories:

- minutiae-based and
- correlation-based.

The **Minutiae-based** techniques find the minutiae points first and then map their relative placement on the finger. Minutiae are individual unique characteristics within the fingerprint pattern such as ridge endings, bifurcations, divergences, dots or islands as shown in figure 1 above.

REPRESENTATION OF EXISTING SYSTEM

The existing system could be depicted as shown in figure 2 below where authentication of the customer is based only on the PIN he/she supplies.

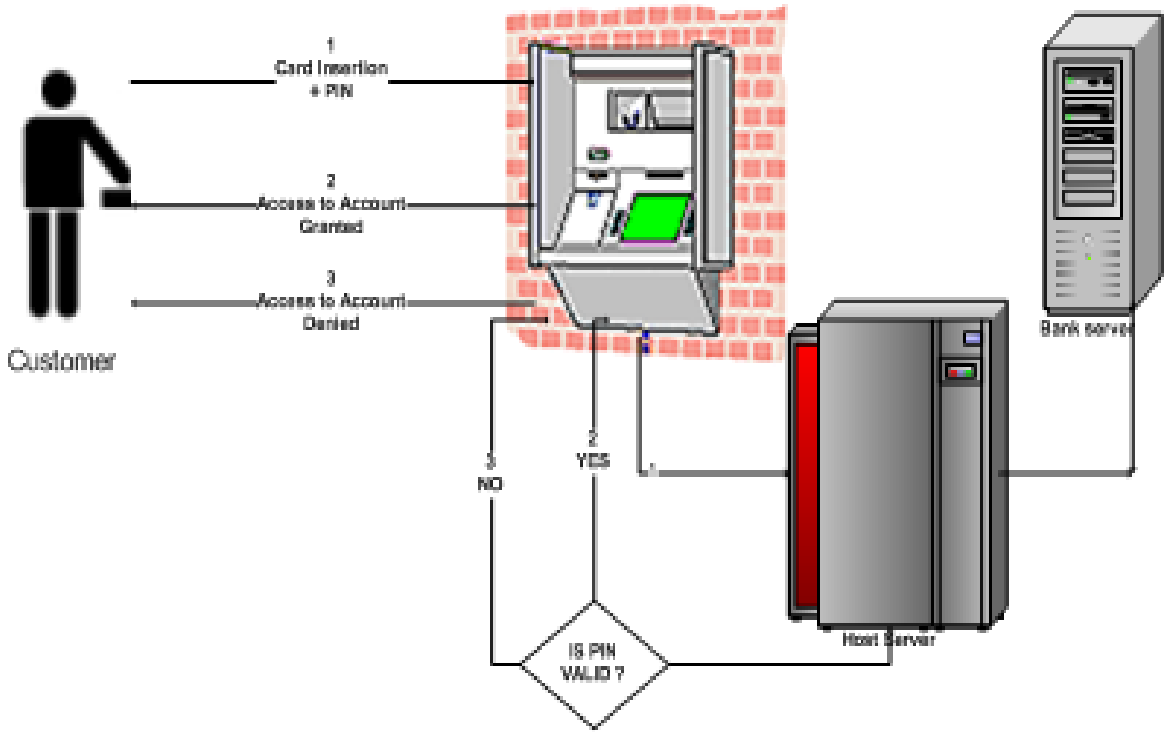

Fig 2 ATM transaction using PIN only

5. RESULT OF SURVEY

The survey was carried out, sampling 200 people in a higher institution, 96.9% of had at least one ATM card and 92.6% at least fear one of the following "card theft", "card damage" and "forgetting of PIN".

It was discovered that 30.7% knew much, 36.2% knew little and about 40% knew nothing about biometrics. It was also

discovered that 88.3% would appreciate the integration of biometric technology into ATM transaction, while 11.7% are either not interested or indifferent.
The table below shows the type of biometric device preferred by people

Table 3 showing preferred biometric device

Biometric Device	Fingerprint	Voiceprint	Iris Scanning	Signature Strokes	Indifferent
Percentage	63%	4%	23%	5%	5%

After closer examination, it was discovered that the respondents prefer Fingerprint followed by iris scanning to the other Biometrics. This is adequately shown by the short Table 3 above showing the percentages of the various types of Biometrics.
It is based on the preference we deduced from this survey that this paper geared towards using fingerprint scanner as a case study.

Data Storage is fundamental to the privacy, security and usability of biometric systems.

There are several points where data must be carefully protected including:

- At point of capture (at the sensor);
  In transmission to the template database; and
- The template database itself.

The template can be stored in a number of locations including:

- The biometric device (sensor);
- A central database accessed by the sensor; or
- A card or token (with bar code, magnetic stripe, RFID chip, PC Card or smart card).

However, for the purpose of this paper, the processed templates are to be stored in a central database where the Host processor (by the service provider) could access them.

In verification systems, the step after enrolment and storage is to verify that a person is who he or she claims to be whenever they are at the Automated Teller Machine for withdrawal or any other form of transaction. After the individual provides finger he or she enrolled with, it is scanned afresh, generating a trial template that is based on the vendor's algorithm. The system then compares the trial biometric template with this person's reference template, which was stored in the system during enrolment, to determine whether the individual's trial and stored templates match as depicted below

Fig 3: Verification process

THE NEW MODEL

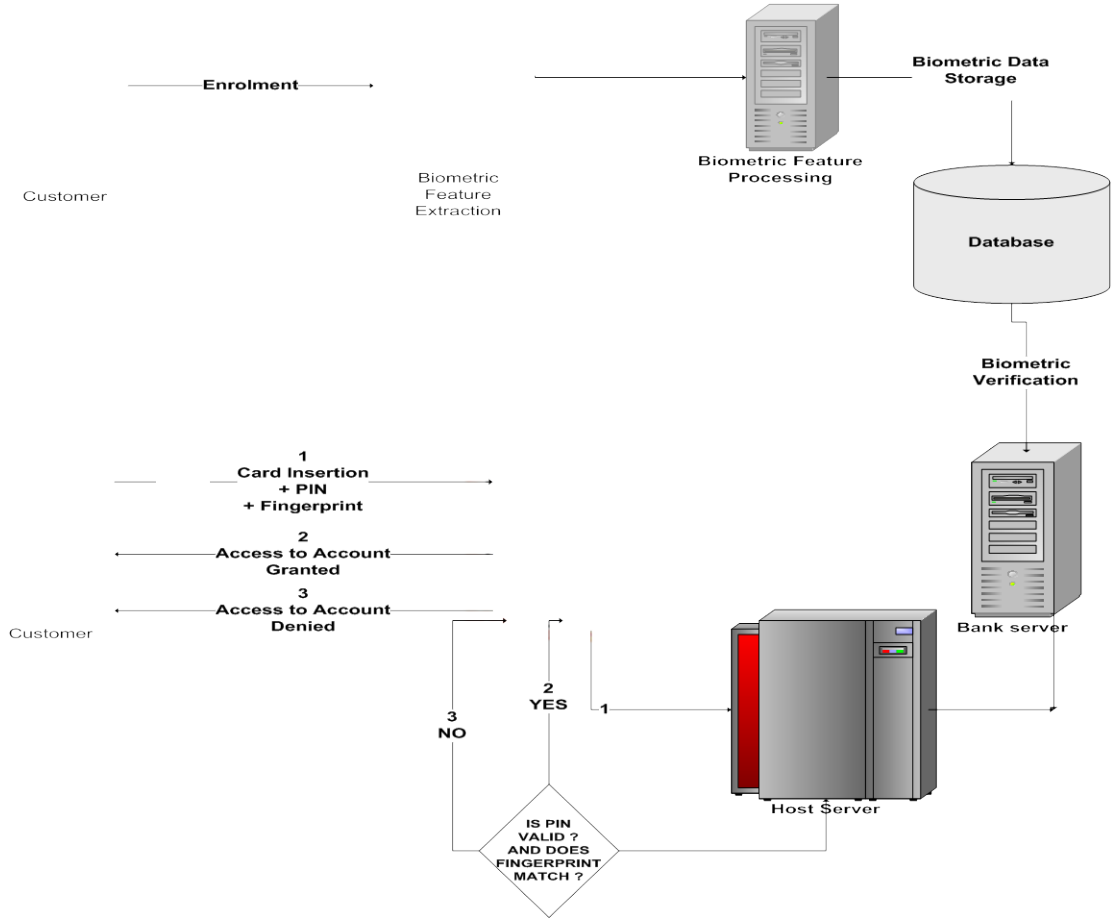

Fig 4: ATM using PIN and Fingerprint for verification

This new model is explicit in the sense that the new system does not require that the old be discarded but that there should enhancement of infrastructure. Firstly, customers do the enrolment of their fingerprints at their various banks where the data is stored against their existing information. Afterwards, any subsequent transaction at the ATMs would require the fingerprint for authentication. The fingerprint scanners that would be employed must be from the same vendor, and the software used for processing and retrieving fingerprint templates must be compatible with the existing operating system platform.

6. MODEL SIMULATION IMPLEMENTATION PHASES AND TOOLS

Although, we do not have an ATM machine, neither do we have the fingerprint scanner with its associated databases to mention a few but the whole concept of the proposed system is portrayed in the remaining part of this section. However to explain the concepts that pertains to this paper, we have employed the following tools for proper and clear illustration

- **SFINGE package** : A synthetic fingerprint generator application that uses up to ten factors to generate unique fingerprints
- **GrFinger package** : A package that aides synthetic fingerprint extraction, processing, storage of unique generated codes for fingerprints generated by SFINGE above
- **Java Program** : Codes written in java to illustrate the Automated Teller Machine

Apart from the fact that the afore mentioned tools are used, the illustration in this paper will also be in three different phases relating to the tasks performed by the tools afore mentioned and likewise relating to the three distinct stages of biometric processing:

- Enrolment (screening, feature extraction and feature processing)
- Storage
- Verification/Authentication

However, the explanation would be made by the tools we have chosen in this paper.

7. GENERATING UNIQUE FINGERPRINT

In this work, the fingerprints used are not from fingerprint scanners but they are generated using SFINGE. In Figure 5, the application is portrayed, but before the unique fingerprint is generated (as shown on the right side of the figure), one as to prompt the system to chose unique degrees of different finger characteristics through ten (10) stages.

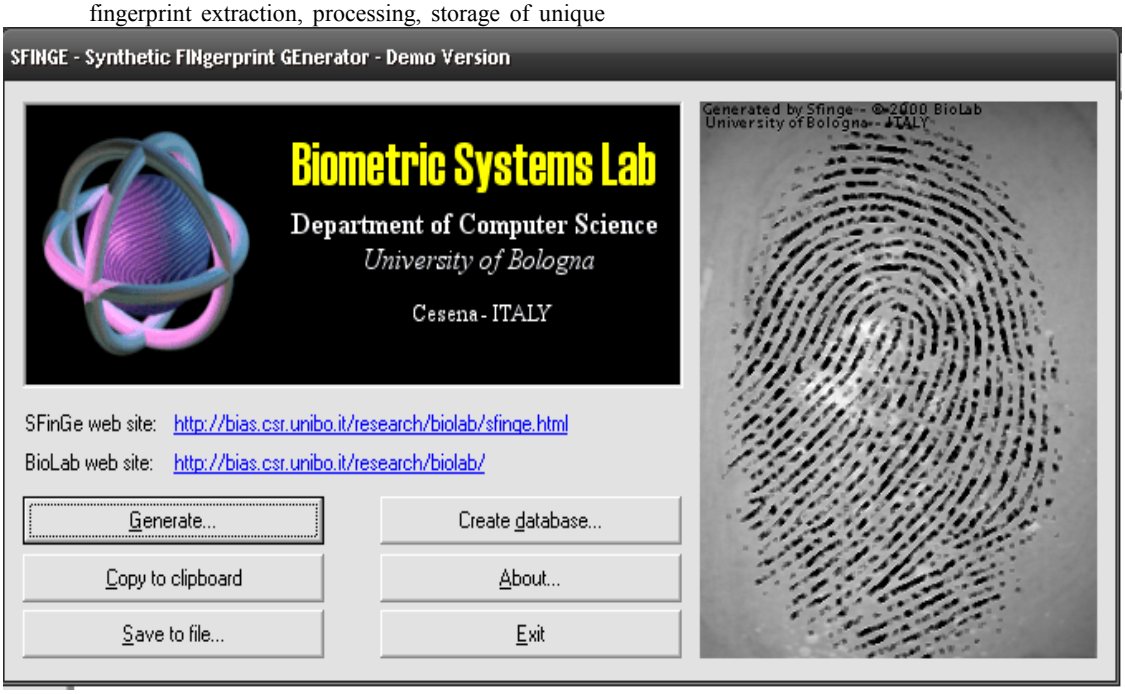

Fig 5: Home page for SFINGE

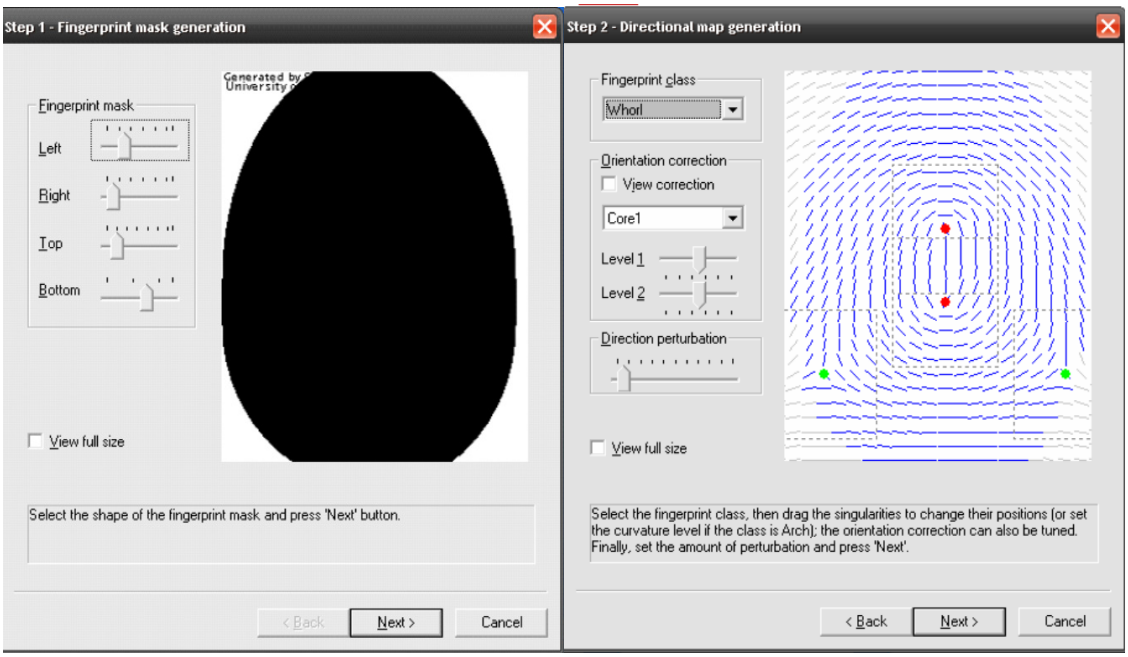

Fig 6: **Steps 1 and Step 2**

In step 1 (figure 6), you are to generate the fingerprint mask, indicating the region the mask covers by the left, right, top and bottom buttons.
In Step 2, you are to indicate the levels of the core or shapes of the arc of the finger and the portion of the finger they are situated (fingerprint class).

Step 3 and Step 4
The third step has to do with the ridge pattern of the finger, one could increase the density of the ridges as well the seed.
Step 4 gives room for applying scratches on the finger which is also a realistic occurrence
In real life applications.

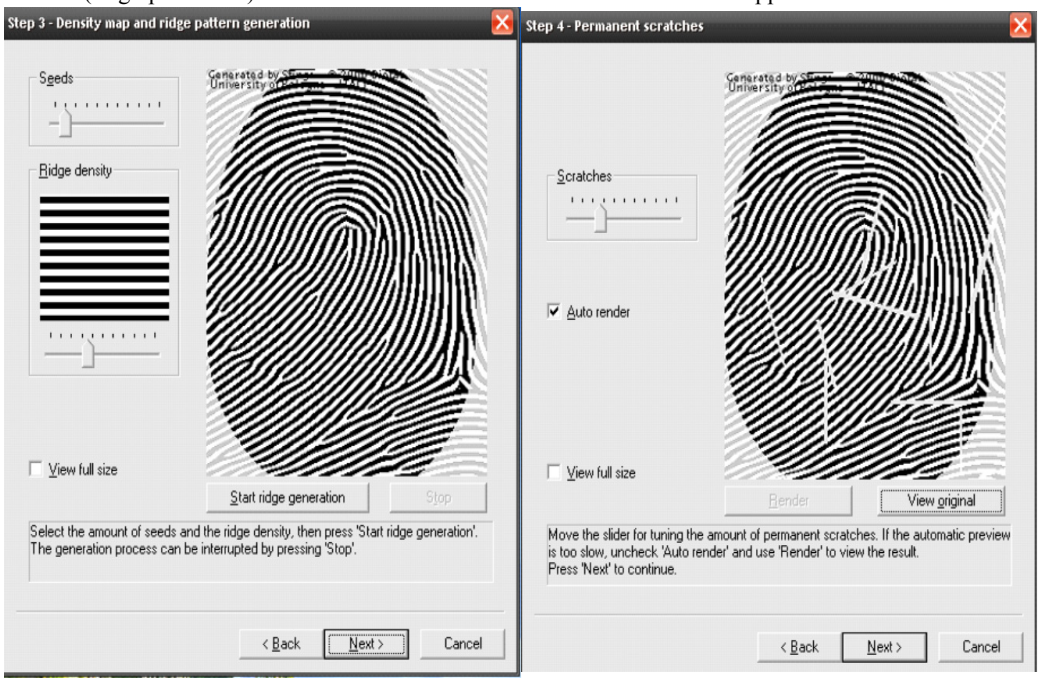

Fig 7: Step 3 and Step 4

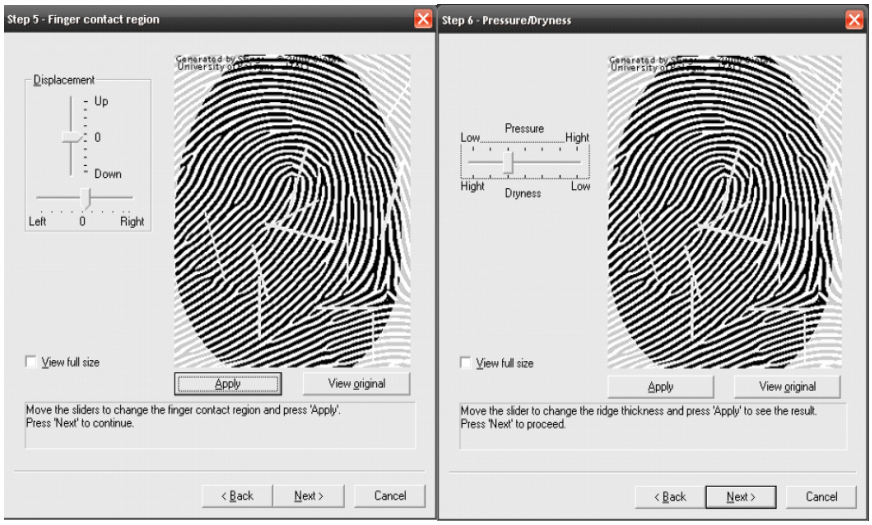

Fig 8: Step 5 and Step 6

Step 5 and Step 6
In step 5, the contact region of the finger is specified by indicating the level of displacement either in the Top-Bottom or Right-Left manner.

In step 6 one may specify the degree of pressure or dryness of the finger (see figure 8)

4.2.5 Step 7 and Step 8
The figure below depicts steps 7 and 8

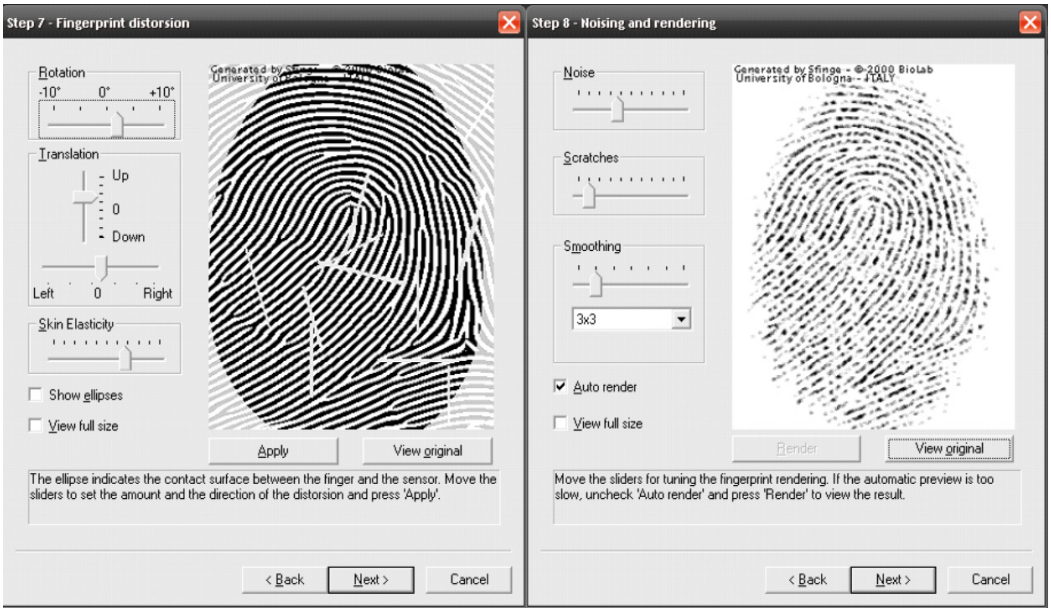

Fig 9: Step 7 and Step 8

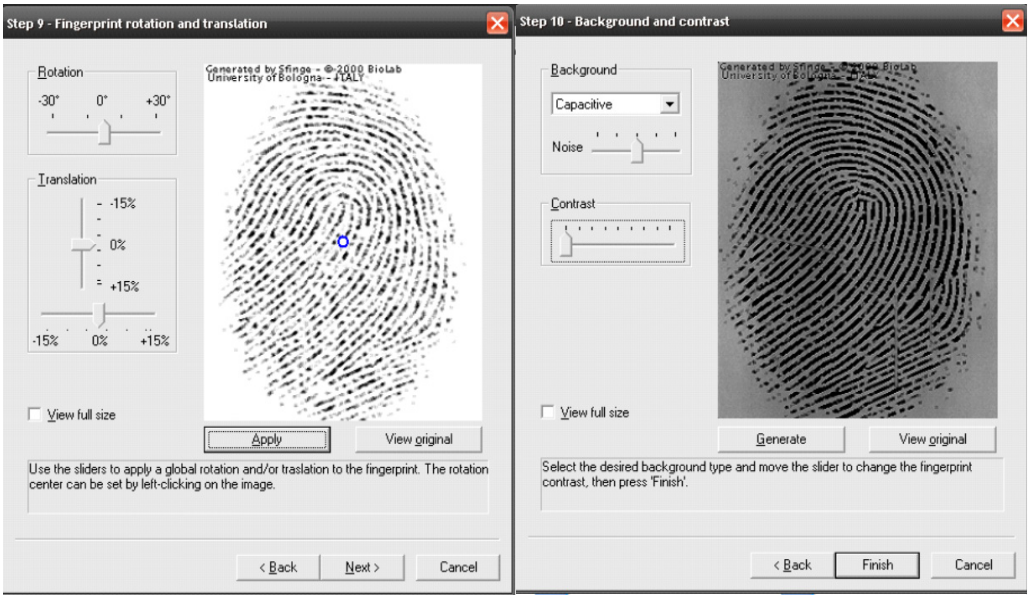

Fig 10: Step 9 and Step 10

Both steps 7 and 8 according to figure 9 could be used to distort or smoothen the finger being generated.

4.2.6 Step 9 and Step 10

The figure10 above shows the last two stages encountered before the template generated in figure 5 is derived.
Step 9 allows for transition and rotation of image generated from step 8 while Step 10 gives room to choose the background of device if it be optical or capacitive as well as indicating the contrast level of image.

Once steps 9 and 10 are through the "save to file" button is pressed while the appropriate folder is chosen to save image. It must be noted that this folder must be accessible by the GrFinger application that will eventually complete the enrolment phase.

7.1 Completing the Enrolment Phase

After the SFINGE application has done the fingerprint generation the GrFinger application is loaded, in the menu bar (See figure 11) one would choose "load from file", and make sure you load from the folder you saved in with SFINGE, after which a dialogue box will ask for resolution (you could choose 256). Once this is done, click on the "Enroll button", this will automatically assign a unique "id" to the enrolled fingerprint.

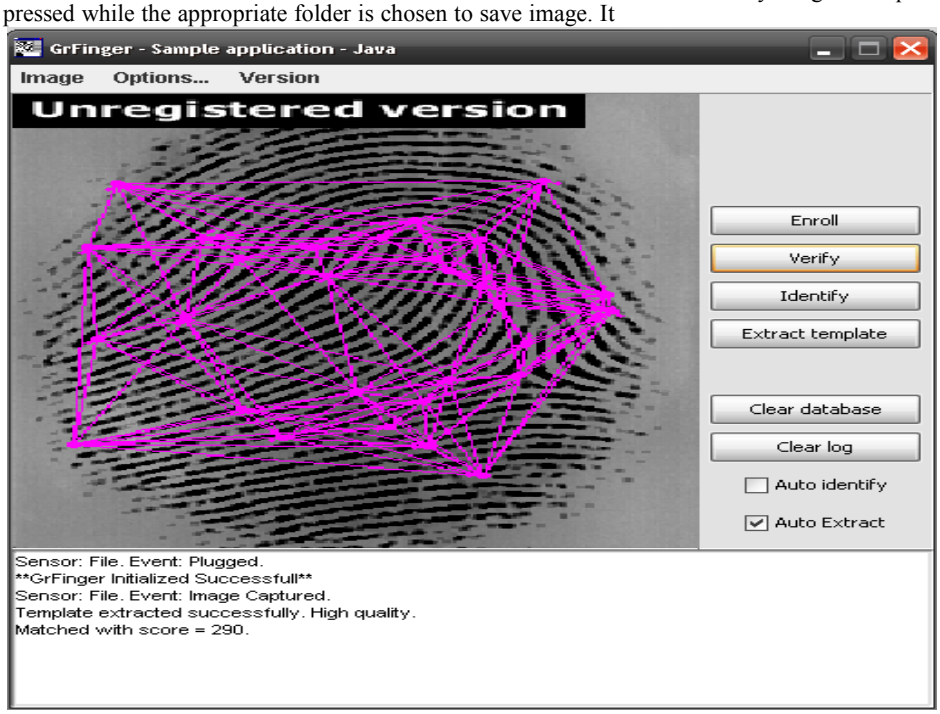

Fig 11 Enrolling and verifying with GrFinger

7.2 Verifying the Fingerprint

After the fingerprint has been enrolled, for one to verify, you will be asked to supply the id of the fingerprint as shown in the dialog box in Fig 4.3.2, after which you click "Verify" if you supply the id of another fingerprint in the database, it will load, compare and report an error but if it tallies it will load, compare and it will be reported that the fingerprint matches. The purpose of this research work is not to identify (i.e. 1:many comparism) but to verify (1 : 1 comparism), therefore, the "identify" button won't be clicked.

7.3 The System Requirements

Apart from the illustration of this chapter, one need to specify the system requirements beyond the scope of simulation especially if it is to be physically implemented.The system being proposed is comprised of different units, components as well as people:

1. Hardware requirements
2. Software requirements
3. People (including experts and personnel)

7.4 Hardware Requirements

1. Automated Teller Machine
2. Fingerprint Scanner
3. Cable connectors (serial or USB) depending on the fingerprint scanner
4. A secure case (also to be attached to/located in ATM housing)
5. UPS (uninterruptible power supply)

7.5 Software Requirements

1. Operating system Software (Windows NT/XP/2000, LINUX)
2. Application Software (Preferably built in Java ,C# or VB.net)
3. Database package (MySQL or Oracle)
4. Fingerprint Scanner drivers and Setup software (depends on the vendor patronised)

7.6 Human Resource Requirements

1. ATM operators
2. Application Software Programmers
3. System Software programmers
4. Fingerprint biometric experts
5. Database administrators
6. System testing engineers
7. Users

8. CONCLUSION

Many private companies and government agencies are seriously considering biometrics for adoption in a broad range of applications outside of law enforcement. It is estimated that losses due to identity fraud in welfare disbursements, credit card transactions, cellular telephone calls, and ATM withdrawals total over $6 billion every year (Microsoft Encarta 2007). For this reason, various organizations are adopting automated systems for identity authentication to improve customer satisfaction, increase cost savings, and improve operating efficiency. ATMs are a good example of the need for better identity authentication. At present an ATM identifies a person as a client after the person inserts an ATM card into the machine and enters a personal identification number (PIN). This method of identification has its drawbacks. According to researches made, the findings proved that it is possible to forget one's PIN or someone else could discover it, while others at one point in time have given their cards out to another person in order to help them withdraw some amount of money. All these and many more would have defeated the protection offered by a PIN when an ATM card is stolen.

Electronic commerce and electronic banking (e-commerce and e-banking) are two of the most important areas where applications of biometrics have emerged. Although it has not been well embraced for integration into ATMs in the western civilized world due to cost as well as the extent to which the ATMs without biometrics have been deployed before now. However, just like India, Nigeria is in its economic growing stage which makes it easier to integrate such biometric technologies without much constraint compared to advanced civilized western communities such as the United States

Apart from the application of biometrics into ATMs, it should not be a surprise that computer networks and security for information systems is another important area for biometric applications. Gaining access to /logging in to remote databases is another. There are forecasts by some experts who anticipate that more and more information systems, computer networks, and World Wide Web sites will use biometrics to control access and for other security purposes.

Cost might be an arguable constraint in the implementation of integrating biometric technology into Nigeria's ATMs but it should however be noted that just as some Nigerians quickly got their way into manipulating and defrauding others through the internet technology barely five years after its evolution in our country, one should know that it would only be a matter of time before the security of ATM transactions would be bridged if proper prevention logistics are not integrated into security of the ATMs.

9. REFERENCES

[1] Automated Teller Machine (2007)http://en.wikipedia.org/wiki/Automated_teller_machine
[2] Biometric (2007); http://en.wikipedia.org/wiki/Biometrics
[3] Chris Roberts November (2005) "Biometrics"
[4] Express Computer (2007) "ATM banking Without A PIN"
[5] Gary Ross (2001) "Biometrics: A Self-Service Viewpoint", NCR Corporation Inc
[6] Gerrit Bleumer "Biometric Authentication and Multilateral Security"AT&T Labs-Research, Shannon Laboratory, Florham Park, NJ 3-4

[7] Jalaynea A.Cooper (2007) "Did I Do That? A Current Analysis of Biometric Technologies"
[8] Jim Bowen (2007) "How ATMs work": http://www.howstuffwoks.com/HowATMworks
[9] Jim Bowen (2007) "How Biometrics work" http://www.howstuffwoks.com/HowATMworks .
[10] Keith A. Rhodes of the General Accounting Office (GAO) of the United State ("Information security : challenges in using Biometrics", September 9 2003)
[11] McGill University: School of Computer Science (1999); DATA STRUCTURES AND ALGORITHMS Project #32: PICTURE REPRESENTATION USING QUAD TREES
[12] Pat Niemeyer ,Jonathan Knudsen (May 2000) "Learning Java "
[13] Quadtree (May 2008); http://en.wikipedia.org/wiki/Quadtree .
[14] I/O Software(TM) (2002) "Requirements and Analysis - The Path to Biometric Standardization"
[15] Sariel Har-Peled (2008) "Quadtrees - Hierarchical Grids"
[16] Stefano Bistarelli, Francesco Santini and Anna Vaccarell (2002) "An Asymmetric Fingerprint Matching Algorithm for Java Card™".
[17] Steve Whelan(2003) "Automated Teller Machines",CGAP IT Innovation Series.
[18] Zdeneˇk Rˇ íha and Václav Matyáš (2000) "Biometric Authentication Systems", FIMU Report Series