International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.2, Issue No.11, pp : 1132-1138 1 Nov. 2013

An Enhanced Technique in ATM Risk Reduction using Automated Biometrics Fingerprint in Nigeria

Alexander .N Ndife[1], Emmanuel .O Ifesinachi [2], Anthony .U Okolibe[3], Davies .K Nnanna[4]
[1] Electronic and Computer Engineering Dept., Nnamdi Azikiwe University, Awka
[2] Electronic Development Institute (ELDI), Awka,
[3, 4] Computer Warehouse Limited (CWL), Lagos.
[1] alexndife2003@yahoo.com, [2] ifesiobi@yahoo.com [3] okolibe2@yahoo.com , [4] kayceyvik@gmail.com

Abstract : ***An Enhanced Technique in Automated Teller Machine (ATM) Risk Reduction using automated Biometrics fingerprint in Nigeria was carried out as a preemptive measure to sub mantle the fraudulent activities of fraudsters in the banking industry. This research was aimed at developing an Automated Fingerprint Identification Machine (AFIM) that will enhance the performance and security of bank customers' accounts now cashless policy is being enforced. This work adopted software development lifecycle (SDLC) as well as secured harsh (SHA) algorithm to determine the interface between the scanner and the proposed system and also the threshold of the scan fingerprint image. A SecuGen Hamster plus device was used on a Dell Inspiron machine for obtaining the fingerprint. Cross-correlation pattern matching schemes for matching and aligning the enrolled sampled image on the single singular point (as a reference point) was adopted for authentication. However, the model implementation showed*** robustness in security and service delivery performance.

Keywords: Automated Teller Machine (ATM), Automated Fingerprint Identification Machine (AFIM), Biometrics, Cross-Correlation.

1 Introduction

No doubt, transition from the traditional monetary instruments from paper and metal based currency to 'plastic money' in the form of credit cards, debit cards etc., brought about the world wide use of ATM as the fastest means of cash dispenser currently in use. Unfortunately, the convenience and safety of this technology has been lessened by the activities of the fraudsters [1]. Incessant complaints by users of ATM facilities in banking industry in Nigeria on the fraudulent activities being carried out in their accounts necessitated this study. Presently in Nigeria, ATM crimes have become a threat not only to customers, but also to bank operators due to its vulnerabilities [2]. Consequently, propensity to participate in this fraudulent practice by ATM fraudsters has increased tremendously following the latest cashless legislation in Nigeria expected to be 100% compliance by 2014. Moreover, the security layout of ATMs in Nigeria is still at password-based authentication only using cryptographic techniques. In a conventional cryptographic system, the user authentication is possession based. Therefore the weakness of such authentication systems has always being that it cannot assure the identity of the maker of a transaction; it can only identify the maker's belongings (i.e. cards) or what he remembers (passwords or PINs etc.) [3]. However, with the advent of biometrics based authentication which has normal PIN login procedure with secured fingerprint ID, security vulnerability will be drastically reduced as well as improved the quality of service. This technique will not only protect the data from theft and alteration but also be used for user authentication. Recently, fingerprint authentication has been the most popular authentication though it is infeasible to encrypt a large volume of fingerprint image using conventional cryptography for the purpose of centralized fingerprint matching [4]. Therefore, it becomes imperative to embrace a more robust technique like the proposed biometric authentication i.e. to integrate encryption key with biometrics (fingerprint) for easy identification and authentication of users to reduce the propensity to fraud.

2 Related Research Efforts

In some related efforts [5], neural network-based methodology was adopted in matching the fingerprint of intended users through the view of the patterns and groove patterns of the fingerprints. The model used in this study works very well on binary images and grayed scanned were achieved. In this research work, once group is tracked, pattern can then be tracked while achieving high accuracy. Incidentally, the limitation of this work is that network inaccessibility could pose a great threat.

In [6], the researcher used a model of multi-layers of convex polygon to implement fingerprint verification. In this work, extraction of fingerprint image was based in specified area in which the dominant brightness value of fingerprint ranges. Its major limitation is that faking is possible and faked authentication cannot be detected easily. However, these reviewed research efforts was carried out using a single biometric check without any form of cryptography, hence, could not guarantee a reliable security solution. Therefore, this limitation necessitated the proposed

biometrics technology that would base on SDLC scheme for easy determination and verification of identity through physical characteristics.

However, this proposed technique would make it possible to confirm or establish an individual's identity based on " who he or she is," rather than by "what he or she possesses" (e.g., an ID card) or "what he or she remembers" (e.g., a password). It will also defined a biometric system as a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database [7].

3 Methodology

This work leveraged on level 1 formal method – a mathematical based technique for specification, development and verification of software and hardware systems. The essence of this is that statistical models contribute to reliability and robustness of any engineering design. Meanwhile, level 1 was adopted due to the fact that it involves safety and security of high performance system. Since this work intends to develop an Automated Fingerprint Identification Machine (AFIM), Software Development Life Cycle (SDLC) model and Object Oriented Analysis and Design (OOAD) model will be used. Computational process model for fingerprint recognition pattern matching for aligning the enrolled and sampled image in the AFIM will be developed for the enhancement of performance and security of customers' bank account. In this work, fingerprint pattern matching and verification was represented in five phases as shown in fig.4. The data acquisition component is the first phase, followed by the second phase comprising the preprocessing steps. The third component employs a feature extraction algorithm to produce a feature vector whose best describe the characteristic of the fingerprint image notwithstanding the quality of the input image. The fourth component of the system generates the subject fingerprint image model. The last component compares feature vectors to produce a score which indicates the degree of similarity between the test fingerprint and subject fingerprint models. A SecuGen Hamster plus device was used on a Dell Inspiron machine while running V.Net framework for developing the software interface for AFIM. The device is the improved version of SecuGen's versatile fingerprint reader with Auto-On™ and Smart Capture™.

3.1 AFIM Design Model

The AFIM system model of this research started with a detail description of the system as shown in the flowchart of fig.1. This was developed bearing in mind the series of events a bank customer normally undergo when using ATM in making withdrawal on his/her account. The implementation approach in this work adds a new feature that will facilitate a pattern matching mechanism for thumb prints. This implies that each customer having their account in the respective branch will have to submit the impression of their thumb while applying for ATM card henceforth. As earlier mentioned, the design approach of this work added a new feature that facilitates a pattern matching mechanism for thumb prints using a secure hashing algorithm (SHA). This embeds the personal details of customer on the magnetic tape via SHA in the context of cryptography. For security functionality of AFIM: personal details of the user have to be hashed including the fingerprint thumb impression stored in the bank database; and SHA function (1) and hashed value must be equal.

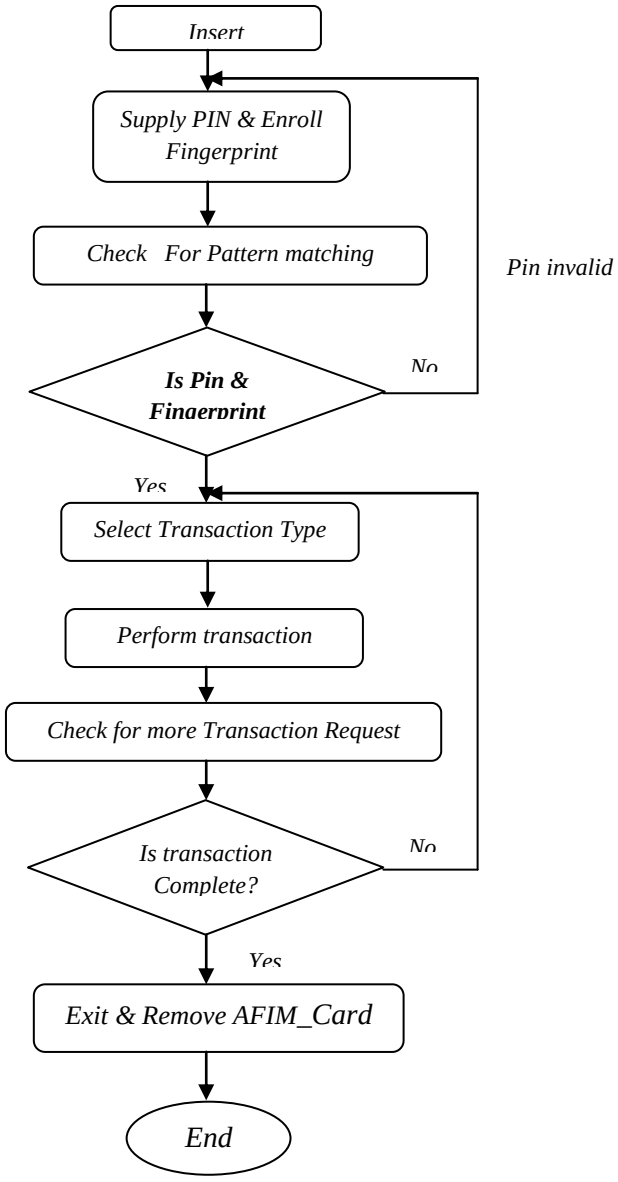

Fig. 1 Design System Flowchart

This work modeled the architectural component of an AFIM with discretional access control. For the purpose of this work, let:

AFIM_Card represent users' cryptographic card
AFIM_keypad represent the device input keypad
AFIM_Finger represent the AFIM finger input instance
AFIM_Monitor represent the display monitor
AFIM_Acct Database represents the users' database
AFIM_Billp represent the bill print out
AFIM_Clock represent the synchronization timing

It was based on these assumptions, that the physical model represented in fig. 2 was developed for better understanding of the model.

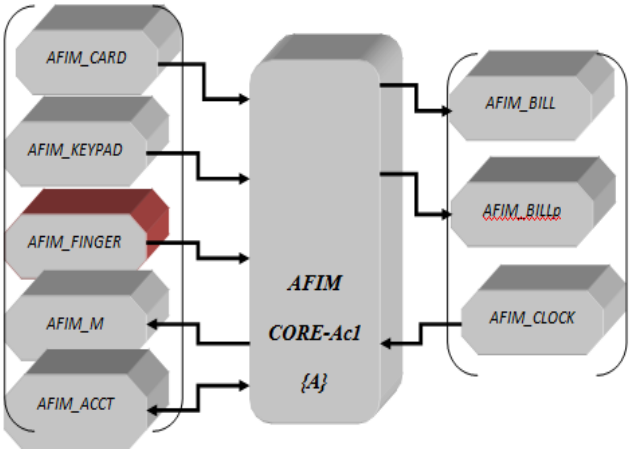

Fig. 2 Physical Model of the AFIM

From fig. 2, the physical model of an AFIM can now be best described by a Finite State Machine (FSM), which adopts a set of states and a set of state transition functions modeled by a transition diagram to describe the configuration, basic behaviors, and logical relationships among components of the AFIM model. It statistical representation is given as follows:

Let an AFIM_core with AFIM Finite State ➔ (A, Σ, a, F, δ)
The objective function would be [8];

Max $\sum_{i=0}^{N=12}\{AFIM\}$ Where $A \leq N$ ……eqn.1

• A is a set of valid states that forms the domain of the AFIM,
A = {A0, A1……A8} where the states are:
A0 ➔AFIM_System,
A1 ➔Welcome
A2 ➔ Check PIN,
A3 ➔Biometric verification,
A4 ➔ Input withdraw amount,
A5 ➔ Seek Approval,
A6 ➔ Verify balance,
A7 ➔ Disburse bills, and
A8 ➔ Eject card;

Parameters of the existing Automated teller machine that the biometric is to be integrated upon are

$\sum_{i=1}^{N=12} AFIM$ ➔ *A set of events that the AFIM may accept and process, and*
Σ = {i0, i1, …, i12}
where:
i0 ➔ Start
i1 ➔Insert card
i2 ➔Correct PIN
i3 ➔ Incorrect PIN,
i4 ➔Request ≤ max,
i5 ➔ Request >max
i6 ➔ Cancel transaction
i7 ➔Sufficient funds,
i8 ➔ Insufficient funds,
i9 ➔ Sufficient bills in ATM,
i10 ➔ Insufficient bills in ATM
i11 ➔Approval granted,
i12 ➔ Approval denied;
• *A is the start state of the AFIM, A = a1 (Welcome);*
• *F is a set of ending states, F = {a1};*
• δ is the transition function of the ATM that determines the next state of the FSM, si+1, on the basis of the current state and a specific incoming event iv, i.e., ai+1 = δ (ai, iv),
where δ = f: A × Σ → A……..eqn. 2

3.2 Policy Algorithm

- *Users insert ATM*
- *The user supplies PIN& Biometric data, seeking access*
- *PIN is verified and Biometric finger print is made& passed.*
- *If verification fails the user has the right to retry 2more times.*
- *If at the third time PIN is confirmed BUT the fingerprint is wrong then there will be a mismatch on the AFIM and transaction is cancelled, Card ejected and ATM is returned to welcome state.*
- *If PIN is correct &Biometric verification passes, then the user selects transaction details*
- *The machine verifies if amount requested is less than available account balance*
- *It also verifies if there is a sufficient bill in the ATM*
- *Disburse bills; eject card and return to welcome state.*

In this model, there are three (3) authentication metrics: the ATM card (ATM ID number + the PIN number) and biometric fingerprint. A conceptual model of fig.3 explains AFIM user identification workflow algorithm. Phase1 represents the existing mechanism whereby the user enters the ATM card into the AFIM system followed by PIN verification and transaction. In phase 2(a), the AFIM asks for fingerprint and cross check with database template. If the fingerprint matches, the process will continue. If it fails, an SMS alert will be sent as a verification code to the mobile number registered and when the user enters the verification code successfully, it proceeds to phase 2(b). In phase 2(b), the personal identification image (PII) is mapped with position of image stored in the database. This image will be ordered using a random function and session identification so that in any case the user has to identify his PII {initially, it has to be registered with a particular image at the registration level}

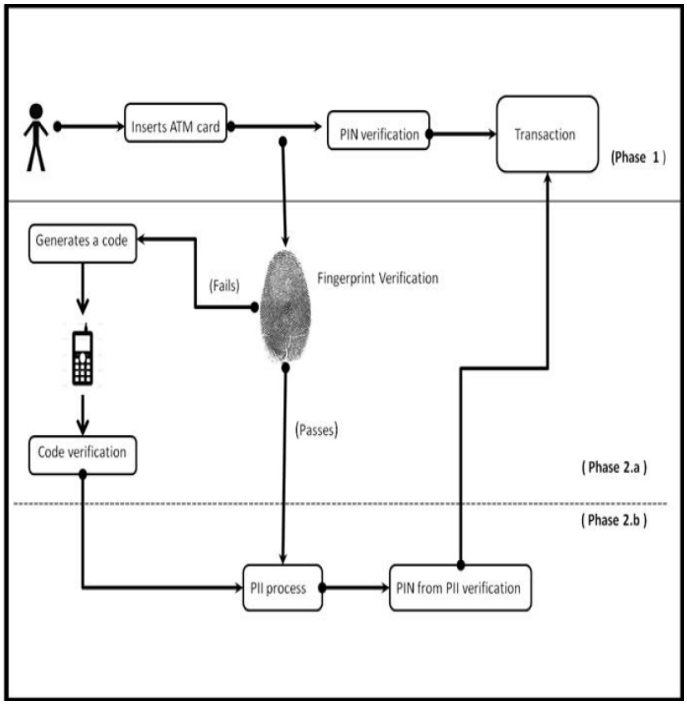

Fig. 3 AFIM User Workflow Algorithm.

3.3 Biometric fingerprint identification and verification

According to [9], there are two types of authentication, namely fingerprint verification and identification. Verification process matches the identity of the claimant by comparing the captured fingerprint image against the corresponding pre-stored fingerprint in the system. Hence, verification is a one-to-one matching process. Identification process recognizes an individual by searching the entire fingerprint database system to find the best match against the captured query fingerprint. Hence, identification is a one-to-many matching process as explained in the previous sections. In this work, secugen device was attached via a hot swappable plug and play USB interface which enabled the application software as shown in code listings to enroll and identify various fingerprint subjects. This facilitates authentication and verification functions that allow the fingerprints templates act like secured digital passwords that cannot be lost, forgotten or stolen. The flowchart of fig.4 shows the biometric fingerprint matching and verification algorithm. The fingerprint image of the customer is captured using secugen Hamster plus device (HSDU03P™) as earlier mentioned. Normalized cross-correlation matching pattern was used to get the best alignment between the fingerprint images at points that are maximally correlated to each other. These fingerprint images were captured as pattern of interleaved ridges and valleys image. The size of each image is 260x300 pixels and its resolution is 500dBi.

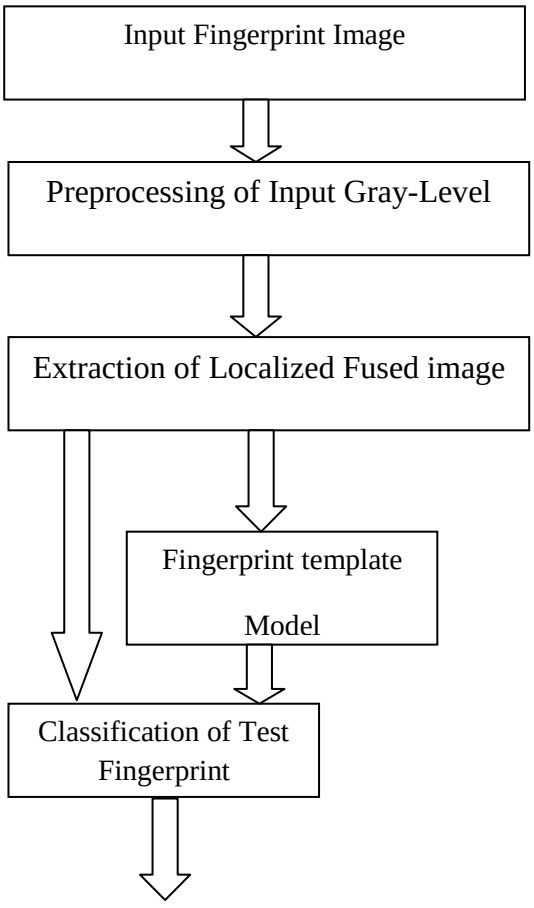

Fig. 4 Algorithm Flow of the Proposed Fingerprint Verification Method

4 Pattern Matching By Cross- Correlation Scenario

Cross-correlation is a remarkably effective method for locating specified patterns within a signal. The following result was generated by computing the two-dimensional cross-correlation between a reference image and the electron micrograph (Fig. 4a) for each of 45 rotations (with an increment of 4° for a total range of 180°) of the reference image, and taking the maximum of each pixel value to yield fig. 4b. The pattern matching algorithm looks for exact matches in the input with pre-existing patterns stored in the database template. With this Fingerprint matching technique the security matching for AFIM is remarkably improved.

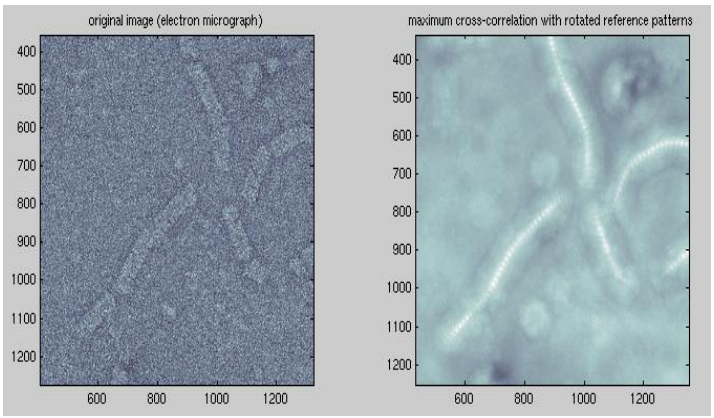

Fig. 4(a) The Original Image Fig. 4(b) Max Cross Correlation

4.2 Design Implementation

The implementation of this work was carried out on a Visual basic Network (V.B.Net) framework using unified modeling language flow diagram in representing how AFIM user interacts with the system. The application was made in six (6) interfaces: login interface, enroll fingerprint interface, transaction type selection interface, withdrawal interface, and view statement of account interface. If the user enters an invalid card number or PIN, a dialogue box appears prompting an invalid PIN or invalid card number and the system returns to enter a valid PIN number. If the PIN number is valid, the customer is directed to the next phase of the authentication process via the authentication box for inputting of the fingerprint. This biometric fingerprint interface is the final interface where the customer is requested to enroll his/her fingerprint since fingerprint of an individual is very peculiar to that individual and no two individuals can have the same fingerprint [10]. The fingerprint reader accepts the fingerprint and seeks to match the live sample with the already enrolled templates in the bank database. If it matches, the customer will be authenticated, otherwise access will be denied. Thereafter, the customer is taken to transaction phase where he/she chooses among transactions. The interface for withdrawal shows the customer current balance by subtracting the amount withdrawn from the previous account balance. At completion of the withdrawal, a dialogue box pops up notifying the customer of his/her successful withdrawal transaction.

5 Conclusion and Recommendation

This research work was undergone to sub-mantle the incessant ATM fraud in Nigeria banking industry by developing an AFIM model utilizing the concept of detonation Real-Time Process Algebra (RTPA) in its analysis. The system encompasses all the functionalities of the traditional ATMs with integration of biometric fingerprint as an innovation. With biometric integration into the design, performance and security vulnerability is completely addressed. Cross-correlation pattern matching schemes for matching and aligning the enrolled sampled image on the single singular point (as a reference point) was adopted for authentication. However, it is expected that banks in Nigeria will optimally deliver their services at acceptable standards and maximum customers satisfaction with this model. Consequently, the model adoption index is evaluated to be over 98% on the basis of the quality of service envisaged to offer to numerous customers compared with the traditional ATM system that lacks extreme intelligence in the context of security risk assessment. Finally, by introducing a biometric strategy in the Nigerian ATMs, performance and security trust will drive the whole system in the context of security and quality of service.

References

I. Johnson Olabode Adeoti, *Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out, Kamla-Raj 2011 J Soc Sci, 27(1): 53-58 (2011).*

II. Richard, B.and Alemayehu, M. (2006); *Developing E-banking Capabilities in a Ghanaian Bank; Preliminary Lessons. Journal of Internet Banking and Commerce, August 2006, vol. 11, no.2. available*

online (http://www.arraydev.com/commerce/jibc/) Accessed 0n 24/11/2009.

III. U.Uludag, S.Pankanti, S.Prabhakar andA. K.Jain, *Biometric cryptosystems.*

IV. Issue and challenges Proceedings of the IEEE, vol.92, no.6, 2004, pp.948- 960.

V. Saropourian, B.; *A new approach of finger-print recognition based on neural network 2nd IEEE International Conference on Computer Science and Information Technology, 2009. ICCSIT 2009 , Publication Year: 2009 , Page(s): 158 -161.*

VI. Myo, N.;"*Fingerprint Identification Based on the Model of the Outer Layers of Polygon Subtraction", International Conference on Education Technology and Computer, 2009. ICETC '09, Publication Year: 2009, Page(s): 201 – 204.*

VII. Lawan Ahmed Mohammed, "*Use of biometrics to tackle ATM fraud" In International Conference on Business and Economics Research vol.1 (2011) IACSIT Press, Kuala Lumpur, Malaysia, pp 331-335.*

VIII. nil k. jain, arun ross, and salil prabhakar; *an introduction to biometric recognition, ieee transactions on circuits and systems for video technology, vol. 14, no. 1, January 2004.*

IX. Santhi. B, Ram kumar.k " *Novel Hybrid Technology In ATM Security Using*

a. Biometrics, In Journal of Theoretical and Applied Information Technology 31st March 2012. Vol. 37 No. 2.

X. Maltoni D, Maio D, Jain AK, Prabhaker S. *Handbook of Fingerprint Recognition. Springer 2003.*