International Journal of Science and Engineering Applications
Volume 5 Issue 3, 2016, ISSN-2319-7560 (Online)

Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication

Frimpong Twum
Department of Computer Science
Kwame Nkrumah University of Science and Technology, Kumasi, Ghana.

Kofi Nti
Department of Computer Science
Kwame Nkrumah University of Science and Technology, Kumasi, Ghana

Michael Asante
Department of Computer Science
Kwame Nkrumah University of Science and Technology, Kumasi, Ghana

Abstract: A wide variety of systems need reliable personal recognition system to either authorize or determine the identity of an individual demanding their services. The goal of such system is to warrant that the rendered services are accessed only by a genuine user and no one else. In the absence of robust personal recognition schemes, these systems are vulnerable to the deceits of an imposter. The ATM has suffered a lot over the years against PIN theft and other associated ATM frauds due to its traditional authentication mode (PIN). In this paper, we proposed a multifactor (PIN and Fingerprint) based authentication security arrangement to enhance the security and safety of the ATM and its users. The proposed system demonstrates a three tier design structure. The first tier is the verification module, which concentrates on the enrollment phase, enhancement phase, feature extraction and matching of the fingerprints. The second tier is the database end which acts as a storehouse for storing the fingerprints of all ATM users' preregistered as templates and PIN as text. The last tier presents a system platform to relate banking transactions such as balance inquiries, mini statements and withdrawal. Microsoft windows 8 was used as an operating system platform for the implementation phase, with C# programming language being the front-end development and SQL server 2010 as backend. The application evaluation was based on False Rejection Rate (FAR), False Acceptance Rate (FAR), Average Matching Time (AMT) and the Total Error Rate (TER) conducted, which show the security and reliability of the proposed system for ATM users authentication and verification.

Keywords: PIN and Fingerprint-Based; Authentication; Security; Verification; ATM; Verification; Multifactor

1. Introduction

The advancement of payment system in the modern world has gone passed cash to cheques, and then to payment cards such as credit cards and debit cards (Batiz-Lazo & Barrie, 2005) Automatic Teller Machine ATM is a terminal installed by banks or other financial institution that enables customers to perform service, like cash withdrawal or cash deposit, balance enquiry, request for bank statements, and money transfer from one account to the other. Some modern ATMs are equipped with mobile money transaction. ATMs are basically independent banking workstations which aims at providing a faster and expedient service to customers (Rasiah, 2010). Barclays bank introduced the first ever ATM in 1967, in its Hendson branch in London, which could dispense a fixed amount of cash when a user inserted a special coded card and since then, ATM has become smaller, faster and easier (Das & Jhunu, 2011). Among all departments in a financial institution, the ATM has been considered as one of the important components of electronic banking infrastructure.

The main benefit of the ATM is its ability to provide a 24hours service daily to customers and users, making the ATM an integral part of our everyday life. Nowadays, ATMs' are employed in various scenarios such as ticket vending machines, quick check-in kiosks and self-service gas stations (Luca, 2011).

ATMs are not only sited at banks, but also a lot of schools, businesses nowadays installed ATM on their premises for customer convenience and more revenue. A global ATM market forecast research lead by Retail Banking Research Limited (Mohammed, 2011) shows that there are 1.8 million ATMs deployed around the world and the figure was forecast to reach 2.5 million by 2013.

ATMs cards authentication methods have changed little since their introduction in the 1960's. The security limitations of ATM are mostly derived from the security pitfalls of the magnetic media. The data on the magnetic stripe are usually coded using two or three tracks, because, it is not difficult or expensive to have the equipment to encode magnetic stripes. The standard covering this area is International Organization for Standardization (ISO) 7811 and the technique for writing of the tracks is known as Friend-to-friend (F/2F). Thankfully, magnetic stripe feebleness has been partly addressed by the introduction of Europay, MasterCard and Visa (EMV) smartcards. Normally, the authentication design involves a trusted hardware device (ATM card or token). The Personal Identification Number (PIN) of the card holder's is usually the only means to attest the identity of the user; this approach is vulnerable to misplacement, unauthorized access, card swallowing, forgetfulness and others (Das & Jhunu, 2011), (Akinyemi, et al., 2010).

Despite the numerous cautions given to the card user, many people continue to choose easily guessed passwords and PINs such as phone numbers, birthdays and social security numbers. However, due to the limitations of this design, an intruder in possession of a user's card can discover the user's PIN with password prediction or guessing (brute force) attack. For instance, in a typical four digits PIN, one in every 10,000 users will have the same number. In spite of all security measures in place, cases of ATM crimes continue to occur globally. A current figure by European ATM Security Team (EAST) affirms that there is a rise in ATM fraud "trend", especially of skimming attacks. An upsurge of 24 % in

skimming attacks at European ATMs, matched to the first half of 2009, is reported for the first half of 2010 in the ATM Crime Report (Gunn, 2010).

In situations where a user has two or more ATM cards, all PINs needs to be memorized by the user. This can easily lead to the user initiating security problems (Adams & Sasse, 1999), thus a card holder or user may decide to write down the authentication token, or use the same authentication token (PIN) across different services or use authentication token (words) that can be found in dictionaries. A notable example of this was shown by Klein, who could crack 25% of 14,000 passwords using a dictionary attack with only 86,000 words (Jermyn, et al., 1999) and (Luca, 2011). This leads to the saying that the user is often referred to as the 'weakest link' in the security chain (Luca, 2011).

With the introduction of internet technology in recent years, the internet communication is exposed to unwanted people giving them access to pose different kinds of attacks on ATM System.

In 2013 Ghana Commercial Bank (GCB) confirms money theft from an ATM of about GH¢3 million (Obour, 2013)and a worldwide gang of criminals stole $45 million in a matter of hours by hacking their way into a database of prepaid debit cards and then draining cash machines around the globe (Modernghana, 2013). ATM's crime has become a nationwide epidemic which faces both customers and bank operators, as well (Das & Jhunu, 2011).

The security breaches in the ATM system have contributed to the less patronage and rejection of the ATM, by some customers of various banks (Ndife, et al., 2013).

The traditional (PIN) ATM cash withdrawal process flowchart is as shown in figure 1.

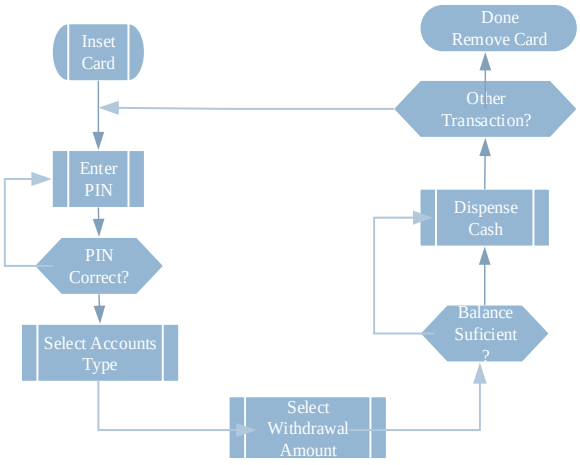


Figure 1 ATM Withdrawal PIN Based

Some method and approaches have been proposed, from text, images and biometric to increase security on ATM. This section of the research looks at some of these techniques, from their strength to weakness.

An enhanced security for ATM machine with One-Time Password (OTP) and facial recognition features was proposed by Mohsin, et al., 2015 to enhance ATM security. The OTP was used for the enrichment of security of accounts and privacy of ATM users. The face recognition technology proposed in their system was to help the ATM to identify each and every user uniquely, by using faces as a key. The researchers concluded that, there are some little flaws associated with the face recognition technique, thus the failure to detect a face when aging, beard, caps and glasses. (Mohsin, et al., 2015). ATM Transaction Security System Using Biometric Palm Print Recognition and Transaction Confirmation System was proposed by (Sanjay, et al., 2014), the researchers acknowledged that, the PIN authentication system only, as used in most ATM machines is not secured. Hence, they sort to enhance the security system by introducing palm print recognition authentication as better and further mode of ensuring security at the ATM. The proposed method was accomplished with a prototype model of an ATM simulator that mimics a typical ATM system. In their conclusion, they recorded a percentage matching of 89.43% for palm-print recognition system and a rejection rate of 10.57% (Sanjay, et al., 2014). Thus, for 53 out of every 500 customers that will visit ATM's enhanced with this authentication system are likely to have problems with their transactions. Make a Force Rejection Rate of the system to be 10.57%. Hirakawa in 2013 prospered a password enhanced mechanism called (Random Board: Password Authentication Method with Tolerance to Video-Recording Attacks) to increase or fortify up security on ATM, by preventing an observation attack for stealing user's password (thus video recording) and brute force attacks. Hirakawa acknowledges that the PIN authentication in traditional ATMs contributes to the immerse rising of ATM frauds, because this PIN, (password) are entered in open spaces which gives a chance to criminals having a mobile phone equipped with cameras and miniature cameras to spy on the user whiles entering his/her PIN. To achieve this Hirakawa proposed two modules, basic method and an improved method. In their basic method, a correct entry position of each password must be provided beforehand. Whiles, in the improved method, a user does not need to provide any information beforehand, other than the password. In his approach, the alphabet board is randomize, thus the letters changes position all times, making it difficult for an observer to see the alphabet entered by the user (Hirakawa, 2013). Lalzirtira proposed an authentication method called Graphical User Authentication to eliminate the defects in the alphanumeric authentication mode of traditional ATM's. In his research, he emphasized that graphical password which make use of images are easy for humans to remember than words or numerals. In his work he sounded that the introduction of the graphical password will eliminate the tendency of user written down their password, hence eliminating ATM frauds (Lalzirtira, 2013).

The use of images as a means of authentication in ATM system has its strength to some point and a big weakness to video recording, hence this method cannot be said to be a definite solution to ATM frauds.

A Dynamic Password (Dyna-pass) techniques was proposed to offer security to ATM transactions by Anand et.al, 2013. In their system, a user access the ATM with a debit card and his or her PIN as in the traditional system, but an SMS that contain a secret code called Dyna-pass is sent to the user mobile phone from the bank server if the PIN giving by the user is correct. The user then enters this new code received on his or her phone for confirmation, this again is checked with the bank server for confirmation, and if correct ATM transaction access is given to the user (Anand, et al., 2013).

This implies that to access a user account at the ATM, you need his or his PIN, debit card and mobile phone. Hence a person close to the user can attain all these and defraud the ATM user. In this same paper an emergency third party authentication was proposed, whereby three to four people can register in the system with own mobile numbers for a friend. So that in the event that the actual account holder can't perform a transaction, these registered people can do transaction for the actual user through the mobile phone (Anand, et al., 2013). Thus, a user is given the chance to give three or four auxiliary phone numbers in addition to his or her mobile number. Lawan proposed that, the fraudulent act associated with ATM's can be eliminated by the use of biometric authentication mechanism incorporated in the ATM security. In his report he looked at an overview of all ATM fraudulent activities and recommended approaches to element or prevents these frauds in ATM. In addition a prototype model for biometric authentication was developed to provide a solution to well-known security breaches in ATM authentication (Mohammed, 2011).

In other research work, a proposed neural network-based was adapted to match the fingerprint of users through the view of the blueprints and groove patterns of the fingerprints. This proposed module function perfectly on binary images and greyed scans; one good side of this proposed module is that, once a group is tracked, pattern can then be tracked with high accuracy. But this approach comes with a great threat where the network becomes inaccessible (Saropourian, 2009). Multi-layers of convex polygon were proposed to implement fingerprint verification to enhance security levels on ATM's. In this work, extraction of fingerprint image was found in a specified area in which the prevailing brightness value of fingerprint ranges. The major limitation is the possibility of falsifying identity and falsified authentication cannot be noticed easily. To conclude these reviewed research efforts was carried out using a single biometric check without any form of cryptography, hence, could not warrantee a dependable security solution (Myo, 2009). An authentication method called fakepointer is proposed to enhance the security levels at ATM's, which make use of a numeric key entry. With this approach, a disposable "answer selection data" is to be retrieved before each authentication. This selective information provides the background mark, like square, triangle, pentagon, hexagon of the numeric password displayed. At the authentication stage or period a user trikes the enter button, which adapts to the password according to the mark at the background. This method is open to twice video recording attack, if the "answer selection data" can be safely retrieved before each authentication. However, this research did not emphasis on how to recover it safely (Takada, 2007) cited by (Tedder, 2009). Zhao & Li proposed an interface for PIN authentication called S3PAS, this mechanism proposed numerous characters to be displayed on an interface. A user at an ATM premises assigns three places where a password character is included in a triangle. This approach guides the user from shoulder surfing attack, but again if the input is recorded; it's exposed to user password to criminal attacks (Zhao & Li, 2007). A pin-Entry password authentication technique using numeric key entry was proposed. In this approach a black or white background is randomly displayed. The ATM user does designate a password rather he/she selects a black or white as background colour for a password. A user designates the background colour by the different colour pattern with four times to enter a password entry of One (1) digit. The method is very safe against shoulder surfing, but an attacker is able to video record the input operation the password is still open to attack (Roth, et al., 2004). (Sakurai, et al., 2004; Sakurai & Munaka, 2008) cited (Hirakawa, et al., 2013) proposed a text-password entry interface known as mobile authentication. With their method every text that is selectable are arranged in a square, with each text having its own background colour. For instance, every password is numeric or alphabetic, and the texts are ordered in 6×6 square in which six colours are used, with each colour appearing only once in each row. The colour pattern of a row is the permitted colour pattern of another row. In this approach, a user provides the correct background colour and a password beforehand. At the authentication (password entry) stage, the user changes the background colour of a pass-character until it matches the correct background colour, and then presses the accept/enter button. This technique comes with a restriction that all available texts must be displayed in the square, but this approach is secure against video attack by twice recording. Their techniques is applicable to numerical passwords but still, a 12-length numerical password is required for secure use, which might be considered too long by most ATM customers. In this method, all of the texts available are presented as squares on the authentication interface. In the case of a four-character password, the columns number should be bigger than or equal to 10 for tolerance to random attacks, and the rows number should be larger than or equal to 9 for tolerance to video-recording attacks. Therefore, the numbers of available pass-texts are equal to or more than 90 for tolerance for both the attacks. And also, in a case where five-character password is used, the columns number should be equal to or greater than 7 and the rows number should be equal to or bigger than 6. Therefore, the method is not used when four or five lengthy alphanumeric password is used as a PIN for authentication (Hirakawa, 2013). A method called AWASE-E was proposed, which has 25 images, with one being a correct pass images. These images are normally displayed on the screen, similar to (Passfaces, 2005) approach, but with the ability to display on a screen in where there is no pass-image. Where the pass image is not part of the images' on the screen, then a user has to select the "no pass-image button". Although this technique offers a quieter security to ATM authentication, it's only safe when taking a shot, is not clear to the attacker (Koike & Takada, 2003) cited (Hirakawa, 2013). The techniques proposed by (Passfaces, 2005) are exposed to shoulder surfing attack, because the user designates a pass-image in the process of authentication. (Ratha, et al., 2001) proposed an embedded fingerprint system for ATM security applications, in their proposed system, bankers will have to collect customers' finger prints and mobile numbers while opening new accounts. With their system a customer wanting to perform a transaction at an ATM will get a text of a 4-digit code message on his/her GSM phone when the customer place a finger on the finger print module attached to the ATM. This message is automatically generated every the customer visit the ATM. The code received by the customer is entered into the ATM machine by pressing the keys on the touch screen. After entering it checks whether it is a valid one or not and allows the customer further access. The main disadvantage of this system is that customers with a lost phone needs a new one or has to updates his records at the bank before he/she can access his account on an ATM. An ATM enhancement technique using secured Personal Identification Image (PII) process was proposed by Santhi and Kumar. This method is secured against shoulder surfing attack, but if a recording

camera is hidden to record the authentication process, the system becomes insecure (Santhi & Kumar, 2012). A highly authenticated biometric security system is proposed by (Subh & Vanithaasri , 2012), to enhanced ATM security. The proposed method implementation however lacks the strength to exclude wrong or false feature and minutiae points from its extracted list.

In light of the above discussions, it appears clearly, that the PIN and Image's authentication approach does not guarantee sufficient ATM security.

This paper seeks to propose a multifactor authentication (PIN and Fingerprint) authentication system for dealing with modern ATM's security challenges and examine its performance.

2. Materials and method

Microsoft Visual Studio 2010 (C#) was used to develop the front end, where system user can graphically interact with the ATM. The back end (database) was developed with Microsoft Structured Query Language (MSSQL) server 2008, MSSQL is a relational database management system (RDBMS) use for creating a database for Microsoft Windows family of servers. MSSQL was chosen over other database management tool, due to its ability to provide a working environment to easily generate a database that can be easily and quickly accessed from the internet, workstation, LAN and so on. To help communicate between the fingerprint scanner a Grfinger software development kit (SDK) was employed in conjunction with the Microsoft visual studio to help in the implementation of the proposed fingerprint enrollment and authentication algorithm.

2.1 Design Concept

Figure 2 portrays the block diagram of the proposed ATM multifactor authentication system, which comprises of customer account details, PIN database, fingerprint database and an ATM machine. The following subsections explain in details how the proposed ATM multifactor Authentication will enhance the level of security on the ATM, to safeguard the users of ATM from various ATM attacks initiated by fraudsters.

The internet, is the first phase of the proposed system, serving as the working environment and platform for the proposed system to communicate between individual ATM terminals and the central bank server. Customers fingerprint and PIN databases are available on the bank servers and a relational database model is used for storing information on the fingerprint and PINs of all registered customers. These information include pattern type, and feature characteristics.

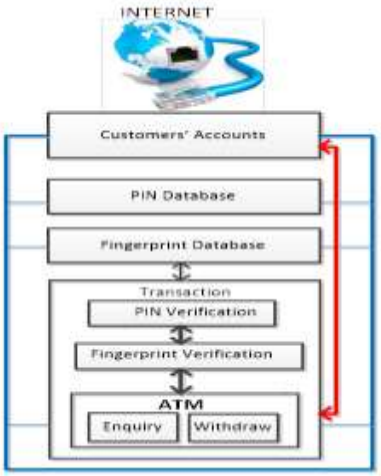


Figure 2 Conceptual Design of Proposed ATM Security Structure

Figure 3 shows the flowchart for the PIN and fingerprint verification components proposed for verifying the authenticity of a user. A user who is already enrolled onto the proposed system, will have to go through the verification process presented in figure 3.

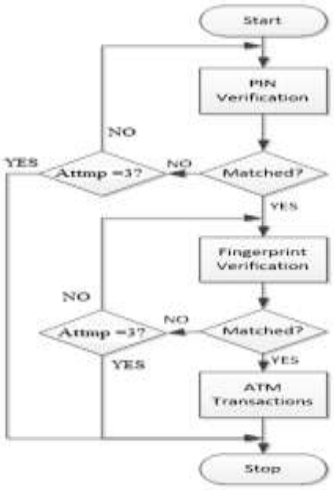


Figure 3 Flow Chart of Proposed System

For the period of image enhancement, the foreground regions of the image which are the regions containing the ridges and valleys are separated, from the background regions, which consist mostly of noise. Segmentation is performed with the view of ensuring that focus is only on the foreground regions, while the background regions are ignored. The segmented fingerprint image ridge structure will be normalized so as to standardize the level of variations in the image grey-level values. By normalizing, the grey-level values will be brought to a range that is good enough for improved image contrast and brightness. The normalized image is then filtered to remove any noise and spurious feature present. The filtering will also preserve the true ridge and valley, and this involves the ridge orientation and frequency estimations. The output obtained after filtering (filtered image) is converted to binary

format and thinned for satisfactory feature extraction. At the feature extraction stage, major features; namely ridge ending and bifurcation are located and extracted from the image. These two main features are the characteristics that establish uniqueness among different fingerprints.

The extracted features from the user template is matched with templates of the other images in the database. A user of the ATM will provide his or her PIN and if it's correct after system check, then the user is granted access to the second level of authentication (fingerprint identification), when the fingerprint of the user is scanned by the fingerprint model incorporated in this system and a match exit when compared to the one in the database during the enrollment of the user, access is granted to the user to perform his/her ATM transactions.

2.2 Software Modules Design

As a requirement of the approach used for implementing the proposed algorithm, five primary phases were required for producing consolidative software levels necessary to meet system objectives and goals. Each module design and tested separately, and then combine together to form a complete application.

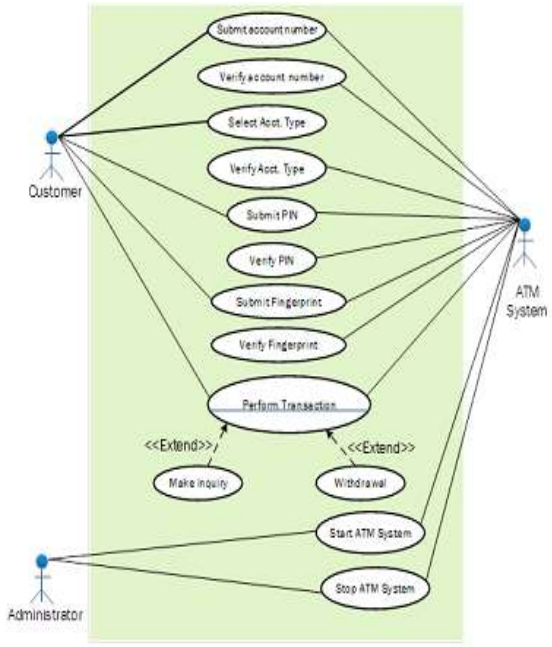


Figure 4 Use Case Diagram for Proposed ATM Multifactor Authentication Module

Figure 4 shows the Use Case Diagram for the proposed ATM multifactor authentication module. The primary actors; Administrator and customer and secondary actor; ATM system triggers the use-cases. Figure 5 shows a pictorial view of the different sub-module, and the relationships that exist between various sections of the program codes, and how each program code interact with another section.

Figure 5 Detail Code Elements and Relation

2.3 Customer Enrollment

Figure 6 shows the enrollment module. This module enables the bank to enroll customers that come to the banking hall directly into the system.

Figure 6 Module for Customer Enrollment onto the Fingerprint System

3. Implementation of Proposed ATM Multifactor Authentication System

Microsoft Windows 8 was used as an operational platform, running on a 32bit Processor with a speed 3.0 Ghz with a system memory at 3Gb.

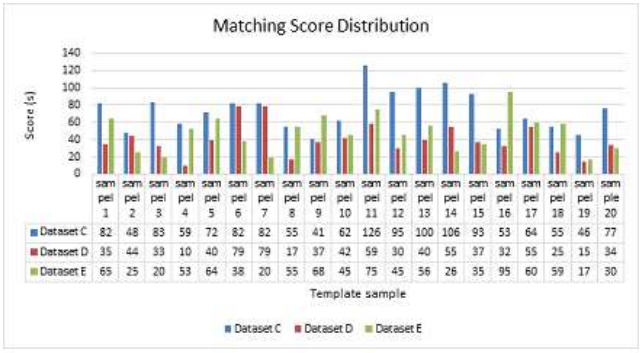
3.1 Results and Discussions

Evaluation and testing of the proposed ATM multifactor (PIN and fingerprint) authentication system was carried out with information/data collected from randomly selected, four hundred and fifty student and staff of the Sunyani Polytechnic Sunyani, Ghana. The performance of the system was measured in terms of False Accept Rate (FAR), False Rejection Rate (FRR) and equal error rate (EER). The FAR is

the percentage of invalid inputs that are incorrectly accepted (match between input and a non-matching template). The FRR is the percentage of valid inputs that are incorrectly rejected (fails to detect a match between input and matching template) (Sainath & Tangellapally, 2010). To test the effectiveness and robustness of the proposed system, two sets of thumbprints data were used for FAR and FRR testing. Since these indicators are the commonest and simplest indicators for checking the effectiveness, accuracy and performance of fingerprint pattern matching (Iwasokun & Akinyokun, 2013). The first dataset (A) had 1,800 thumbprints, accounting for Four (4) thumbprints collected from the right thumb of each of the four hundred and fifty (450) respondents. The other dataset (B) also contained the same amount of thumbprints collected from the left thumb of respondents. Datasets (C), (D) and (E) contains 450 thumbprint each from the right thumbs of each subject with different thumb pose for intra-class variation test. All the three thousand, six hundred (3,600) thumbprints from the right and left of respondent were enrolled onto the system for a period of hundred and twenty (120) days , using a digital persona (U.are.U 4500) USB fingerprint reader with 512dpi pixel resolution and 18.1mm length by 14.6mm width capturing area.

3.2 Intra-class variations test

To ascertain how the proposed system will react to intra-class variation, each of the four hundred and fifty (450) enrolled templates in the dataset (C) was matched with templates in the dataset (C), (D) and (E) by the same client and the match score recorded. The matching score (also called weights) gives or express the measure of similarity or a distance measure between two minutiae patterns. The greater the score is, the higher is the similarity between them, and for a genuine client the score (S) must be greater than the threshold (T). Figure 7 shows a graph of the score obtain from randomly selected 20 fingerprint templates in (C) matched against fingerprint in the dataset (D) and (E) from the same respondent. The pronouncement of whether a match exists is completed by comparing the matching score (S) to a decision threshold value (T), and if $S \geq T$, then the identity claim is assumed correct.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Dataset C	82	48	83	59	72	82	82	55	41	62	126	95	100	106	93	53	64	55	46	77
Dataset D	35	44	33	10	40	79	79	17	37	42	59	30	40	55	37	32	55	25	15	34
Dataset E	65	25	20	53	64	38	20	55	68	45	75	45	56	26	35	95	60	59	17	30

Figure 7 Intra-Class Variations Matching Score Distribution

From figure 7, it can be deduced that the scores obtained by clients differs from dataset to another dataset. These discrepancies in score rate can be attributed to the different poses clients made during the enrollment stage. If clients were to authenticated with the template stored in dataset D and E, there would have been seven (7) imposters in the dataset (D) and six (6) in the dataset (E) making a total of eleven (13) which equal 65% out of the twenty samples taken at random. From this result, it can be concluded that if client are not guided at the enrolment stage to position their thumbs well on the sensor, there will be a high rate of FAR at the authentication stage.

For FAR and FRR testing purpose, three categories of experiments I, K and L were conducted. The first category (I) experiment (FRR test), was carried out on dataset (A), by matching every single thumbprints in dataset (A) with the remaining three other thumbprints from that same thumb in dataset (A), but escaping symmetric matches, by employing the implemented fingerprint matching algorithm. This was to verify the possibility that two match-samples will be acknowledged falsely as unmatched, thus the match score will be lesser than the threshold value.

3.3 False Rejection Rate

Figure 8 False Rejection Rate Score

Figure 8 shows an outcome score for randomly picked 50 (templates) samples in the FRR experiment on dataset (A).

Out of the fifty (50) samples, one (1) false reject was accounted. Thus FRR equals (2%) out of 50 as compared with 3.33% out of 30 (Manish, et al., 2011) and 10.57% (Sanjay, et al., 2014), it can be approximated that for all the four hundred and fifty samples that was put under FRR test nine (9) false rejecting will be accounted, making an overall FRR equals nine (9). The Genuine Acceptance Rate (GAR) is the fraction of genuine scores above the threshold (T). Therefore GAR =1 – FRR (1 – 0.02 = 0.98).

3.4 False Acceptance Rate

To determine FAR, the four thumbprints of each thumb, from each respondent in datasets (A) and (B) were matched with the one thousand seven hundred and ninety six (1,796) thumbprints from the 449 remaining respondents' thumbprints at different threshold values. This is to determine the probability that two non-match thumbprints will be mistakenly confirmed as a match.

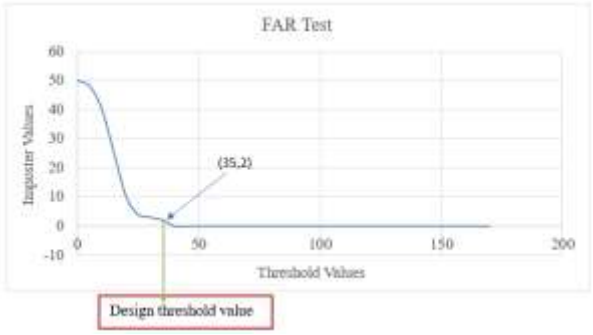


Figure 9 False Acceptance Test

Figure 9 shows the output curve for the FAR test on dataset (A). From the graph it can be realized that, for a threshold value of thirty-five (35), two imposter values were recorded as a genuine record out of fifty (50) sample taken at random. Hence FAR equals (4%) for this work as compared to (6.6%) for (Manish, et al., 2011) for 30 samples. The TER is 6% for a total access of 50 and compared to 13.3% (Manish, et al., 2011) for a total access of 30 and 8.27% (Iwasokun & Akinyokun, 2013).

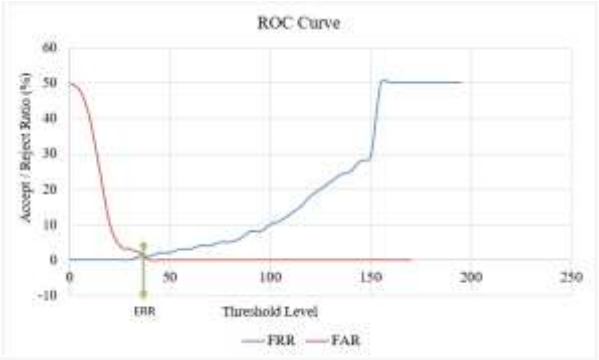


Figure 10 ROC Curve

With a TER of 6%, it shows that the developed system is 94% accurate as compared with 89.43% (Sanjay, et al., 2014). Figure 10 shows the ROC curve. An average matching time of 1.023, 1.075 and 1.155 were recorded for dataset A, B and A + B respectively.

4. Conclusions And Recommendations

The conclusions arising out of this research, based on the findings, are given below.

- ✓ The proposed fingerprint and PIN system has an overall efficiency of 94%, FAR 4%, FRR 2%, TER 6% and GAR 98%.
- ✓ Compared to other fingerprint identification and verification systems, the proposed system provides an improved performance in matching time and partial elimination of false minutiae from its fingerprint database.
- ✓ The proposed system is a good cost effective measure for implementing a well secure ATM transactions to protect ATM users from fraudsters.

The recommendations of this research could be summarized as follows:

Decision-makers need to appreciate the level of security assured through the usage of biometric systems and the transformation that can exist between the perception and the authenticity of the sense of security delivered.

The Bank of Ghana (BoG) and the Ghana Association of Bankers (GAB) which has the mandate to implement strategic actions in the banking sector of Ghana should pilot the installation of ATM enhanced with this system as a cost reduction strategy and security for their customers and clients.

The great difference obtained on Intra -class variations test in this research indicates that, if clients thumb pose at enrollment do not match with thumb pose at verification, a falsehood rejection will occur. Hence the Electoral commission (EC) of Ghana should ensure that, the thumbs of voters at enrollment and voting days are positioned well on the fingerprint scanner,

to prevent false rejection, causing confusion at voting days. Experimental validation should be conducted to confirm the results presented in this research work.

- ✓ The proposed system is a good cost effective measure for implementing a well secure ATM transactions to protect ATM users from fraudsters.

5. Acknowledgments

We give all our praises and extreme thanks to God Almighty for how far He has brought us faithfully in life.

6. References

1. Adams, A. & Sasse, M. A., 1999. Users are Not the Enemy. Commun.. *ACM 42, 12*, pp. 40-46.

2. Akinyemi, I., Omogbadegun, Z. & Oyelami, O., 2010. Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria EBanking System.. *International Journal of Electrical & Computer Sciences IJECS-IJENS 10*, pp. 68-73.

3. Anand, D. A., Dinesh, G. & Naveen, H. D., 2013. A Reliable ATM Protocol and Comparative Analysis on Various Parameters with other ATM Protocols. *International Jouranl of Communication and Computer Technologies (IJCCT), ISSN: 2278-9723*, 01(56), pp. 192-197.

4. Batiz-Lazo, B. & Barrie, . A., 2005. *The business and technology history of automated teller machine in the UK*. London, Queen Mary University, pp. 1-10.

5. Das, S. & Jhunu, D., 2011. Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System. *International Journal of Information and Communication Technology Research*, pp. 197-203.

6. Gunn, L., 2010. *European ATM crime report. Technical Report 1.2*, s.l.: European ATM Security Team (EAST),.

7. Hirakawa, Y., 2013. Random Board: Password Authentication Method with Tolerance to Video-Recording Attacks. *International Journal of Innovation, Management and Technology, Vol. 4, No. 5*, pp. 455-460.

8. Iwasokun, G. B. & Akinyokun, O. C., 2013. A Fingerprint-based Authentication Framework for ATM Machines. *Journal of Computer Engineering & Information Technology*, pp. 1-8.

9. Jermyn, I. et al., 1999. *The design and analysis of graphical passwords.*. s.l., USENIX Association, pp. 1-1.

10. Lalzirtira, 2013. *Graphical User Authentication*, India: Department of Computer Science and Engineering National Institute of Technology Rourkela.

11. Luca, A., 2011. *Designing Usable and Secure Authentication Mechanisms For Public Spaces (Doctoral dissertation, lmu)*, s.l.: s.n.

12. Manish, . M., Ajit , S. K., Thakur, S. S. & Sinha, D., 2011. Secure Biometric Cryptosystem for Distributed System. *International Journal Communication & Network Security (IJCNS)*, Volume-I(Issue-II), pp. 28-32.

13. Modernghana, 2013. *Modernghana.* [Online] Available at: http://www.modernghana.com/news/463043/1/hackers-steal-45-million-in-atm-card-scam-federal.html [Accessed 10 June 2015].

14. Mohammed, L. A., 2011. *Use of biometrics to tackle ATM fraud*.. Malaysia,, IACSIT Press, Kuala Lumpur, pp. 331-335.

15. Mohsin, K., Saifali, K., Sharad, O. & Dr.D.R.Kalbanded, 2015. *Enhanced security for ATM machine with OTP and Facial.* s.l., Elsevier B.V., pp. 390-396.

16. Myo, N., 2009. Fingerprint Identification Based on the Model of the Outer Layers of Polygon Subtraction. *International Conference on Education Technology and Computer*, p. 201 – 204.

17. Ndife, .. A., Ifesinachi, .. E., Anthony, .. O. & Davies, .. ,., 2013. An Enhanced Technique in ATM Risk Reduction using Automated. *Volume No.4*, 06 June , pp. 1132-1138.

18. Obour, S. K., 2013. [Online] Available at: http://graphic.com.gh/news/general-news/8459-gcb-confirms-money-theft-from-atm-but-says-amount-is-lower-than-gh-3-million.html

19. Passfaces, Corporation, 2005. [Online] Available at: http://www.realuser.com/enterprise/about/about_passfaces.htm [Accessed 9 July 2015].

20. Rasiah, D., 2010. ATM Risk Management and Controls. *European Journal of Economics, Finance and Administrative Sciences , 21, ,* 2014 January.pp. 161-171.

21. Ratha, N., Connell, J. & Bolle, R., 2001. Enhancing Security and Privacy in Biometrics-based Authentication Systems. *IBM Systems Journal, vol. 40, no. 3,* pp. 614-634.

22. Roth, V., Richter, K. & Freidinger, R., 2004. A Pin-Entry Method Resilient Against Shoulder Surfing. pp. 236-245.

23. Sanjay, S. G. et al., 2014. ATM Transaction Security System Using Biometric Palm Print Recognition and Transaction Confirmation System. *International Journal Of Engineering And Computer Science,* pp. 5332-5335.

24. Santhi, B. & Kumar, R., 2012. Novel Hybrid Technology in ATM Security Using Biometrics. *Journal of Theoretical and Applied Information Technology,* pp. 217-223.

25. Saropourian, B., 2009. A new approach of finger-print recognition based on neural network," Computer Science and Information Technology, 2009. ICCSIT 2009. *ICCSIT 2009. 2nd IEEE International Conference ,* pp. 158-161.

26. Subh , M. & Vanithaasri , S., 2012. A Study on Authenticated Admittance of. *International Journal of Advances in Engineering & Technology 4,* pp. 456-463.

27. Takada, . T., 2008. FakePinter: The authentication technique which has tolerance to video recording attacks. *Information processing society of Japan (IPSJ) transaction, vol. 49, no. 9,* pp. 3051-3061.

28. Tedder, K., 2009. *A Review of Fraud Costs and Trends,* s.l.: s.n.

29. Zhao, H. & Li, X., 2007. "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-graphical Password Authentication Scheme. *IEEE Advanced Information Networking and Applications Workshops,* pp. 467-472.