Turkish Journal of Computer and Mathematics Education Vol.12 No.6 (2021), 5151-5160

Research Article

ATM Management System

Risabh Sharma [a], Vipul Chaudhary[b]

[a,b]Department of Computer, Science, Galgotias University G. Noida (UP)

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: The various types of programs require the trust of each program to authorize or determine the identity of the person seeking its services. The purpose of this program is to ensure that the services provided are only available to the user personally and not to anyone else. If there are no solid personal recognition schemes, these programs are at risk of being deceived by a fraudster. ATMs have suffered a lot in recent years due to PIN theft and other ATM frauds due to authentication (PIN) mode. In this paper, we have proposed a multifactor certificate (PIN and Fingerprint) that strengthens the safety and security of ATMs and their users. The proposed plan shows the formation of three levels. The first phase is the verification phase, which focuses on the registration phase, the development phase, the removal of features and fingerprint matching. The second stage is the end of the data that serves as a repository for all ATM users registered as indicators and PIN as text. The final section describes the platform for discussing banking transactions such as balance questions, small statements and withdrawals. Microsoft windows 8 has been used as a startup application platform, with advanced C # programming language and 2010 SQL server as a backend. The application test was based on the False Rejection Rate (FAR), False Acceptance Rate (FAR), Medium Term Matching (AMT) and Total Error Rate (TER) performed, indicating the safety and reliability of the verification and authentication system of the proposed ATM user

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

1. Introduction

The development of the payment system in the modern world conveyed cash, then to payment cards such as credit cards and bank cards (Batiz-Lazo & Barrie, 2005). asking for balance, request for bank statements, and transfer of funds from one account to another. Some modern ATMs are fitted with cash transactions. ATMs are primarily private banking operations that aim to provide fast and efficient services to customers (Rasiah, 2010). Barclays Bank introduced the first ATM in 1967, at its Hendson branch in London, which could issue a fixed amount of money when a user entered a special card with a code and since then, the ATM has become smaller, faster and easier (Das & Jhunu, 2011). Of all the departments in the financial institution, ATMs are considered to be one of the most important aspects of electronic banking infrastructure.

The main advantage of ATMs is its ability to provide 24-hour daily services to customers and users, making ATM an integral part of our daily lives. Nowadays, ATMs 'are employed in a variety of situations such as ticket machines, fast-moving kiosks and self-made gas stations (Luca, 2011).

ATMs are not only deposited in banks, but also in many schools, businesses these days have installed ATMs on their premises. 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.

ATM card verification methods have changed little since they were first introduced in the 1960s. ATM safety standards are largely found in the safety traps of magnetic resources. The information on the magnetic field is usually coded using two or three tracks, because, it is not difficult or expensive to have magnetic straps. The standard that covers this area is the International Organization for Standardization (ISO) 7811 and the track record system is known as Friend-to-friend (F / 2F). Happily, the weakness of the magnetic field has been addressed through the introduction of Europay, MasterCard and Visa (EMV) smartcards. Typically, authentication formats include a trusted hardware device (ATM card or token). Personal Identification Number (PIN) card holders are usually the only way to prove who the user is; this method is at risk of improper placement, unauthorized access, card swallowing, forgetfulness etc. (Das & Jhunu, 2011), (Akinyemi, et al., 2010).

In addition to the many warnings given by the card user, many people continue to choose predictable passwords and PINs such as phone numbers, birthdays and social security numbers. However, due to the limitations of this design, an intruder with a user card can obtain a user PIN by password prediction or speculation (harassment) attack. For example, in a standard four-digit PIN, one in every 10,000 users will have the same number. Despite all the safety measures in place, cases of ATM crimes continue to occur globally. A current A number of the European ATM Security Team (EAST) confirms that there is an increase in ATM "fraudulent" methods, especially sudden attacks. A 24% increase in sudden attacks on European ATMs, equivalent to the first half of 2009, is reported to be the first half of 2010 in the ATM Crime Report (Gunn, 2010).

In cases where the user has two or more ATM cards, all PINs need to be memorized by the user. This can easily lead to a user initiating security issues (Adams & Sasse, 1999), so the cardholder or user may decide to write the authentication token, or use the same verification token (PIN) for different services or use the authentication token (names) can be found in dictionaries. A notable example of this is Klein, who was able to crack 25% of 14,000 passwords using dictionary attacks in 86,000 words (Jermyn, et al., 1999) and (Luca, 2011). This leads to the claim that the user is often referred to as the 'weakest link' in the security network (Luca, 2011).

With the introduction of internet technology in recent years, internet communication has been exposed to unwanted people giving them access to various types of ATM attacks.

In 2013 Ghana Commercial Bank (GCB) confirms theft of GH ¢ million ATMs (Obour, 2013) and gangs around the world steal $ 45 million in a few hours by logging into a database of paid bank cards and withdrawing cash machines all around the world

(Modernghana, 2013). ATM crime has become a national epidemic against customers and bankers, too (Das & Jhunu, 2011).

Security breaches in the ATM system have resulted in slow handling and disposal of ATMs, by some customers of various banks (Ndife, et al., 2013).The traditional (PIN) ATM cash withdrawal process flowchart is as shown in figure 1.

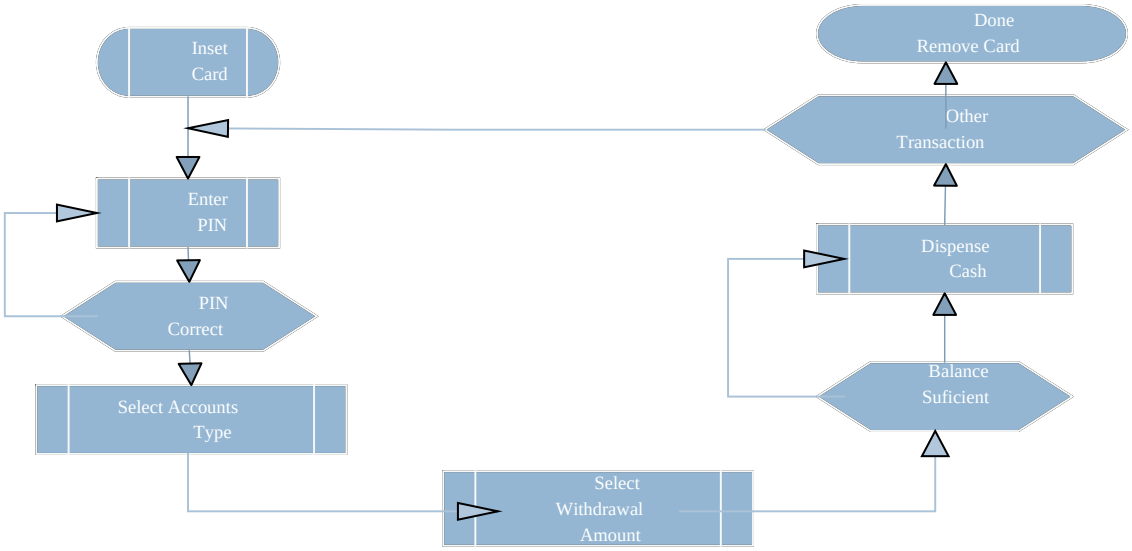

Figure 1 ATM Withdrawal PIN Based

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.

Improved security of ATM machine with Single Password (OTP) and face recognition features proposed by Mohsin, et al., 2015 to improve ATM security. OTP was used to enhance account security and privacy for ATM users. The face recognition technology proposed in their system was to help the ATM to identify each user differently, using the face as a key. Investigators concluded that there were minor flaws in the facial recognition process, hence the inability to detect facial expressions, beards, caps, and glasses. (Mohsin, et al., 2015). ATM Transaction Security System Using the Biometric Palm Print Recognition and Transaction Confirmation System proposed by (Sanjay, et al., 2014), researchers agree that the PIN-only verification system, as used in many ATM machines, is not secure. Therefore, they plan to improve the security system by introducing palm print printing as the best and most continuous way to ensure security at ATMs. The proposed method was implemented with an example model of an ATM simulator that mimics a standard ATM system. In their conclusion, they recorded the same 89.43% palm-print system recognition and rejection rate of 10.57% (Sanjay, et al., 2014). Therefore, of the 53 out of 500 customers who will visit the upgraded ATMs with this authentication system they may have problems with their transactions. Make the Force Rejection Rate of the system 10.57%. Hirakawa in 2013 developed a password development method called (Random Board: Password Authentication Method with Tolerance to Video-Recording Attacks) to increase or strengthen security at ATMs, by preventing visual attacks from stealing user password (thus video recording) and greater attacks . Hirakawa agrees that the authenticity of the PIN at traditional ATMs contributes to the rise of ATM fraud, as this PIN, (password) is entered in open spaces which allows criminals with cell phones with cameras and small cameras to check the user enter his PIN. To achieve this Hirakawa proposed two modules, a basic method and an advanced method. With their basic

method, the correct location for each password entry should be provided in advance. Whiles, in an advanced way, the user does not need to provide any information ahead of time, other than a password. In his own way, the alphabet board acts randomly, so the letters change shape all the time, making it difficult for the observer to recognize the characters entered by the user (Hirakawa, 2013). Lalzirtira has proposed a authentication method called Graphical User Authentication to eliminate defects in the alphanumeric authentication mode of traditional ATMs. In his research, he emphasized that a graphic password that uses images is easier for people to remember than words or numbers. In his work it has been suggested that the introduction of a click-through password will remove the user's tendency to write down their password, which is why it eliminates ATM fraud (Lalzirtira, 2013).

The use of images as a means of authenticity in the ATM system has a certain up to date and a serious weakness in video recording, which is why this method can be considered a straightforward solution to ATM fraud.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's mobile phone from the bank server if the PIN provided by the user is true. The user then enters the new code obtained from his phone for verification, this is also checked with the bank server for verification, and if proper access to ATM transactions is granted to the user (Anand, et al., 2013).

This means that to access a user's ATM account, you need his or her PIN, bank card and cell phone. So someone close to the user can find out all of this and trick the ATM user. In this paper a third-party emergency verification has been proposed, in which three to four people can sign up for the program with their mobile numbers.

a friend. In order in the event that the account holder himself is not able to make the transaction, these subscribers can make the actual user transaction by mobile phone (Anand, et al., 2013). Therefore, the user is given the opportunity to provide three or four auxiliary phone numbers in addition to his mobile phone number. Lawan suggested that the fraudulent use of ATMs could be eliminated by using a biometric authentication method installed at ATM security. In his report he looks at everything that is being done with all ATM scams and recommended ways to make or prevent these scams at ATMs. In addition a model model of biometric authentication was developed to provide a solution to known security breaches in ATM authentication (Mohammed, 2011).

In another research project, the proposed neural network-based was modified to match users' fingerprints by looking at plans and finger groove patterns. This proposed module works perfectly for binary images and gray scanners; one positive aspect of this proposed module is that, if a team is followed, the pattern can be followed with high accuracy. But this approach poses a serious threat where the network is inaccessible (Saropourian, 2009). Convex polygon multilayers are proposed to use fingerprint authentication to improve ATM security standards. In this operation, fingerprint extraction was obtained at a fixed location where the amount of light available was the width of the fingertips. A major limitation may be that fraudulent ownership and fraudulent verification cannot be easily detected. To conclude these revised research efforts were performed using a single biometric check without any form of cryptography, therefore, they could not find a reliable security solution (Myo, 2009). A authentication method called fakepointer is proposed to improve security standards at ATMs, which use numerical key inputs. In this way, discarded "answer selection data" will be obtained before each verification. This selected information provides a background symbol, such as a square, a triangle, a pentagon, a hexagon of a numeric password he displayed. In the verification phase or time the user traces the input button, which corresponds to the password by going to the back icon. This method is open to double-video video attacks, provided that "response selection data" can be safely accessed before each verification. However, this study did not focus on how to get it safely (Takada, 2007) identified by (Tedder, 2009). Zhao & Li have proposed a PIN verification interface called S3PAS, which has suggested a number of characters to be displayed on the interface. The user on the ATM premises assigns three locations where the password is character is included in a triangle. This approach guides the user in shoulder surfing attack, but also when input is recorded; is displayed in the user's password in a criminal attack (Zhao & Li, 2007). Suggested password verification process is suggested using the numerical key input. In this way a black or white background is displayed randomly. The ATM user chooses a password instead of a black or white color as the background color of the password. The user selects the background color with a different color pattern four times to enter a single (1) digital password entry. This method is very safe for clapping, but the attacker is able to record the video encryption function while the attack is open (Roth, et al., 2004). (Sakurai, et al., 2004; Sakurai & Munaka, 2008) have been identified (Hirakawa, et al., 2013) suggesting a password login interface known as mobile authentication. In their own way all the selected text is square, with each text having its own background color. For example, all passwords are numeric or alphabetical, and texts are ordered in a 6×6 square where six colors are used, each color appearing only once in each line. A line color pattern is a allowed color pattern for another line. In this way, the user provides the appropriate

background color and password for the front. In the Authentication (password entry) section, the user changes the background color of the passcode to the appropriate background color, and then presses the accept / enter button. This method comes with the limitation that all available text must be displayed in the forum, but this method is safe from double-barreled video attacks. Their tactics apply to numerical passwords and yet, a 12-digit long password is required for secure use, which can be considered too long by most ATM customers. In this way, all available documents are presented as squares in the visual interface for authentication. In the case of a four-letter password, the number of columns must be greater than or equal to 10 to tolerate random attacks, and the number of rows must be greater than or equal to 9 to tolerate video attacks. Therefore, the number of available passtexts is equal to or more than 90 to withstand all attacks. Also, in the case of a five-letter password, the number of columns should be equal to or greater than 7 and the number of rows should be equal to or greater than 6. Therefore, the method is not used when a four- or five-hour alphanumeric password is used as a PIN to authenticate (Hirakawa, 2013). AWASE-E has been proposed, with 25 photographs, one for the appropriate passing images. These images are usually displayed on the screen, similar to the method of (Passfaces, 2005), but with the ability to display on a screen where there is no image. When the earth image is not part of the images' on the screen, then the user must select the "no-pass-image" button. Although this method provides strict security in ATM authentication, it is only safe when shot, it is not clear to the attacker (Koike & Takada, 2003) quoted (Hirakawa, 2013). The techniques proposed by (Passfaces, 2005) are exposed to the shoulder surfing attack, because the user selects a passing image while authorizing it. (Ratha, et al., 2001) have proposed a fingerprint system for ATM security systems, in their proposed system, banks 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 ATM will receive a four-digit text message on its GSM cell phone when the customer enters

finger on the fingerprint module attached to the ATM. This message is automatically generated every time a customer visits an ATM. The code received by the customer is entered into the ATM machine by pressing buttons on the touch screen. After installing it checks whether it is real or not and allows the customer to continue accessing it. The worst thing about this program is that customers with a lost phone need a new one or have to update their bank records before they can log into their ATM account. The ATM development process using the Personal Identification Image (PII) secure process was proposed by Santhi and Kumar. This method is protected from shoulder attack surfaces, but when the recording camera is hidden to record the verification process, the system becomes unsafe (Santhi and Kumar, 2012). A certified biometric security system is proposed by (Subh & Vanithaasri, 2012), in improving ATM security. Implementation of the proposed method however has the potential to remove the incorrect or false element and minutiae points from its extracted list.

As a result of the above discussions, it is clear that the PIN and the image verification method do not guarantee adequate ATM security.

This paper seeks to propose a multifactor authentication system (PIN and Fingerprint) to address the modern challenges of ATM security and test its effectiveness.

2. Materials and method

Microsoft Visual Studio 2010 (C #) was used to upgrade the front, where the system user was able to better communicate with the ATM. The background (database) is built on the 2008 Microsoft Structured Query Language (MSSQL) server, MSSQL is a relational management system (RDBMS) used to create a Microsoft Windows database for family servers. MSSQL was chosen over another database management tool, due to its ability to provide a workplace to easily create a database that can be easily and quickly accessible from the Internet, workspace, LAN and so on. To facilitate communication between the fingerprint scanner the Grfinger software development kit (SDK) was hired in partnership with Microsoft visual studio to assist in the registration of fingerprints and algorithm enhancement.

2.1 Design Concept

Figure 2 shows a block diagram of the proposed ATM authentication system, which contains customer account details, PIN database, fingerprint database and ATM machine. The following paragraphs explain in detail how the ATM multifactor Authentication guarantee will increase the level of security at the ATM, to protect ATM users from various ATM attacks initiated by fraudsters.

The Internet, is the first phase of the proposed system, which serves as a platform and platform for the proposed system to communicate between individual ATM terminals and the central bank server. Customers with fingerprints and PINs are available on bank servers and the associated information model is used to store information on all fingerprints and PINs. registered customers. These information include pattern type, and feature characteristics.

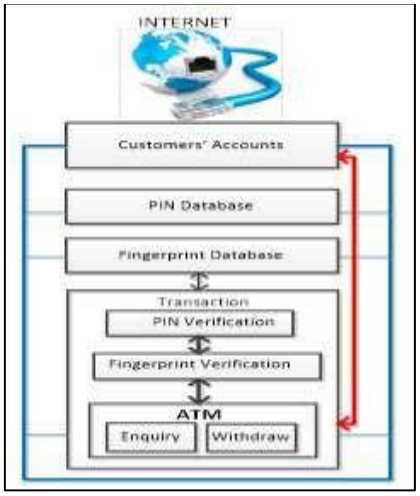

Figure 2 Conceptual Design of Proposed ATM Security

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.

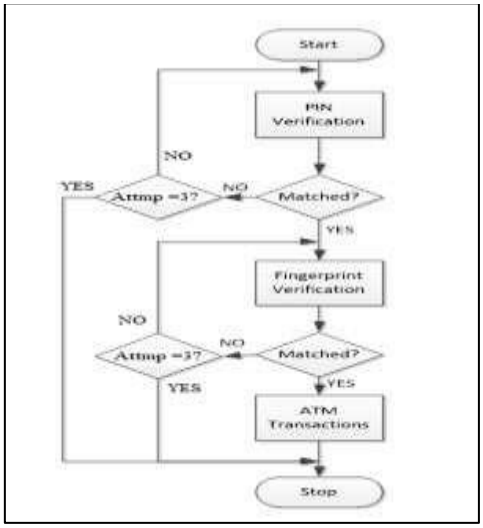

Figure 3 Flow Chart of Proposed System

During image enhancement, the front of the image regions which are groups containing groups and valleys are separated, from the background regions, which contain the most noise. The segregation is done to ensure that the focus is on the front areas only, while the back areas are ignored. The structure of the split fingerprint image will be set up in the normal way to strengthen the degree of variation in the gray values of the image. Generally, gray-level values will be brought to a level sufficient for image brightness and brightness. Normal image is filtered to remove any noise and false positives. Sorting will also preserve the true ridge and valley, and this involves the ridge orientation and frequency estimations. The output the results obtained after filtering (filtered image) are converted to binary format and reduced to the release of a satisfactory feature. In the element output phase, the main features; i.e. spinal ends and spatial segments are obtained and extracted from the image. These two main features are the features that distinguish between different fingerprints.

Features extracted from the user template are matched with templates for other images in the archive. The ATM user will provide his or her PIN and if correct after the system check, the user will be given access to the second level of authentication (fingerprint identification), where the user's fingerprints are scanned by the installed fingerprint model and the game exit compared to that stored during user registration, access is granted user to perform his ATM functions.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.

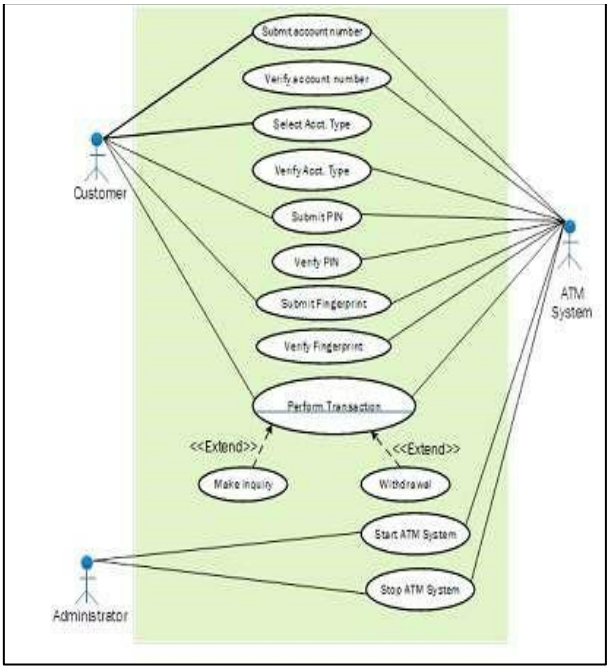

Figure 4 Use Case Diagram for Proposed ATM Multifactor Authentication Module

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.

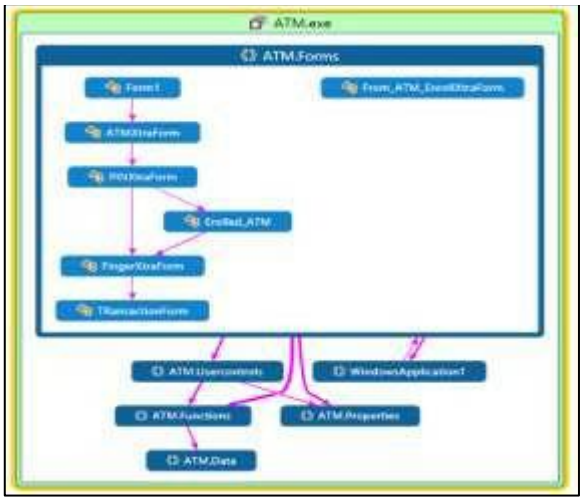

Figure 5 Detail Code Elements and Relation

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 Percentage of invalid input received incorrectly (match between input and inconsistent template). FRR is the percentage of invalid input that is negatively denied (failed to find similarities between input and analog templates) (Sainath and Tangellapally, 2010). To evaluate the effectiveness and durability of the proposed system, two sets of FAR and FRR fingerprints were used. As these indicators are the most common and simple indicators to assess the effectiveness, accuracy and functionality of the similarity of the finger pattern (Iwasokun & Akinyokun, 2013). The first database (A) had 1,800 thumbs, including four (4) thumbs collected from the right thumb of each of 450 respondents. Another database (B) also contained the same number of thumbnails collected on the left thumb of the respondents. Datasets (C), (D) and (E) consist of 450 thumbs each from the right thumb of each question with a separate thumb for the internal variance class. All three thousand, six hundred (3,600) fingerprints from the right and left of the respondent were registered on the system for 120 days, using a digital persona (U.are.U 4500) USB fingerprint reader with a resolution of 512dpi pixels and a length of 18.1mm with 14.6mm wide shooting range.

3.2 Intra-class variations test

To determine how the proposed system will respond to internal modification, each of the 450 categories listed in Database (C) resembles templates in Database (C), (D) and (E) with the same client and the recorded sports school. The same score (also called weight) gives or implies a degree of similarity or a measure of distance between two minutiae patterns. The points are more, the chances are higher, and for the faithful buyer the points (s) must be greater than the limit (T). Figure 7 shows a school graph obtained from 20 randomly selected templates in (C) compared to the inclusion of information opposition (D) and (E) in the same respondent. The declaration of existence of the game is completed by comparing the same points (s) with the decision limit (T), and in the case of $S \geq T$, the ownership claim is considered correct.

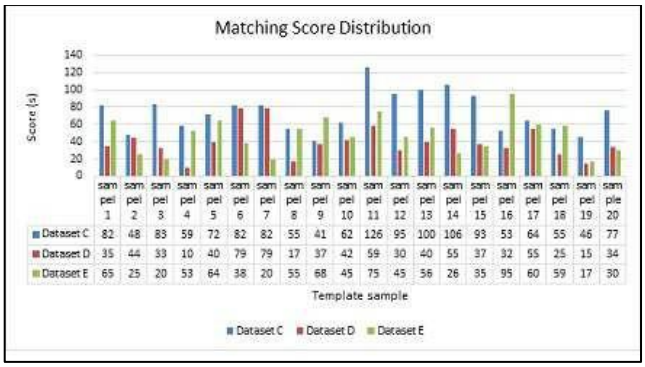

Figure 7 Intra-Class Variations Matching Score Distribution

From figure 7, it can be clarified that the scores obtained by clients vary from database to database. This inconsistency in the points ratio can be created for the various customers that appear at the time of registration. If clients could be verified with a template stored in databases D and E, there would be seven (7) fraudsters in database (D)and six (6) in databases (E) make up eleven (13) equal to 65% of the twenty random samples. From this result, it can be concluded that if the client is not directed to the registration phase to place his or her thumb properly on the sensor, there will be a higher FAR level in the verification phase.

For the purpose of testing FAR and FRR, three phases of test I, K and L were performed. The first phase (I) experiment (FRR test), performed on a database (A), by comparing all available thumbnails (A) with the remaining three thumbs from that thumb (D), but avoiding measuring similarities, using the included fingerprint algorithm . This was to determine whether it was possible for two match samples to be falsely accepted as unmatched, so match points would be less than the limit value.

3.3 False Rejection Rate

Figure 8 False Rejection Rate Score

Figure 8 shows the result of the results of 50 randomly selected samples (templates) in the FRR test in database (A).

Of the fifty (50) samples, one (1) false denial was reported. The FRR is therefore equal (2%) to 50 compared to 3.33% of the 30 (Manish, et al., 2011) and 10.57% (Sanjay, et al., 2014), it can be estimated that for all four hundred and fifty samples placed under the FRR test nine (9) false positives will be counted, making the total FRR equal to nine (9). Real Admission Rate (GAR) is a fraction of the actual scores above the threshold (T). Thus GAR = 1 - FRR (1 - 0.02 = 0.98).

3.4 False Acceptance Rate

To determine FAR, the four thumbs of each thumb, from each respondent in databases (A) and (B) are compared with 1,796 thumbs from the thumbs of the remaining 449 respondents at different threshold levels. This is to determine whether it is possible for two non-match thumbs up to be mistaken for a match.

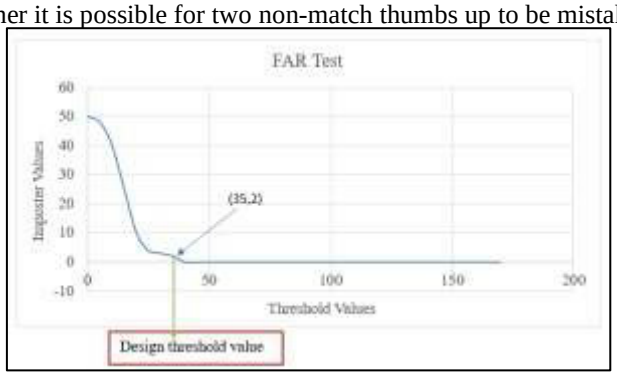

Figure 9 False Acceptance Test

Figure 9 shows the output curve of the FAR test in database (A). From the graph it can be seen that, at a limit of thirty-five (35), two deceptive values are recorded as the actual record in fifty (50) samples taken randomly. FAR is therefore equivalent (4%) of this activity compared to (6.6%) of (Manish, et al., 2011) by 30 samples. TER is 6% of total access to 50 and compared to 13.3% (Manish, et al., 2011) of total access to 30 and 8.27% (Iwasokun & Akinyokun, 2013).

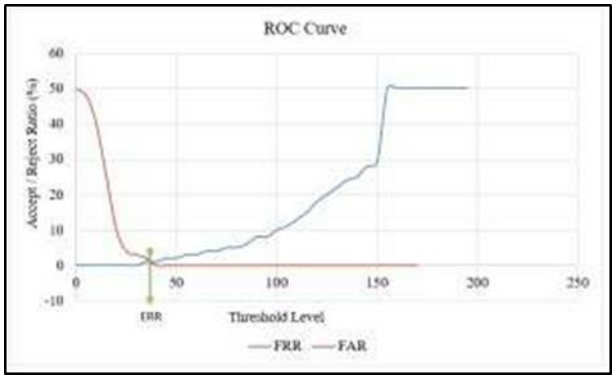

Figure 10 ROC Curve

With a TER of 6%, it shows that the improved system is 94% accurate compared to 89.43% (Sanjay, et al., 2014). Figure 10 shows the ROC curve. Average time rating of 1.023, 1.075 and 1.155 was recorded for data A, B and A + B respectively.

4. Conclusions And Recommendations

The conclusions from this study, based on the findings, are given below.

Proposed Proposed fingerprint and PIN system works perfectly with 94%, FAR 4%, FRR 2%, TER 6% and GAR 98%.

Compared to other fingerprint identification systems and verification systems, the proposed system provides improved simultaneous performance and partial elimination of false minutiae on its fingerprint site.

The proposed system is a good way to charge the cost of starting a secure ATM transaction to protect ATM users from fraudsters.The recommendations of this study can be summarized as follows:

Decision-makers need to value a guaranteed level of security through biometric systems and the potential for change between perception and reality.

The Bank of Ghana (BoG) and the Ghana Association of Bankers (GAB) which is responsible for strategic action in the banking sector in Ghana should initiate the installation of improved ATMs through this system as a strategy to reduce costs and security for their customers and customers.

The significant differences found in the Intra -class variability study in this study indicate that, if clients thumbprints are not different from the thumb when verified, a false positive will be rejected. The Electoral Commission (EC) of Ghana should therefore ensure that voters' thumbs during registration and voting days are properly placed on a fingerprint scanner, to prevent false positives, causing confusion on polling days. Test verification should be done to verify the file

 The proposed system is a good way to charge for the cost of starting a secure ATM transaction 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.

References

1. Adams, A. & Sasse, M. A., 1999. Users are not the Enemy. Commun .. ACM 42, 12, pages 40-46.
2. Akinyemi, I., Omogbadegun, Z. & Oyelami, O., 2010. Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria Banking System .. International Journal of Electrical & Computer Sciences JECS-IJENS 10, pages 68- 73 .
3. Anand, D. A., Dinesh, G. & Naveen, H. D., 2013. Reliable ATM Agreement and comparative analysis for various parameters and other ATM Protocol. International Jouranl Communication and Information Technology (IJCCT), ISSN: 2278-9723, 01 (56), pages 192-197.
4. Baptiz-Lazo, B. & Barrie,. A., 2005. Business history and technology of automatic tell machine in the UK. London, Queen Mary University, page 110.
5. Das, S. & Jhunu, D., 2011. Designing Biometric Strategy (Fingerprint) Measures To Strengthen ATM Security in Indian Banking System Foreign Journal of Information and Communication Technology Research, pages 197-203.

6. Gunn, L., 2010. European ATM crime report. Technical Report 1.2, sl. European ATM Security Group (EAST),.
7. Hirakawa, Y., 2013. Random Board: Password How to prove authenticity by tolerating video attacks. International Journal of Innovation, Management and Technology, Vol. 4, No. 5, pages 455-460.
8. Iwasokun, G. B. & Akinyokun, O. C., 2013. A fingerprint Authorization Framework for ATMs. Computer Engineering & Information Technology Journal, pages 1-8.the results presented in this research work.
9. Jermyn, I. et al., 1999. Composition and analysis of graphical passwords .. s.l., USENIX Association, pages 1-1.
10. Lalzirtira, 2013. Graphical User Authentication, India: Department of Computer Science and Engineering National Institute of Technology Rourkela.
11. Luca, A., 2011. Building Effective and Safe Use of Public Spaces (Doctoral qualifications, lmu), sl: s.n.
12. Manish,. M., Ajit, S. K., Thakur, S. S. & Sinha, D.,. 2011. Secure Biometric Cryptosystem for Distributed System. International Communication and Security Network (IJCNS),Volume-I (Issue-II), pages 28-32.
13. Modernghana, 2013. Modernghana. [Online] Available at: http://www.modernghana.com/news/463043/1/hack ers-steal-45-million-in-atm-card-scam-federal.html [Accessed 10 June 2015].
14. Mohammed, L. A., 2011. The use of biometric to deal with ATM fraud .. Malaysia ,, IACSIT Press, Kuala Lumpur, pages 331-335.Mohsin, K., Saifali, K., Sharad, O. & Dr.D.R.Kalbanded, 2015. Enhanced ATM machine security with OTP and face. sl, Elsevier BV, pp. 390-396.
15. Myo, N., 2009. Identification of fingerprints Based on External Layers Model Polygon. International Conference on Technology and Computer Technology, p. 201 - 204.
16. I Died, .. A., Fesach, .. E., Anthony, .. O. & Davies, .,., 2013. Enhanced Technique at ATM Risk Reduction using Automated. Volume No. 4, 06 June, pages 1132-1138.
17. Obour, S. K., 2013. [Online]Available at: http://graphic.com.gh/news/generalnews/8459-gcb-confirms-money-theft-from-atmbut-says-amount-is-lower-than-gh-3-million.html
18. Passfaces, Corporation, 2005. [Online] Available at: http://www.realuser.com/enterprise/about/about_pas sfaces.htm[Accessed 9 July 2015].
19. Rasiah, D., 2010. ATM Risk Management and Control. European Journal of Economics, Finance and Management Science, 21 ,, 2014 January.pp. 161-171.
20. Ratha, N., Connell, J. & Bolle,