Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) DOI: 10.7176/IKM
Vol.9, No.7, 2019

Enhancing Security of Automated Teller Machines Using Biometric Authentication: A Case of a Sub-Saharan University

Ohene Kofi Afriyie
Dept. of Science, Wesley Grammar School, c/o Methodist University, Ghana

Valentina Arkorful*
College of Distance Education, University of Cape Coast, PMB, Cape Coast, Ghana

Abstract
A wide variety of systems need reliable personal recognition systems to either authorize or determine the identity of an individual demanding their services. The goal of such systems 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 impostor. The ATM has suffered a lot over the years against PIN theft and other associated ATM frauds. In this research is proposed a fingerprint and PIN based authentication 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. The last tier presents a system platform to relate banking transactions such as balance enquiries, mini statement and withdrawal. The system is developed to run on Microsoft windows Xp or higher and all systems with .NET framework employing C# programming language, Microsoft Visio studio 2010 and SQL server 2008. The simulated results showed 96% accuracy, the simulation overlooked the absence of a cash tray. The findings of this research will be meaningful to Banks and other financial institutions.
Keywords: SQL Server, ATM, Fraud, .NET framework, financial institutions
DOI: 10.7176/IKM/9-7-02
Publication date: August 31st 2019

1. Introduction

The advancement of payment systems in this modern world has gone past cash to cheques, 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 aim 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 financial institutions 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 in a lot of schools, businesses nowadays have installed ATM on their premises for customer convenience and more revenue

ATMs card authentication methods have changed 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 stripes 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 the writing of tracks is known as Friend-to-friend (F/2F). 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 caution given to card users, 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).

In 2013 Ghana Commercial Bank (GCB) confirmed 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 draining cash machines around the globe (Modernghana, 2013). ATM's crime has become a nationwide epidemic which face both customers and bank operators, as well (Das & Jhunu, 2011).

1.1 Design Criteria and Concept

Fingerprint as a means of a person's identification, was introduced a long time ago and it is accepted, that the fingerprint of every person is unique. Hence fingerprint matching is universally considered as one of the most dependable techniques of identifying a person.

Figure 3.2 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. In the software development process, the standard Software Development Life Cycle (SDLC) model and Object Oriented Analysis and Design (OOAD) model are used in the design and implementation stages.

The following subsections explain in detail 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.

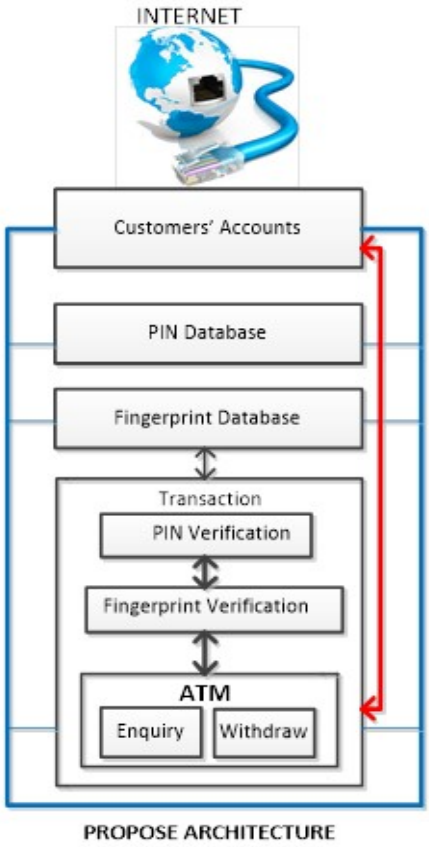

Figure 1: Conceptual Design of Proposed ATM Security Structure.

Figure 1 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 below:

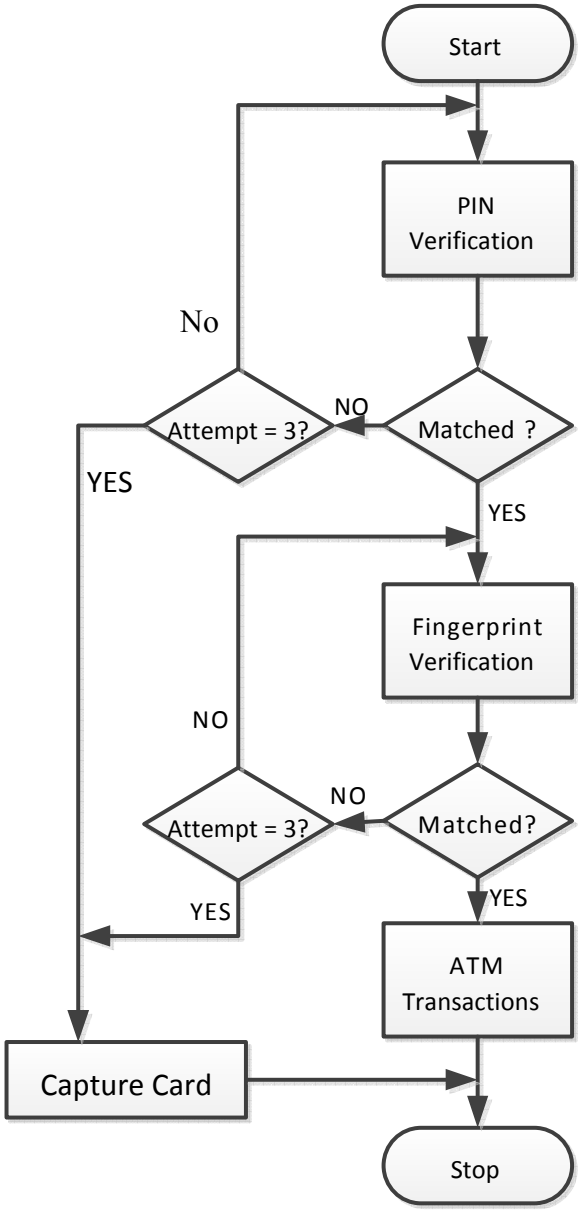

Figure 2: Flow Chart of the Proposed System

User Fingerprint enrolment involves enhancement, feature extraction and matching and storage as shown in Figure 2

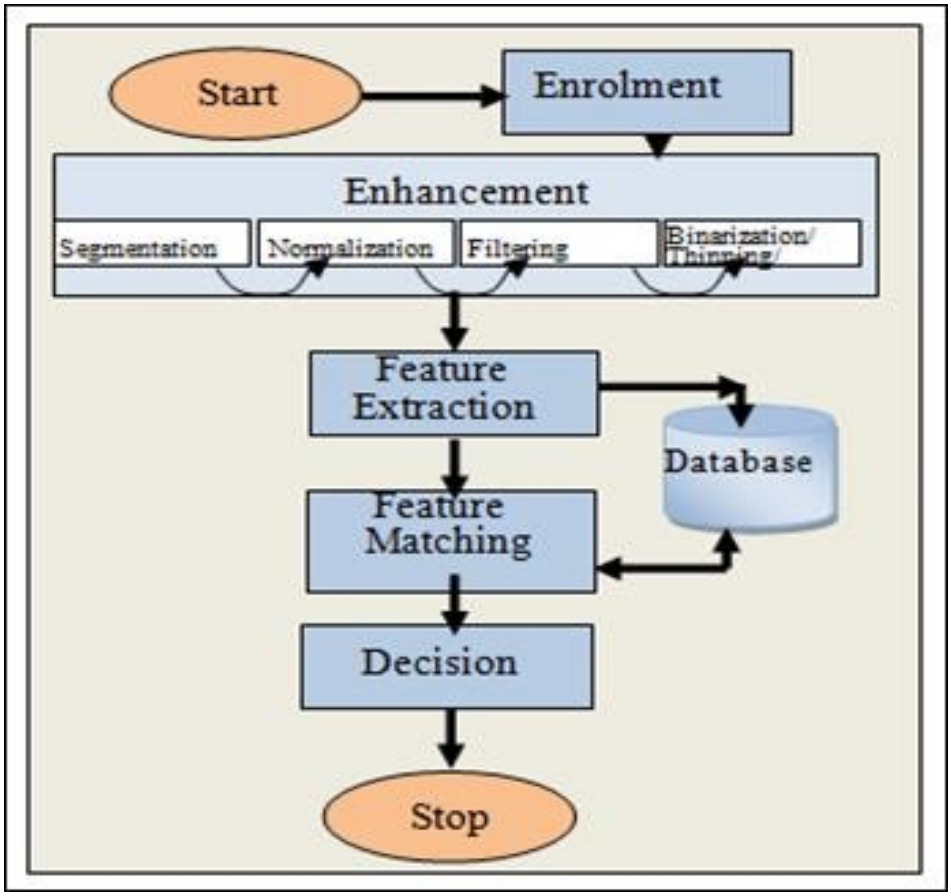

Figure 3: Block Diagram of User Fingerprint enrolment

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.
The performance evaluation criteria of this design are as follows:

i. False Match Rate (FMR) or False Acceptance Rate (FAR)
ii. False No match Rate (FNMR) False Rejection Rate (FRR)
iii. Failure-to-Enroll Rate (FTE) System Failure-to-Enroll Rate
iv. Total Error Rate (TER)
v. Efficiency
vi. Complexity of Implementation

False Match Rate (FMR): this is when the system matches a user's fingerprint template extracted for verification with a different user's enrolment template in the database. Thus, this can be explained as an imposter being recognized by the system as a rightful user. This is generally the most critical accuracy metric, as it's a good system security design to keep imposters out in most applications.
False Non-match Rate (FNMR): this Error appears when there is a mismatch of a legitimate user's verification

template with his enrollment template. This can be explained as a rightful user not being recognized by the system. Even though FNMR is not serious as FMR, high false, matching in a system can lead to low productivity and frustration of users.

Failure-to-Enroll Rate (FTE): this type of error happens when the system fails to take out consistent, unique and replicable characteristic from the sample presented whiles enrolling. Thus the system is not able to create a new enrollment template for a new system user. This error can be attributed to user behavioral reasons, such as the movement of an enrollee during the data acquisition process and physical reasons, e.g. wear and aging of the enrollee causing faint patterns.

2. Fingerprint Identification Algorithm

The good nature of a fingerprint image in terms of the adequacy level of the implementation algorithm as well as quality are part of the basic deterministic parameters of the performance level of Automatic Fingerprint Identification Systems (AFIS) in their various assigned tasks (Iwasokun, et al., 2012).

The study employs a Fingerprint Identification System presented by Shallita, et al., (2010). The algorithm by Shallita, et al., (2010) involves two main processes namely enrollment and authentication.

The enrollment process is where a person's fingerprint is captures using a fingerprint capturing device and saved in a database.

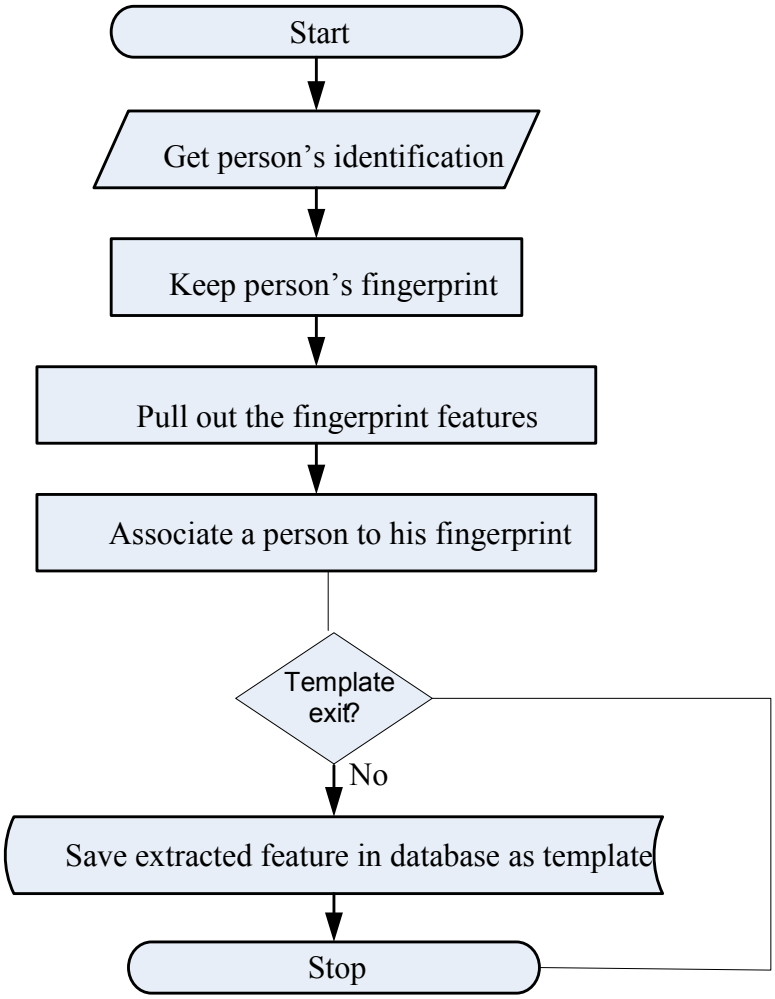

Figure 4: A flow chart for fingerprint enrollment process

Figure 4 shows the flow chart for the enrollment phase. The fingerprint of a user is captured with a fingerprint scanner, features are extracted as a template and then saved in the database.

Authentication is a process where a person claiming to be whom he or she is, is verified. This process consists of a comparison between a captured fingerprint at the ATM terminal to an enrolled fingerprint template stored in the database, in order to determine whether there's a match, and if there is a match, the user is permitted to conduct his or her ATM transactions. This process is as shown in figure 4.

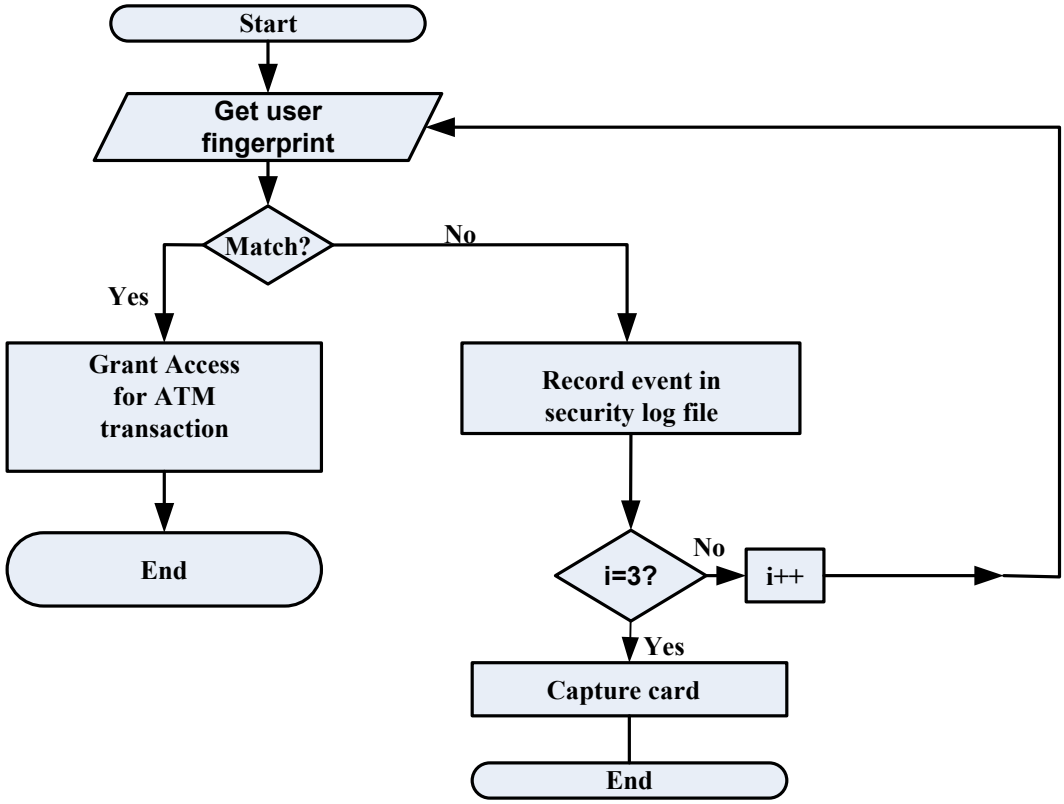

Figure 5: Authentication Process Flow Chart

2.1 Fingerprint Image Enhancement

The dependability and authenticity of fingerprint technology employed in an AFIS are preceded with proper detection and extraction of features in the fingerprint image. To obtain proper and sound feature extraction from any fingerprint, such fingerprint must be enhanced first. A well enhanced image brings about clarity in separation between spurious minutiae and valid ones.

Minutiae points created as a result of artefacts or noise are called spurious minutiae. This research work adapts the algorithm proposed by Babatunde, et al., 2012 and Iwasokun, et al., 2012 for image enhancement with little modification. The main steps of this approach are image/ridge segmentation, ridge/image local normalization, ridge filtering and ridge binarization/thinning.

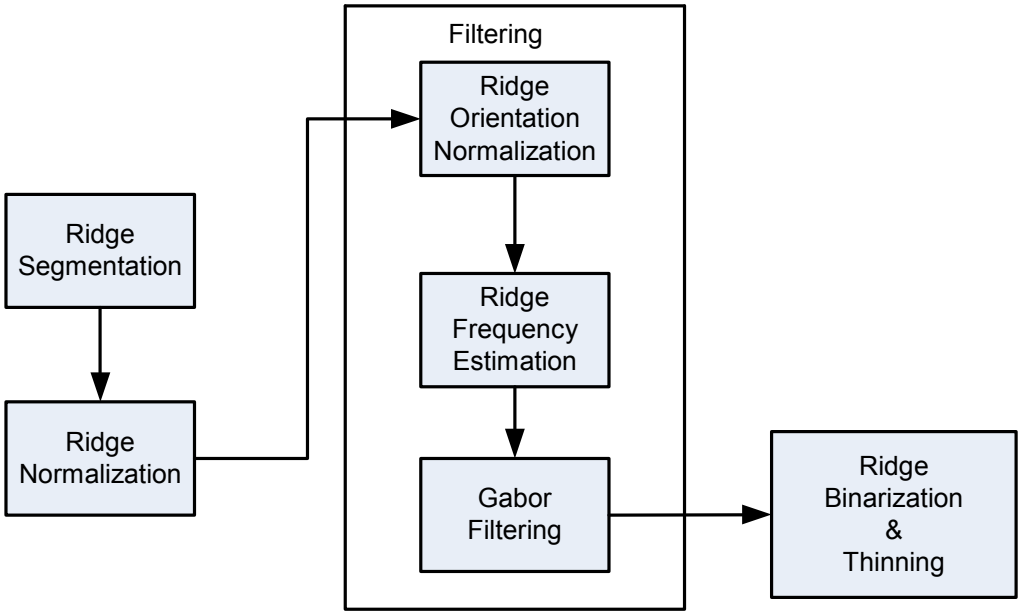

Figure 6: The Conceptual Diagram of the Fingerprint Enhancement Algorithm

Image Segmentation

All fingerprint images are described by two regions, namely foreground region and background region. The valleys and ridges are in the Regions of Interest (RoI) or foreground regions as shown in Figure 6. These regions are called the RoI, because they contain the feature points. During enrollment, some noise is introduced into the image, this happens outside the foreground regions and are called the backgrounds as shown in Figure 6. The importance of the segmentation is to separate the foreground regions from the background regions of the image, this paves way for a reduction in difficulty accompanying preceding stages of the image enhancement by making sure that the focus is only in the foreground.

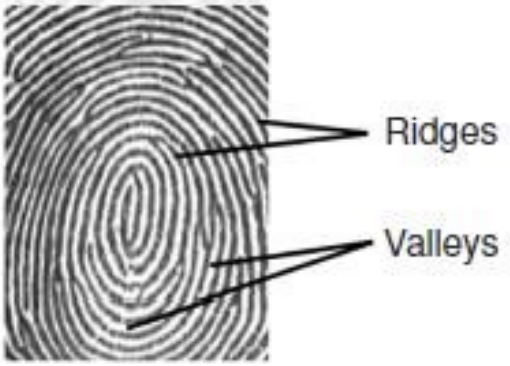

Figure 7: Ridges and Valleys on a Fingerprint Image

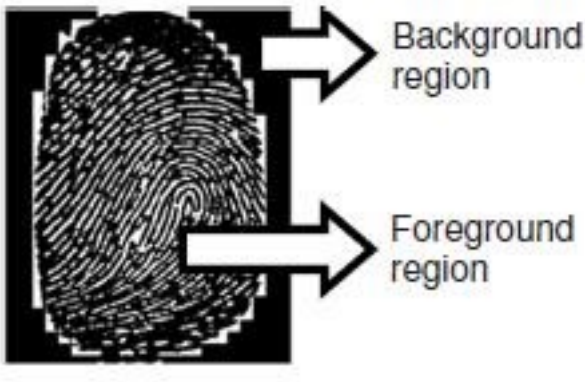

Figure 8: A Fingerprint Image and its Foreground

The foreground region holds very high grey-level variance values, whiles the background regions holds very low grey-level variance values.

The grey-level variance values are obtained through a block processing approach instead of pixel approach (Thai, 2003) cited by (Iwasokun, et al., 2012) and (Babatunde, et al., 2012).

Image Normalization

The output of the image ridge structure obtained after segmentation is normalized to standardize the grey-level values that make up the image. By normalizing the image, the grey-level values are restricted to an acceptable range that is good for improving brightness and contrast. The first process in the normalization proposed (Iwasokun, et al., 2012) is embraced in the research work, thus dividing the segmented image into various blocks of size S x S. A comparison is then made with each grey-level pixel in the segmented image and the average grey-level value within the host block. Assuming for comparison, M_o and V_o are used as mean and variance, respectively, then for a pixel $I(i, j)$ which belongs to a block having M as average grey-level, it comparing result produces an output normalized grey-level value N(i,j) which is computed from the equation.

$$N(i,j) = \begin{cases} M_0 + \sqrt{\dfrac{V_0(I(i,j)-M)^2}{V}} & if\ \ I(i,j) > M \\ M_0 - \sqrt{\dfrac{V_0(I(i,j)-M)^2}{V}} & otherwise \end{cases}$$

Image Binarization and Thinning

The output filtered image from Gabor filtering in converted into binary for better performance. The image binarization technique, proposed by (Iwasokun, et al., 2012) is used in this research with a threshold assumption (T) that reduces overlap and enable a good separation within clusters.

The steps outline to determine the true value of T, is as follows:

1. Separate the pixel into two clusters with respect to the threshold
2. Determined the then of each cluster
3. Square the difference between the mean
4. Determine the product of the number of pixels in each cluster

The difference between the clusters means determines the operational success of the process. The threshold (T) is said to be at optimum when it maximizes the variance of between-class or, contrariwise, the value that minimizes the within-class variance. For each cluster its within-class variance is calculated as the absolute sum of the variance. Details of the fingerprint image enhancement, extraction and binarization algorithm can be found in (Iwasokun, et al., 2012)

Fingerprint matching and decision-making module

The matching process is one of the difficult stages in the fingerprint authentication system, due to quality in deviations of the fingerprint from the same user, as time changes. These variations are due to changing noise due to sensor malfunction, skin conditions, changes in ambient conditions and errors produced during extraction. At

this level the extracted features from the clients during enrollment are compared with the stored templates in the database. With fingerprint-based biometric environment, a matched score is determined from the number of match minutiae existing between the input and the stored template feature sets. The match score is dependent on the quality of the biometric data presented. The matching module has a decision module, which uses the match score to authenticate a claimed identity or gives a ranking of the enrolled individualities in order to identify an individual. Some of the fingerprint matching techniques are

1. Minutiae-based matching,
2. Correlation-based matching,
3. Ridge feature-based matching.

3.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.

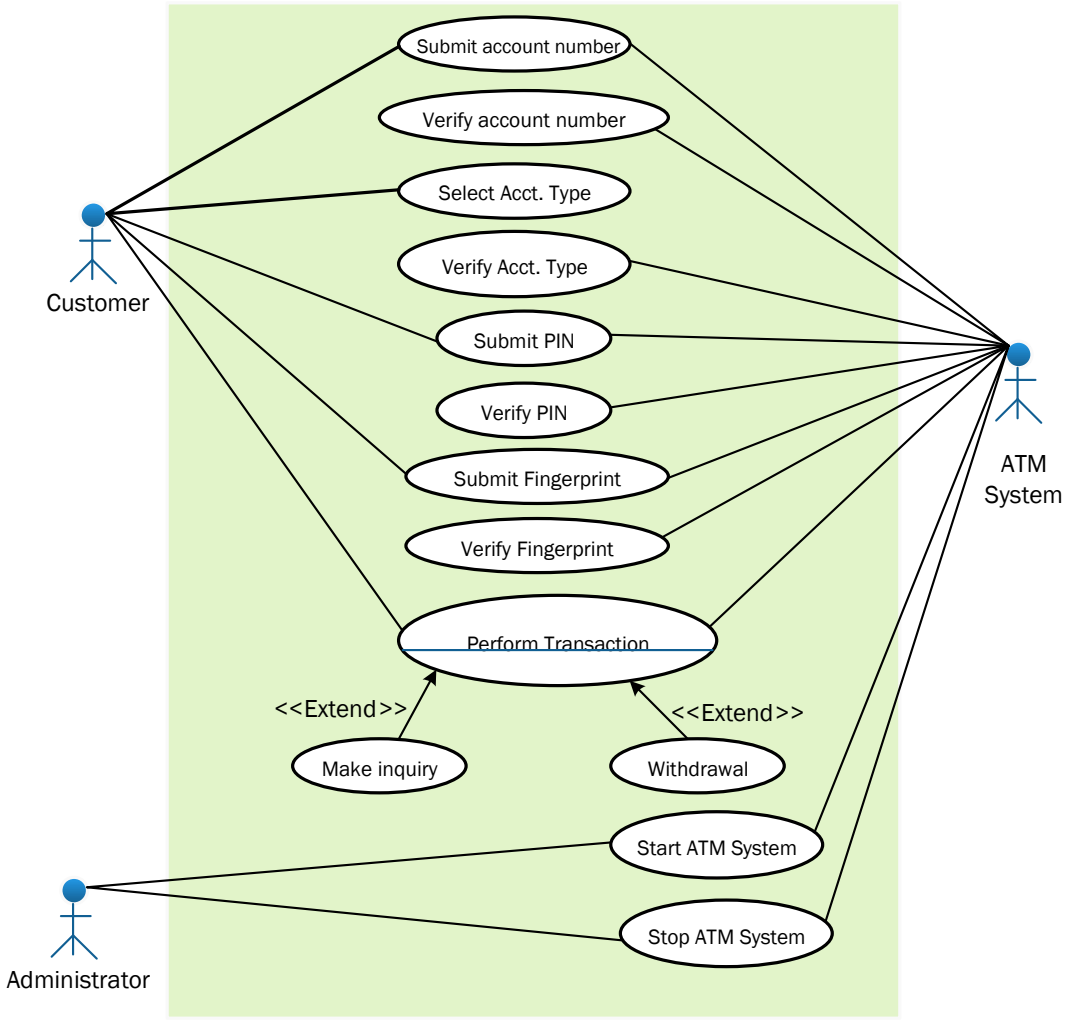

Figure 9: Use Case Diagram for Proposed ATM Multifactor Authentication Module

Figure 9 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 9 shows the a pictorial view of the different functions, windows forms, user controls and the relationships that exist between various sections of the program codes, and how each program code interact with another section.

Methodology

Evaluation and testing of the proposed ATM PIN and fingerprint authentication system was carried out with information/data collected from randomly selected, four hundred and fifty student and staff of the Accra Technical University, Ghana to verify if people who have more than one ATM card from a different bank or

same bank, tend to use the same PIN for all their ATM cards.

4. Findings

A question was asked if respondent use the same PIN for all their ATM cards, and out of the whole. two hundred and fourty nine (249) respondents had more than one ATM card, 159 representing 63.86% answered yes and 93 representing 36.14% answered no.

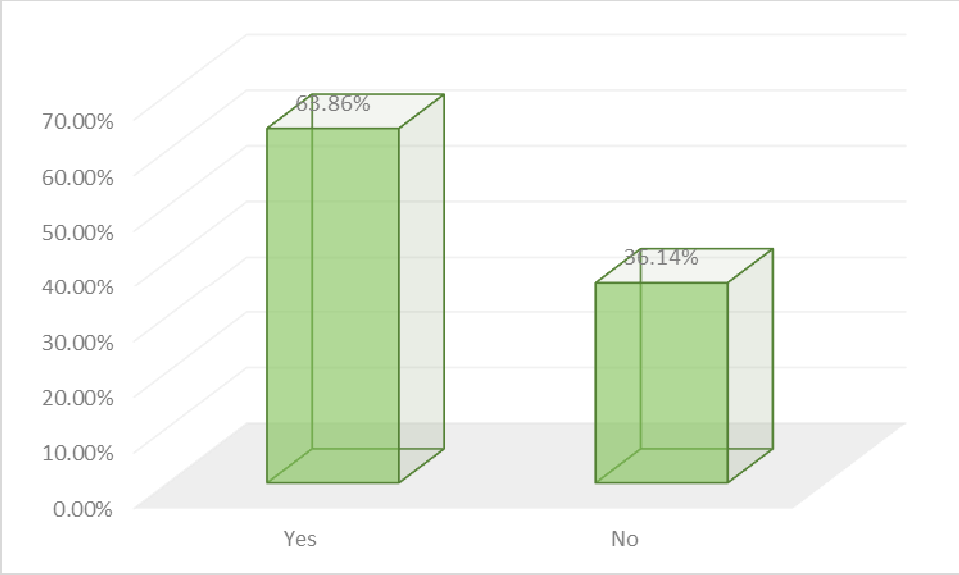

Figure 10. Same PIN for two or More ATM Card

4.3 Software Testing

The performance of a biometric system is usually measured in terms of false accept rate (FAR), False rejection rate (FRR) and equal error rate (EER). The false accept rate is the percentage of invalid inputs that are incorrectly accepted (match between input and a non-matching template). The false reject rate 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 PIN and fingerprint ATM authentication module, two sets of thumbprint data were used for false match rate (FMR) or false acceptance rate (FAR) and False Non-Match Rate (FNMR) or false rejection rate (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 digitalpersona (U.are.U 4500) USB fingerprint reader with 512dpi pixel resolution and 18.1mm length by 14.6mm width capturing area. At the initial enrollment stage, some technical and human errors were encountered, these errors were caused by;

1. Incorrect positioning of respondents/subjects thumbs on the scanner.
2. Some moisture effects affecting the scanner platen.
3. Nature of respondents/subject thumb.
4. Working environment (heat).

These problems were resolved as follows, as enrollment progressed, by gathering more technical knowledge on the web.

1. Respondents were guided to position their thumb at the centre of the scanner lens, to give accurate scanning.
2. Restarting the scanner by unplugging and wiping the lens with a clean cotton, wait for some few seconds and plugging it back.
3. Some of the respondents had hardened and rough thumbs which made it a little bit difficult scanning their thumbs, this was resolved by applying a little amount of Vaseline lotion on the thumb, and wipe off after some few seconds to soften the thumb.

4.3.1 Intra-class variations test

The performance of the matching and verification algorithms mostly depends on a different pose variations of

the system user thumb or finger on the sensor and something due to deformation of the finger or thumb. 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 4.2 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. For the purpose of this research the threshold minimum value was set to thirty (35). 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.

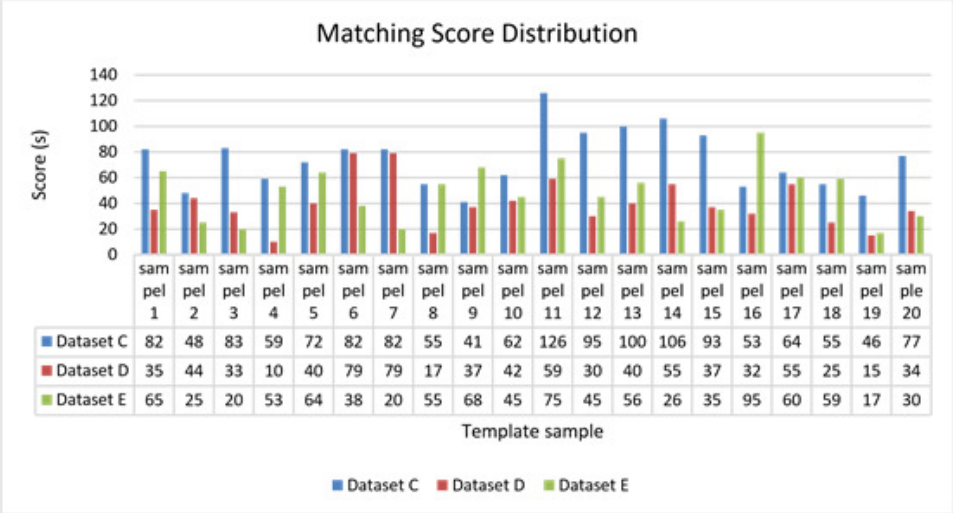

Figure 10. Intra-Class Variations Matching Score Distribution

From the bar chart shown in figure 10, 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 be 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 '8their thumbs well on the sensor, there will be a high rate of false rejection at the authentication stage.

False Rejection and False Acceptance Rate

False Rejection Rate

The extracted minutiae are passed via the proposed fingerprint verification module function, which match two minutiae patterns and produce a match score. Experiments were performed and this assumption was deduced; for larger deviances from the correct registration factors we may expect to find local optima. This was also confirmed by experiments. However, the matching score also depends on other factors like softness and hardness of thumb and the positioning of the thumb. In principle, a client score (score of pattern of a person known by the system) should always be higher than the score of impostor. If this would be true, a single threshold, that separates the two groups of scores, could be used to differ between clients and impostors. The equal error rate indicates the accuracy of the system. The false accept rate and false reject rate intersect at a certain point which is called the equal error rate (the point in which the FAR and FRR have the same value). 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 (i.e., if the template of image f is authenticated against image g, template g is not authenticated against image f); 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.

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.

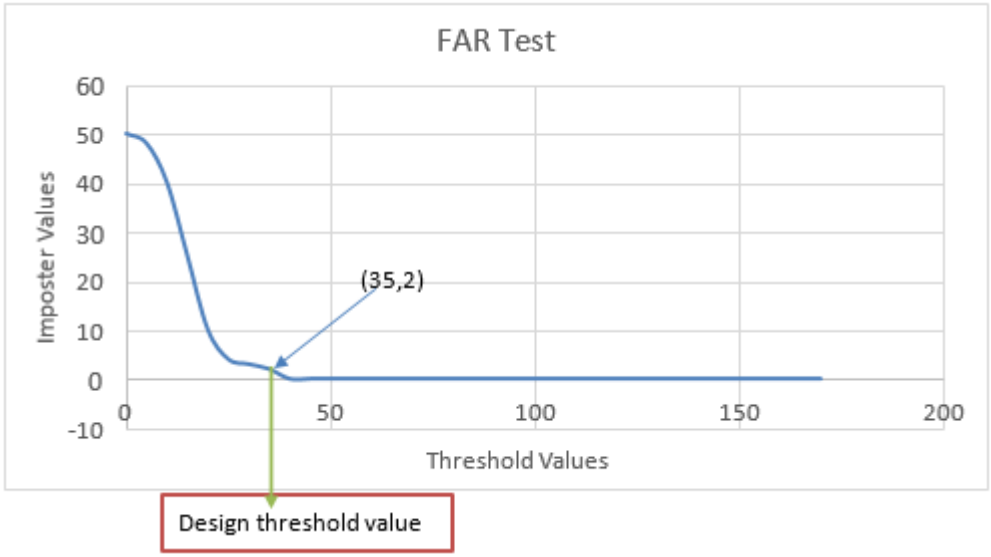

Figure 11: False Acceptance Test

Figure 11 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) which is the system set value, two imposter values are 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. In an ideal situation the FAR and FRR should equal zero with the imposter and genuine distributions being disjoint.

Total Error Rate TER which is defined as:

$$TER = \frac{No.\ of\ FAR + No.\ of\ FRR}{Total\ number\ of\ access} \quad ---(4.1)$$

$$TER = \frac{(2+1)}{50} = 0.06 = 6\%$$

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 4.5 gives the result of the receiver operating characteristic curve (ROC), which demonstrates a true or genuine acceptance rate (1-FRR) plotted against FAR for all thumbprints possible matching thresholds and also a measure of the performance of the entire system on dataset (A).

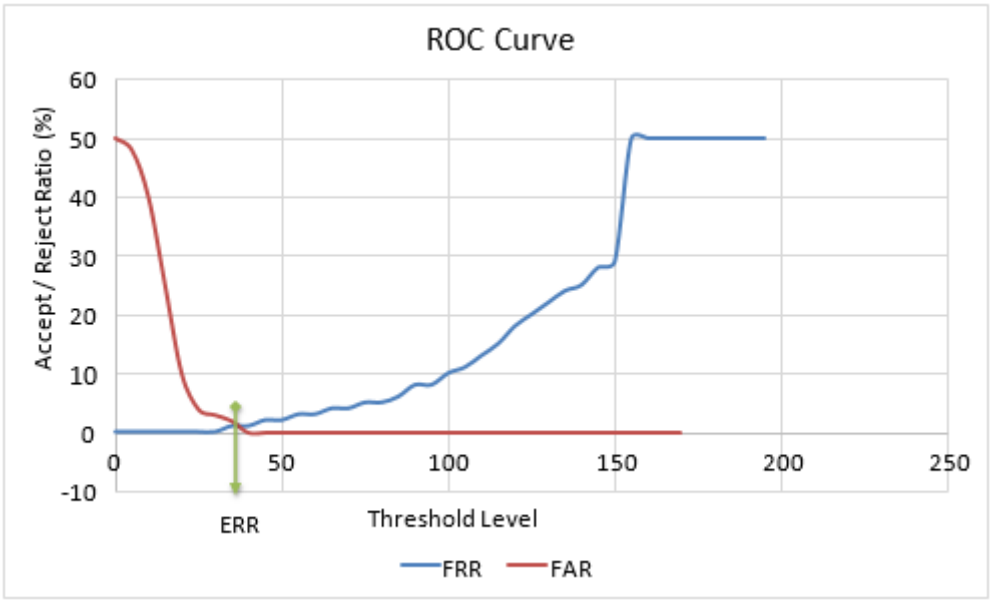

Figure 12: ROC Curve for Experiment on Dataset (A)

Every point on the curve shows a particular threshold value. With a TER of 6%, it shows that the developed

system is 94% accurate as compared with 89.43% (Sanjay, et al., 2014). The TER and ROC curve in figure 4.5 shows that the performance of this system depends on the quality of the fingerprint image obtained from the enrollee at the enrollment stage.

The Average matching time for all three datasets

Dataset	Matching time (S)
A	1.023
B	1.075
A + B	1.155

4 shows the average matching times recorded for all the three categories of experiments performed, thus (I), (K) and (L). A standard deviation of 0.066493107 as compared with 0.0702 (Iwasokun & Akinyokun, 2013) was recorded for the average matching time results of the three sets of experiments, this shows that they are considerably closed. These results, obtained depicts the images equalities in datasets (A) and (B) in terms of qualities, features and resolution/size. The low matching times also indicate that the system is good for identification and verification of individuals at a minimal time.

Conclusion

This worked focused on the use of a fingerprint in addition to the normal PIN to formulate a very strong, secure and dependable identification and verification system to boost ATM security. The key purpose for introducing biometric in ATM systems is to enhance the overall security. Biometrics give greater security and ease than traditional methods of personal recognition (Khan, 2010). The recorded values of FAR, FRR, TER and ROC curve indicates that, the proposed system is a well secured system for providing a strong technique for checkmating the activities of system invaders/imposters as well as providing smooth and reliable access for genuine users.

Recommendation

The recommendations of this research could be summarized as follows:

i. 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.
ii. Future studies should look at reducing the Total Error Rate (TER) via integrated and optimized algorithms and also a combination of fingerprint and other biometrics such as the face and voice for the identification and verification of ATM users.

REFERENCES

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

Agarwal, T., (2010). *How ATMs Work.* [Online] Available at: http://www.elprocus.com/automatic-teller-machine-types-workingadvantages [Accessed 5 January 2017].

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.

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.

Anil , K., Jianjiang , F. & Karthik , N., (2010). Fingerprint Matching. *IEEE Computer Society,* pp. 36-44.

APCA, (2014). *Australian payments fraud details and Data ,* Australia: s.n. Babatunde, G.,

Akinyokun , C. O. & Olatunbosun, O., (2012). A Mathematical Modeling Method for Fingerprint Ridge Segmentation and Normalization. *International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555,* II(02), pp. 263-267.

Bhosale, S. T. & Sawant, D. B. ,., (2012). Security in E-Banking via Card Less Biometric ATMs. *International Journal of Advanced Technology & Engineering Research (IJATER),* p. Volume 2.

Bianchi, A., Oakley, I. & Kwon, D. S., (2010). *The secure haptic keypad: a tactile password system..* s.l., ACM, pp. 1089-1092..

Bond , M. & Zielinski, P., (2004). *Encrypted? Randomised? Compromised? (When cryptographically secured data is not secure).* Gold Coast, Australia, s.n.

Burelli, F., Gorelikov, A. & Labianca, M., 2014. *ATM Benchmarking Study 2014 and Industry Report,* London SW1P 3HQ, UK: Value Partners Management Consulting Ltd Kings Buildings, 7th Floor,16 Smith Square.

Chakrabarty, K. C., 2013. *Fraud in the banking sector – causes, concerns and cures.* New Delhi, ASSOCHAM, pp. 1-13.

Dare, T., 2011. *ATM Security annual report,* Nigeria: NCR .

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.

Diebold, I., 2002 . *ATM fraud and security: White Paper,* New York: s.n.

Gazal, B. & Ranjeet, K. S., 2014. Fingerprints in Automated Teller Machine-A Survey. *Volume-3*, April, pp. 1-4.

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

Han, F. et al., 2006. *A Novel Hybrid Crypto-Biometric Authentication Scheme for ATM Based Banking Applications.* Hong Kong, China, Springer Berlin Heidelberg, pp. 675681.

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.

Ihejiahi, R., 2009. How to fight ATM fraud online. *Nigeria Daily News, June 21,* p. P. 18.

Iwasokun, G., Akinyokun, O., Alese, B. & Olabode, O., 2012. Fingerprint image enhancement: Segmentation to thinning.. *International Journal of Advanced Computer Science and Applications Indian 3,* pp. 50-89.

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

Jegede, C. A., 2014. Effects of Automated Teller Machine on the Performance of Nigerian Banks. *American Journal of Applied Mathematics and Statistics 2 (1),* pp. 40-46.

Khan, H. Z. U., 2010. Comparative Study of Authentication Techniques. *International Journal of Video& Image Processing and Network Security IJVIPNS-IJENS ,* 10(4), pp. 9-13.

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

Lavanya, K. & Raju, C. N., 2013. A Comparative Study on ATM Security with Multimodal Biometric System. *International Journal of Computer Science & Engineering Technology (IJCSET),* IV(06), pp. 808-812.

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

Madu, C. & Madu, A., 2002. Dimensions of e-quality. *International Journal of Quality & Reliability Management, 19(3),* pp. 246-58.

Mandal, S., 2013. A Review on Secured Money Transaction with Fingerprint Technique in ATM System. *International Journal of Computer Science and Network,* 2(4), pp. 8-11. 40.

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.

Modernghana, 2013. *Modernghana.* [Online] Available at: http://www.modernghana.com/news/463043/1/hackers-steal-45-million-inatm-card-scam-federal.html [Accessed 10 January 2017].

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

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.

Mudholkar , S. S., Shende , P. M. & Sarode, M. V., 2012. Biometric Authentication Techhniques for Intrusion Detection System Using Fingerprint Recogbition. *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT),* pp. 57-65.

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.

Obiano, W., 2009. *How to fight ATM fraud Online,* Nigeria: Daily News, June 21, P.

Omari, R. K. B., 2012. *An assessment of the use of Automated Teller Machine (A.T.M) of* Barclays *Bank Ghana Limited Akim Oda Branch,* Akim Oda: s.n.

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

Sainath , M. & Tangellapally , R. S., 2010. *Implementation and Evaluation of NIST Biometric Image Software for Fingerprint Recognition,* Sweden : Blekinge Institute of Technology.

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.

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

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.

Shaikh, S. A. & Rabaiotti, J. R., 2010. Characteristic trade-offs in designing large-scale biometric-based identity management systems. *Journal of Network and Computer Applications vol. 33,* p. 342–351.

SpiderLabs, 2012. *Trustwave Holdings Inc.*. [Online] Available at: https://www.trustwave.com/Company/SpiderLabs/ [Accessed 07 January 2017].

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

Susmita, M., 2013. A Review on Secured Money Transaction with Fingerprint Technique in ATM System. *International Journal of Computer Science and Network, Volume 2, Issue 4,* pp. 8-11.

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.

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

Thai, R., 2003. *Fingerprint Image Enhancement and Minutiae Extraction, PhD Thesis Submitted to School of Computer Science and Software Engineering,* Australia: University of Western .

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