Towards A Secured Financial Transaction: A Multi-Factor Authentication Model

Lala, O.G.[a]*, Aworinde, H.O.[b] & Ekpe, S.I.[c]
[a,b] College of Computing and Communication Studies, Bowen University, Iwo, Nigeria
[c]Platohub Inc., New Castle, USA
[a]**E-mail:** segun.lala@bowen.edu.ng; [b]aworinde.halleluyah@bowen.edu.ng, [c]samuel@platohub.com
Contact Phone Number: +2348034472477

ABSTRACT

The need to secure financial transactions beyond token and knowledge-based approach is imperative, hence, the need for biometric-based authentication model which authenticates based on "who you are" in contrast to "what you have or know". This research, therefore, is aimed at presenting a multi-factor model for financial transaction with particular emphasis on ATM transactions using both Personal Identification Number (PIN) and Facial recognition biometric feature. Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) algorithms were used to match faces and extract facial features for the purpose of identification and authentication. A Multi-factor authentication model presents a fool-proof approach to securing financial transactions beyond the general PIN based transaction.

Keywords: Multi-factor Authentication, PCA, LDA, Biometrics, ATM, Financial Transactions

25th iSTEAMS Trans-Atlantic Multidisciplinary Conference Proceedings Reference Format
Lala, O.G., Aworinde, H.O. & Ekpe, S.I. (2020): Towards A Secured Financial Transaction: A Multi-Factor Authentication Model. Proceedings of the 25th iSTEAMS Trans-Atlantic Multidisciplinary Virtual Conference, Laboratoire Jean Kuntzmann, Universite Laboratoire Jean Kuntzmann, Universite Grenoble, Alpes, France June – July, 2020. Pp 139-146 www.isteams.net/France2020.

1. BACKGROUND OF RESEARCH

As technology is advancing, fraudsters device modern approach to beat the security of financial transactions. Various forms of fraud are perpetuated ranging from ATM card theft, skimming, pin theft, etc. There are problems with current technique of Automated Teller Machine Transaction (ATM) transactions, these include possible loss or misplacement of card, duplication of card, economic loss due to ATM related fraud attacks, the need to request for new cards after two or three years of usage and so on. The global ATM market accounted for US$18.44Bn in 2018 and is expected to grow at a CAGR of 10.4% over the forecast period 2019-2027, to account for US$44.18Mn by 2027. The market is experiencing rapid growth with regards to investments and technological integrations in the product and their adoptions (www.businesswire.com/news/home)

According to European ATM Security Team (EAST, 2013), there is a continuous shift away from high tech skimming attacks to lower tech card and cash trapping attacks, as well as transaction reversal fraud. Losses due to ATM related attacks rose by 13% between 2011 and 2012. Advanced persistent threats (APTs) at the ATM continue to occur around the world despite constant hardware and software updates (www.inetco.com/blog/2019/06/state-of-the-industry-atm-fraud/).

While many banks and credit unions have upgraded their ATM hardware and payments software to prevent sophisticated fraud attempts, it is still worrisome that 14 out of 21 of European countries reported ATM card skimming in 2018 (EAST Fraud Update, 2018). With the fast rate at which hackers and attackers of ATM are making headway, there is virtually no authentication technique that cannot be compromised (Mohammed, 2014; Computer Laboratory, 2012). Authentication is using one or multiple mechanisms to show that you are who you claim to be. It is a process of identifying the registered or already known user to provide some services and to protect user information from an intruder. The three majorly referred authentication process are token-based authentication, knowledge-based authentication and Biometric supported authentication (Aworinde, *et al.*, 2019; Parmar, Nainan & Thaseen, 2012; M'raihi, *et al.*,2005).

The main objective of multifactor authentication is to create a layered defense and thereby, make it difficult for an unauthorized person to access a system or service. Multifactor authentication system uses more than one authenticating factor that require a user to provide information before accessing a service. The moment the identity of the human or machine is demonstrated, it is then human, or machine is authorized to grant some services (Prasad & Aithal, 2018). Multifactor authentication is achieved by combining two or more independent credentials for validation and access. Krishnan (2018) worked on multifactor authentication model in which different methods of iris recognition were studied with their features. The work discussed fingerprint Hash code generation using Euclidean distance. Fingerprint Hash code used in the model acts as identity-key or index-key to uniquely identify individual persons. Fingerprint hash code combined with Iris image with the aid of the neural network and OTP makes authentication process robust and highly secure.

De Marsico, et al., (2014) proposed biometrics for mobile engagement, using face and iris recognition, multimodal biometrics referred as "FIRME" which is specially designed and embedded in mobile devices using the Android operating system. Both design and implementation of face and iris are considered as a separate module, whose flow of work separate and finally two modules are fused. They claim that this multimodal authentication can be effectively used to find the identity of the user. Kumar, D., & Ryu, Y. (2009) surveyed biometric payment system used for various kinds of payment systems, in contrast to username and password no need of remembering anything. They also suggest in their study that when more and more customer use the biometric system, cost of biometric reader will decrease and even small business firms also can use biometric systems (Aithal, 2015; Aithal,2016).

Aloul, et al., (2009) explains that two-factor authorization gives more security for mobile- based financial transactions other than usual username and password, by utilization biometric identification mechanism. They develop One Time Password (OTP) which is valid for the only short duration of time which is generated based on IMEI number, IMSI number, username, hour, pin, minute etc and can be effectively used for online banking, ATM or mobile banking services. Jakobsson, et al., (2009), introduced a new concept implicit authentication which is based on some actions carried out by the mobile user. They developed a model to implement implicit authentication and their preliminary investigation found that the approach is meaningful for usability or security purposes.

Hence, the need for financial institutions not to depend solely on any single control for authorizing high risk transaction but rather a multi-layered approach is imperative, which is the essence of this research.

2. RESEARCH METHODOLOGY

A review of the existing authentication model used in ATM was carried out. Verifying and matching a live image of a user, capturing and extracting the facial features with a predefined image was done using linear discriminant analysis (LDA) and Principal Component Analysis (PCA) algorithms which were implemented on Luxand Face Recognition Software Development Kit. Snapshot of live image of the ATM user and a database file to store sample images of the user was carried out as well. PCA takes large set of correlated data and transforms them into small set of uncorrelated data (also called principal components). This is one of the most popular appearance based algorithm used for dimensionality reduction in compression and recognition problems. PCA uses a global feature extraction method from high-dimensional dataset. This method can also be used to identify patterns in data, and expressing the data in such a way as to highlight their similarities and differences. This is an effective technique and have been used for dimensionality reduction.

LDA uses projection bases which separate different classes and compresses the classes as far as possible i.e. LDA deals directly with the discrimination between classes, while PCA deals with the data(template) in entirety without paying attention to the underlying class structure (Onsen and Adnan,2003). The system architecture which uses an Asynchronous Client Server (Distributed Server) Architectural Model. The System accepts the account number of the customer and captures customer's face from the client and the server running attempts to provide access to the account with the personal identification number of the customer is as shown in figure 1. If the face of the customer matches that in the account, then authentication is granted to the customer.

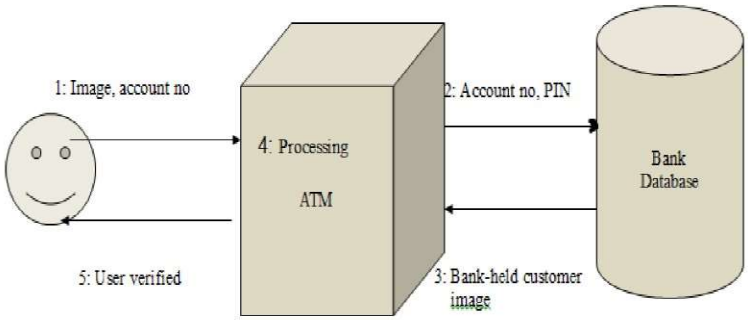

Figure 1: System Architecture showing verification process

Figure 2 presents the structure of the authentication model which contains three main stages: enrollment/identification, recognition phase and validation/authentication phase. It begins with the Enrollment stage (this only occurs in the bank) in which a user presents to the camera his/her face for identification/verification and authentication; if the user already has account, the system moves to the recognition phase where the captured face template is compared with those in the database if the user's face is recognized then the user is granted access in the authentication phase, otherwise the user is rejected. The advantage of this system is that it will grant access only to the required user whose face is presented (if the user has a bank account) and the required PIN for the account.

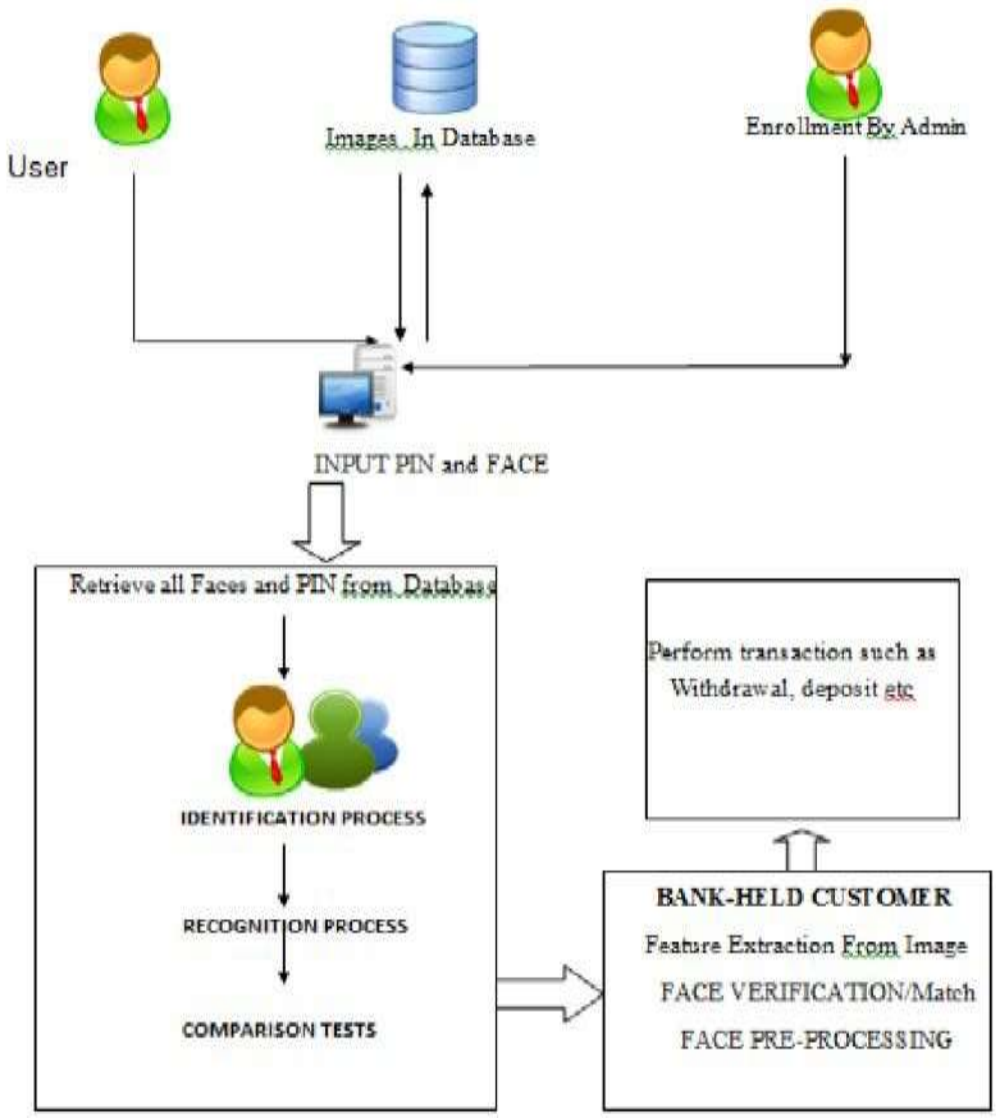

Figure 2: Structure of the authentication model

The following are the functionalities required to be performed by the system:

i. Register user (this is done by a bank staff i.e. as the Admin at the bank).
ii. Retrieve image of customer from the database. (i.e. registered user).
iii. Extraction of the facial features i.e. the Discriminant features of each image from the database which is required for identification/verification and authentication process. (using the LDA and PCA algorithm implemented in the Lux and SDK).
iv. Verify a particular image of the user.
v. Authorize the user to perform the banking transaction

3. RESULTS AND DISCUSSION

In this work different techniques have been applied like Principle Component Analysis (PCA), color based technique and Linear Discriminate Analysis (LDA) for face detection and for feature extraction. For detection, Color based technique was implemented, which depends on the detection of the human skin color with all its different variations in the image. The skin area of the image is then segmented and passed to the recognition process. For recognition, PCA technique has been implemented which a statistical approach that deals with pure mathematical matrixes used for facial feature extraction and detection. LDA is used for facial feature classification which increases the speed of the detection process.
The face recognition program was implemented using java programming language; Luxand faceSDK (software Development Kit) and Database file to store the user data and link (directory) for the associated face template of the user.

The system uses a three-step process; **enrolment, identification and authentication**. The user enrollment process occurs at the bank by the administrator and five user face template is automatically captured and stored in the database including the customer details. The next step is the identification, recognition and authentication process which occurs at the ATM terminal; the face template of users that are registered are compared with the acquired template (live recognized face) are allowed to login. The second level of authentication (which involves the use of PIN is performed) and authenticated users are granted access to perform banking transactions.

Face templates are captured automatically, the system captures five accurate templates (the system ensures that it captures user face template that best portray the perfect and clear image). This automatic process has advantage over a manually controlled capture process because the system captures the image that it considers accurate (this will speed up the identification and authentication process), rather than manually capturing the image that we feel is accurate. Figure 3 depicts an automatic enrollment of user face by capturing user face template that best portray the full image (that is, clear). The face template is captured every three (3 seconds) and five of the images are stored in data structure.

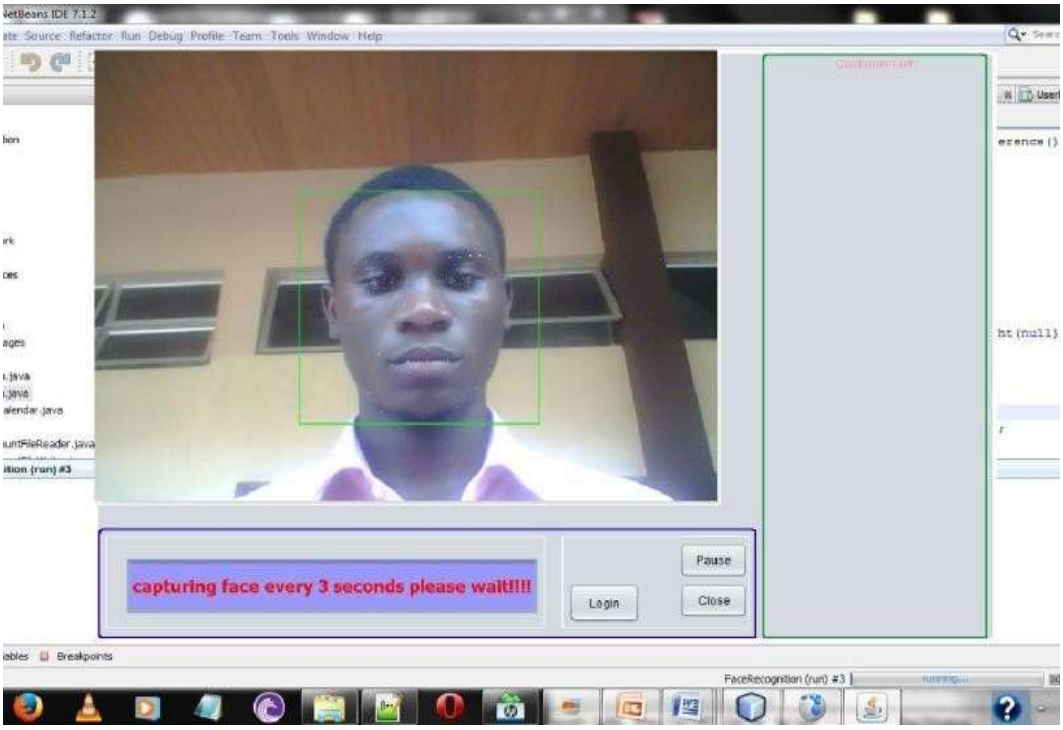

Figure 3: User Automatic Face Template Capture

4. PERFORMANCE EVALUATION

The drawback from the review of past works includes the following: Time in recognition of user, performance of the face recognition system in dark environment, possibility of identification of identical twins, and denied authentication when a face is damaged. Therefore, this section is centered around measuring the performance of the system with respect to these constraints. Time: This raise questions as to determining the time difference for recognition, verification and authentication when compared with the current/ existing system. From observation carried out on the current system, it is observed that the Automated Teller Machine takes about 2.5 seconds in average to recognize the smartcard, in contrast with this proposed system (based on the logs and intensive software test) shows that the application takes approximately 1 second for identification and authentication.

Lightning conditions: This raises question concerning the performance of the system in dark environment. As proposed, ambient, fluorescent and sunlight are required for maximum performance of this system, however, the software application was tested in a dark environment (operating with only the light of the computer system, sufficient enough to illuminate the face), the performance was fine, but the recognition rate was low. About 1 minute in contrast with the 0.99millisecond performance with fluorescent light. Therefore, as proposed earlier, there should be illumination (at least ambient or fluorescent light) at the ATM stand. Performance when face is damaged: a damaged face was simulated, with bandages but the facial features was not affected by this damage. The performance of the system was still normal; this is because the system only performs comparison using the facial features, not the nature or look of the face.

Performance with identical Twins: the system has undergone series of test on subjects with identical faces (twins) and it performed excellently well. The similarity threshold value in the application was set to 0.99999, out of 1. i.e. 99.99% due to the delicate nature of security. Taiwo's face similarity value was an average of 0.5% thus, was rejected and denied access to Kehinde's account. On the other hand, KEHINDE was authenticated and identified with similarity value of 0.9999.

5. CONCLUSION

There are several cases of theft and hacking currently associated with the use of ATM smart cards in the banking industry because, these systems authenticate users based on what they have such as PIN, smart cards, Token etc., instead of who they are. Over the years, biometric method of authentication has sounded promising and proven to be well efficient in ensuring that users are authenticated and verified based on who they really are. This therefore has led to the development of fingerprint biometric authentication model for some ATM system, however with the problems associated with this model, such as wear and tear, and possibility of easily acquiring finger templates, therefore the need to proposed a more secured multi-feature model for securing ATM using face recognition.

REFERENCES

1. BusinessWire (2019). Global ATM Market Forecast Report, 2019-2027. Retrieved from Businesswire website: www.businesswire.com/news/home 06 July 2020
2. Inetco (2019). Are ATMs still alive? Retrieved from www.inetco.com/blog/2019/06/state-of-the-industry-atm-fraud/
3. European ATM Security Team (2018.) EAST Fraud Update. Retrieved from www.association-secure-transactions.eu/east-publishes-fraud-update-2-2018
4. European ATM Security Team (2013). ATM Fraud and Hacks. Retrieved from EAST website: https://www.european-atm-security.eu 24 November 2013
5. Mohammed Tamara (2014). Security of Multifactor Authentication Model to Improve Authentication Systems. *Information and Knowledge Management 4(4).* ISSN 2224-896X
6. Computer Laboratory, University of Cambridge, UK, Information Trust Institute, University of Illinois at Urbana-Champaign, 1308 West Main St, Urbana, Illinois 61801, United States, 2012, Elsevier
7. Parmar, H., Nainan, N., & Thaseen, S. (2012). Generation of secure one-time password based on image Authentication. Journal of Computer Science and Information Technology, 7, 195-206
8. M'raihi, D., Bellare, M., Hoornaert, F., Naccache, D., & Ranen, O. (2005). Hotp: An hmac-based onetime password algorithm (No. RFC 4226).
9. Aworinde, H.O., Afolabi, A.O., Falohun, A.S.; Adedeji, O.T. (2019). Performance Evaluation of Feature Extraction Techniques in Multi-Layer Based Fingerprint Ethnicity Recognition System. *Asian Journal of Research in Computer Science 3(1), 1-9. ISSN: 2581-8280*
10. Krishna Prashad, K. & Aithal P.S. (2018). A Study on Multifactor Authentication Model Using Fingerprint Hash Code, Password and OTP. *International Journal of Advanced Trends in Engineering and Technology 3(1), 1-11.*
11. Krishna Prasad, K. (2018). Multifactor Authentication Model using Fingerprint Hash code and Iris Recognition. *International Journal of Management, Technology and Social Sciences (IJMTS), 3(2), 47-56*
12. De Marsico, M., Galdi, C., Nappi, M., & Riccio, D. (2014). FIRME: face and iris recognition for mobile engagement. Image and Vision Computing, 32(12), 1161-1172

13. Kumar, D., & Ryu, Y. (2009). A brief introduction of biometrics and fingerprint payment technology. International Journal of advanced science and Technology, 4, 25-38
14. Aithal, P. S. (2016). A Review on Advanced Security Solutions in Online Banking Models, International Journal of Scientific Research and Modern Education (IJSRME), 1(1), 421-429. DOI: http://doi.org/10.5281/zenodo.160971
15. Aithal, P. S. (2015). Biometric Authenticated Security Solution to Online Financial Transactions. International Journal of Management, IT and Engineering (IJMIE), 5(7), 455-464, DOI: http://doi.org/10.5281/zenodo.268875
16. Aloul, F. A., Zahidi, S., & El-Hajj, W. (2009). Two factor authentication using mobile phones. In AICCSA pp. 641-644
17. Jakobsson, M., Shi, E., Golle, P., & Chow, R. (2009). Implicit authentication for mobile devices. In Proceedings of the 4th USENIX conference on hot topics in security pp. 9-9. USENIX Association.
18. Önsen, T., Adnan, A., (2003), "Face Recognition Using PCA Approaches On Colored Images" Journal Of Electrical & Electronics Engineering Istanbul University 1(4).