Multi-Factor Authentication Model for Integrating Iris Recognition into an Automated Teller Machine

Akinola Kayode E.
Computer Science Department
Babcock University, Ilisan-Remo, Ogun State, Nigeria

Adekunle Y. A.
Computer Science Department
Babcock University, Ilisan-Remo, Ogun State, Nigeria

Adebayo A. O.
Computer Science Department
Babcock University, Ilisan-Remo, Ogun State, Nigeria

Okolie S. O.
Computer Science Department
Babcock University, Ilisan-Remo, Ogun State, Nigeria

ABSTRACT
The emergence of computer has greatly fuelled the advancement of Science and Technology and drastically changed the way human live. Beside these advancements is increasing sense of insecurity and apprehension. Security issues, particularly those relating to users, which include identification, authentication, authorization and accountability, have always been a challenge to banking transactions. As the number of customers in banking system increases, the banking channel becomes a target for criminals to carry out their activities. Series of security challenges in automatic teller machine (ATM) transactions are: Identity Theft, Impersonation, Skimming, Entrapping of smartcard, personal identification number (PIN) theft, Phishing, Insider attacks and physical attack. The existing ATM authentication method involves PIN and smartcard usage for customer privacy protection and fraud prevention. Hence, this research is focused on developing a model that allows Iris recognition into an automated teller machine authentication processes.

Iris authentication combine with PIN were adopted for authentication in ATM transaction in this study due to its accuracy, relatively low cost, small size, and ease of integration into different programming language. Window based application (IriSoft) was developed using NetBeans 8.0 IDE and Wamp Server 2.4 x86 to build database application package. In the iris recognition approach, to implement iris localization, segmentation and normalization VeriEye Software Development Kit (SDK) version 10.0 extended SDK which contain iris extractor and iris comparism component were utilized. The process involves a pre-enrolment of users with PIN and irises in the database. While during verification, user will stand in front of camera attached to the computer for scanning of the iris, after which the comparism of the sample iris image would be matched with the sample feature which had been stored up in database.

The model developed was tested and verification exercise was successfully carried out. The new system was found out to be more efficient when compared with the existing PIN authentication method. The verification time was very small and measured in seconds. Furthermore, the program (IriSoft) was subjected to standard indicator for checking the effectiveness, accuracy and performance of iris pattern matching. The Fake Acceptance Rate (FAR) was 0% while Fake Rejection Rate (FRR) was found to be 99.94% implying that it was not possible for any fraudster, to match the identity of another individual in the database; whereas there was a chance of 1.6% of an authentic user to be denied access which is very minimal.ATM users should be security conscious while withdrawing money to prevent forced withdrawal. Banks should also ensure end-to-end encryption is in place to protect data as it travels from users through internet to bank servers. Government should be involved in awareness campaign. Having realized the importance of iris recognition authentication in ATM, a holistic approach is recommended that individual users, bank and government play their role; bearing in mind that no security systems can be wholly full proof.

Keywords
Automatic Teller Machine (ATM), Fake Acceptance Rate (FAR), Fake Rejection Rate (FRR), Iris Recognition, Multi-Factor Authentication (MFA).

1. INTRODUCTION
Technology has become a major enhancement tool in driving banking processes and activities. Due to advancement in technology, banks are fast moving away from traditional banking to automate their processes through other channel activities thereby decongesting the banking hall. Other channels in use include cards on ATM, Point of Sale (PoS) and Mobile Banking. The massive implementation and deployment of the Internet banking system has been followed by increased vulnerability of attack. Furthermore, issues related to security is one of the biggest challenges that the banking industry faces, banking online has contributed to this risk in multiple ways. The process involving online banking is such that it potentially keeps the isolated systems (for example ATM) vulnerable to an environment which is open as well as risky. There have been cases of users asking unknown person(s) to assist in withdrawing money from ATM machine, which most of the time often lead to attacks resulting in heavy fund transfer or withdrawer from customer's account. Biometric authentication releases the users from the difficulties of remembering and protecting passwords as required by traditional authentication systems. Among all the biometrics in use today, eye biometrics (iris and retina) offers the highest level of uniqueness, universality, permanence, and accuracy. Despite these convincing properties of iris and retina biometrics, they have not been in widespread use.

2. STATEMENT OF PROBLEM

ATMs have brought so much relief to the financial world. Various problems were solved with the advent of these machines ranging from keeping the banking hall free of traffic with its attendant issues. However, as man begins to realize the gains of technology brought about by this machine to supplement human tellers, little did one know that the joy shall be short lived by the various sharp practices leading to financial losses. The existing Identification and Authentication (I & A) method of using one time password, card-based authorization codes, transaction password and digital certificate that are commonly used as security measure are not reliable due to probable compromise. These security implications underscore the need for a robust identity management structure to authenticate and ensure secure banking transactions. The focus of this study is to propose a model for a multi-factor authentication mode of operation in banking sector (particularly in the use of ATM) to reinforce the use of personal identification number (PIN) and card that are commonly used as security measure in most Automatic Teller Machine (ATM) transactions.

3. LITERATURE REVIEW

3.1 Automatic Teller Machine (Atm)

The ATM is a modern service delivery method in banking sector, that offers wide range of financial services like cash withdrawal, funds transfer and so on. Michael (2016) reported that installed base of ATM machines is increasing with an estimated 3.2 million units installed in 2014 up by 12.4% compound annual growth rate (CAGR) from the 2.0 million units in operation in 2010. The numbers are projected to grow to over 3.5 million by 2020. ATM is known by diverse names such as: automatic banking machine (ABM), Automated Transaction Machine (ATS), Cashpoint, Money Machine (MM), Bank Machine, Cash Machine, Hole-In-The-Wall, Autoteller, Cashline Machine, Bankomat, Multibanco (after a registered trade mark, in Portugal), Minibank in Norway, Geld Automaat in Belgium and the Netherlands, and All Time Money in India (Jegede, 2014).

Table 2.1: Summary of Past Related Studies on Different Authentication Models

AUTHORS	OBJECTIVE	METHOD EMPLOYED	GAP(S)
Jimoh and Babatunde (2014).	Developed an algorithm for enhancing ATM authentication system using Short Message Service (SMS) verification.	1. Heuristic evaluation with the aid of a questionnaire with the use of validated software for usability metrics. 2.Conducted a usability testing of the proposed system	1. Network failure or fluctuation can truncate the transaction process. 2. The developed algorithm only considered a minimum withdrawal amount.
Supakit and Boonkrong (2015)	Design a two factor authentication by combining user name, password and drawing of an image by the user	Interface was designed to accommodate user name, password and drawing of an image attached to user for authentication.	1. The developed system was two seconds longer than the existing system. 2. User login failure was experienced.
Muhammad et al., (2015)	Developed second level authentication comprising ATM and short message service	Simulation method with the use of Java programming language with MySQL was employed	1. Damage or loss of SIM would lead to a compromise
Frimpong, Kofi and Michael (2016)	Implemented multi factor authentication method using finger print scanner.	Microsoft visual studio 2010 (C#) was used to develop the front end while Microsoft structured query language server 2008 was used to design the back end and finger print scanner a Grfinger software development kit (SDK) was employed in the implementation .	The system has an overall efficiency of 94%, FAR 4%, FRR 2% and TER 6%.
Ankit and Neelu (2017)	Proposed multi factor fraud reduction in ATM using voice recognition and encrypted PIN.	The system consists of training the database of an authorized person. The real voice input through the use of microphone will then be compared. The comparing process is carried out by feature extraction and feature matching with that of the stored samples of authorized person in the database.	The draw back in this proposed system was that; the system was not built as an enhancement of the existing system.
Jayakumar et al., (2017)	Proposed multi factor authentication model using smartcard, short message service, iris and finger print of the customer.	The smartcard would be inserted into the ATM, then the machine would request for the PIN, scan the iris and recognize finger print before allowing the legitimate owner of account to withdraw money. If somebody tries to break the ATM an alert message is sent to the nearest police station and the ATM shutter is automatically closed.	The draw back in this proposed system was that; the system was not built as an enhancement of the existing system.

4. RESEARCH METHOD

To implement Iris recognition, virtual –server arrangement was adopted, the virtual server which serves as bank database was hoisted in the cloud and this is because bank may not accept the use of their platform for this research due to risk involved. In the iris recognition approach, to implement iris localization, segmentation and normalisation VeriEye Software Development Kit (SDK) version 10.0 extended SDK which contain iris extractor which extracts a single iris template in 1.2 seconds and iris matcher component which matches 40,000 irises per second was used. VeriEye Software Development Kit (SDK) version 10.0 extended SDK incorporate MySQL server for the database, Java Development Kit (JDK) 8 as the programming language. The second method used in implementing iris recognition in this research involved the building of application called IriSoft using Java programming language. The study implementation requires PIN, smartcard and iris recognition. The existing control over ATM banking requires only PIN and smartcard to authenticate transaction; but, iris recognition was adopted in this research due to its high level of accuracy and reliability. In the proposed system, customer will stand in front of camera attached to the ATM for scanning of the iris, then matching of extracted feature (image) with the sample feature already stored in database was carried out. An application called IriSoft to receive the biometric input which would be routed to the Authentication Server was developed using Java programming language. This was due to language's ability to provide managed code execution that runs under the Common Language Runtime (CLR), resulting in robust, stable and secure applications. In real life scenario, a computer device with internet facilities and front camera of a high resolution will be used to receive input from user and matched against already stored biometric details attached to the customer's smartcard and account number.

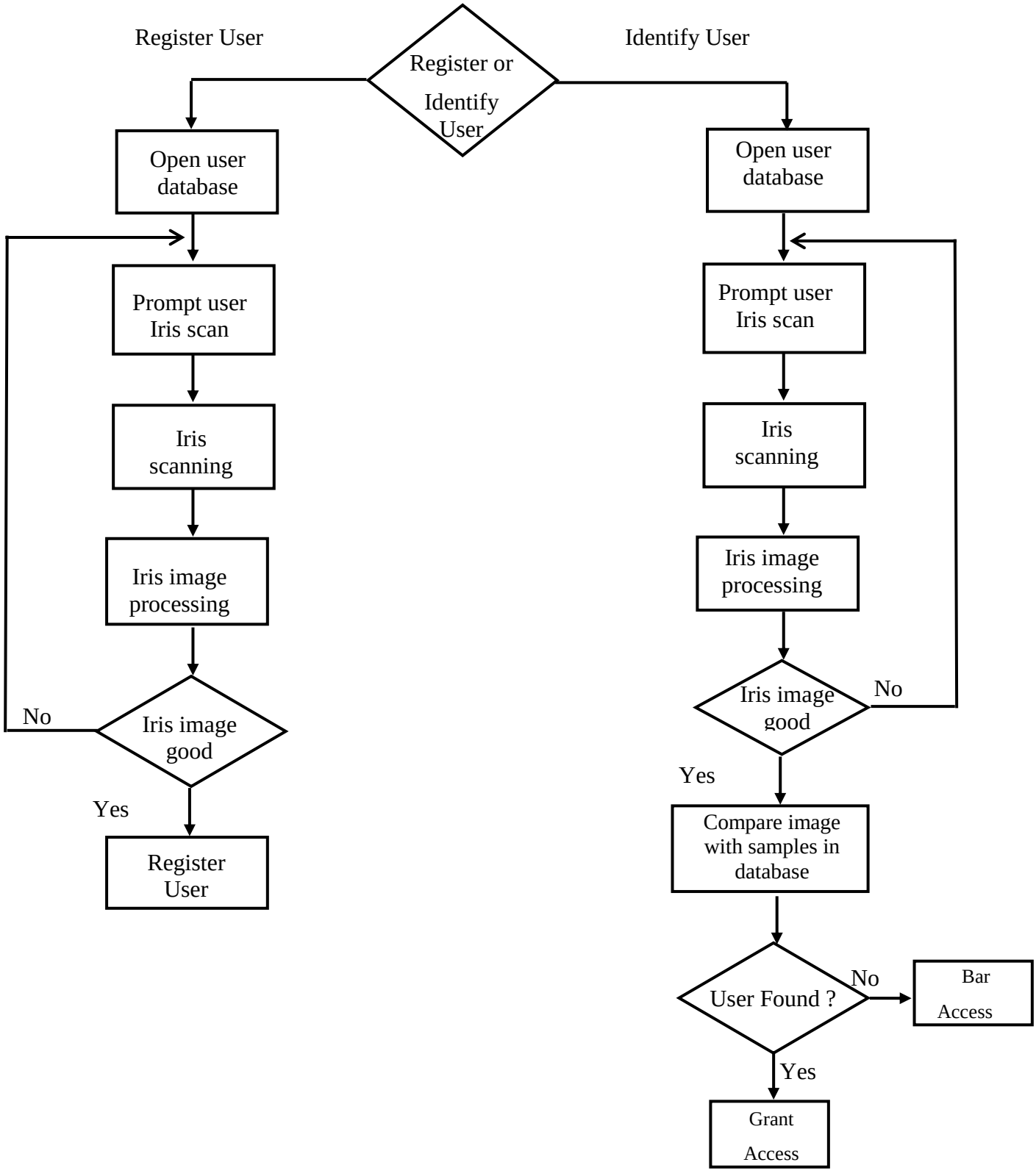

Figure 3.1: IriSoft ATM Enrolment and Authentication Model (Flowchart)

(Source: Researcher)

5. DATA PRESENTATION AND RESULTS

The **False Reject Rate (FRR)** measures the probability that an individual who has enrolled into the system is not identified by the system. It is also known as Type-I error

FRR can be calculated as:

FRR(n)

$$\frac{Number\ of\ rejected\ verification\ attempts\ for\ a\ qualified\ individual\ n}{Total\ number\ of\ verification\ attempts\ for\ that\ qualified\ individual\ n}$$

And Where N is the total number of enrolments.

The **False Acceptance Rate (FAR)** measures the probability that an individual who may have or have not enrolled into the system is identified as another individual. It is also known as a Type-II error.

FAR can be calculated as:

And

$$FAR(n) = \frac{Number\ of\ successful\ \ imposter\ attempts\ for\ a\ qualified\ individual\ n}{Total\ number\ of\ imposter\ attempts\ for\ that\ qualified\ individual\ n}$$

Where N is the total number of enrolments.

Table 4.1. Tabulated result from the new system

Recognition Method	Number of qualified individuals	Number of attempts	Number of acceptance	Number of rejection
GP + GI	1000	60	59	1
FP + GI	1000	60	0	60
GP + FI	1000	60	0	60
FP + FI	1000	60	0	60

GP means Genuine PIN, that is valid PIN

GI means Genuine Iris, that is valid Iris in the database

FP means Fake PIN, this is invalid PIN

FI means Fake Iris, this is Iris not present in the database

TRR means True Rejection Rate, that is, the percentage of valid or invalid users rejected by the system (IriSoft). The formula is (100-FRR).

Table 4.2. Tabulated result from FRR, FAR and TRR of the new system

Recognition Method	FRR %	FAR %	TRR % (100-FRR)
FP + GI	0.06	0.00	99.94
GP + FI	0.06	0.00	99.94
FP + FI	0.06	0.00	99.94

Table 4.2 shows Iris and PIN recognition rate in the new system (IriSoft), the result shows that FAR was 0% while FRR was found to be 99.94% for FP + GI, GP + FI and FP + FI respectively, implying that it was impossible for the fraudulent or fake individual to gain access into the system whereas from table 4.1 there was a chance of 1.6% of an authentic user to be denied access which is very minimal.

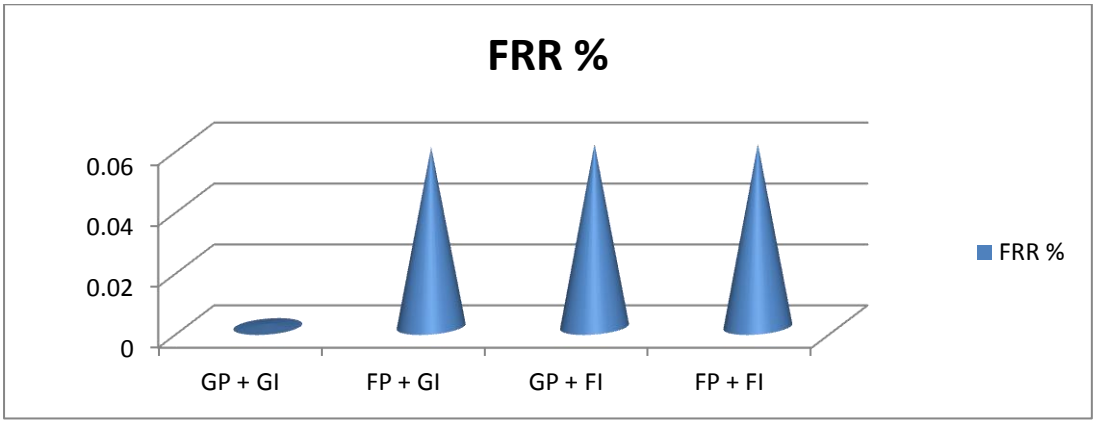

Figure 4.1 Comparison of FRR for Iris recognition system

From figure 4.6, it was observed that the FRR was 0.06% for FP + GI, GP + FI and FP + FI respectively which were the highest when compared to GP + GI is 0.059%. It shows that rejection rate for fake individual was high compared to rejection rate for genuine individuals.

6. SUCCESSFUL IRIS AND PIN VERIFICATION WINDOW

In the simulation approach, during the verification process, the individual supply PIN and the system ask the user to face the camera for iris capturing, when both PIN and iris is captured, then "verify button" is pressed to verify the user as is shown in figure 4.3 and 4.4. The verification or authentication process takes the supplied input and compares it with the PIN and Iris image stored in the database, when both supplied data is correct, the IriSoft pop up the similar image stored in the database and flagged valid on the window.

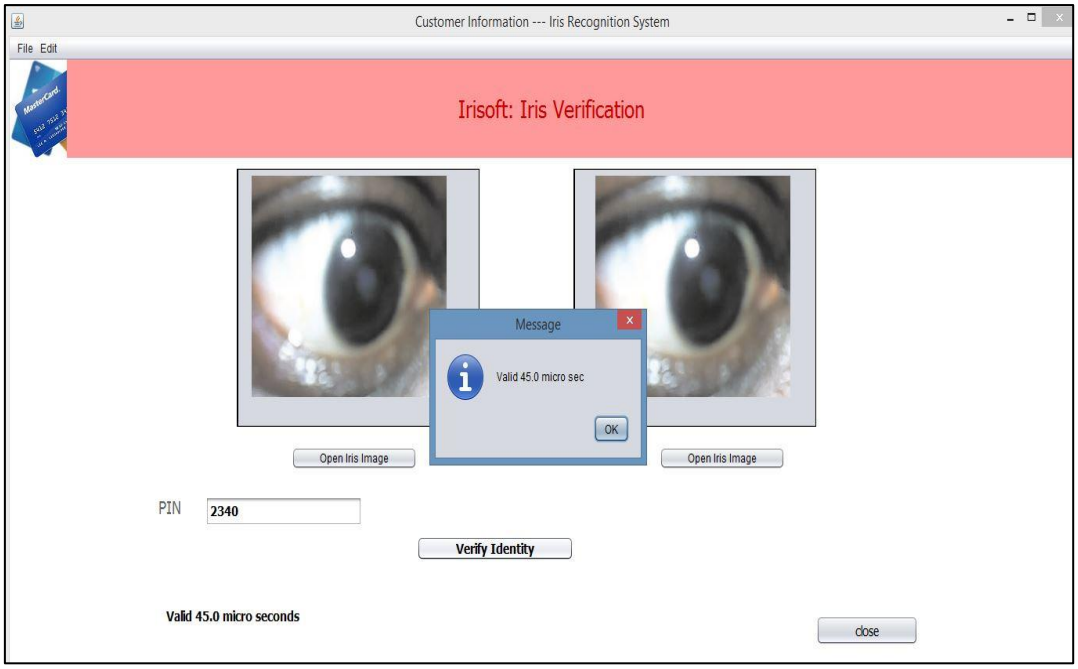

Figure 4.3 showing user with Valid Iris and PIN during authentication

Verification time is 45.0 micro seconds

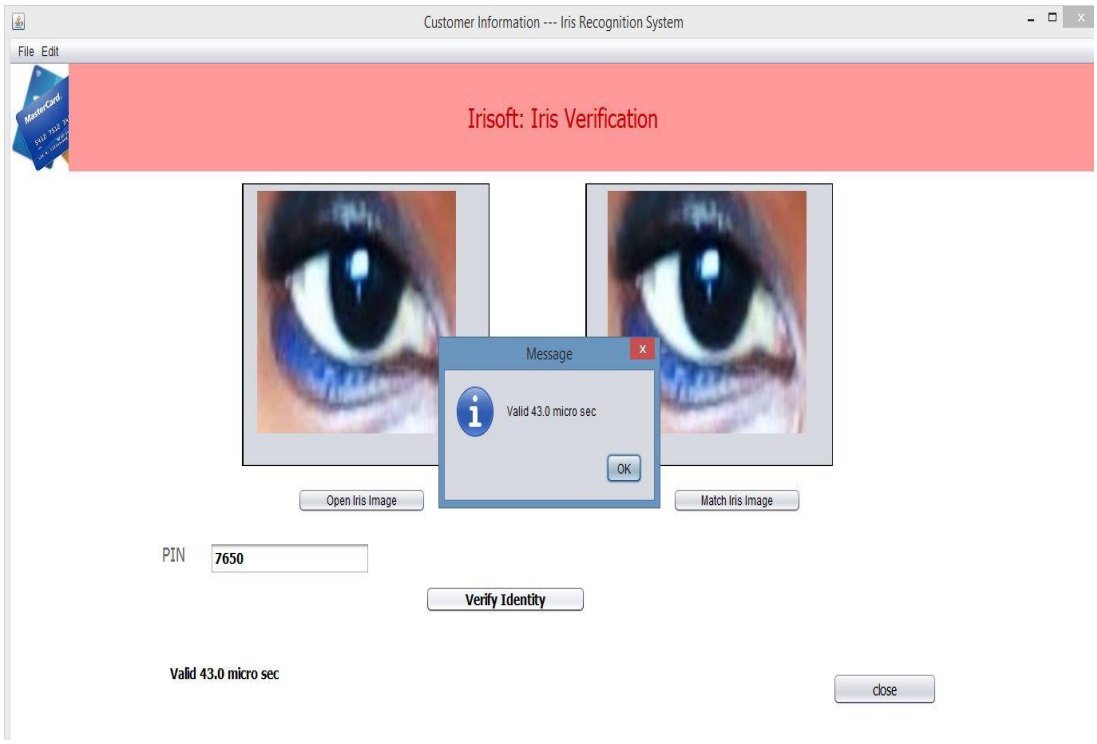

Figure 4.4 showing user with Valid Iris and PIN during authentication.

Verification time is 43.0 micro seconds

7. FAILED AUTHENTICATION WINDOW

During the verification process, the individual supply PIN and the system ask the user to face the camera for iris capturing, when both PIN and iris is captured, then "verify button" is pressed to verify the user. The verification or authentication process takes the supplied input and compares it with the PIN and Iris image stored in the database, when either of the PIN or Iris supplied data is incorrect, the "match image" button on the right is empty and the program flagged invalid on the window interface (figure 4.5 and 4.6). In the real life, the ATM will just display invalid user. An unsuccessful attempt can be tracked by the internal control mechanism in the bank to analysed and get useful information about the intruder.

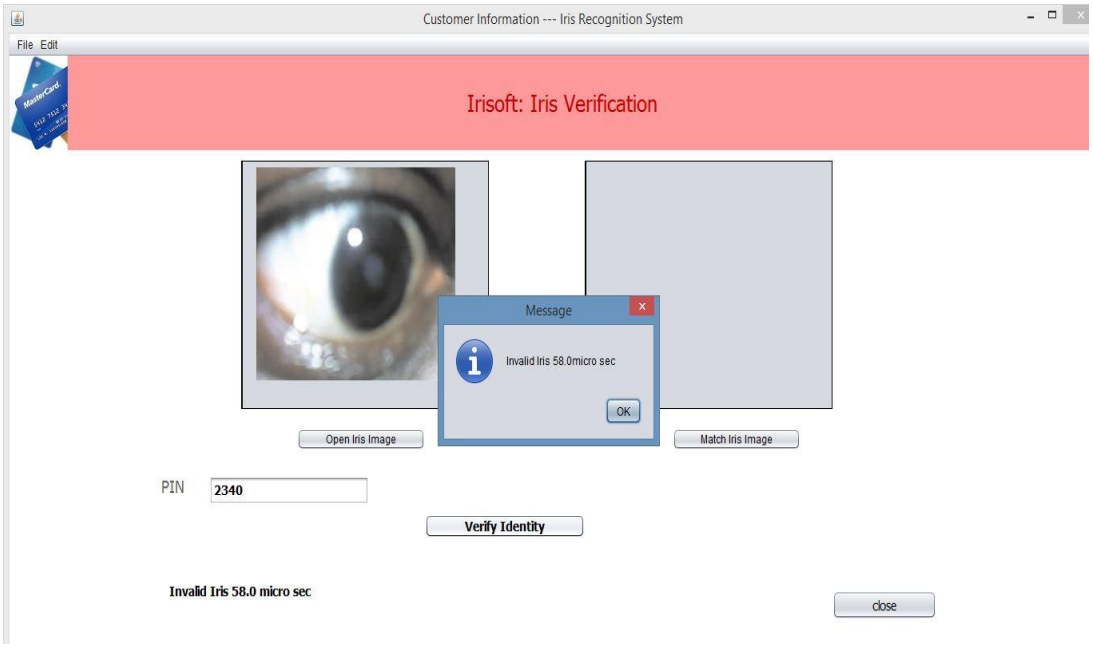

Figure 4.5 showing user with an invalid Iris, PIN or both during authentication

Verification time is 58.0 micro seconds

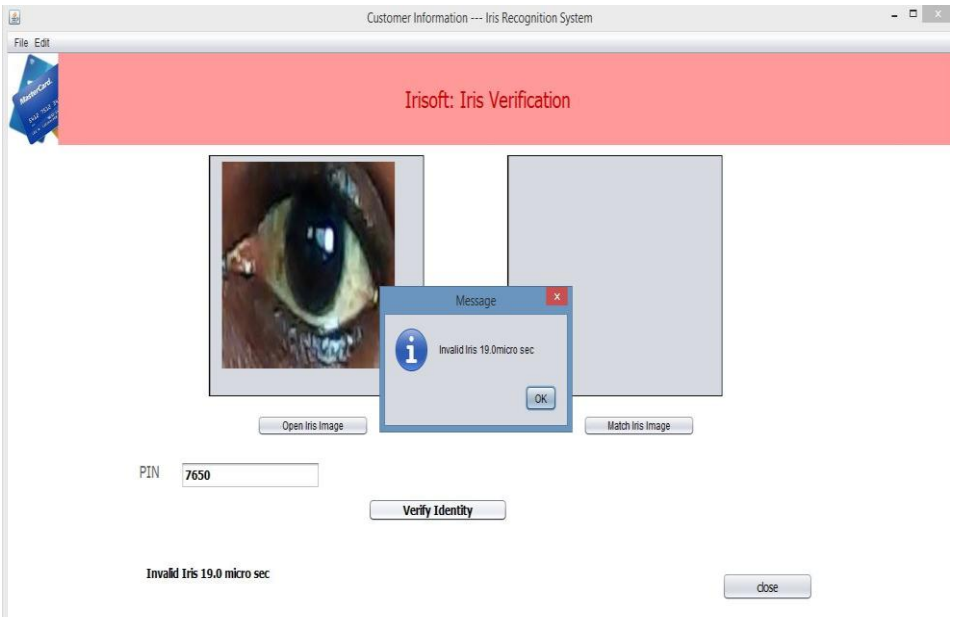

Figure 4.6 showing user with an invalid Iris, PIN or both during authentication

Verification time is 19.0 micro seconds

8. CONCLUSION

This study addressed the authentication issue in ATM transaction with the use of PIN, smartcard and iris recognition. The research has been able to demonstrate the effectiveness of PIN and iris recognition model in real life environment. The results from this model further affirm that biometric features like iris and retina are unique and have accuracy and difficult to break by fraudster when used for authentication. Since every iris is unique, irises of the same person are not similar (that is, iris from left and right eye of the same person is not identical) make the use of biometric a secure authentication technique. Evaluation and testing of the developed model was done. Furthermore, the program (IriSoft) was subjected to standard indicator for checking the effectiveness, accuracy and performance of iris pattern matching. The Fake Acceptance Rate (FAR) was 0% while Fake Rejection Rate (FRR) was found to be 99.94% implying that it was not possible for any fraudster, to match the identity of another individual in the database; whereas there was a chance of 1.6% of an authentic user to be denied access which is very minimal.

9. REFERENCES

[1] Ankit, S. and Neelu, J. (2017). Fraud Reduction in ATM Machines using Voice Recognition- A Review. International Journal of Innovative Research in Science, Engineering and Technology(ijirset), *6*(5), 7525-7530.

[2] Awodele, O. and Akanni, A. (2012). Combatingautomated teller machine frauds through biometrics. *International Journal of Emerging Technology and Advanced Engineering*, *2*(11), 441 -444.

[3] Frimpong, T., Kofi, N., and Michael, A. (2016).Improving Security Levels In Automatic Teller Machines(ATM) Using Multifactor Authentication. *International Journal of Science and Engineering Applications. 5*(3), 126-134.

[4] Jayakumar, S., Alamelu, Radhika , Ramya , Dharani and Senthil J., (2017). Enhanced way of Securing Automated Teller Machine to track the mis-users using secure monitor tracking analysis. IOP Conf. Ser.: Mater. Sci. Eng. 263 042032. doi:10.1088/1757-899X/263/4/042032

[5] Jegede,C.A.(2014).Effects of Automated TellerMachineon the Performance of Nigerian Banks. *American Journal of Applied Mathematics and Statistics*, *2*(1), 40–46. https://doi.org/10.12691/ajams-2-1-7

[6] Jimoh, R.G. and Babatunde, A. N. (2014). Enhanced Automated Teller Machine using Short Message Service authentication verification. World Academy of Science, Engineering and Technology. *International Journal of Computer, Information Science and Engineering*. *8*(1). 14-17.

[7] Michael, L.(2016). ATM Benchmarking StudyandIndustryReport.http://www.accenture.com/_acnmedia/pdf_10/accenture-banking-ATM-benchmarking, Retrieved April 16, 2018.

[8] Muhammad,B.L.,Alhassan M.E. and Ganiyu, S.O. \(2015).An Enhanced ATM Security System using Second-Level Authentication. International Journal of Computer Applications. 111(5). 8-15.

[9] Oko,S.and Oruh, J.(2012): Enhanced ATM securitysystem using biometrics. IJCSI. *International Journal of Computer Science Issues.* 9(5). 352-357.

[10] Supakit,M.and Sirapat, B.(2015). Improving Securitywith Two-factor Authentication Using Image. KMUTNB Int J Appl Sci Technol. 8(1), 33-43