European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 7, Issue 4, 2020

Smart ATM Security Using Face Recognition

Darwin Nesakumar A[1]*, T Suresh[2], Nivedha T[3], K Nivedha S[4], Priyadharshini G[5], P Mugilan[6]

R.M.K. Engineering College, Department of ECE12345, Senior System Engineer, Tractors and Farm Equipment Ltd6

*(*Corresponding author's e-mail: darwin114@gmail.com)*

ABSTRACT: In this modern world, every people use ATM machines for withdrawal and transferring cash. This research is based on implementing recognizing Fingerprint mechanism in the ATM System. We selected this in order to increase the security of the customers to make easy transaction. Each human being has different fingerprint minutiae characteristics hence this process will be more applicable. There is no fear of losing the ATM card and no requirement to carry ATM card always. By comparing various technologies that are used so far in ATM security, it is observed that fingerprint recognition technology performs better and safer than other technologies. This is making easy and protected transaction and also maintaining user-friendly environment with the user.

This process is one of the most promising technologies at electronic money transaction. The growth in the field of electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. People greatly depend on the Automated Teller Machine (ATM) for conveniently meeting their banking needs. However, there are numerous advantages in this system, the ATM fraud has recently become more threatening issue. This system helps in preventing the ATM robberies and misused by wrong person. We proposed the system to prevent the actions of breaking or damaging the machines, threating the ATM user's denial of transactions and any other ATM user by invalid users or mask.

Keywords- ATM, Bio-metric, Fingerprint, PIN.

1. INTRODUCTION

Nowadays, banking sector is one of the most important parts of human's daily life. Banking facilities are widely used by people for their economy's activities. Automated Teller Machine is an electronic system which is used for accessing a bank account from anywhere without the help of bank staff. The user can perform several banking activities like accessing their bank deposits for making all kind of financial transactions mostly cash withdrawal, money transfer with the help of ATM. It is observed that the number of crimes related to ATM is increased hence there is a necessity to provide enhances security to ATM machine.

Previous technologies provide security to transactions for identification of authorized user. But there is limited for secure transactions with ATM machine. Previous works focused on biometric technique to provide enhanced security to ATM transaction whereas GSM based technique is also implemented for the same purpose. Whereas, some system uses both techniques. Currently, ATM security is given to the transactions only.

In this regard our proposed model is GSM based security is provided in which One Time Password (WEBPAGE REQUEST) is send to registered number for transaction. Only when card holder allows the person has the ability to access. To find the illegimate/fraud customer the image will be sent to the owner's registered mail id. Thus, the chances of abduction will be reduced and security will be increased.

2. RELATED WORKS

In the paper [3] S.P. Balwir proposed a model of designing an embedded system for augmentation of the ATM security. Serial communication is managed by the system to scan cardholder's database, which then spontaneously generates message to the mobile of authorized user's through 89C51 microcontroller connected GSM module. The main theme of the paper proposed by Bharati Nelligani [4] is used to make practical and effective usage of embedded system and advanced technologies to designs to realize the appearance of the card owner and fingerprint to identify and verify legal customer. Through GSM it is to send SMS between two addresses and GPS helps to identify the place where box is stolen. In paper [5] T. Guru Sarath developed an ATM security system to monitor all ATM's in the city with a centralized private server. Many types of sensors and switches are used hereto capture security related information which is then analysed and dispatched to the central main server to experiment. Utilizing the data obtained from different ATMs, a statistical vulnerability test is made out through the system and a vulnerability quotient is assigned to all ATM machines. Whereas this method is little complicated and continue monitoring is needed. The proposed system [6] focuses on saving time and solving sensitivity issue of the system. If the user wants to know their balance there is no need to go through the verification system. This model claims that fraudsters will never gain any positivity of the system. Hence, the security will never be compromised. In paper [7] to increase the safety of electronic money transfer via EDC an embedded fingerprint technique with PIN has been introduced. It's a design to secure swipe card transaction by applying bio-metric feature like fingerprint identification with traditional PIN. There are many proposals to raise the safety of the transaction using bio-metric recognition system [8]. In this given model pin number is completely replaced with bio-metric system such as e-fingerprint, retina and so on. Thus, this serves as an entirely different model from others. The computer operated machine which allows withdrawing the cash from their respective bank account is called as Automated Teller Machine (ATM). During the transaction of money, the card owner has to provide required information for effective transaction which is supported through keypad and card reader. Through the magnetic stripe of the credit or debit card the card reader collects the account related data of the card owner when the person presses the keypad.

Besides, the card owner has their PIN (personal identification number) which is converted into the encrypted form and delivered to the host processor which is responsible for routing the request to the concerned bank. From customer's checking account an electronic fund transfer (EFT) process is taken place to host processor's account based upon cash request. Whenever the host's bank account receives the transferred fund it sends the ATM an approval code to dispense the amount and simultaneously cash is also transferred to the merchant's bank account. During swiping the card information is sent to the merchant's payment system. Each and every data is sent to the payment processor for processing and the data which is processed is further sent to the payment brand and finally it is forwarded to the issuing bank. After verification process an authorized number is generated and routed to the concerned brand to perform payment. As a final process the authorization number is routed to the merchant's payment system from the processor. This is the overall process carried out and after this process the card holder collects his/her receipt. But this has the disadvantage that anyone can enter the ATM centre by using any others card and may withdrawal money if they know the PIN of the card.

3. PROPOSED METHODOLOGY

In this proposed system, the valid card holder is allowed and only by the knowledge of account holder others can enter into the ATM by using account holder's ATM card. Once the customer inserts the card inside the ATM machine the card reader collects the information stored in the magnetic strip of the card and then passes into the host for comparing the fingerprint and image of the person which is already updated in form of data. This can be performed with the help of USB camera and finger print module. If everything is matched then ATM machine will allow for transaction. Incase if any unauthorized person inserts ATM card, finger print and image will be verified since it won't match so their image along with an OTP will be sent to account holders mail, only after entering that OTP in this system it will allow the user to withdrawal the money or else it will stop the process. The entire control is provided by using Raspberry pi controller. Now let us discuss about the processing carried out in this security system.

The entire process of our proposed model is explained as a flow chart which gives a clear view of the system. The flow chart of the proposed method is shown in figure1.

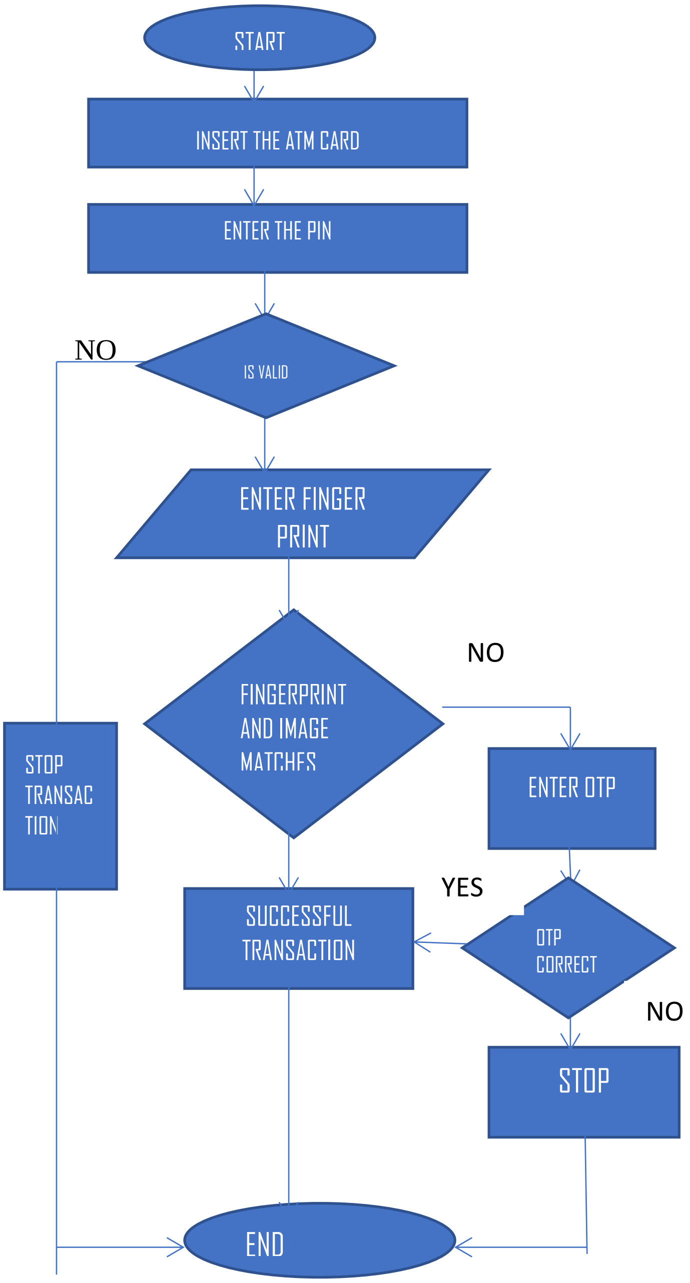

Figure.1 Flow chart of the proposed method

Finger print technology is the mostly widely used technology in biometrics. It provides high recognition accuracy and it also employs small size acquisition devices which made it more promising to use. This process doesn’t require any complex user system interaction. The Bio Secure Benchmarking Framework for Fingerprints, uses the NIST Fingerprint Image Software (NFIS2), the publicly available MCYT-100 database, and two evaluation protocols. Many research systems follow this proposed framework. The evaluated system performs different approaches for fingerprint processing. Fusion experiments involve different combinations of the presented systems. Here we use NFIS2 software. TheNFIS2 software is used to obtain the fingerprint scores for the multimodal experiments in the field of Bio Secure Multimodal evaluation. Overall process of the proposed method is shown in figure2.

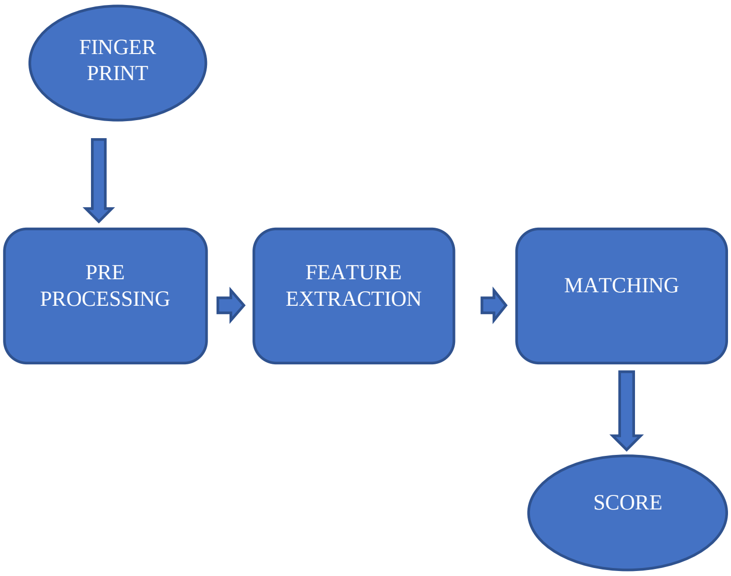

Figure 2. Process of proposed method

Once the fingerprint has been pre-processed, a feature extraction is the next step to be performed. Minutiae matching system is mostly used for fingerprint recognition, so that reliable minutiae extraction is needed. Usually, the pre-processed image of the fingerprint is converted into a binary image, which is then thinned using morphology. The thinning step decreases the ridge thickness to one pixel, allowing straight forward minutiae detection. During that thinning step, many spurious imperfections may appear and thus, a post processing step is sometimes performed to remove the imperfections from the thinned image. Several approaches have been proposed for binarization, thinning and minutiae detection. However; binarization and thinning suffer from several problems such as: a) Spurious imperfections b) Structural information loss, c) Computational cost and) Absent of robustness in the low-quality fingerprint images.

One of the major issues in fingerprint verification is the robustness lack in image quality degradation. Finger print image quality heavily affects the working of a fingerprint recognition system. The fingerprint image quality is determined through several factors such as skin conditions (e.g., dryness, wetness, dirtiness, temporary or permanent wounds and bruises), sensor conditions (e.g., dirtiness, noise, size), user cooperation, etc. Many of these factors cannot be avoided and some may vary over time. Low quality images will result in spurious and missed features, thus degrading the overall performance of the system. Hence, it is very important in fingerprint recognition to estimate the quality and validity. Incorporating automatic quality measures in fingerprint verification have been concentrated in recent times. A successful approach to enhance the fingerprint verification system performance is to combine the results of different recognition algorithms. Many simple fusion rules and complexly trained fusion rules have been proposed. Examples for combining minutia- and texture-based approaches are to be found. Also, a comprehensive study of the combination of variously obtained fingerprint recognition systems is done. That simple fusion approaches are always not outperformed by more complex fusion approaches, calling for further studies of the subject. Another recent issue in fingerprint recognition is the utilise of multiple sensors, either for sensor fusion or for sensor interoperability. Fusion of sensors provides some important potentialities a) The overall performance of the system can be improved substantially, b) Population coverage can be advanced by reducing enrolment and verification failures, c) This may naturally resist spoofing attempts against biometric systems. Regarding sensor interoperability, most of the biometric systems are designed in such a way that the data to be compared is obtained separately for every sensor, thus being restricted in their ability to match or compare biometric data originating from different sensors in practice. Thus, changing the sensor may affect the performance of the system. Recent improvement has been made in the format of common data exchange to facilitate the exchange of feature sets between vendors. Here we are using raspberry pi as controller so we need a software and suitable operating system for carrying this process. Linux is a UNIX compatible operating system where the operating system's kernel has been reprogrammed. Because of this compatibility issue most of the free applications programmed for UNIX are always available for Linux When comparing Linux and Windows as operating systems, the major differences are that Linux is an open-source project and Windows is a closed-source project. In the closed-source project the users can able to know only the finished product but don't have knowledge of how it is done. In open-source projects everything is made fully open to the public. In practice this can be used in Linux's easy customization for different platforms. Such process is called porting. There are several distributions ported to the Rasp-berry Pi's BCM2835 chip. One of the important distributions is called Raspbian Wheezy. Raspbian Wheezy is completely a free operating system which is based on Debian distribution. It is created by a small team of developers who had craze over Raspberry Pi. Raspbian is optimized system for the Raspberry Pi's hardware and it comes with over 35 000 packages and pre-compiled software. Raspbian is still under active development and it works in order to improve the stability and performance of the Debian packages. Raspbian is officially recommended for beginners as it is simple to work with and it includes a graphical desktop environment called LXDE. Python is a flexible and powerful programming language and also it is simple to learn and follow. The clear syntax of Python makes it a adorable tool for users who wants to learn programming. This is one of the reasons why it is recommended by the Raspberry Pi Foundation. Python is published under an open-source license and it is available for different operating systems. Python runs on Linux, OS X and Windows computer system. Future technologies will be fully based on python as it has more scope and it is also one of the simplest languages. Python language is mostly recommended by the Raspberry pi association for accessibility thus it is widely preferred than others.

4. VI.RESULT AND CONCLUSION

Nowadays, the ATM robberies are common. In this proposal, a real-time monitoring system for ATM security based on accelerometer sensor, camera module, and fingerprint module is proposed. The proposed work concludes with the following points. Itis a secure way of accessing an ATM by authorized persons using face recognition module. Eliminates the drawback of previous system like manual controlling camera modules and doors the system is cost effective as compare to existing manual technique. The live video of the ATM centre can be monitored through web server which make ATM better safe from thefts. This is completely accessed through card holder and it is one of the major advantages of this proposed system. However, this system has some disadvantages which can't be a major risk but it has to be considered. Fingerprint won't work when it is wet or wounded. Sometimes finger print module may won't work properly. Such kinds of issues are there but in general this system offers better security than before proposed systems. This process can be improved in the future by using upcoming technologies like Nano technology. In future more development may occur and thus the security can be improved further.

5. REFERENCES

1. Onyesolu MO, and Ezeani IM, "ATM Security Using Fingerprint Bio-metric Identifier: An Investigative Study," International Journal of Advanced Computer Science and Applications, 2012, Vol. 3, no.4, pp. 68– 72.

2. Daniel Peralta, Mikel Galar, Isaac Triguero, Oscar Miguel-Hurtado, Jose M. Benitez, and Francisco Herrera, “Minutiae filtering to improve both efficacy and efficiency of fingerprint matching algorithms,” Engineering Applications of Artificial Intelligence, June 2014, Volume 32, Pages 37-53.
3. S.P. Balwir, K.R. Katole, R.D. Thakare, N.S. Panchbudhe, and P.K. Balwir, "Secured ATM Transaction System Using Micro-Controller", International Journal of Advanced Research in Computer Science and Software Engineering, April 2014, vol. 4, no. 4, pp. 1358-1362.
4. Bharati M Nelligani, Dr. N V Uma Reddy, and Mr.NithinAwasti, “Smart ATM Security System Using FPR, GSM, GPS”, International Conference on Inventive Computation Technologies (ICICT), 26-27 Aug. 2016.
5. T. Guru Sarath, “Centralized Server Based ATM Security System with Statistical Vulnerability Prediction Capability,” IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), 2017, pp.61-66.
6. Sweta Singh, Akhilesh Singh, and Rakesh Kumar, “A Constraint based Biometric Scheme on ATM and Swiping Machine,” International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 2016
7. Akhilesh Singh, Sweta Singh, and Rakesh Kumar,” Secure Swipe Machine with Help of Biometric Security,” International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016, pp.1056-1061.
8. G. Renee Jebaline, and S. Gomathi, “A Novel Method to Enhance the Security of ATM using Biometrics,” International Conference on
Circuit, Power and Computing Technologies [ICCPCT], 2015.
9. K. Vengatesan, Rohit Ravindra Nikam, S. Yuvaraj,Ankoshe Malakappa Shankar, Punjabi Shivkumar Tanesh and Abhishek Kumar"A Random Forest-based Classification Method for Prediction of Car Price",International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 03, 2020.
10. Dr. Mohammed Aref, Dr. Sameen Ahmed Khan,Dr. Sayyad Samee, K. Vengatesan and Abhishek Kumar," Early Detection of Outbreaks by Monitoring the Over-the-Counter Pharmacy Sales" International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 04, 2020.
11. V.D. Ambeth Kumar, ∗, S. Malathia, R. Venkatesan, K. Ramalakshmi, K. Vengatesan, Weiping Ding and Abhishek Kumar,"Exploration of an innovative geometric parameter based on performance enhancement for foot print recognition",Journal of Intelligent & Fuzzy Systems. Scopus (
12. Saravana Kumar, E., Vengatesan, K. Trust based resource selection with optimization technique. Cluster Comput 22, 207–213 (2019)
13. Prabu, S., V. Balamurugan, and K. Vengatesan. "Design of cognitive image filters for suppression of noise level in medical images." Measurement 141 (2019): 296-301.
14. Jignesh J. Patoliya, and Miral M. Desai, “Face detection-based ATM
Security system using embedded Linux platform”, 2nd International Conference for Convergence in Technology (I2CT), 2017, pp 74-78
15. I.F. Akyildiz, and K.L. Bernhardt, "ATM Local Area Networks, ASurvey of Requirements, Architectures, and Standards", IEEE Communications Magazine, July 1997, vol. 35, no. 7, pp. 72-80.