THE SECURITY OF AN ATM TRANSACTION

Baby Shamini P[1], Arun Kumar S[2], Dinesh V[3], Gokulnath S[4].

Assistant Professor, Computer Science and Engineering, Rajalakshmi Institute of Technology[1], Chennai, India.

UG Student, Computer Science and Engineering, Rajalakshmi Institute of Technology[2, 3, 4],
Chennai, India.

babyshamini.p@ritchennai.edu.in[1] arunkumarsivagurunathan96@gmail.com[2] dineshv0812@gmail.com[3]
itsmegokulsathya@gmail.com[4]

Abstract: Our everyday life we use ATM for cash disbursement. Security is one of the important parameters that have to be provided during ATM transactions. Nowadays ATM is having less security. For user authenticate purpose we use finger vein sensor. Each and every human finger vein differs. Biometrics technology is one of the developing technology and biometric validation has grown in popularity as a means of personal identification in ATM Validation setups. The biometric methods used for validation include fingerprint, palm print, handprint, face recognition, speech recognition, dental and eye biometrics. In this paper, a microcontroller based prototype of ATM cashbox ingress setup using finger vein sensor unit is implemented. The necessary software is written in Embedded 'C' and the setup is tested.

Keywords: Finger Vein Matching, GSM, Microcontroller.

I. INTRODUCTION

The need for foolproof security in money transactions due to increase in the frauds today has lead the technology to introduce a smart solution of biometrics to us. Bio is life and metry is to measure thus biometrics is nothing but live measurements of physiological or behavioral characteristics of a person for his/her identification. In the near future with the rapid growth in the use of biometric setup the need to use password and PIN numbers for authentication will be avoided. This biometric setup can be implemented in the Automatic Teller Machine which the existing self-banking setup is providing a 24 hours service and easy money transactions. Thus there is a misuse of the ATM cards and PIN numbers the traditional ATM setup has been replaced by the biometric ATM setup[5].

The Biometric setup being broadly divided into physiological and behavioral biometric. The physiological biometrics is supposed to include the face, fingerprint, hand, eye and the behavioral biometrics is to include the signature, voice, keystroke. Taking into consideration accuracy and reliability among the various biometric setup the most popular are the ones based on fingerprint matching and iris recognition. The security of a multi-biometric setup is much more preferred over the single biometric setup. Further image quality assessment for liveness detection is used to find out if the image captured is a fake or real image sample by comparing the different qualities which could include the degree of sharpness, color luminance levels, local artifacts, entropy, structural distortion or natural appearance[1].

This survey-based paper is structured as follows sections: 1.Introduction, 2.Literature survey 3.General pin number and password based ATM transaction, Section 4.The original password setup merged with the biometric technology of identification, Section 5. ARM7 based biometric ATM using GSM technology, Section 6.Security of ATM transaction with OTP and facial recognition, Section 7.The image quality assessment for liveness detection used in biometric setups. 8. Comparative conclusions are drawn signifying the advantages and disadvantages of various setups described in this paper.

II. LITERATURE SURVEY

Automated Teller Machine -ATM provides non-stop cash solution near to the home by which it is getting popularity almost every country in the world. Recently researches on Automated Teller Machine (ATM) and its security enhancements have been gaining rapid impetus. So far, research has aimed to ensure reliable and secure performance of an ATM in the modern banking setup. However, developments of new features over the existing setup can be expensive. This paper describes the development and implementation of a low cost ATM with currency exchange capability named as Hybrid ATM (H-ATM) which has currency exchanging facility integrated with typical money transaction facility. This proffered H-ATM, capable of executing standard workings but involves a more advanced setup where it includes computer as well as microcontroller embedded setup. This advanced setup has shown considerable improvements in performance, troubleshooting and implementation with higher level of security and consistency. Finally, the low cost of implementing this machine signifies the room for potential improvements with respect to the existing ATM setup.

The authors Akira Shiozak, Akio Ogihara and Hiroyuki Matsumura, Biometric Verification Using Keystroke Motion and Key Press Timing for ATM User Authentication We proffer a biometric verification method using the biometric feature in keystroke working for ATM (automatic teller machine) user authentication. In the proffered method, ATM user authentication is performed by using the 10 types of biometric feature of hand-shape which are extracted from keystroke motion in ATM working. We calculate the similarity between current ATM operator and genuine user in consideration of key-press timing. The proffered method can improve the safety of the present situation without special additional working, physical load and psychological burden.

Anil K. Jain, Patrick Flynn and Arun A. Ross Design and implementation of anti-theft unit for ATM machine Frauds related to the ATM (Automatic Teller Machine) are increasing day by day which is a serious issue. ATM security is used to provide protection against these frauds. Though security is provided for ATM machine, cases of robberies are increasing. Previous technologies provide security within machines for secure transaction, but machine is not neatly protected. The ATM machines are not safe since security provided traditionally were either by using RFID reader or by using security guard outside the ATM. This security is not sufficient because RFID card can be stolen and can be misused for robbery as well as watchman can be blackmailed by the thief. So there is a need to proffer new technology which can overcome this problem. This paper proffers a setup which aims to design real-time detecting and controlling setup. The setup is implemented using Raspberry Pi and fingerprint unit which make the setup more secure, cost effective and stand alone. For controlling purpose, Embedded Web Server (EWS) is designed using Raspberry Pi which serves web page on which video footage of ATM center is seen and controlled. So the proffered setup removes the drawback of manual controlling camera unit and door also this setup is stand alone and cost effective.

Mr Abhijeet S. Kale and Prof. Sunpreet Kaur Nanda Fingerprint Security for Protecting EMV Payment CardsEMV chip based payments cards have been used to combat fraudulent transactions such as counterfeit, lost and stolen cards. Despite of improved security measures payment cards are still not immune to some known threats and vulnerabilities such as card cloning, eavesdropping at POS and shoulder sniffing. A comprehensive study of the all possible threats and present security measures in payments cards is presented. This paper describes how fingerprint can be used for securing payment cards and further enhance the security of EMV environment. Comparison with presently practiced and implemented CHIP and PIN methods is shown elaborating the enhancing security and transaction time reduction by biometric cardholder authentication. Different methods of implementing fingerprint security in payment cards are provided. Major attacks on fingerprinting authentication are discussed and mitigation strategy is presented.

Bin Li, Kuan-Quan Wang and D. ZhangOn-line signature verification for e-finance and e-commerce security setup

Online signature verification is a new and active topic in the research and application fields of biometrics. This paper proffers a low cost online signature verification method based on the matching of curves about x- and y-axis attaching some dynamic features. Comparing with human being's behavior, different local weight, and unfixed threshold are introduced to improve the performance of signature verification setup. Finally, this paper presents some applications of online signature verification on ATM, onsite credit card verification and Internet e-commerce.

Ali Karounia, Bassam Daya and Samia Bahlakb "Offline signature recognition using neural networks approach," The signature verification is the oldest security technique to verify the identification of persons. Recently, the signature recognition schemes are growing in the world of security technology. It offers two different types of schemes those are offline and online method. The offline technique means to verify a signature written on paper which is scanned to convert it into a digital image, whereas the online setup required an online device such as Tablet PC, touch screen detect by a pressure sensitive pen to verify the signature. It addresses the offline signature verification technique using Artificial Neural Network (ANN) approach.Thus it explains the fundamental characteristics of offline signature verification processes and highlights the comparison among various offline signature verification approaches and various signature recognition issues.

III. GENERAL PIN NUMBER AND PASSWORD BASED ATM TRANSACTION

In the PIN & password based setup the person begins the transaction by inserting his/her ATM debit card, after scanning if the card is found to be a valid one then he/she needs to enter a personal identification number (PIN) which is a four-digit password. The setup will check if the PIN entered is a valid one or not. If the PIN is valid then it allows the further transaction. The traditional method which was used is the PIN number and passwords is not safe to use because the person with whom we have shared our card and PIN may later misuse it. Moreover, if we think of memorizing the password or carrying a smart card or think of managing multiple passwords and smart cards for different setups it may prove to be a significant overhead to the users[6]. Moreover being artificially associated with a particular user it cannot be truly used for user authentication. The identification of the individual being done by a PIN there is a possibility of hacking passwords i.e. the security of a customer account is not

Table 1

S.NO	NAME OF THE AUTHOR & PAPER	INFERENCE/RESULT
1.	Mr Abhijeet S. Kale and Prof. Sunpreet Kaur Nanda, "**Design of Highly Secured Automatic Teller Machine System by Using Aadhaar Card and Fingerprint**,	This system using ARMCONTROLLER on “BIOMETRICS” and “AADHAAR CARD” in order to improve authentication of customers using ATM machine and confidence in the banking sector.
2.	Mr. Mahesh A. Patil, Mr. Sachin P.Wanere, Mr. Rupesh P.Maighane and Mr. Aashay Tiwari, "**ATM Transaction Using Biometric Fingerprint Technology**,"	The main objective of this system is to use for ATM security applications. In these systems, bankers collect the customers’ finger prints and mobile number while opening the accounts, only then the customer can access an ATM machine. ATM machine works when customer places finger on the finger print module and enters 4-digit dynamic code from mobile phone message.
3.	Bin Li, Kuan-Quan Wang and D. Zhang, “**On-line Signature Verification for E-Finance and E-Commerce Security System**,”	A low cost on-line signature verification method based on the matching of curves about x-axis and y-axis attaching some dynamic features. Just as human being's behavior, different local weight and unfixed threshold are introduced to improve the performance of signature verification system. Also the paper presented some applications of on-line signature verification on ATMs, on-site credit card verification and Internet E-Commerce.
4.	Ofir Pele and Michael Werman, "**The Quadratic-Chi Histogram Distance Family**"	an existing algorithm called The Quadratic-Chi Histogram Distance Family matching algorithm is considered for simulation on handwriting signature matching. It is suggested for the implementation to use any of the better algorithms with the model from the existing researches, which is already ensuring maximum accuracy.

guaranteed by PIN. To overcome the disadvantage of this traditional setup our prime concern should be the security over money transaction since the attackers have turned their attention equally to soft assets present in the ATM such as PIN and account data. In figure1 the flow chart shows how the transaction is made in the traditional ATM setup using an ATM card and a pin.

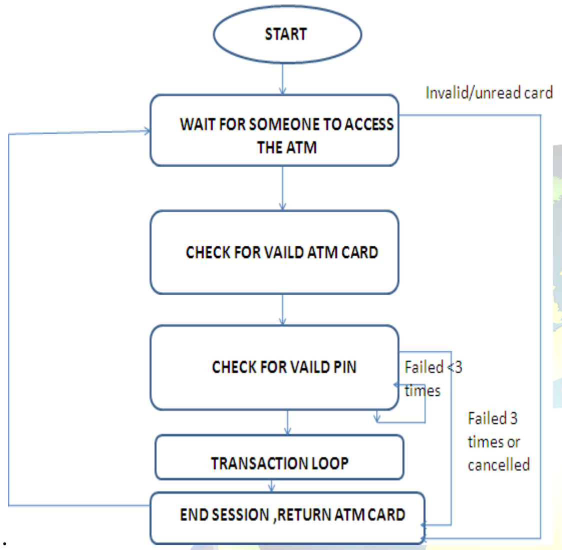
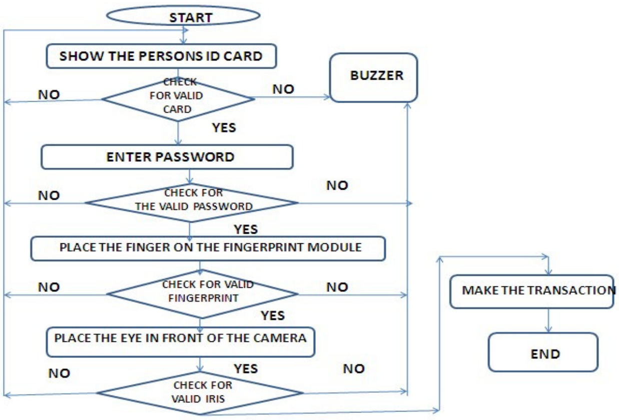


Figure 1: State chart diagram of the general transaction

IV. THE ORIGINAL PASSWORD SYSTEM COMBINED WITH THE BIOMETRIC TECHNOLOGY OF IDENTIFICATION

The password authentication method was merged with the biometric technology for identification in the ATM machine has improved the security of the transaction with increasing security given to the automated personal identification needs to be added to the traditional ATM setup to overcome its disadvantages. In this setup, the person who needs to make a transaction begins by placing his/her id card in front of the card reader. If it is a valid one then the process is carried on else there is an interruption indicated by a buzzing sound. After the verification of the card, the user needs to enter a password. If the password is correct then the controller in the setup will ask for a fingerprint access else it will alert by a buzzing sound. In the fingerprint accessing method it will check if the incoming fingerprint matches with the stored authorized fingerprint of the person then it proceeds to the next step else there is a buzzing alert. In the proceeding step the captured iris image is matched with the one in the database. If it matches the transaction is permitted else the process is halted and alerted by a buzzer [6]. The figure 2 shows the working flow of the setup in which the biometric identification technology is merged with the traditional ATM setup. The ID cards which were used initially in this setup could be lost. So there was a need to generate an OTP (One time password) to achieve better identification and to relieve the person from carrying an ID card to verify his/her identity. In the next section, the GSM technology is described for OTP technology is described for OTP.



biometric system

V. ARM7 BASED BIOMETRIC ATM USING GSM TECHNOLOGY

An extension to the previous setup was done by adding GSM technology to it. This setup begins with the placing of the finger on the fingerprint unit, if the fingerprint is valid then the customer needs to enter a fixed 4 digit PIN. After the 4 digit code matching with entered PIN code the setup will automatically generate another different 4 digit code i.e. OTP.GSM modem connected to ARM7 is used to send a message to the registered mobile number. It is only after correct entering of the OTP that the person is allowed to make a transaction. The OTP being used here is different for each payment increasing the security of the money transaction [5]. The GSM (Global Setup for Mobile Communication) technology can also be used with the RFID(Radio frequency identification) card reader where after swiping the ATM card the GSM unit is used to send a message having 3 options "Yes, No, Action" to the card holders phone who may reply "Yes" if he/she wants to make a transaction, "No" if he/she doesn"t want to make a transaction or "Action" if he/she has misplaced or lost the card and someone is misusing it. Both these setups were built on the technology of embedded setups which improved the safety, reliability and ease of using the setup [4].The flowchart in figure 3 shows how the traditional ATM setup merged with GSM technology operates.

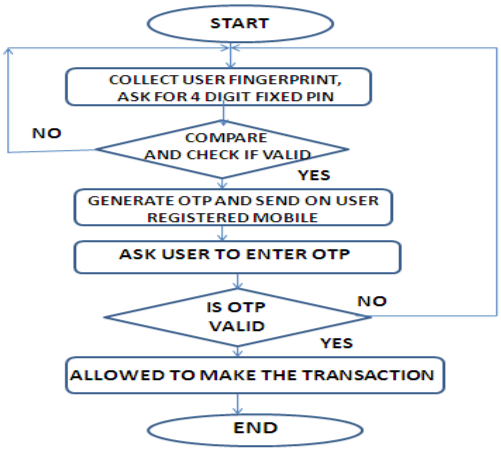

START
COLLECT USER FINGERPRINT, ASK FOR 4 DIGIT FIXED PIN
NO
COMPARE AND CHECK IF VALID
YES
GENERATE OTP AND SEND ON USER REGISTERED MOBILE
ASK USER TO ENTER OTP
IS OTP VALID
NO
YES
ALLOWED TO MAKE THE TRANSACTION
END

Figure 3: Flowchart for the ATM access using GSM technology.

VI. AN ATM MACHINE WITH OTP AND FACIAL RECOGNITION

Compared to the earlier described setups in this setup security of accounts and privacy of users were achieved by using features like face recognition and one time password. The setup made the face as a key in order to eliminate the chances of fraud caused by theft attacks and duplicity of ATM cards. The setup used a 6 digit OTP to avoid the need to remember passwords. The working of the setup will begin like the original setup by swiping the ATM card. The live image of the face is captured which is compared with the one which is saved in the database. Only after it matches an OTP will be sent on the registed mobile phone. The transaction will proceed successfully only if the entered OTP is correct. The model in this setup uses Principal Component Analysis to build eigen faces. The 6 digit OTP was generated by random number generation technique. But the facial recognition technique used in this setup proved to be more challenging compared to the other biometric setups. The drawback of the eigenface method is that it can sometimes be spoofed by face masks or photos of an account holder. [2] Moreover if a particular network service is down it becomes difficult for the user to receive OTP which may halt or delay the transaction [2].The figure 4 shows how the model of the ATM with an OTP and facial recognition will operate.

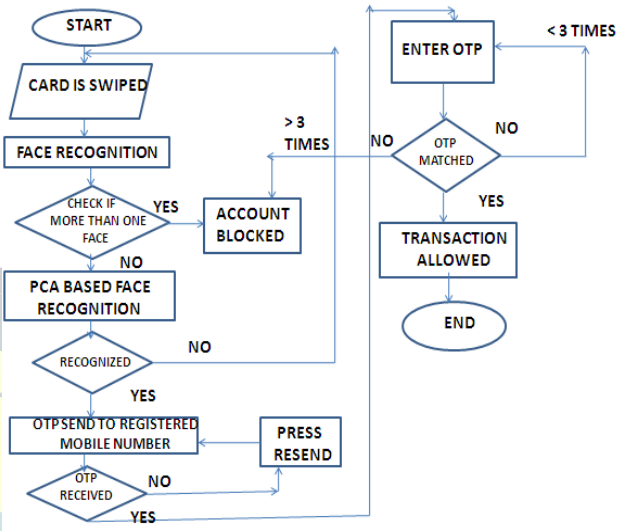


Figure 4: Model of ATM with OTP and facial recognition

VII. IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION USED IN BIOMTERIC SYSTEMS

The requirement of this technique was to ensure the actual presence of a real legitimate trait and detect different types of fraudulent access. This software based detection method uses 25 general image quality features extracted from one image to distinguish real biometric samples from the fake traits. According to this method the fake images captured due to fraud attacks will have different quality than a real sample acquired in normal workings. In this setup image quality assessment was applied to iris, fingerprint and face. It was observed that the fake iris image captured from printed paper appear blurred and out of focus due to trembling, the fake faces were slightly bigger than the real ones, the fingerprints captured from gummy fingers presents local acquisition artifacts like spots and patches [1].This method operates on the whole image and does not search for any trait specific properties. Computational load is minimized since there is no need of any preprocessing steps to be performed prior to image quality feature computation. A feature vector is generated from each image sample which is classified as genuine or fake sample by Linear Discriminant or Quadratic Discriminant Analysis classifier. The results are reported in terms of False Genuine Rate

(FGR) which accounts for the number of false samples being classified as real ones and False Fake Rate (FFR) which gives the probability of an image coming from a genuine sample being considered as fake. After this the Half Total Error Rate is computed as HTER= (FGR+FFR)/2. To avoid the direct or spoofing attacks on biometric setups and to reinforce maximum security to it the biometric based ATM setup should be implemented considering the image quality assessment for fake detection [1].

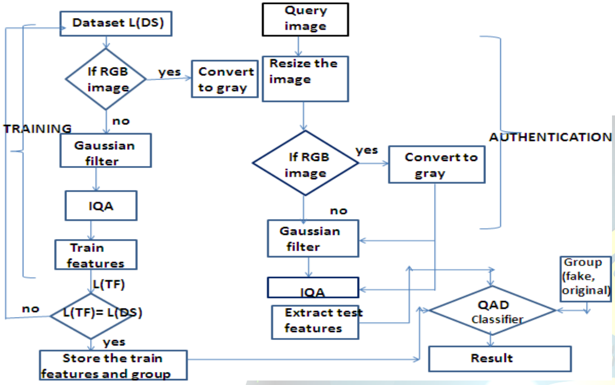


Figure 5: IQA for fake biometric detection

VIII. CONCLUSION

This paper provides the various ways in which an ATM transaction can be done. It shows how security in the transaction is being improved. It also shows how the use of biometrics for authentication is improving the security and ease of the transaction. The paper also gives us an idea how the OTP can be used in order to avoid the overheads of remembering passwords. Finally it presents the concept of image quality assessment for fake detection which can be used further to prevent the biometric ATM transactions from direct or spoofing attacks.

IX. REFERENCES

[1] Javier Galbally, Sebastien Marcel and Julian Fierrez, ”Image Quality Assessment for Fake Biometric detection Application to Iris, Fingerprint and Face recognition”,IEEE trans.on image processing ,vol. 23,No.2 February 2014.

[2] Mohsin Karovaliya,Saifali Karedia,Sharad Oza, Dr.D.R.Kalbande, ”Enhanced Security for ATM machine with OTP and facial recognition features”,International Conference on Advanced ComputingTechnologiesandApplications(ICATA-2015).

[3] Karthik Nandakumar and Anil K.Jain ,”Biometric Template Protection”,IEEE Signal Processing Magazine September 2015.

[4] Mrs.S.P.Balwir,Ms.K.Katole,Mr.R.D.Thakare,Mr.N.S .Pnchbudhe,Mr.P.K.Balwir,"SecuredATMtransaction system using micro-controller”, International Journal of Advanced Research in computer science and software engineering “,Vol.4,Issue4,April 2014.

[5] Khatmode Ranjit P, Kulkarni Ramchandra V,”ARM7 Based Smart ATM Acess and Security System Using Fingerprint Recognition and GSM Technology”,International Journal of Emerging Technology and Advanced Engineering ,Vol.4,Issue 2,Feb. 2014

[6] D.Shelkar Goud,Ishaq Md,P.J.Saritha,”A Secured Approach for Authentication system using fingerprint and iris”,Global journal of Advanced Engineering Technology,Vol,Issue3-2012.

[7] J.Galbally.F.Alonso-Fernandez,J.Fierrez,and J.Ortega- Garcia,”A high performance finger print liveness detection method based on quality related features,” FutureGenerat.Comput-Syst;vol28;no.1,pp.311-321,2012.

[8] M.C.Stamm and K.J.R.Liu,”Forensic detection of image manipulation detection using statistical intrinsic fingerprints IEEE trans.Inf.Forensics Security,vol.5,no.3,pp.492-496,Sep 2010.

[9] Pavel Moravec and Vaclav Snasel ,”Dimension Reduction methods for iris recognition Department of Science ,FEECS,K.Richta,J.Pokomy,V.Snasel Dates 2009,pp.80- 89ISBN.

[10] Kelvin.W .Bowyler,Karen Hollingworth,Patrick J.Flynn;”Image understanding for iris biometrics:survey “,Computer Vision and image understanding 110(2008)281-307.

[11] Rowe, R.K., Nixon, K.A., Butler, P.W.: „Multispectral fingerprint image acquisition‟ in Ratha, N., Govindaraju,V.(Eds.):„Advances in Biometrics‟ (Springer, London,08), pp. 3–23