International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Survey on the Security of an ATM Transaction

Joyce Soares[1], Dr. A. N. Gaikwad[2]

[1, 2]Zeal College of Engineering and Research, Sr.No 39,Off Mumbai-Bangalore Express Highway, Narhe, Pune, India

Abstract: ***The previously used signature based system was replaced by a pin number in an ATM system. But due to risks of fraudulent activities the pin number was replaced by the biometric system. The biometric system may be a fingerprint, iris, retina, veins, etc. In this system the cash would be dispersed only if the user is an authenticated person. Further direct or spoofing attacks have today motivated us to enhance the security of the biometric system by using image quality assessment for liveness detection. This paper emphasizes in a general way on how the ATM transaction has been made secured by presenting a literature survey of the previous systems and comparing it with the recent biometric system using image quality assessment for fake detection which will show the improvement in the security level of the financial transaction being made using the ATM machine.***

Keywords: Biometrics, Fingerprint Matching, GSM, Image Quality, Iris Recognition

1. 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 system the need to use password and PIN numbers for authentication will be avoided. This biometric system can be implemented in the Automatic Teller Machine which the existing self banking system is providing a 24 hours service and easy money transactions. Since there is a risk of misuse of the ATM cards and PIN numbers the traditional ATM system has been replaced by the biometric ATM system[5].

The Biometric system 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 system the most popular are the ones based on fingerprint matching and iris recognition. The security of a multi-biometric system is much more preferred over the single biometric system. 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 degree of sharpness, color luminance levels, local artifacts, entropy, structural distortion or natural appearance[1].

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

2. General PIN Number and Password Based ATM Transaction

In the PIN & password based system 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 system will check if the PIN entered is a valid one or not. If the PIN is valid then it allows further transaction. The traditional method which involved 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 smartcard or think of managing multiple passwords and smartcards for different systems 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 guaranteed by PIN. To overcome the disadvantage of this traditional system our prime concern should be the security over money transaction, since the attackers have turned their attention equally to soft assests 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 system using an ATM card and a PIN

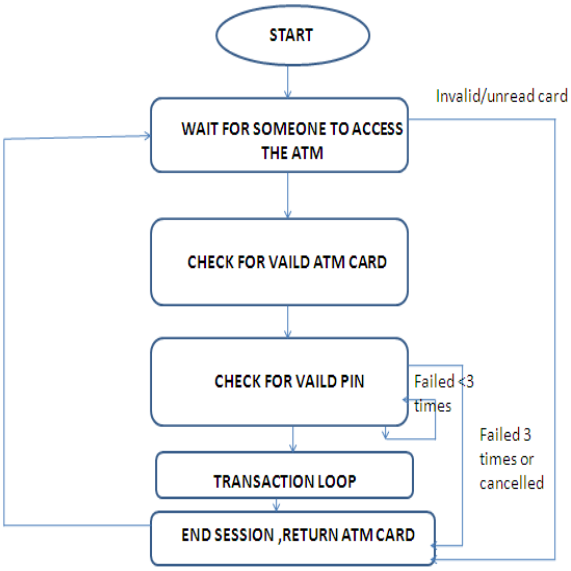

Figure 1: State chart diagram of the general transaction

3. The Original Password System Combined With the Biometric Technology of Identification

The original password authentication method combined with the biometric technology for identification in the ATM machine has improved the security of the transaction with increasing emphasizes given to security automated personal identification needs to be added to the traditional ATM system to overcome its disadvantages. In this system 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 system will ask for a fingerprint access else it will alert by a buzzing sound. In fingerprint accessing 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 operation flow of the system in which the biometric identification technology is combined with the traditional ATM system. The ID cards which were used initially in this system 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.

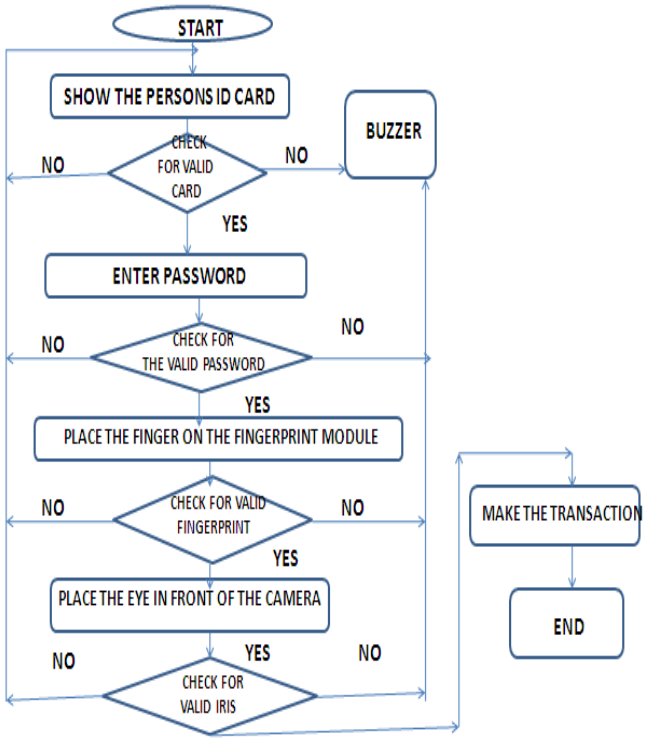

Figure 2: Operation flow of system combined with biometric system

4. ARM7 Based Biometric ATM Using GSM Technology

An extension to the previous system was done by adding GSM technology to it. This system begins with the placing of the finger on the fingerprint module, 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 system 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 System for Mobile Communication) technology can also be used with the RFID(Radio frequency identification) card reader where after swiping the ATM card the GSM module 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 systems were built on the technology of embedded systems which improved the safety, reliability and ease of using the system [4].The flowchart in figure 3 shows how the traditional ATM system combined with GSM technology operates.

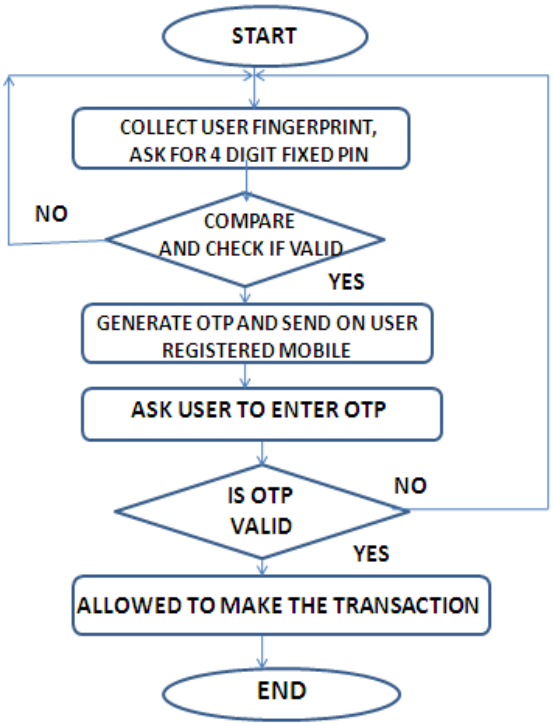

Figure 3: Flowchart for the ATM access using GSM technology.

5. An ATM Machine with OTP and Facial Recognition

Compared to the earlier described systems in this system security of accounts and privacy of users were achieved by using features like face recognition and one time password. The system made the face as a key in order to eliminate the chances of fraud caused by theft attacks and duplicity of ATM cards. The system used a 6 digit OTP to avoid the need to remember passwords. The operation of the system will begin like the original system 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 registered mobile phone. The transaction will proceed successfully only if the entered OTP is correct. The model in this system 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 system proved to be more challenging compared to the other biometric systems. 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.

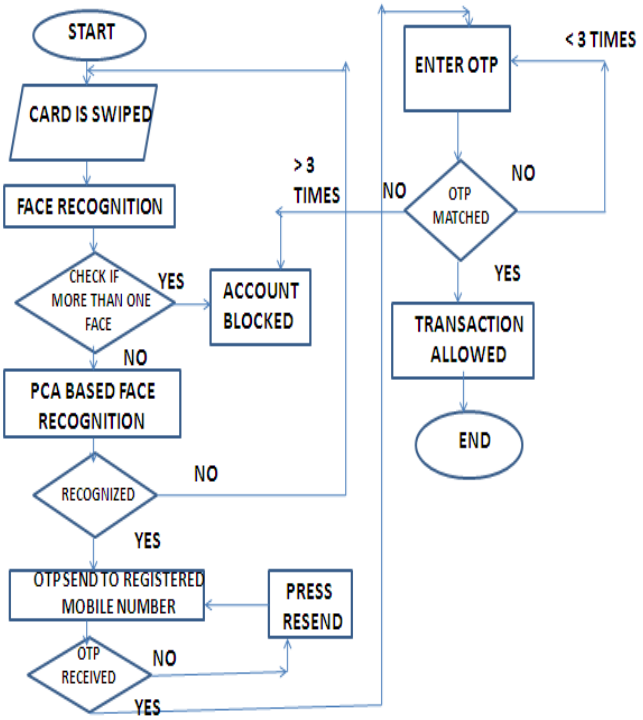

Figure 4: Model of ATM with OTP and facial recognition

.

6. Image Quality Assessment for Liveness Detection Used in Biometric 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 operations. In this system 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 systems and to reinforce maximum security to it the biometric based ATM system should be implemented considering the image quality assessment for fake detection [1].

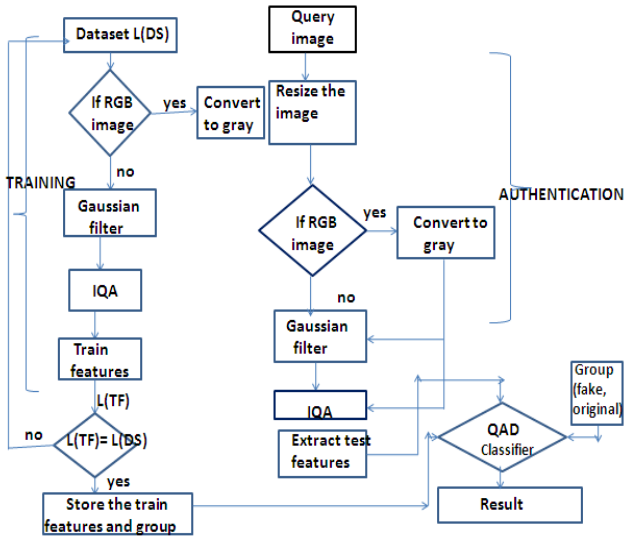

Figure 5: IQA for fake biometric detection

7. Conclusion

This paper gives a brief idea about 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.

8. Acknowledgment

I would like to thank the anonymous referees for their helpful guidance that has improved the quality of this paper. I would also like express my gratitude and sincere thanks to my guide **Dr. A. N. Gaikwad** for his valuable support, help and guidance in the completion of this paper.

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.Panchbudhe,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 ,”Future Generat.Comput-Syst;vol 28;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

Author Profile

Soares Joyce Victor completed her B.E. degree in Electronic and Telecommunication Engineering from Savitribai Phule Pune University in June 2014.Her interested areas of research are Biometrics, Image Processing Embedded Systems and Digital Electronics.

Dr. A .N . Gaikwad completed his B.E. in Electronic and Telecommunication Engineering from COEP-Govt. College of Engineering, Pune in the year 1983. He completed his M.E. in Electronic and Telecommunication Engineering from COEP-Govt. College of Engineering, Pune in the year 1994. He completed his PhD in Vector Distance Approach for Minutiae Matching in Fingerprint Verification in the year 2005. He worked as an Assistant Professor in Bansilal Ramnath Agarwal Charitable Trust"s Vishwakarma Institute of Technology, (VIT) from 18th July 2000 to 30th June 2005. He worked as a Professor in Bansilal Ramnath Agarwal Charitable Trust"s Vishwakarma Institute of Technology, (VIT) from 1st July. 2005 to 31st January 2007. He worked as a Principal in Society for Computer Technology and Research"s Pune Institute of Computer Technology, (PICT) from 1st Feb. 2007 to 30th Sept. 2010.He also worked as a Principal in Marathwada Mitra Mandal"s College of Engineering, (MMCOE) from 1st October. 2010 to 31st August. 2012.Since 1st September 2012, he is working as a Principal at Zeal Education Society"s Zeal (formerly Dnyanganga) College of Engineering & Research, Pune. He has a total experience of 30.5 years which includes 21.5 years as an Assistant Professor/Lecturer,8 years as a Professor/Principal and 10 years Research. His areas of interest of research are Embedded Systems and Biometric IP.