Journal of Theoretical and Applied Information Technology
31st March 2012. Vol. 37 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

NOVEL HYBRID TECHNOLOGY IN ATM SECURITY USING BIOMETRICS

[1]SANTHI.B,[2]RAM KUMAR.K

[1]Professor,School of Computing, SASTRA University
[2] 4th year, B.tech(ICT) ,School of Computing, SASTRA University

E-mail: [1]santhi@sastra.edu, [2]raamsk7@sastra.edu

ABSTRACT

In this modern world ATM is being used by many of us. The security that is being currently used for ATM indeed has a few backdoors and it can be improved further. For the same reason biometric verification were introduced. But even the biometric system does not seem to be completely reliable and hence a contingency plan is needed in order to prevent catastrophes. Objective of this paper is to provide enhanced security to ATM by enhancing the already proposed biometric system and making it still secured by PII[Personal Identification Image] process. So a detailed study on various existing biometric systems is studied and also its limitations are listed. This paper proposes a novel method to meet out the challenges and strengthen the security mechanism. In the proposed security algorithm two phases are defined. These two phases provide two tier security and there by increases the security of ATM machine.

Keywords: *ATM Security Enhancement, Biometric In ATM, Fingerprint In ATM Security,Fingerprint Verification, Image Processing In ATM*

1. INTRODUCTION

Biometrics technology allows determination and verification of identity through physical characteristics. To put it simply, it turns the human body in to his/ her password, which cannot be impersonated by others. The biometric values are stored in the database for the comparison purposes. The terms *"Biometrics"* and *"Biometry"* have been used since early in the 20th century to refer to the field of development of statistical and mathematical methods applicable to data analysis problems in the biological sciences. Recently, these terms have also been used to refer to the emerging field of information technology devoted to automated identification of individuals using biological traits, such as those based on retinal or iris scanning, voice patterns, dynamic signatures, fingerprints, face recognition, or hand measurements, especially for authentication purposes. Thus biometrics can be defined as the science and technology of measuring and statistically analyzing biological data. They are measurable physiological and / or behavioral characteristics that can be utilized to verify the identity of an individual.

Fingerprint verification, Iris scanning, facial recognition, and voice verification are the methodologies for incorporatingbiometric systems with ATM machine.

2. COMPARISON OF BIOMETRIC SYSTEMS

Method	Pros	Cons
Finger print	Compares using several features of the fingerprint pattern (arch, loop, whorl)	Creating forged, latent fingerprints is dangerously easy.
Iris	Digital templates encoded from patterns by mathematical and statistical algorithms allow unambiguous positive identification of an individual	Iris scans be forged by wearing contact lenses with an iris pattern on them
Face	Identifying or verifying a person from a digital image or a video frame from a video source	Serious disadvantage is that many systems are less effective if facial expressions vary. Even a big smile can render the system less effective
Voice	Provides two way security with your voice and word you have a password	Mimicry can't be identified. Once recorded , faking becomes easy

3. AVAILABLE BIOMETRIC TECHNIQUES FOR SECURITY PURPOSES

The following are the few papers proposed by various authors for enhancing the security using biometric methods

Title	Author (Year of publication)	Method	Significance	Strengths	Limitations
Formation of Elliptic Curve Using Finger Print and Network Security	B.Thiruvaimalar Nathan[06]	Finger Print	Minutiae co-ordinate points are extracted from biometric templates and elliptic curve algorithm is applied	Finger Print is used as biometric template	Missed to explain about what failure case .
Efficient Finger Print Image Classification And Recognition using Neural Network Data Mining	K.Uma maheswari [07]	Finger Print	Uses minutiae and combines with data mining techniques (K-nearest algorithm)	Fast ,accuracy, reliable	No backup plan suggested to overcome the failure of fingerprint system.
A Fast Fingerprint Classification Algorithm by Tracing Ridge-flow Patterns	Neeta Nain[08]	Finger Print	Using Tracing Ridge-flow algorithm	Accuracy is perfect (98.75)	People fail to suggest an alternative in case of failure of fingerprint verification.
A New Approach of Finger-Print Recognition based on Neural Network	Behnaz Saropourian[09]	Finger Print	Based on View patterns and groove pattern	Large accuracy, works fine on binary images and gray scanned	Once group is tracked , pattern can be tracked.

				photo	
Fingerprint Identification Based on the Model of the Outer Layers of Polygon Subtraction	Nae Myo[09]	Finger Print	Uses model of multi-layers of convex polygon to implement fingerprint verification.	Extraction is based in a specific area in which the dominant brightness value of fingerprint ranges	Faking is possible and fake one can't be detected .
A New Localization Method for Iris Recognition Based on Angular Integral Projection Function	Ghassan J.Mohammed [09]	Iris	Finding Iris inner and outer boundary and eyelids and uses the angular integral projection to detect iris	Uses False Accept rate and False reject rate and improves the efficiency	Makes the machine costlier and proper maintenance is needed periodically.
Non orthogonal Iris Recognition System	Chia-Te Chou (10]	Iris	Parameters are estimated using the detected elliptical pupillary boundary	Error rates are much low (0.04%)	Can be faked and that can’t be detected.
A Robust Segmentation Approach to Iris Recognition Based on Video	Yu Chen jin Wang [07]	Iris	Instead of verifying Iris with image , video was used for betterment	Takes one step ahead of other Iris verification techniques	Can’t be reliable under all cases.
Face and ear Fusion Recognition Based on Multi-Agent	Yong-Mei Zhang [08]	Face	Face(eye brow) and ear recognition using 3D human head	More accurate and authenticates more perfectly.	Fails if people resemble one another
Patch based Face Recognition from Video	Changbo Hu [09]	Face	Video provides more information than image	Face patches are used to recognize and more accurate than image recognition	Consumes time and for authentication and video recording is not reliable.
Improving ATM security via Face Recognition	K John Peter [09]	Face	Face recognition is used as authentication system	Provides enhanced security along with PIN	No secondary methodology suggested in case of injuries and how faking

					will be detected was not explained
Security System Using Biometric Technology: Design and Implementation of Voice Recognition System(VRS)	Rozeha A. Rashid [08]	Voice	Recognize an individual's unique voice characteristics	Hacking is much complicated and possible only if u know the word	It is not much accurate as there biometric system , Device costs more
Microprocessor Based Voice Recognition System Realization	Nihat Ozturk [10]	Voice	Uses PIC18F452 microcontroller	Low cost and easily applied prototype	Can be cracked by playing recording voices

4. EXISTING METHODOLOGIES:

All the above listed papers propose a single biometric check and it has been pointed out that a single biometric is not a security solution on its own. Two or more methods are to be incorporated to make it more efficient. But using biometrics such as Iris identification, Voice verification costs much and the maintenance will be difficult. This makes the system more costly and complicated. Another biometric method for replacing the failure of one biometric makes the machine more complicated and cost factor is affected. Having such a sophisticated system may fit to urban areas and can't be much easier in rural areas.

5. NEED FOR STUDY:

Many authors tried working on enhancing security using biometrics and these methodologies. Although these methodologies emphasis on some key features in it, it has its own draw back too. Moreover they have not mentioned the case if the system fails

6. PROPOSED ALGORITHM:

This paper analysis the limitations in the above papers of making the system unreliable if the biometric fails or making the system complex by combining more than one biometric system i.e. Iris, Voice, Face recognition. This emphasis on using PII concept as a backup methodology on the failure (Physical damage, user may get injured) of biometric (fingerprint) and enrich the security and forms a two tier security. Using the proposed algorithm user will be able to access even if the biometric fails (using mobile verification) and he can safeguard himself as the card gets blocked when he is forced by stranger(only 3 attempts for PII) and provides a secured environment and reliable all the time. (Physical damage, user may get injured) and makes the process unreliable. A user should be able to access even if the biometric fails or he should be safeguard when he is forced to access.

PERSONAL IMAGE IDENTIFICATION: To make this process simple, secure and cost effective than the existing PIN verification method, this paper proposes the usage of biometric method and Personal Image identification provides enriched Security to the ATM systems and provides a user friendly and secured service. The increased need of privacy and security in our daily life has given birth to this new area ofscience. In Figure 1 Phase 1 depicts the existing methodology and Phase 2 explains the proposed algorithm as follows.

7. WORK FLOW DIAGRAM:

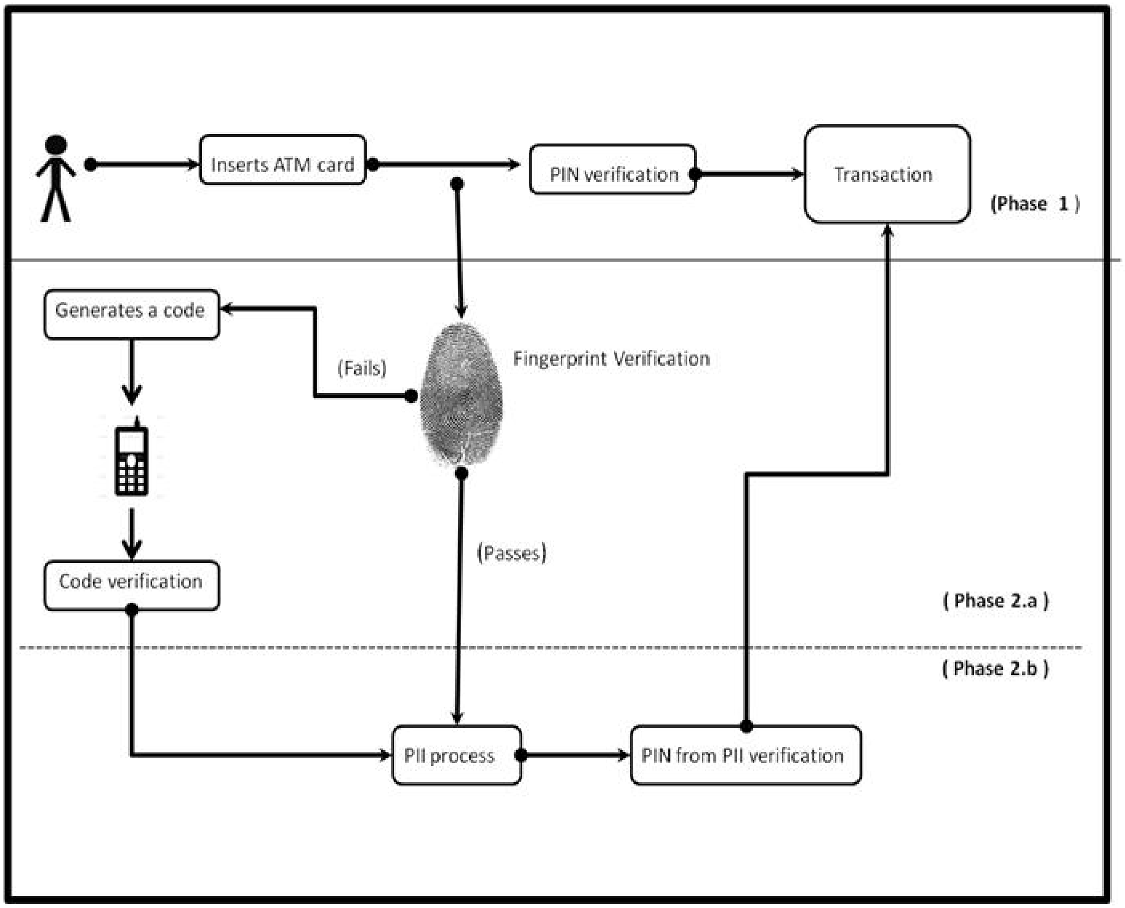

Figure 1 Proposed algorithm

PHASE 1:

This is the existing mechanism. The user enters the ATM and inserts the card and enters the PIN and enters the Transaction mode.

PHASE 2a:

Once the user inserts the ATM card, the ATM machine asks for his fingerprint and checks with the database. If the fingerprint matches with the database, he will be directed to phase 2.b. If the fingerprint doesn't match, it will send SMS verification code to the mobile number he registered and when the user enters the verification code and he passes to phase 2.b if he enters the right one.

PHASE 2b:

- The PII is mapped with position of the image stored in the database for that transaction.
- The images will be ordered using a random function and a session id will be used for the transaction
- The user has to identify his PII image [Initially it has to be registered in register with particular image in registration level itself]PIN number has to be found by the user (Eg. 4th row 2ndcolumn, 4224). PIN number found here will be reset after the transaction

The proposed algorithm provides 2 phase security and acts as a two tier security. User can't access others account as they have other's ATM card and knows the PII image. He needs to have his mobile phone and finger print too. It makes the process more secured than existing algorithm using PIN number. (Phase1). The proposed algorithm increases the security and efficiency and decreases the probability of misusing others account. Thus this provides a two tier security

7. ALGORITHM

STEP 1: User insert ATM Card and give his/her fingerprint (as input) on the finer scan pad.

STEP 2: Fingerprint verification

STEP 3: If Validated

GOTO STEP 5

ELSE

GOTO STEP 4

STEP 4: Verification code will be generated and sent to user's mobile phone

STEP 5: PII Process

STEP 6: User gets authenticated

STEP 7: Executes Transaction

8. CONCLUSION:

The proposed method overcomes the limitations that exists in other methods and provides a secured and safe environment that saves the hard earned money of the user. The user when gets hurt in finger can be authenticated via mobile after code verification and when forced can block the account's transaction with PII and even if the stranger tries trial and error, maximum of 3 times PII will function and gets blocked for 24 hrs. This provides two tier security.

In future this algorithm will be experimented using a biometric system to check the fingerprint and a SMS gateway has to be connected to send a verification code which should be updated in Database too. PII process in Phase 2b in this proposed algorithm is the main back up and enhances the security still more. The efficiency of proposed algorithm will measured using performance metrics and detailed analysis will be done.Finally, more extensive experimentation is necessary, in order to obtain statistically significant results and thus verify the conjecture of this proposed method. The increased need of privacy and security in our daily life has given birth to this new concept of generating PIN number through **PII process** and enhances the security. Even if the biometric system fails due to injury and other reason this proposed PII process allows the user to do transaction in a secure way.

REFERENCES:

[1] Nathan, B.T.; Meenakumari, R.; Usha, S.;"Formation of Elliptic Curve Using Finger Print for Network Security", Process Automation, Control and Computing (PACC), 2011 International Conference on Publication Year: 2011 , Page(s): 1 - 5

[2] Umamaheswari, K.; Sumathi, S.; Sivanandam, S.N.; Anburajan, K.K.N.; "Efficient Finger Print Image Classification and Recognition using Neural Network Data Mining" Signal Processing, International Conference on Communications and Networking, 2007. ICSCN '07, Publication Year: 2007, Page(s): 426 - 432

[3] Nain, N.; Bhadviya, B.; Gautam, B.; Kumar, D.; Deepak, B.M.; "A Fast Fingerprint Classification Algorithm by Tracing Ridge-Flow Patterns",IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008. SITIS '08. Publication Year: 2008 , Page(s): 235 - 238

[4] Saropourian, B.; A new approach of finger-print recognition based on neural network 2nd IEEE International Conference on Computer Science and Information Technology, 2009. ICCSIT 2009 , Publication Year: 2009 , Page(s): 158 - 161

[5] Myo, N.;"Fingerprint Identification Based on the Model of the Outer Layers of Polygon Subtraction", International Conference on Education Technology and Computer, 2009. ICETC '09, Publication Year: 2009 , Page(s): 201 - 204

[6] Mohammed, G.J.; Hong BinRong; Al-Kazzaz, A.A.; Abdullah, M.Y.; "A New Localization Method for Iris Recognition Based on Angular Integral Projection Function" ,First International Workshop on Education Technology and Computer Science, 2009. ETCS '09,Volume: 3 ,Publication Year: 2009 , Page(s): 316 - 320

[7] Chia-Te Chou; Sheng-Wen Shih; Wen-Shiung Chen; Cheng, V.W.; Duan-Yu Chen;"Non-Orthogonal View Iris Recognition System" , IEEE Transactions on Circuits and Systems for Video Technology, Volume: 20 , Issue: 3 , Publication Year: 2010 , Page(s): 417 - 430

[8] Yu Chen; Jin Wang; Changan Han; Lu Wang; Adjouadi, M.; "A robust segmentation approach to iris recognition based on video",37th IEEE Applied Imagery Pattern Recognition Workshop, 2008. AIPR '08, Publication Year: 2008 , Page(s): 1 - 8

[9] Yong-Mei Zhang, Li Ma, Bo Li, "Face and Ear Fusion Recognition Based on Multi-Agent", Proceedings of the seventh international Conference on Machine Learning and Cybernetics, Kumming, 2008 , pp.46-51.

[10] Changbo Hu; Harguess, J.; Aggarwal, J.K.;"Patch based Face Recognition from Video",16th IEEE International Conference on Image Processing (ICIP), 2009 ,Publication Year: 2009 , Page(s): 3321 – 3324

[11] Peter, K.J.; Nagarajan, G.; Glory, G.G.S.; Devi, V.V.S.; Arguman, S.; Kannan, K.S.;"Improving ATM security via face recognition ",3rd International Conference on Electronics Computer Technology (ICECT), 2011, Publication Year: 2011 , Volume: 6 Page(s): 373 – 376

[12] Rashid, R.A.; Mahalin, N.H.; Sarijari, M.A.; Abdul Aziz, A.A.;"Security system using biometric technology: Design and implementation of Voice Recognition System (VRS)", International Conference on Computer and Communication Engineering, 2008. ICCCE 2008. , Publication Year: 2008, Page(s): 898 – 902

[13] Ozturk, N.; Unozkan,U.; "Microprocessor based voice recognition system realization", 4th International Conference on Application of Information and Communication Technologies (AICT), 2010, Publication Year: 2010 , Page(s): 1 – 3

[14] Gonzalez, R. C., Woods, R. E., and Eddins, S. L. [2009]. Digital Image Processing UsingMATLAB, 2nd ed., Gatesmark Publishing, Knoxville, TN.