http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (2): 297-305, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.297.305
© 2013 Asian Network for Scientific Information

Privacy-protected Multimodal Biometric-based Group Authentication Scheme for ATM

B. Shanthini and S. Swamynathan
Department of IST, Anna University, Chennai, India

Abstract: Biometrics based authentication is a potential candidate to replace token-based authentication especially in Automatic Teller Machines (ATMs). The financial sector has used ATMs as a means to make payments and to offer financial services for its clients. But, security is a major issue in accessing these machines in particular for authenticating a group of users who have joint account in the financial institutions. So, in this study, a simple but efficient group authentication mechanism is proposed in which multimodal biometric is used for authenticating the group of customers instead of the existing practice of using multi ATM cards. Privacy and revocability are the main concern while using biometrics. So the biometric used are not stored as such instead a cancelable form, generated by genetic operator is stored and by that way privacy is protected and also revocability is ensured.

Key words: Multimodal biometrics, fingerprint biometrics, face biometrics, automatic teller machine, security, group authentication

INTRODUCTION

ATMs (Yanez and Gomez, 2004) are electronic banking machines situated in different places of the cities which allow the customers to do the basic transactions without the aid of bank staff. Using these machines the customers can withdraw cash and receive the balance report of the account holder. For example a group of customers (Family members or business partners) have a joint account each of them are provided with a card by which they can access the terminal separately and independently.

Authentication (Stallings, 2005) is the security service by which the electronic systems may securely identify the users. These authentication systems will answer the questions such as who is using the system and whether they are genuine users or not. In order to verify the identity of a user, the authenticating system typically challenges the user to provide his unique information and if the authenticating system can verify that the response given by the user was correct, the user is considered authenticated.

In conventional ATMs (Yanez and Gomez, 2004), the user authentication is either possession based (ATM card or smart card) or knowledge based (Personal Identification Number or password) or both. In these cases many difficulties are faced such as the cards may be lost, simple PINs can be guessed or complex passwords can be forgotten. Also banks face a multitude of problems at ATMs concerning authentication of a group of customers who have joint accounts. Usually each member will be provided with a separate ATM card and the same can be used for further transactions. First, many people have problems memorizing their PIN and pick either trivial PINs or write them on the ATM card and their partners can misuse them. Also the attacks like shoulder surfing, card cloning and card skimming are made directly onto the customers. There are many incidents of fraud by man-in-the-middle attacks, in which the hackers will attach fake keypads or card readers to the machine and record the customers' PINs and other card information to access their accounts illegally.

Biometrics (Jain *et al*., 2008) refers to the methods for uniquely recognizing human based upon one or more intrinsic physical and behavioral traits. Also, biometrics is a distinctive characteristic of human beings which is more reliable indicator of identity than other traditional authentication systems (Tian *et al*., 2006).

The best biometric that can easily be deployable is fingerprint recognition (Maltoni *et al*., 2003) and face recognition (Li and Jain, 2005) as these biometric have been successfully deployed in much civilian identification for years. Biometrics can't be plagiarized, stolen or forgotten and faking is practically impossible. It is a natural identity tool that gives greater security and suitability than traditional methods. Although biometric technology has more advantages it also has many security and privacy concerns as given below: biometrics

Corresponding Author: B. Shanthini, Department of IST, Anna University, Chennai, India

is authentic but not undisclosed, it cannot be cancelled or revoked, if a biometric is lost once, it is compromised forever.

To overcome these disadvantages, instead of using a single biometric, multimodal biometrics (Ross *et al*., 2006) which may have the combinations of different biometric like fingerprint, face, teeth, iris, handwriting and voice (Kim and Hong, 2008; Humm *et al*., 2009; Rubesh Anand *et al*., 2010; Komninos *et al*., 2007) or biometrics combined with challenge-response method (Chen *et al*., 2012) like password can be used for the security system. But if the original biometric is used as such privacy of the biometric is affected and so a set of features are extracted from them and applied in authentication process. Also genetic two-point crossover operator is used to randomize the feature set to obtain a revocable feature set so that if a biometrics is compromised, it can be simply reenrolled using another genetic operator and thus the revocability and privacy of the biometrics is preserved.

For these reasons a secured efficient authentication system is proposed which comprises both group authentication and individual authentication separately. Group authentication can precede individual authentication, in order to increase security and protect users' identities. Facial images are used for authenticating the group of customers and fingerprint images are used for individual user's authentication in the proposed system.

AUTHENTICATION IN ATM

A few research works that has been done for authentication in ATMs are briefly presented here. An Automated Teller Machine (ATM) is a safety-critical and real-time system that plays an increasingly important role in the life style of many human since it has a number of services which facilitate its customers. At the same time authentication plays a vital role in the successful implementation of ATMs. So, to increase security Mohammed *et al*. (2002) proposed two authentication protocols which used asymmetric encryption algorithms to encrypt the information shared by the User and that cipher is transmitted to the Bank. In these protocols, ATM terminal simply acted as the middleman and forwarded messages to and from User and Bank. But since these two authentication protocols are not using any timestamp or sequential number these are easily attacked by replay attacks as explained by Raphael and Phan (2003).

Biometrics systems are highly accurate and use a part of one's body and now it become the ideal

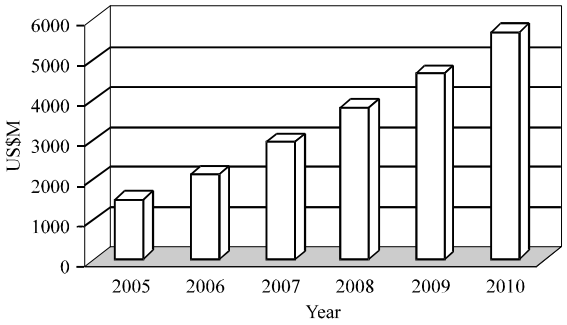


Fig. 1: World biometric market size (Hashimoto, 2006)

answer to these heightened security needs in ATM applications and are already being adopted worldwide. According to the factsheet of the International Biometrics Group (IBG), the world biometrics market reached US$5.7 billion by 2010 (Hashimoto, 2006) as shown in Fig. 1.

To gain the advantages of biometrics Yanez and Gomez (2004) developed a model which integrated biometric technology on ATMs by utilizing the existing infrastructure and, therefore, minimize the investment on technology upgrade. That model integrated fingerprint biometric technology into the transaction authorization process in ATMs. The authorizing system software authorized the customer by instructing the biometric system to read and validate the fingerprint biometric and then entered into the ATM system. Since, it is possible that data obtained during biometric enrollment of the customers may be used in ways for which the enrolled individual has not consented storing the biometric as such is not advisable.

As far as security is concerned, privacy is the most important requirements and recently, a number of dynamic ID-based user authentication schemes have been proposed. However, most of those schemes have more or less weaknesses and/or security flaws. In the worst case, user privacy cannot be achieved since malicious servers or users can mount some attacks, i.e., server spoofing attack and impersonation attack, to identify the unique identifier of users and masquerade of one entity as some other. Shao and Chin (2012) analyzed two latest research works and demonstrated that they cannot achieve true anonymity and have some other weaknesses.

Privacy is the main concern for the biometric-based software too and for that reason Selvaraju and Sekar (2010) proposed an embedded crypto-biometric authentication scheme for ATM banking systems. In this scheme, cryptography and biometric techniques are fused together for person authentication to ameliorate the security level. The fingerprint feature templates are stored

at the central banking server during enrolment. At the time of transaction fingerprint image is acquired at the ATM terminal and is encrypted using 128 bit AES algorithm. The encrypted image is transmitted to the server at the banking central server and the image is decrypted using the same AES key. From the decrypted image, minutiae extraction and minutiae matching are done and the presented fingerprint image is verified with the stored information and by that way authentication is ensured.

Peter *et al.* (2011) proposed a system which uses face recognition technique for verification in ATM system. This face biometric methodology in this study established the analysis framework with PCA algorithms for each type of images that the face recognition started with a picture, attempting to find a person in the image and it included movement, different skin tones and blurred human shapes. But the main issues in implementing security measures in ATM systems are replay attacks and group authentication. The study discussed above did not take any measures in solving these problems and our proposed system tries to solve these.

PROPOSED SYSTEM

In the proposed Privacy-protected Multimodal Biometric-based Group Authentication Scheme for ATM (PMBGAA), two biometric say, fingerprint and face are used to provide individual and group user authentication. This system not only authenticates the users but also protects the privacy of the users' biometric and resolves the replay attack problems. Our proposed biometric-integrated ATM system has Webcam and Fingerprint Reader along with the other traditional parts of ATM as shown in Fig. 2.

Steps involved in the proposed scheme are explained as follows:

Step 1: Enrolment: The group of users who have joint account in a financial institution should enrol their biometric say fingerprint and facial images in the concerned branch while applying. Their sample fingerprints biometric are captured using the fingerprint biometric sensor and their facial images are captured using webcams

Step 2: Pre-processing: These samples are not stored in the database as such instead the fingerprint images are undergone pre-processing processes and the fingerprint features are extracted and stored. At the same time the facial images of the group of users are trained by using the eigenface-based recognition system and the eigenfaces as well as the mean face are generated. This eigen mean face will be stored in database along with their original facial images

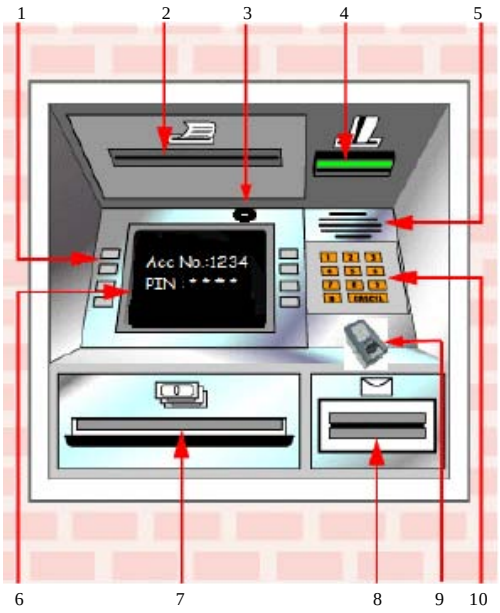


Fig. 2: Overview of the proposed biometric-integrated ATM system, 1: Screen buttons, 2: Receipt printer, 3: Webcam, 4: Card reader, 5: Speaker, 6: Display screen, 7: Cash dispenser, 8: Deposit slot, 9: Fingerprint reader, 10: Keypad

Step 3: Authentication: This process includes a general verification of the account number and the Personal Identification Number (PIN), group authentication using face biometric and then the individual authentication using fingerprint biometric

Enrolment of biometric and pre-processing

Face biometrics: Group authentication is done by the face biometrics of the users and the proposed model use Eigen face-based facial recognition algorithm for verification. In this process, a color based technique is implemented for detecting human faces in images. First, skin regions are separated from non-skin regions and then the human face within the skin regions is located, cropped and normalized. Once all the images are normalized the eigenfaces are generated and from that the mean image is created as explained by Shanthini and Swamynathan (2011a). The sample face images of four business partners belonging to one group are given in Fig. 3. The cropped face training set, normalized training set, eigenfaces and their mean image are shown in Fig. 4a-d, respectively. This mean image is stored in the central server for further verification.

Fingerprint biometrics: In this proposed model PMBGAA, fingerprint images of the customers belonging

Fig. 3: Sample face image database

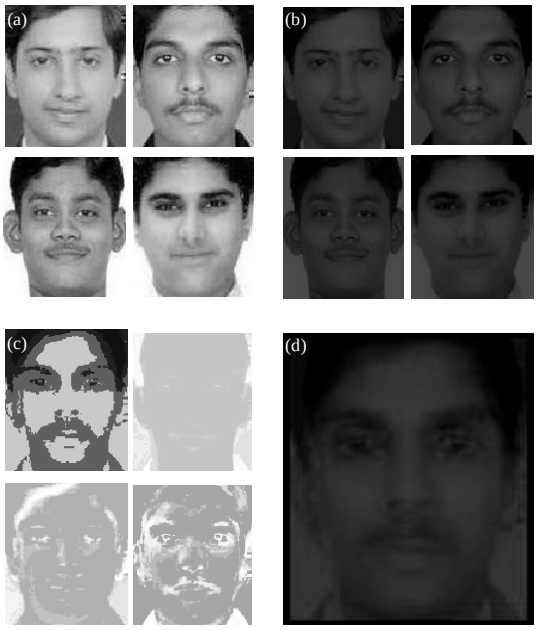


Fig. 4(a-d): Images of cropped faces (a) Training set, (b) Normalized training set, (c) Eigenfaces and (d) Mean image

to a group are acquired using fingerprint sensor. These images are preprocessed as explained by Shanthini and Swamynathan (2011b). These steps involved normalization of the images, enhancement, binarization, finding the orientation field map and region of interest, thinning, removal of H breaks, removal of spikes and finally after removing the spurious minutiae the actual fingerprint features are extracted. Figure 5 shows the different pre-processing steps and how the features are extracted from the fingerprint image.

This extracted fingerprint features are stored in the financial institution's central database. During verification process of the individual user the same fingerprint features in the central database are used.

Authentication process: Authentication process includes three steps:

Step 1: Initially the customer has to enter his/her joint account number and PIN which is provided by the bank using the key pad of the ATM. This personal information are sent to the central server and verified with the database. If verification is positive then its corresponding mean image and fingerprint feature set are identified for further verification

Step 2: After this general verification, the user is instructed via the ATM screen to take a snap of him/her using the webcam attached with the ATM. This facial image is transformed into its Eigen face component (Shanthini and

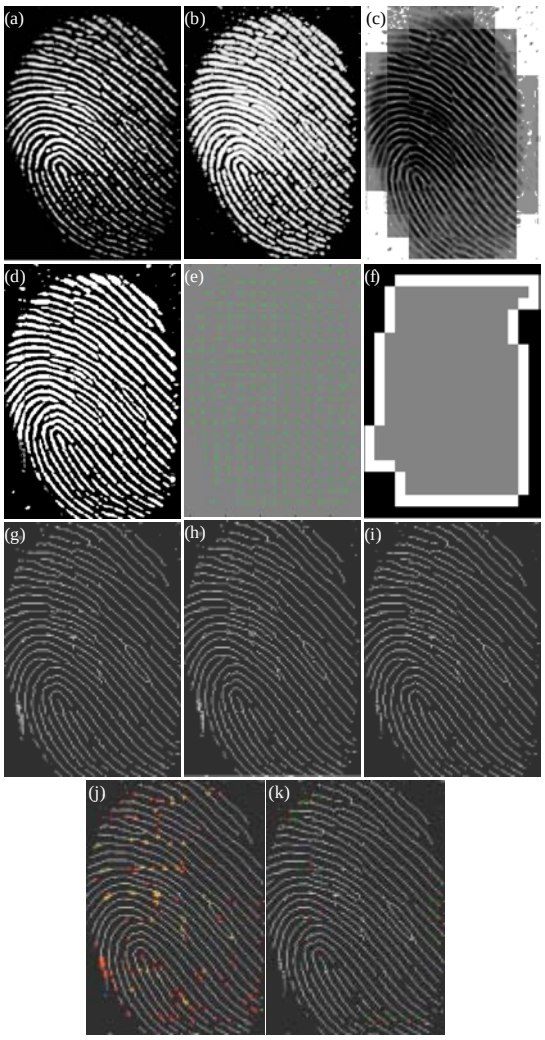


Fig. 5(a-k): Fingerprint pre-processing and minutiae extraction of (a) Original image, (b) Normalized image, (c) Enhanced image, (d) Binarized image, (e) Orientation field map, (f) Region of interest (g) Thinned image, (h) Removal of H breaks, (i) Removal of spikes, (j) Extracted minutiae, and (k) Removal of spurious minutiae

Swamynathan, 2011a) and transmitted to the central server system. Then this image is compared with the mean image stored in the database using Eigen face-based recognition system as explained (Shanthini and Swamynathan, 2011b) and verified. By this way, group is authenticated using facial biometric

Step 3: Once the user is recognized as a member of the group, then for verifying the individual authenticity fingerprint biometrics is used. The user is allowed to take the fingerprint sample using the fingerprint reader installed in the ATM and also the current timestamp value is stored in the system. Then the fingerprint image is pre-processed, the features are extracted and a genetic two-point cross over operation is applied to the features with this stored timestamp

The resultant bits and the timestamp are sent through the secured channel to the central server where all biometric databases say mean image database and fingerprint features database are kept. Finally, the same genetic operation is done in the central server and the features of the individual is verified. In this way individual authentication is done and at the same time by the usage of timestamp this scheme resolves the problem of replay attacks.

The steps involved in the proposed PMBGAA system are shown in the Fig. 6. It shows how enrolment and pre-processing of the biometric are done and how group authentication and individual authentication is verified using facial biometric and fingerprint biometric are shown.

The fingerprint features extracted from the input image is not sent as such instead a cancelable form of it is

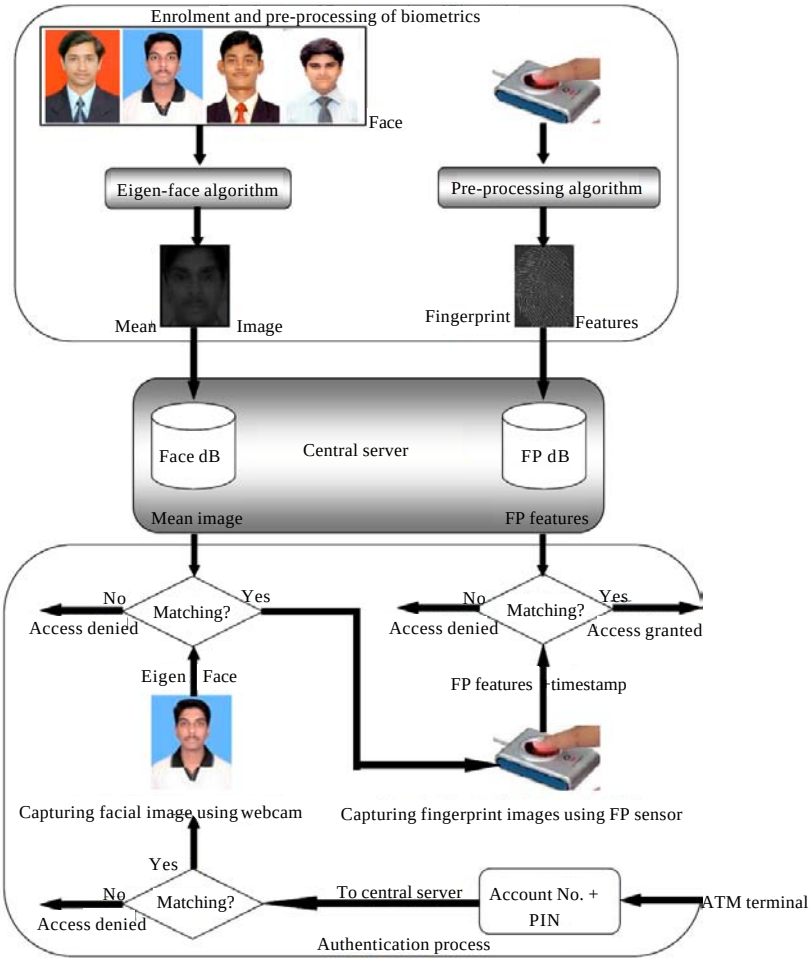


Fig. 6: Steps involved in the proposed system

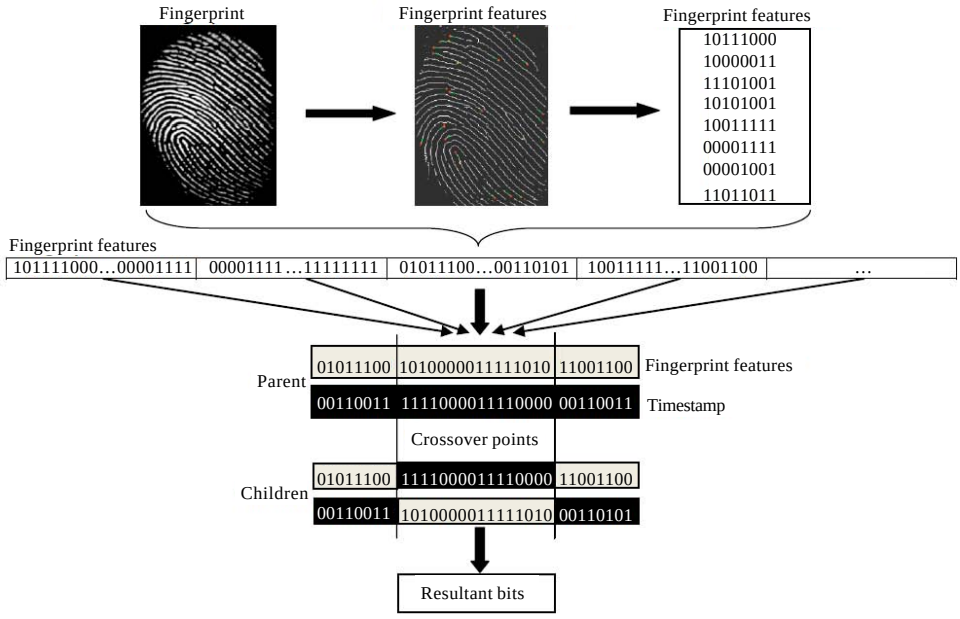


Fig. 7: Two-point crossover operation on fingerprint feature set and timestamp

generated by applying genetic two-point crossover operation onto the features and the timestamp as shown in Fig. 7 and the resultant bits and timestamp are sent to the central server for verification. By this way replay attack is evaded.

SECURITY ANALYSIS

Replay attack countered by PMBGAA: A replay attack occurs when an attacker copies a stream of messages between two parties and replays the stream to one or more time. Unless mitigated, the computers subject to the attack process the stream as legitimate messages, resulting in a bad consequences, such as redundant authentication. Suppose Alice wants to access the services of a Bank, the Bank requests her proof of identity which Alice dutifully provides. Meanwhile, Bob is eavesdropping on the conversation and keeps the secret information. After the interchange is over, Bob posing as Alice connects to Bank; when asked for a proof of identity, Bob sends Alice's information read from the last session which Bank accepts. By that way the services of the Bank can be accessed by intruders.

To avoid replay attacks the following countermeasures may be used:

- **Session tokens:** A session token or ID is typically granted to a visitor on his first visit to a site. It is typically short-lived and may become invalid after a certain goal has been met
- **One-time passwords:** These are similar to session tokens in that the password expires after it has been used or after very short time. They can be used to authenticate individual transactions in addition to sessions
- **Nonce:** It is an arbitrary number used only once to sign a cryptographic communication
- **Timestamp:** It is a sequence of characters, denoting the date or time at which a certain event occurred. Timestamps are typically used for logging events or in a sequence of events, in which case each event in the log or SOE is marked with a timestamp

In the proposed PMBGAA system, the replay attack is prevented by using the timestamp. For the individual authentication, the fingerprint image is read by the fingerprint sensor installed in the ATM and the current timestamp is stored in the system. Then the features are extracted from the input image and are combined with the timestamp by applying two-point crossover operation as shown in Fig. 7 and the resultant bits are sent to the central server for verification along with the timestamp. Every time the timestamp is also verified by the central system and by this way replay attack is evaded completely by this scheme.

Analysis on face recognition system: For a new face input say 'k' to be verified, as explained by Shanthini and Swamynathan (2012) after finding the average weight vector Ω and kth facial image's weight vector Ω_k, the Euclidean distance is calculated for this kth face by using the formula 1:

$$\varepsilon_k = \|\Omega - \Omega_k\|^2 \quad (1)$$

If this Euclidean distance is less than a threshold value θ, then the input face is classified as 'known' and if this distance is greater than the threshold value then the image may be classified as 'unknown' (Turk and Pentland, 1991) In this experiment a face library that contained nearly 160 face images, 80 genuine users and 80 fake users was used. All members of genuine users were grouped into 4 groups and they were in the training set. Then, the Euclidean distance of every member of the face library was found out and verified.

Figure 8 shows an example of 4 groups of users, 2 business groups and 2 family groups, each containing 4 members. From the Fig. 8 it is understood that the threshold value found is 300 and it is seen that all genuine members were classified 100% correctly and all fake members were not classified as genuine members by this algorithm (Shanthini and Swamynathan, 2012).

An AdaBoost-based face detection system proposed by Xiao *et al*. (2012) who used a new hardware-software partition method and the whole face detection system is divided into several parallel tasks implemented on two Reconfigurable Processing units and one micro Processors unit. Implementation results show that the detection rate was over 95% which is less than our proposed approach.

Analysis on combined face and fingerprint recognition system: The system was tested using the fingerprint images of FVC 2004 database (http://Bias.Csr.Unibo.It/Fvc2004/). The database was developed using optical sensor, the image size is 640×480 pixels and resolution is 500 dpi. The database contains a total of 160 fingerprint images.

The accuracy of the system is quantified for different combinations of face and fingerprint images in terms of Genuine Rejection Rate (GRR), Genuine Acceptance Rate (GAR), False Rejection Rate (FRR) and False Acceptance Rate (FAR). These basic error measures of a verification system are defined in the following equations:

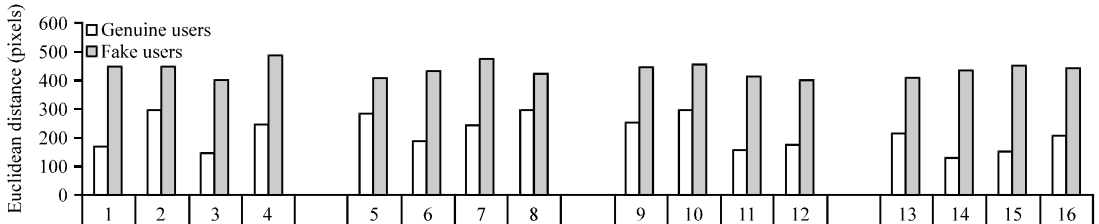
Genuine rejection rate (GRR $_i$): It is an average of number of genuinely rejected transactions. If n is a transaction and x(n) is the verification result where, 1 is genuinely rejected and 0 is genuinely accepted and N is the total number of transactions then the Genuine Rejection Rate for user i is given by Eq. 2:

$$GRR_i = \frac{1}{N}\sum_{n=1}^{N} x(n) \quad (2)$$

Genuine acceptance rate (GAR $_i$): It is an average of number of genuinely accepted transactions. If n is a transaction and x(n) is the verification result where, 1 is a genuinely accepted transaction and 0 is falsely accepted transaction and N is the total number of transactions then the personal Genuine Acceptance Rate for user i is Eq. 3:

$$GAR_i = \frac{1}{N}\sum_{n=1}^{N} x(n) \quad (3)$$

False rejection rate (FRR $_i$): It is an average of number of falsely rejected transactions. If n is a transaction and x(n) is the verification result where, 1 is falsely rejected, 0 is falsely accepted and N is the total number of transactions then the personal False Rejection Rate for user i is Eq. 4:



	1	2	3	4		5	6	7	8		9	10	11	12		13	14	15	16
Genuine users	175	300	153	249		286	197	251	300		257	300	161	177		217	135	158	207
Fake users	453	449	406	488		412	436	476	426		444	456	415	402		410	434	452	442
	Business group 1					Business group 2					Business group 3					Business group 4			

Fig. 8: Recognition of genuine and fake users using Euclidean distance

$$FRR_i = \frac{1}{N}\sum_{n=1}^{N} x(n) \quad (4)$$

False acceptance rate (FAR $_i$): It is an average of number of falsely accepted transactions. If n is a transaction and x(n) is the verification result where, 1 is a falsely accepted transaction and 0 is genuinely accepted transaction and N is the total number of transactions then the personal False Acceptance Rate for user i is Eq. 5:

$$FAR_i = \frac{1}{N}\sum_{n=1}^{N} x(n) \quad (5)$$

The maximization of true events (GAR, GRR) and minimization of error events (FAR, FRR) are the signs of an efficient algorithm. As a result of our proposed approach PMBGAA, a FAR of 1.25% was obtained for an FRR of 2.5% whereas GAR and GRR was 100% for the used database.

CONCLUSION AND FUTURE WORK

Although, biometrics is a very promising technology, challenges are slowing its development and deployment. Fingerprint images and face images are chosen due to their unique physiological traits. In the proposed system, as the first verification if the Personal Identification Number which is entered along with the account number is not correct then the next stage of verification say group authentication is not done. After crossing the first stage if the facial image of a user is not recognized as a member of the group he is not allowed to proceed with the individual authentication. Also if there is any mismatch in the fingerprint biometric the entire conversation is disapproved and banned. Also replay attack is avoided by using timestamp. The same authentication system may be used for a single user also by adding his/her facial and fingerprint images into a random group during enrolment and applying the same procedure as explained. By these steps, an efficient and secured authentication system which has three-factor authentication in ATMs is brought out.

REFERENCES

Chen, C.L., C.L. Lee and C.Y. Hsu, 2012. Mobile device integration of a fingerprint biometric remote authentication scheme. Int. J. Communi. Syst., 25: 585-597.

Hashimoto, J., 2006. Finger vein authentication technology and its future. Proceedings of the Symposium on VLSI Circuits, Digest of Technical Papers, June 15-17, 2006, Honolulu, HI., USA., pp: 5-8.

Humm, A., J. Hennebert and R. Ingold, 2009. Combined handwriting and speech modalities for user authentication. IEEE Trans. Syst. Man Cyber. A., 39: 25-35.

Jain, A.K., P. Flynn and A. Ross, 2008. Handbook of Biometrics. Springer, USA., ISBN: 9780387710419, pp: 1-22.

Kim, D.S. and K.S. Hong, 2008. Multimodal biometric authentication using teeth image and voice in mobile environment. IEEE Trans. Cons. Electron., 54: 1790-1797.

Komninos, N., D.D. Vergados and C. Douligeris, 2007. Multifold node authentication in mobile ad hoc networks. Int. J. Communi. Syst., 20: 1391-1406.

Li, S.Z. and A.K. Jain, 2005. A Book of Face Recognition. 1st Edn., Springer, New York, USA.

Maltoni, D., D. Maio, A.K. Jain and S. Prabhakar, 2003. Handbook of Fingerprint Recognition. Springer, New York, USA., Pages: 348.

Mohammed, L.A., A.R. Ramli, V. Prakash and M.B. Daud, 2002. Building secure transactions with smart cards. Proceedings of the 2nd World Engineering Congress, ICT Conference, July 22-25, 2002, Kuching, Malaysia, pp: 356-360.

Peter, K.J., G. Nagarajan, G.G.S. Glory, V.V.S. Devi, S. Arguman and K.S. Kanna, 2011. Improving ATM security via face recognition. Proceedings of the 3rd International Conference on Electronics Computer Technology, April 8-10, 2011, Kanyakumari, India, pp: 373-376.

Raphael, C. and W. Phan, 2003. Attacks on ATM authentication protocols proposed at WEC2002. Proceedings of the 3rd International Conference on Information Technology in Asia/CITA'03, July 17-18, 2003, Kuching, Malaysia, pp: 275-227.

Ross, A.A., K. Nandakumar and A.K. Jain, 2006. Handbook of Multibiometrics. 1st Edn., Springer, New York, USA.

Rubesh Anand, P.M., G. Bajpai and V. Bhaskar, 2010. 3D signature for efficient authentication in multimodal biometric security systems. IACSIT Int. J. Eng. Technol., 2: 177-184.

Selvaraju, N. and G. Sekar, 2010. A method to improve the security level of ATM banking systems using AES algorithm. Int. J. Comput. Appl., 3: 5-9.

Shanthini, B. and S. Swamynathan, 2011a. A secure authentication system using multimodal biometrics for high security MANETs. Proceedings of the 1st International Conference on Advances in Computing and Information Technology, July 15-17, 2011, Chennai, India, pp: 290-307.

Shanthini, B. and S. Swamynathan, 2011b. A secured authentication system for MANETs using voice and fingerprint biometrics. Eur. J. Sci. Res., 59: 533-546.

Shanthini, B. and S. Swamynathan, 2012. Multimodal biometric-based secured authentication system using steganography. J. Comput. Sci., 8: 1012-1021.

Shao, M.H. and Y.C. Chin, 2012. A privacy-preserving dynamic ID-based remote user authentication scheme with access control for multi-server environment. IEICE Trans. Inform. Syst., E95: 161-168.

Stallings, W., 2006. Cryptography and Network Security: Principles and Practice. 4th Edn., Prentice Hall, New Jersey, ISBN: 0130914290.

Tian, J., L. Li and X. Yang, 2006. Fingerprint-based identity authentication and digital media protection in network environment. J. Comput. Sci. Technol., 21: 861-870.

Turk, M. and A. Pentland, 1991. Eigenfaces for recognition. J. Cognitive Neurosci., 3: 71-86.

Xiao, J., J. Zhang, M. Zhu, J. Yang and L. Shi, 2012. Fast Adaboost-based face detection system on a dynamically coarse grain reconfigurable architecture. IEICE Trans. Inform. Syst., E95: 392-402.

Yanez, M. and A. Gomez, 2004. ATM and biometrics: A sociotechnical. Business Model P7-9, University of Miami, School of Business Administration.