International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.04, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

MULTI-MODULAR BIOMETRICS IN ATM TRANSACTIONS - A REVIEW

Moazam Farhan Banday[1], Mahroosh Banday[2]

[1]*Student (B.Tech.), Department of Computer Science Engineering, BGSBU, Rajouri*

[2]*Research Scholar, Department of Electronics and Communication Engineering, National Institute of Technology, Srinagar*

ABSTRACT

Biometric recognition systems provide a reliable personal recognition schemes to either confirm or determine the identity of an individual. Biometric systems are used widely to recognize individuals and control access to information, services, physical spaces, and to other rights or benefits, including the ability to cross international borders. Biometrics help in improving the convenience and efficiency of routine access transactions, reducing fraud, and enhancing public safety and national security. Applications of such systems also include computer systems security, secure electronic banking, mobile phone access, credit cards, secure access to offices, social and health services. By using biometrics, a person could be identified based on "who he/she is" rather than "what he/she has" (card, token, key) or "what she/he knows" (password, PIN, pattern). This paper outlines opinions about the usability of biometric authentication systems, comparison between different techniques, limitation, and their advantages and disadvantages with new and innovative model for biometric Automatic Teller Machines which replace card system by biometric technology for operating them. This proposed model provides high security in authentication which also protects end user from unauthorized access to his/her bank account by authenticating himself with a biometric identification (Fingerprint/Iris etc.), Personal Identity Number (PIN) and selection of bank, branch and account thus saving cost, time, and labour in comparison with card based ATMs and solves the problem of environmental pollution caused due to the excess number of plastic cards as the person is not required to carry multiple ATM cards along with himself as all his bank accounts will be linked to his biometric identity (Fingerprint, Iris etc.). This method will also help the people who don't know how to access ATMs with cards and also who feel it bulky to carry multiple cards with them and even saving on their time. This method will also prevent frauds in banking as the customers can be carefree about the loss of their ATM cards or their duplicity by hackers etc. as no physical equipment would be required by the customer except his own self which will also enhance the portability.

Keywords: Biometrics, Fingerprint Recognition, Multi-modular ATM security, Verification, Identification, Security, ATM

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.04, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

I INTRODUCTION

Biometrics is a term that refers to metrics related to human characteristics. Biometrics authentication is used as a form of identification and access control mechanism [1]. It may also be used to identify individuals that are under surveillance.

Biometric identifiers are used to automatically recognize individuals on the basis of their distinctiveness and their measurable characteristics [2]. Biometric identifiers are often divided into two categories as physiological and behavioural characteristics [3]. Physiological characteristics are related to the shape of the body such as fingerprint, iris recognition, face recognition, palm veins, palm print, and retina. Behavioural characteristics are related to the pattern of behaviour of a person, like typing rhythm, gait [4], and voice.

Some traditional means of access control include token-based identification systems, such as a driver's license or passport, credit/debit cards and knowledge-based identification systems, such as a password or personal identification number (PIN) [2]. Since biometric identifiers are distinct to every individual, they are more reliable in verifying identity than token and knowledge-based methods [2].

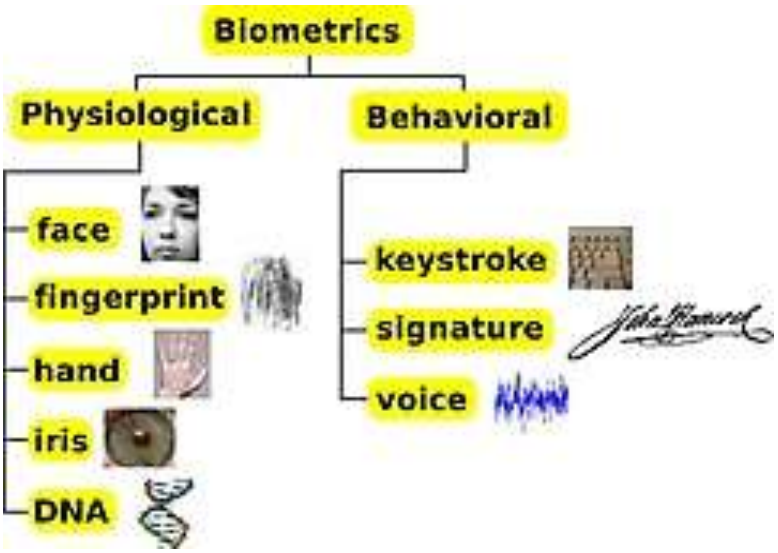


Fig. 1. Division of biometrics [7]

II AUTOMATIC TELLER MACHINE(ATM):

Automatic Teller Machine(ATM) provides customers with the convenient banknote trading. However, the financial crime caseshave risen largely in recent years; a lot of criminals tamper with the ATM terminal and steal user's credit/debit card and PIN by illegal means usually called ATM skimming. Moreover, if user's bank

card is lost and the PIN is stolen, the criminals/thieves can draw all cash in the leasttime, bringing heavy financial losses to the customers. Traditional ATM systems generally authenticate by using the credit/debit card and the PIN, the method has some limitations. Using credit card and PIN cannot verify the client's identity exactly. In recent years, the algorithms for biometric recognition are continuously updated and creating binary code by the controller has offered advanced level of security. Theprevailing PIN authentication method coalesced with the biometric identification technology help in verifying the customer's identity better and achieve the purpose of using ATM machines more safely and effectively [6].

2.1 ATM Card Frauds and Risks: [8]

There are a number of risk factors that accompany the use of ATM cards, the primary being fraud.

There are five main types of debit/credit card frauds:

Card skimming: It remains the number one threat globally in which a thief installs a machine or camera at an ATM in order to pick up card information and PIN numbers when customers use their cards.

In-person fraud: This type of fraud is committed when thieves steal your card and use it to make purchases at different merchants.

Online fraud: Online fraud occurs when your card information is compromised while making a transaction online. In this case, thieves could use card information to make online purchases or assume your identity.

ATM fraud: ATM fraud occurs when a thief is able to acquire your card and/or pin number and withdraw money from the machine.

Card Trapping: Trapping is the stealing of the physical card itself through a device fixed to the ATM.

All of the forms of fraud have a great impact on the victim, which is why consumers are advised to know the risks involved before using a debit/credit card.

2.2 Biometric ATMs

Accordingto Security Experts Automatic Teller Machine (ATM) in future will get biometric authentication techniques to verify customer's identity for transaction. In countries like japan and poland, many banks have introduced fingerprint technology as an embedded part of ATM systems, where customers use fingerprint in place of PIN or Password for general identification with their ATM cards.

Nowadays, there are devices meant for the purpose of biometric identification and authentication using fingerprint, hand, retina, iris, face, and voice which make the ATM transactions more secure. ATM transactions become more secure with biometric ATMs when compared with a card and PIN based system. Several ideas for biometric authentication have been mapped out by researchers which include different attributes such fingerprint, iris and retina, voice, face etc.A brief idea about several biometric technologies has been given below.

2.3 Fingerprint Verification:

Fingerprint scanning is the oldest and most commonly deployed biometric technology that utilize distinctive features of the fingerprint to identify or verify the identity of individuals which is used in a broad range of physical access and logical access applications. All fingerprints have unique characteristics and patterns which are made up of ridges and valleysthrough the pattern of which a unique fingerprint is matched for verification and authorization.

On average, a typical live scan produces 40 “minutiae” and according to a report submitted by Federal Bureau of Investigation (FBI), no more than 8 common minutiae can be shared by two individuals.

3 Hand/Palm scanning:

Hand/palm scanning involves the verification or identification of an individual by reading his/her palm/hand for access. It identifies people based on the pattern of veins in their palms, which are as distinctive as fingerprints. It uses a contactless device which requires a person to hold his/her hand over the sensor, so it's hygienic and easy to use. The system must detect blood flowing through the veins before it will issue an authorization to avoid frauds.

4 Voice Recognition:

This technique involves prerecording of words, numbers etc. in the voice of a customer for enrolment purpose. Once enrolment is done, a person is asked to say some words which match the voice print of his original pre-recorded voice and is thus given access to his account.

5 Retina scanning:

This technique identifies unique patterns of the blood cells of retina of the customers. retinal scanning devices are the most accurate physical biometric available today as there are no known ways to replicate retina because of the fact that the network of blood vessels in the retina is not entirely genetically determined and hence, even identical twins don't even share same pattern of blood vessels.

6 Iris scanning:

Iris scanning is type of biometric system related to eye. iris scan involves the scans analysing the features that exist in the coloured tissue surrounding the pupil of the eye. It requires a camera to capture image of coloured portion of eye outside the pupil and doesn’t need any intimate contact between user and the reading device.

7 Facial Scanning:

Facial recognition involves analysing the characteristics of a person's face. Access is only granted if the face matches the one already stored in the database at the time of enrolment. A person needs to stand in front of a camera, usually standing about two feet from it such that the overall facial structure including distances between eyes,nose, mouth and edges of jaw are measured.

The comparison between different biometric technologies is given below:

Biometric Trait	Universa-lity	Unique-ness	Perman-ence	Collect-ability	Perfor-mance	Accept-ability	Circumven-tion
Iris	High	High	High	Medium	High	Low	High
Fingerprint	Medium	High	High	Medium	High	Medium	High
Retina	High	High	Medium	Low	High	Low	High
Keystroke Dynamics	Low	Low	Low	Medium	Low	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Face	High	Low	Medium	High	Low	High	Low
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Voice	Medium	Low	Low	Medium	Low	High	Low
Signature	Low	Low	Low	High	Low	High	Low
DNA	High	High	High	Low	High	Low	Low

Table 1. Comparison of Various Biometric technologies[9]

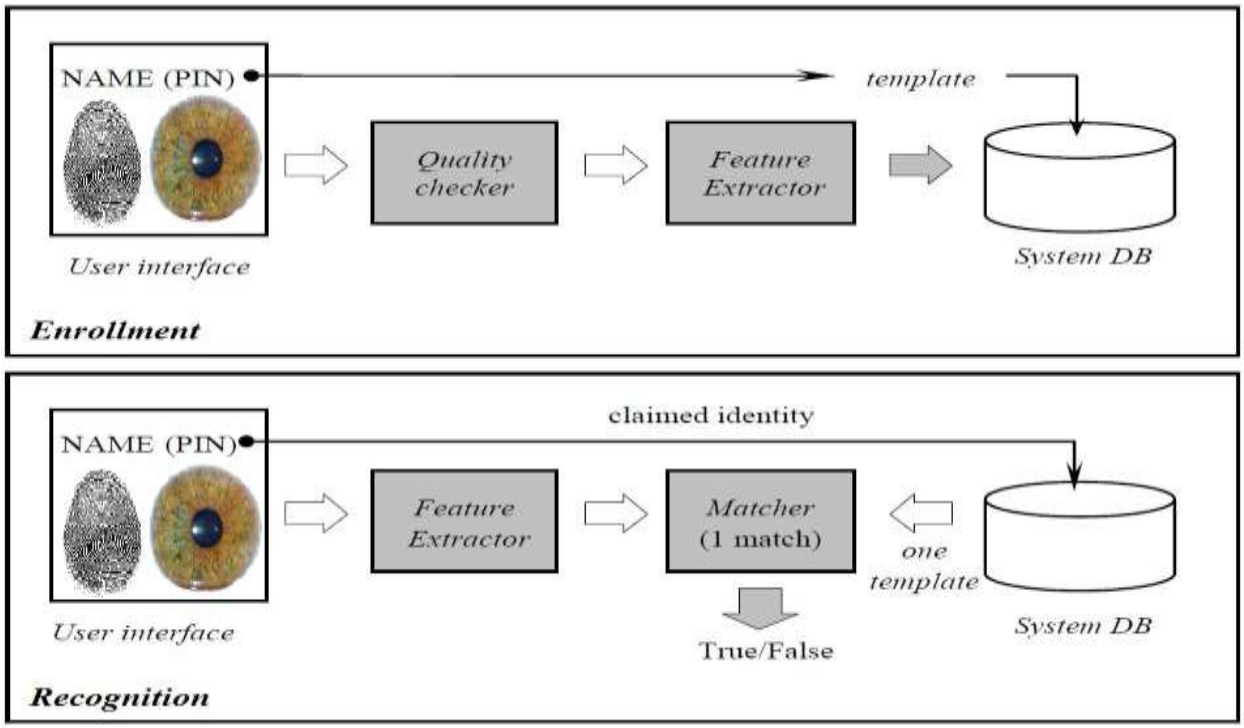
There is practically no universal 'best' biometric authentication system. However, the above table signifies that using fingerprint and iris for biometric authentication serve as the most favourable methods for secure ATM transactions. However,in some cases an individual may attempt to forge the biometric trait. This is particularly easy when signature and voice are used as an identifier. So, in order to remove the flaws in single module biometric system a multi-modular system can be used which integrates different information at various levels.

8 Multi-modular ATM Security

The flaws in the single module biometric ATMs were that in some rare cases an individual may forge the biometric identity of a person or he may abduct him/her after making the person unconscious. However, to overcome this difficulty a person is required to identify himself by his biometric traits preferably fingerprint and iris instead of his ATM card followed by the PIN associated with his identity. When both PIN and the biometric traits are matched from the database which holds the biometric identity and PIN while enrolment, the user gets the access to his account and hence overcomes the drawbacks of single module biometric security systems.

This system can be much effective as many banks these days have already embedded fingerprint scanners in their ATM machines but is not operational yet. This will also reduce the cost of installing new ATM machines as very little additional hardware would be required and software changes would be made. The flow of information in a multi-modular ATM security with fingerprint and PIN is shown below in the figure:

Fig. 2 Enrolment and Recognition phases in multi-modular biometric ATMs [10]



Enrolment:

During enrolment, a user's physical or behavioural trait is captured with a camera and sensor and placed in an electronic template along with the PIN. This template and PIN are securely stored in a central database.

Recognition:

During recognition, a sensor and camera captures a biometric trait. The trait is then analysed with an algorithm that extracts quantifiable features, such as fingerprint minutiae or iris pattern. A matcher takes these features and compares them to an existing template along with the PIN in the enrolmentdatabase. [10]

9 Conclusion

In the above proposed model, we lead to a conclusion that biometric ATMs are much more secure than traditional card and PIN based ATMs as they reduce the risks of thefts to a large extent as it is nearly impossible to copy a person's biometric trait. Moreover, if by any means, in a single module biometric security system a person manages to forge with his biometric identity, he won't be able to do that in a multi modular biometric ATM security system. Hence, multi modular biometric ATMs provide a robust way to prevent ATM frauds and keeping a bundle of ATM cards in wallet saving time and money.

REFERENCES

[1]. "Biometrics: Overview". Biometrics.cse.msu.edu. 6 September 2007. Archived from the original on 7 January 2012. Retrieved 2012-06-10.

[2]. Jain, A.; Hong, L. and Pankanti, S. (2000). "Biometric Identification". Communications of the ACM, 43(2), p. 91–98. DOI 10.1145/328236.328110

[3]. Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics". In Jain, AK; Flynn; Ross, A. Handbook of Biometrics. Springer. pp. 1–22. ISBN 978-0-387-71040-2.

[4]. Damaševičius, R.; Maskeliūnas, R.; Venčkauskas, A.; Woźniak, M. Smartphone User Identity Verification Using Gait Characteristics, Symmetry 2016, 8, 100.

[5]. D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, "Handbook of Fingerprint Recognition", Springer, London, 2009

[6]. PENNAM KRISHNAMURTHY MR. M. MADDHUSUDHAN REDDDY, Implementation of ATM Security by Using Fingerprint recognition and GSM, International Journal of Electronics Communication and Computer Engineering Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X pp-83-86.

[7]. http://misbiometrics.wikidot.com/

[8]. http://www.businessinsider.com/debit-cards-are-the-riskiest-form-of-payment-2012-1?IR=T

[9]. A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 4-19, January 2004

[10]. http://biometrics.cse.msu.edu/info/