Role of Biometric Technology over Advanced Security and Protection in Auto Teller Machine Transaction

Navneet Sharma, Vijay Singh Rathore

Abstract: ***In modern era, security is one of an important tool of each organization. If we talk about money it gives major importance. In the banking system, it is also a very confidential issue. The major issue in each bank to safeguard the public deposits and to provide better and effective liquidity. For this purpose, the ATM was developed to facilitate cash availabity to the consumers (public) in any time i.e. 24 X 7.***

The main object of ATM machines to keep safeguard of money and provide availability of cash very fast. But, in present era, there are several security problems arise in ATM's. The customers are very conscious about their funds and they afraid to use the machines. Over the last few years banking and Auto Teller Machine frauds increasing day by day. For banking financial operation user are now more dependent on ATM outside the bank premises .Mostly bank are providing the single (PIN) password authentication to their customers for ATM transactions but now a day it is not sufficient to protect the information and verify the authentic user. It is so easy for fraudsters to get the PIN and make fake operation on ATM. To protect these type of frauds bank can use dual user verification system so that banking operations make more safe. To make dual verification system we can use any biometric technology for security. In this paper, different biometric techniques related security topics regarding ATM has been discussed. An effort has been made to explain these issues in easy language in a layman style so a layman can understand it easily. in this paper list few biometric technologies which may use for dual authentication and user verification.

Key words: ***Auto Teller Machine, Biometric, Fingerprint, Iris, PIN, Vein Pattern.***

I. INTRODUCTION

Automated teller machine is a mechanical device that allows the bank customers to carry out banking transactions like, deposits, transfers, balance enquiries, mini statement, withdrawal and fast cash etc. its final data maintained in the accounts and records of a banking system (server), ATM provides financial services to an increasing segment of the population in many countries. In to days fast life no one want to stand in long queues for banking operation, they don't want to wait for too long time before they are attended to and this has led to the increasing services being offered by banks to further improve the convenience of banking through the electronic banking. Crime at ATM"s has become a nationwide issue that faces not only customers, but also bank operators [1].ATM is a substitute outside the banking premises where customers can do various financial operations 24 x 7 without going to bank. but outside a bank premises Security measures play a critical, contributory role in preventing attacks on customers where no bank representative is available on ATM and customers can make a part of fraud. To protect customer ATM card and related its security there is a single PIN (password) but now a day it is no more safe. There are so many fraud cases and techniques by which hackers or fraudsters can hack the card and pin from the customers and get their funds using fraud transactions . We can protect the ATM data and make genuine transactions and protect customers using biometric user authentication so that hackers can not make unauthorized transactions. Biometrics based authentication is a technique to replace password-based authentication. biometrics, fingerprint based identification is one of the most usable technique. At the time of transaction fingerprint image is acquired at the ATM terminal using high resolution fingerprint scanner. Security measures at banks can play a critical, contributory role in preventing attacks on customers. Banks must set certain standards to ensure a safe and secure banking environment for their customers. This paper focuses on various types of biometric types to prevent the banking operations with unauthorized users. A biometric measure as a means of enhancing the security for banking system for both customer"s & bankers also. For dual security process costumers insert their card & PIN, if costumers insert valid PIN then access is grant to another security approved process i.e. biometric process. Using valid PIN & biometric verification costumer can access ATM transaction process i.e. deposits, transfers, balance enquiries, mini statement, Fast cash & withdrawal etc. By using biometric recognition customers are more comfortable with the idea of saving their money with the bank because they understand that if they lose their ATM card, no one can replicate their biometric clone and take their money.

In this paper we discuss some biometric uses to prevent the fraud at the time of ATM transaction a biometric measure as a means of enhancing the security for banking system for both customers & bankers also. Biometric authentication can be further divided into some different biometric options i.e. Fingerprint scanning, Face recognition, Iris scanning etc.

II. ATM AUTHENTICATION:

To continue the ATM operation we authenticate the valid identity of a customer using three different parameters:

a. What we have i.e. an ATM card
b. What we know i.e. a PIN code or a Password
c. What we are i.e. Biometrics it may be Fingerprint, Face, Iris etc.

We usually authenticate the user with combination of what we have and what *we know* but a password can be easily guess or can be trapped and an atm card can be lost or borrowed. But with a dual combination of three way authentication which is a card, a password and with the addition of biometric

Manuscript received on August 25, 2012

Navneet Sharma, Research Scholar Dept. of Computer Science and Engineering Suresh gyan Vihar University, Jaipur. Rajasthan, India.

Dr. Vijay Singh Rathore, Director Shri karni College, Jaipur Rajasthan, India

technique we can protect our ATM transaction more safely.

Biometric System:

A Biometrics system could be:

"Biometrics allow a customer (account holder) to be validate or authenticate using physical, behavioral attribute or their characteristics. These characteristics must be verifiable automatically".

The biometric authentication has the advantage of checking the user's personal attribute or characteristics. These characteristics can be physical ones such as fingerprints, face, iris or behavioral such as voice, handwritten signature, keyboard tapping etc. This leads to a possible split in the usually called what we are i.e physical Biometrics and what we do i.e. behavioral Biometrics. Behavioral characteristics are less stable than physical characteristics.

Working of biometric system:

To authenticate the user in biometric system first we have to capture the data through sensors then we remove the other artifacts from the sensor to improve the input data quality. After this it compare the previously stored pattern with new scanned pattern .if the old pattern matched with new scanned pattern then it allows user to process the operation.

We can divide the biometric authentication in two different areas:

I. Physical

II. Behavioral

Table - 1

Physical	**Behavioral**
Fingerprint	Handwriting Signature
Face recognition	Handgrip dynamics
Retina	Voice dynamics
Iris	Lips dynamics
Voice	Gait
DNA	
Ear Shape	

In the above table there are few biometric recognition patterns are shown.

Fingerprint Recognition

Fingerprint recognition is based on the imaging of the fingertips. The structure of a fingerprint's ridges and valleys is recorded as an image or digital template (a simplified data format, minutiae-based most of the time) to be further compared with other images or templates for authentication or verification, see

Figure 1 Images of fingertips are captured with specific fingerprint sensors.

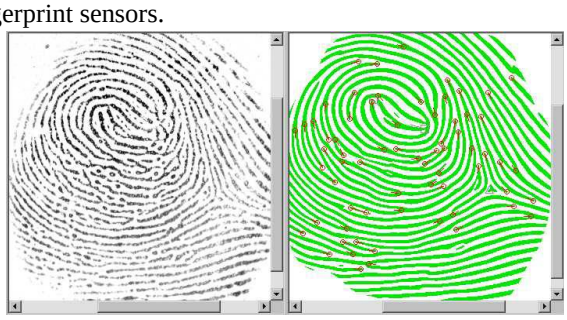

Figure 1

Among all the biometric techniques, fingerprint-based identification is more popular method which has been successfully used with ATM user authentication. A fingerprint is a set of skin lines, locally parallel, named *ridges* and empty space between two consecutive ridges named *valleys*. The three global shapes of this pattern, divided in arches, loops and whorls, are the first level of information we may examine to classify fingerprints. The average value of ridge to ridge frequency is of about half a millimeter and the average value of valley to ridge height is of about 0.1mm. By convention, the fingerprint image is displayed as the trace the inked finger would leave on a paper, or, in other words, as the latent print of the finger. Of course this first level information is useless to proceed with fingerprint verification [2].

The second level of information is *minutiae*. These are specific points of the Fingerprint where a ridge is ending or bifurcating. Tens of such points may be extracted from a fingerprint, and are enough to proceed with reliable fingerprint verification. This is the way by which authentication process can be done to check the authenticity of the user.

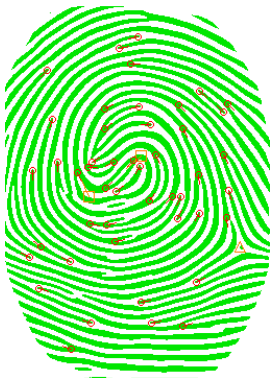

Figure 2

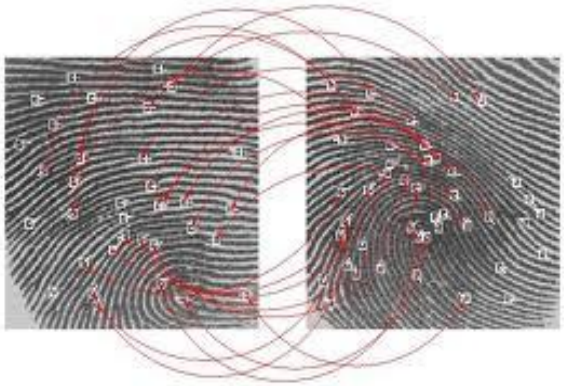

Figure 3

Criminal sciences have been conducting fingerprint identification for more than one hundred years. Other, but not sufficient, second level information are *core(s)* and *delta(s)* location, The pattern of ridges and valleys, with its minutiae, core(s) and delta(s) are unique to each individual (different even for identical twins) and this pattern is known to be stable during the lifetime. The third level information is *pores* location along the ridges. The use of pores location is young, and coming with the improvement of new generation fingerprint sensors, able to capture such details [4]. As of today, fingerprint recognition algorithms using this technique

are not mature enough to replace minutiae-based ones.

Iris/Retina Recognition

User authentication based on the eye splits in two families:

1- Iris recognition is based on the extraction of representative data from the externally visible colored ring around the pupil, whereas
2- Retina recognition is based on the analysis of the blood vessel pattern located in the posterior portion of the eye.

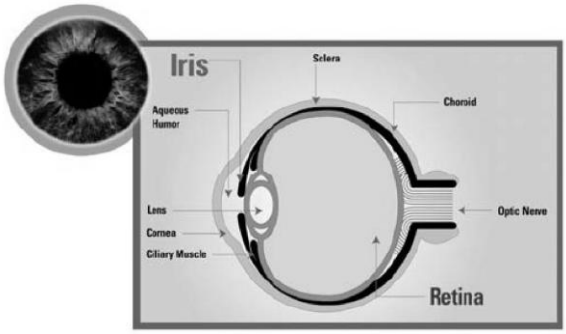

Figure 4

The automated method of iris recognition is relatively young, existing in patent only since 1994. The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. The color is based on the amount of melatonin pigment within the muscle. Iris imaging requires use of a high quality digital camera. Today's commercial iris camera typically use near infrared light to illuminate the iris without causing harm or discomfort to the customer.

III. VEIN PATTERN RECOGNITION

The Vein Pattern technology works on identifying the subcutaneous (beneath the skin) vein patterns in an individual's hand. When a user's hand is placed on a scanner, a near-infrared light maps the location of the veins.

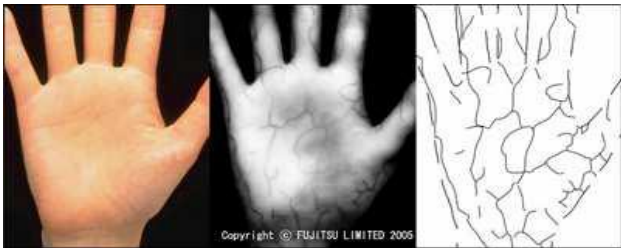

Figure 5

The red blood cells present in the veins absorb the rays and show up on the map as black lines, whereas the remaining hand structure shows up as white. After the vein template is extracted, it is compared with previously stored patterns and a match is made.

Face Recognition

Face recognition is based on the imaging of the face. Structure of the face is recorded as an image or digital template a plenty, non-mature, simplified data formats for further comparison. Early face recognition algorithms used simple geometric models,

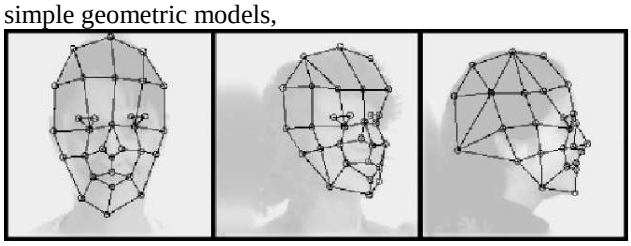

Figure 6

But the recognition process has now moved into a science of sophisticated mathematical representations and matching processes. Major advancements and initiatives in the past ten years have propelled this technology into the spotlight.

The authentication process is a comparison between a preregistered reference image, or template (representative data extracted from the raw image, built during an registration step) and a newly captured candidate image, or template[3]. Depending on the correlation between these two samples, the algorithm will determine if the applicant is accepted or rejected. This statistical process leads to a False Acceptance Rate (FAR) i.e. the probability to accept a non-authorized [3]. User and a False Rejection Rate (FRR) i.e. the probability to reject an authorized user [4].

IV. CONCLUSION

In this paper we have discussed importance of dual verification process in present scenario for Auto teller Machine transaction and authenticate the user with dual recognition system .instead of using single authentication (PIN or password) in dual verification system (PIN and Biometric) is more safe. We can use any one of biometric system along with PIN verification with ATM card . using dual verification technique and protect the financial transaction more safe .further we can make more algorithms for user verification and make the financial operations outside the bank premises and protect the user accounts ,their authenticity in a better and safe process.

REFERENCES

1. Richard, B.and Alemayehu, M. (2006) Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons. *Journal of Internet Banking and Commerce*, August 2006, vol. 11, no.2.
2. Davide Maltoni, Dario Maio, Anil Jain, and Salil Prabhakar. *Handbook of Fingerprint Recognition*. Springer, 2003.
3. Stan Z. Li and Anil K. Jain. *Handbook of Face Recognition*. Springer, 2005.
4. Anil K. Jain, Yi Chen, and Meltem Demirkus. Pores and ridges: High-resolution fingerprint matching using level 3 features. IEEE Trans. Pattern Anal. Mach. Intell., 29(1):15– 27, 2007.
5. ISO/IEC 19794-8. Information technology - Biometric data interchange formats – Part 4: Finger pattern skeletal data, 2006.
6. ISO/IEC 24745. Information Technology- Security Techniques- Biometric Template Protection (Committee Draft), 2009.
7. John Woodward, Nicholas M. Orlans, and Peter T. Higgins. BioMetrics: Identity Assurance in the Information Age. Broché, 2003.
8. Use of biometrics to tackle ATM fraud 2010 International Conference on Business and Economics Research vol.1 (2011).