International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 02 | Feb-2021 ISSN: 2582-3930

Review Paper on Biometric Automatic Teller Machine (ATM)

Mrs. Jaya Shashikant Mane

Assistant Professor, Department of Computer Engineering, Modern Education Society's College of EngineeringPune.

Abstract -During earlier days, people did almost all their bank related transactions manually, the customers have to form a long queue in the bank which was very time consuming and irritating process. This had leaded the bank to the utilization of an electronic device known as Automatic Teller Machine (ATM) for performing transaction without the physical presence of a bank delegate. The ATM has become popular among the people and gained wide utilization due to the 24 hours service it provides to customers. ATM transaction is initiated by inserting the ATM card and typing the PIN (Personal Identification Number) of that specific card. PIN typically in a form of four digit combination of numbers. This conventional ATM systems authentication method has some limitations. Using ATM card and password cannotverify the client's identity exactly. This leads to many fraud cases related to ATM card transaction. On the other hand if Biometrics based authentication techniques are used it will increase ATM security and reduce fraud cases. In this paperpalm vein technology and other biometric authentication techniques are discussed to increase ATM security.

Key Words:ATM, biometric authentication, Palm Vein technology.

1.INTRODUCTION

Nowadays security has become very basic for every organization. When it's a matter of money it becomes very essential and important. In banking system it is a sensitive issue now. ATM is a machine that allows the bank customers to carry out banking transactions like deposits, transfers, balance enquiries, mini statement, withdrawal and fast cash etc. The main purpose of ATM machine is to make available cash to the bank customer immediately and easily whenever they need it. But there is some security issues now coming forward related to ATM. Most of the bank provide ATM card with PIN to their customer to carry out ATM transactions. As this is not enough to identify the customer, it becomes easy for fraudsters to misuse the ATM system. As PIN is only 4 digit numbers it is easy for them to guess someone PIN and misuse ATM facility. This has leads to huge amount of cashlost from ATM every year. To avoid this type of frauds bank can implement better dual authentication system at ATM centers using biometric authentication with traditionalPIN method for customer identification.

2. Need of Biometric ATM

Common frauds and attacks with conventional ATM for customer identification process are as follows:

- ATM scanner can be fixed to acquire encoded information from ATM card that can be used by fraudster to duplicate card.
- PIN can be guessed, captured or stolen to do fraudulent activity.
- If ATM card lost it can be misused. Sometimes PIN is written with ATM card.

These frauds can be avoided if traditional ATM system is combined with biometric authentication. The resultant dual authentication system is as follows:

- First authentication with ATM card and PIN, and
- Second authentication with Biometrics based features.

Other way to reduce these frauds is to replace conventional ATM by purely Biometric ATM.

3. Biometric authentication techniques

Biometrics based authentication can be one of the technique used for increasing ATM security. Biometric is a Greek Words, Bio means life and metric means measuring some objects that have life. Biometric authentication can be divided into two categories as follows:

1) Based on static features like face, iris, and fingerprint etc. which are physical characteristics of human being.

2) Based on dynamic features like electrocardiographic (ECG) signal, voice, keystroke etc. which are behavioral characteristics.

These characteristics are used to uniquely identify an individual.They are connected to an individual and cannot be guessed, forgotten, stolen, shared or easily hacked like passwords or PIN.

Following are advantages of Biometrics authentication

- The biometric information is unique for each individual.
- It can identify the individual.
- It provides strong authentication.
- It can be easily implemented on any existing system.
- There are very less chances of two people having same biometric features.

Out of all these biometric features Finger Print technology is the initial biometric science that uses unique features of the fingerprint to identify or verify the identity of an individual. Fingerprint is currently being used during voting process, biometric attendance system for school and offices. It is also used for controlling access to highly secured places like offices, equipment rooms, control centers, server rooms and so on.

Other biometric features like face, iris, and voicecan be also used for unique identification of individuals at ATM centers. But while focusing on different types of biological characteristics, various attacks can be possible to cheat the system, discussed as follows.[1]

- Attacks on face recognition:

Nowadays face images can be obtained from various resources like WhatsApp, social networking sites. There is no need to steal or hack this information. It is now easily available. With this obtained data face recognition system can be cheated.

- Attacks on iris recognition:

With the help of high-resolution camerairis images can be captured and used to cheat iris recognition system. Cost of this type of attack is relatively high.

- Attacks on fingerprint and palm-print:

Various types of material like Silica gel, latex, and gelatin can be used to make fake finger. Also the finger print can be generated from the surface user has touched. This fake data can be used for authentication purpose.

- Attacks on voice:

Voice can be easily collected by attacker as sound travel in all direction in open environment. This captured data can be replayed for authentication purpose and it leads to ATM fraud.

All these biometric features has some common drawbacks

- These can be captured easily by fraudster
- These features are external to the human body.

To overcome these drawbacks a better biometric feature need to be used for authentication which will be difficult to capture and duplicate.

4. Palm Vein Technology

Palm Vein technology uses palm vein as a biometric feature for authentication. As vein are under human skin it is difficult for someone to copy or steal them so palmvein is more secure as compared to previously discussed biometric features. Palm vein pattern is very diverse and complex in structure.It is also contactless feature for biometric authentication.

For authentication purpose palm vein images of user palm can be capturedusing near-infrared raysby two different methods.

- Reflection method and
- Transmission method.

In reflection method palm is illuminated and image is captured from the front side of user palm. So both devices can be integrated to create a new compact device as direction of illumination and capturing of palm vein image is same.

In transmission method palm is illuminated from back side and image is captured from front side of user palm. Thus in transmission method illumination and image capture device are facing each other across the user palm.

Figure 1 shows sample image of palm vein captured by experimental device.

As Palm Vein technology is contactless method it is more preferred for publicly used devices and location like ATM center. [2]

Palm vein Technology has following advantages:

- It works in contactless manner which is preferable for public usage.
- It is simple and easy to use as user need to expose their palms to the device.
- Palm vein patterns are difficult to hack and complex in structure.
- Palm vein are hidden under human skin so cannot be predicted.
- The image captured is very stable.
- It is difficult for fraudster to duplicate or steal image to cheat authentication system.

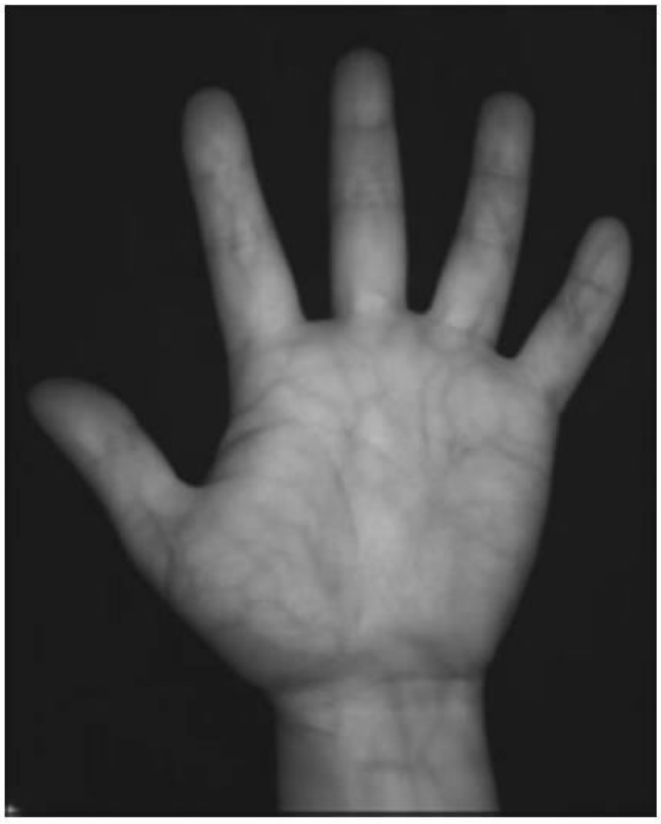

Fig -1: Palm Vein Image[2]

5. Palm Vein Authentication Process

First stage of palm vein authentication process is extraction of palm vein from the near-infrared image taken by Palm vein sensor. Palm vein are under human skin and not clear and visible like other biometric features so proper extraction of vein pattern is more important. This extracted captured Palm vein is later used to find out similarity with the registered template stored in database. Various methods can be used to find out the similarity. User is verified if the similarity score is greater than or equal to the threshold value.In this waythe user

authentication is done. At ATM centre Palm vein authentication can be done as follows.[2]

Palm vein is registered at a bank counter and it also stored on a smart card when user open an account in the bank. During verification process for ATM transaction Palm vein pattern of user is captured by the device and sensor at ATM center.This captured pattern is then transferred to the user's smart card and compared to the template which was stored in smart card during initial registration process. Matching result score is transmitted back and user authentication is done.User is then allowed to do to ATM transactions further.If fraudstertry to use the ATM card, Palm vein authentication restrict it to proceed further as vein pattern will not match.

Japan andBrazil adopted Palm vein authentication at their ATM centers.It is now becoming popular due to its high level of verification accuracy, complex and hidden pattern,contactless and hygienic process.

6. CONCLUSIONS

In this paper I have reviewed possible biometric authentication techniques that can be used for authentication process to reduce ATM frauds. I also reviewed common possible attacks that can happen with biometric feature like face, iris, fingerprint and voice. I tried to explore one advanced biometric feature palm vein pattern for better and secure biometric authentication. Palm vein technology is secure as authentication data exists inside body and so it is difficult to attack as compared to other biometric feature.

REFERENCES

1.Zhang Rui1 AndZheng Yan:A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification,IEEE Access volume 7, 2019

2. T. Shinzak: A. Uhl et al. (eds.), Handbook of Vascular Biometrics, Advances in Computer Vision and Pattern Recognition, First Online: 14 November 2019,

Use Case of Palm Vein Authentication | SpringerLink
https://doi.org/10.1007/978-3-030-27731-4_5