ATM Authentication System Using Fingerprint Biometrics

Amit H. Mane¹ Pradip C. Jadhav² Sachin U. Bade² Sameer P. Maner¹ Omkar P. Maske²

¹²³⁴⁵ Department of Information Technology
Dr. Daulatrao Aher College of Engineering, Karad – 415110

Abstract— Now-a-days, in the self-service banking system has got extensive popularization with the characteristic offering high-quality 24 hours service for customer. Using the ATM (Automated Teller Machine) which provides customers with the convenient banknote trading is very common. In the existing system it is designed by using ATM card and PIN, however this system is not safe to use because anybody can access the system if they have the card and pin number and may miss use it. Many incidents like shoulder surfing and card skimming have been occurring now—a-days, which is the main disadvantage of the existing system. To overcome this shortcomings of piracy in money transactions the idea of using fingerprint of customer as a password in place of traditional pin number is used. Biometric fingerprint recognition systems are easy to access and they provide high security to the customers [1]. The main objective of this system is to develop an embedded system, which is used for ATM security applications [1].

Key words: Fingerprint, biometrics, minutiae detection, fingerprint verification, authentication, ATM (Automated Teller Machine) terminal, features-extraction

I. INTRODUCTION

Biometrics is automated methods of recognizing or identifying a person based on a physiological or behavioral characteristic. Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The various features used are face, fingerprints, hand geometry, handwriting, iris, retina, vein, voice [2].

Fingerprinting or fingerprint-scanning technologies are the oldest and most widely used of the biometric sciences and utilize distinctive features of the fingerprint to identify or verify the identity of individuals. Fingerprint-scan technology is the most commonly deployed biometric technology, used in a wide range of physical access and logical access applications. All fingerprints have unique characteristics and patterns that is they are universal [2].

A fingerprint is made up of lines and spaces between those lines. These lines are called as ridges and spaces between the lines are called valleys. The ridges are the dark area whereas valleys are the white area between two ridges. Minutiae are the major features of a fingerprint; they can be used for comparison of two fingerprints [2].

In order to detect minutiae from the fingerprint image first of all the segmentation of the fingerprint should be done. The algorithm proposed focuses on minutiae-based fingerprint detection method.

The important minutiae features are: ridge ending and bifurcation. Ridge ending may be defined as the point where a ridge ends abruptly and ridge bifurcation may be defined as the point where a ridge diverges into branch ridges [3].

II. LITERATURE SURVEY

Now a day’s traditional ATM systems have security measures like ATM card and PIN for performing the transactions but they do not provide security for transactions that’s why the project provides a highly secure and unique measure for safety that is the fingerprint recognition.

Survey of papers given as in reference, the current system is not safe. The proposed system will be designed using fingerprint biometrics. Security for the customer’s account’s not guaranteed by PIN. Personal Identification Number (PIN) is an important aspect of the current ATM system in providing security and it is a commonly used method in protecting the transactions of one’s account.

But sometimes PIN’s strength is decreased as the tracking of the code is increased. “Most commonly PINs are 4-digit numbers in the range 0000-9999 resulting in 10,000 possible numbers, so that an attacker would need to guess an average of 5000 times to get the correct PIN.” If PIN is correct, the system allows for transaction.

III. OBJECTIVE

1) To study the scope of fingerprint biometric authentication techniques in ATM terminals.
2) To generate module that will help for easy and convenient operations of ATM terminals with secure authentication.

IV. IMPLEMENTATION

The typical biometrics authentication process involves two steps: First is the creation of the account holder’s biometric sample i.e. fingerprint recognition and its storage in the account holder’s database in respective account holder’s bank. This authorization procedure is done by the bank. At the time of actual authentication at the ATM terminal, the user or the account holder is required to provide a sample of the same nature i.e. finger print, then the system will generate fingerprint image.

Fig. 1: Architecture Diagram of proposed system
This image is usually sent across through network to the server. On the server side, the user’s current sample compared with the one stored in the database. If the two samples match with each other to the expected degree on the particular values, the users is considered as authenticate user and is allowed to proceed further for transactions, otherwise the user is considered as invalid or unauthorized user and then terminates session.

This is the Architecture diagram of the proposed system. This system shows two processes one is enrollment of fingerprint to the database and other is verification or identification of fingerprint from the database. At the time of enrollment when the user punches his fingerprint on scanner, a fingerprint image is captured, then features are extracted from the image and they are stored to the database. This process is indicated by dotted line. Next time when the user will punch his fingerprint at the ATM, image of fingerprint will be captured its features will be extracted and those will be compared with those in database.

V. DRAWBACKS OF EXISTING ATMS

(1) Existing ATM system is card based, so it requires more time to access the cards.
(2) In some case, if the ATM card is lost or stolen there is possibility of misuse of the card.
(3) Also if the ATM card is lost or stolen then the respective bank requires more time to regenerate new card and also it is costly for the customer as well as for the bank.
(4) After some years due to repeated transactions, the card will be unable to operate due to its wear and tear, hence bank should have to provide new card to the account holder which is expensive in terms of cost and also it is time consuming.
(5) If any account holder has multiple numbers of ATM cards then it will be difficult for him to handle and use those cards [4].

VI. REQUIREMENT AND WORKING CONDITIONS

(1) ATM terminals must be embedded with biometric fingerprint reader for biometric authentication.
(2) User Authentication is required per transaction.
(3) If user fails more than 3 times to identify himself then there should be provision to block that user’s account for that day for security purpose.
(4) If such blocks more than 4 times (within 3 months) then block the user account and tell him to regenerate new authentication in their home bank [5].

VII. ADVANTAGES OF FINGERPRINT BASED ATMS

(1) Provides secure authentication.
(2) Fingerprint biometric system replaces card system with physiological characteristics.
(3) Ideal for Indian rural and illiterate masses.
(4) It is more helpful to senior citizens because it is difficult to carry and maintain card with them.
(5) Complaints regarding card such as - stolen cards, regenerating new cards, maintaining and recording of cards etc. will be eliminated. Thus it is helpful to bank to reduce cost, time and efforts for card process.
(6) Due to biometric authentication no one is able to access others account [6].

VIII. LIMITATIONS

(1) This method is more costly and requires additional hardware to be installed in ATM centers.
(2) Due to biometric only account holder can access account [7].

IX. PROBLEMS WITH BIOMETRIC

(1) Biometrics techniques are relatively new, and some people find their use inconvenient.
(2) Biometrics recognition devices are costly, although as the devices become more popular, their cost goes down [8].
(3) Although equipments are improving, there are still false reading / recognition.
(4) The speed at which recognition must be done limits accuracy [9].

X. CONCLUSION

The security and efficiency analysis shows that the new system makes not only transactions secure but also system is easier to use, more flexible and efficient. The proposed model is designed for the ATM users for performing various transactions like cash withdrawal, balance enquiry, cash transfer, and mini statement. Due to unique method of authentication it reduces cost, time, and efforts of both banks as well as service users. This paper proposes the use of the biometric fingerprint as a strong substitute for the traditional PIN (personal identification number). We all know that fingerprints are the most acceptable and most widely used biometrics all over the world for identifying a person. In this paper fingerprint are chosen for their uniqueness, ease of use and convenience of user; fingerprints cannot be stolen, they are not transferable.

XI. FUTURE SCOPE

Now-a-days ATMs are operating on the basis of card and PIN, where as for better security biometric authentication has growing demand. According to security experts, fingerprints can easily be lifted and replicated. In future solar powered and biometric PIN based ATMs will be launched by banks, especially in rural areas.

REFERENCES

International References:


