SMART ATM PIN RECOVERY AND SECURED ATM TRANSACTIONS BASED ON FINGERPRINT IDENTIFICATION

PROJECT REFERENCE NO.: 41S_BE_0265

COLLEGE : TONTADARYA COLLEGE OF ENGINEERING, GADAG
BRANCH : DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
GUIDE : Prof. VENKATESH A. BHANDAGE
STUDENTS : MS. ANKITA SHETTY
            MS. POOJA HUILGOL
            MS. PRIYANKA KULKARNI
            MS. SHRAVANI MAHENDRAKAR

Keywords:
Fingerprint; ATM; PIN; Harris corner detection algorithm; SURF algorithm.

Introduction:
ATM (Automated Teller Machine) is an electronic telecommunication device that is used to perform financial transaction without need for human clerk or bank teller. ATMs extend traditional banking hours by dispensing cash and making other transaction available 24 hours a day. In ATM machines, the user is identified by inserting an ATM card and authentication is provided by the customer entering a PIN. The PIN provided to the customer is compared with recorded reference PIN number in the bank server. In the existing system, the user has to insert the card and the PIN number. If the PIN is correct, the system allows for the transaction. Otherwise, the system asks for the PIN again and it allows maximum of three times to enter it. After 3 trials the ATM card will get blocked. To reactivates the card user need to visit the bank and do the bank formalities, which is tedious and time consuming job.

Biometrics is the science of establishing the identity of an individual based on physical, chemical or behavioral attributes of a person. Fingerprint is a pattern of ridges and valleys on the surface of a fingertip. It is often used for biometric identification. Fingerprints are detailed, nearly unique, difficult to alter and durable over the life of an individual. To reactivate that ATM card in the ATM center itself we are using fingerprint biometric.

Objectives:
Usually the user inserts the ATM card in the ATM machine and enters Personal Identification Number (PIN) for the transactions. If the user forgets the PIN and enters the wrong PIN then the ATM machine will provide two more attempts to enter the valid PIN. If the user fails to provide the correct PIN after three attempts, the bank server will block the ATM card of the user. Now user has to visit the bank to reactivate his/her ATM card, which is time consuming

1) To avoid the user to visit the bank and do the formalities to reactivate his/her ATM card.
2) To activate the ATM card of the user at the ATM centre itself with the help of fingerprint of the user.
3) To alert owner of the ATM card in case of misuse.
Methodology:

The proposed methodology is based on identification of fingerprint of the ATM user. The user inserts the ATM card and enters PIN to perform transactions. If the user enters the invalid PIN for three times, an alert message will be sent to registered mobile number and also a pop-up window will open on the ATM machine. The pop-up window displays the message “You have entered wrong PIN; please give your registered fingerprint to create new PIN”. User provides the fingerprint impression for authentication. If fingerprint matches then the bank server will provide flexibility for the user to create his/her new PIN on the ATM machine itself. After that user will get message that you have successfully got new PIN. Now user can continue transactions with this new PIN as earlier. Figure 1 shows the activity diagram of proposed system.

![Activity Diagram of Proposed System](image)

Figure 1: Activity Diagram of Proposed System

Algorithm for fingerprint recognition

**Input**: Image of fingerprint.

**Output**: Detection of key points.

1. Input image is converted into greyscale image then it is converted into binary image.
2. Skeleton image is obtained.
3. Using Harris corner detection algorithm, key points of fingerprint are detected.
4. Using key points, the fingerprints are matched.

The Matching Algorithm plays a key role in fingerprint recognition steps. We are using matching algorithms and they are SURF (Speeded-Up Robust Features) algorithm and Harris corner detection algorithm.

**Hardware specification**

- RAM: 4GB
- Fingerprint scanner with USB cable
- Processor: Intel core-i5, 64-bit

**Software specification**

- OS: Windows 7 & above
- Back-end: Python
- Front-end: Java
Results and Conclusion:
The proposed ATM security system provides a mechanism for recovery of ATM PIN by using fingerprint identification. The developed system is able to authenticate the user based on fingerprint identification. The system is able to send an alert message to ATM card owner for entering the wrong PIN. The alert message is also sent to the owner of the card upon successful creation of new PIN.

From the tests carried out we have been able to prove that, the biometric identification for ATM transactions can be practically implemented in a real time environment. The developed system provides ATM users with the facility to change the PIN in the ATM machine itself.

Scope for future work:
Bank can provide helpline number to block the ATM card. In case if the ATM card is being misused, user will get the message of transaction which is performed through his/her card. By referring that message, user can call to helpline number to block the ATM card through the registered mobile number.