IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 63-65
www.iosrjournals.org

Card-less ATM and Swiping Gadgets

Prof. Rajesh Kamath[1], Pooja Naik[2], Nisha Harikantra[3], Archana Vernekar[4]
[1](Department of computer science and engineering, Girijabai Sail Institute of Technology, India)
[2](Department of computer science and engineering, Girijabai Sail Institute of Technology, India)
[3(]Department of computer science and engineering, Girijabai Sail Institute of Technology, India)
[4](Department of computer science and engineering, Girijabai Sail Institute of Technology, India)

Abstract: *The main objective of this system is to develop a system, which is used for ATM security applications. Card-less ATM is a desktop application where fingerprint of the user is used as an authentication. The user has to login using his fingerprint and a unique pin number to do any banking transactions. The fingerprint features are unique for each human being so the user can be identified uniquely and is also the safe and secure method.*

Keywords: *ATM, biometric, fingerprint scanner, pin, security.*

I. Introduction

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two fingerprints. Fingerprints are one of many forms of biometrics used to identify an individual and verify their identity. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (10 fingers) available for collection, and their established use and collection by law enforcement and immigration. Indian banks are going to great lengths to use biometrics to its full potential. According to TechSci report, the biometrics market in India will grow at a CAGR of 31 percent from 2016 to 2021 and will surpass $3 billion by 2021[1]. There are two types of systems that help automatically establish the identity of a person: 1) authentication (verification) systems and 2) identification systems. In a verification system, a person desired to be identified submits an identity claim to the system, usually via a magnetic stripe card, login name, smart card, etc., and the system either rejects or accepts the submitted claim of identity. In an identification system, the system establishes a subject's identity (or fails if the subject is not enrolled in the system data base) without the subject's having to claim an identity [2].

II. Problem Statement

Using the ATM (Automated Teller Machine) which provides customers with convenient banknote trading is very common. However, the financial crime case rises repeatedly in recent years, a lot of criminals tamper with the ATM terminal and steals user's credit card information and password by illegal means [3]. About 30 lakh bank debit cards have come under threat after a security breach at a private bank's ATM raised fears of potential fraud, according to media reports. Though this is just about half a percent of total cards issued in the country, this could be the biggest security breach in the Indian banking industry.

III. System Design

The system is initialized to implement specific task, such as checking ATM system, GSM communication and so on, and then each module reset for ready to run commands. Before using ATM terminal, the mobile number and fingerprint of customer is required.

First the system is required the owner's fingerprint. If all the recognition is right, the system would send password to the account holder and he will enter the same password in on the keypad for accessing terminal. If authentication failure exists, then it sends the alert message to the account holder and bank. A biometric verification system makes two types of errors:

1) mistaking biometric measurements from two different persons to be from the same person (called *false match*) and 2) mistaking two biometric measurements from the same person to be from two different persons (called *false non-match*). These two types of errors are often termed as *false accept* and *false reject,* respectively. There is a tradeoff between false match rate (FMR) and false non-match rate (FNMR) in every biometric system. In fact, both FMR and FNMR are functions of the system threshold; if is decreased to make the system more tolerant to input variations

and noise, then FMR increases. On the other hand, if is raised to make the system more secure, then FNMR increases accordingly [4].

A variety of factors should be considered when designing a multimodal biometric system. These include (a) the choice and number of biometric traits, (b) the level in the biometric system at which information provided by multiple traits should be integrated, (c) the methodology adopted to integrate the information, and (d) the cost versus matching performance trade off. The choice and number of biometric traits is largely driven by the nature of the application, the overhead introduced by multiple traits (computational demands and cost, for example), and the correlation between the traits considered (uncorrelated information is preferred since the performance improvement is more pronounced in this case) [5].

The four main steps in our feature extraction algorithm are
a) determine a reference point and region of interest for the fingerprint image;
b) tessellate the region of interest around the reference point;
c) filter the region of interest in eight different directions using a bank of Gabor filters (eight directions are required to completely capture the local ridge characteristics in a fingerprint while only four directions are required to capture the global configuration);
d) compute the average absolute deviation from the mean (AAD) of gray values in individual sectors in filtered images to define the feature vector or the FingerCode [6].

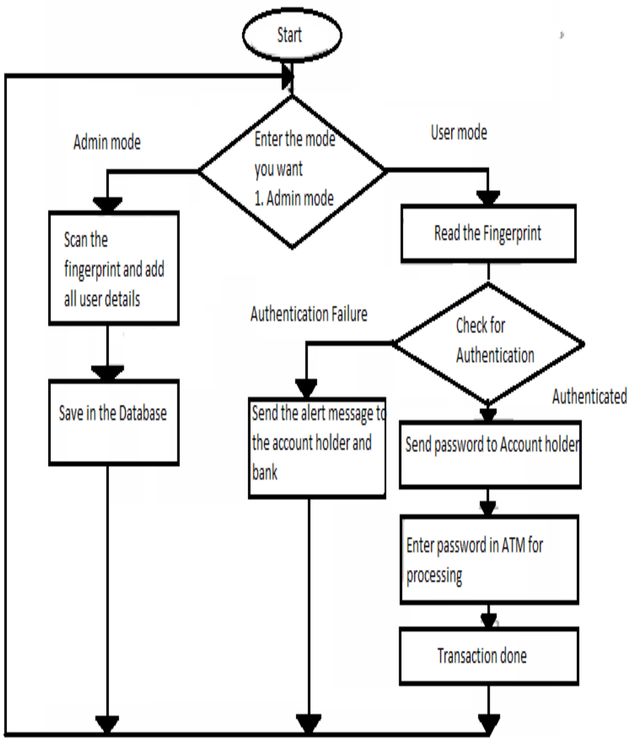
Start
Admin mode
Enter the mode you want 1. Admin mode
User mode
Scan the fingerprint and add all user details
Read the Fingerprint
Authentication Failure
Check for Authentication
Save in the Database
Send the alert message to the account holder and bank
Authenticated
Send password to Account holder
Enter password in ATM for processing
Transaction done

Fig: 3.1. The overall flow chart of software

IV. Methodology

The system consists of two modules:
1. Admin module
2. User module

Admin module:

The bank authority should login into specific computer using the username and password. Once the admin has logged in, he can create an account for the customer by filling the form (including name, age, type of account, photo, fingerprints and other essentials).After creating the account successfully, the bank will provide unique username and pin number to the customer with which he can proceed with the transactions.

User module:

The user needs to enter the username and pin number provided by the bank authority. The user can further do the following transactions such as check balance, withdrawal, money transfer, bill payment, money deposition. The user needs to select the type of account as in savings or current. Display the remaining amount in his/hers account after transactions are completed.

Expected Outcome

To overcome people's misconception over cyber security, network connectivity and so on.
To prevent illegal use of cards
To completely eradicate usage of card system and take a step towards digital India

V. Conclusion

The main reason for introducing biometric system is to increase overall security, as it is the safest means for preventing ATM frauds. The implementation of ATM security by using fingerprint recognition is more stable and reliable method.

References

[1]. Fingerprint Recognition using Image Segmentation by Sangram Bana and Dr. Davinder Kaur.
[2]. An Identity Authentication System using Fingerprint by Anil Jain , Salil Prabhakar, Lin Hong and Sharath Pankanti.
[3]. ATM Transaction Using Biometric Fingerprint Technology by Mahesh Patil, Sachin Wanere, Rupesh Malghane and Aashay Tiwari.
[4]. An Introduction to Biometric Recognition by Anil Jain , Salil Prabhakar and Arun Ross.
[5]. Multimodal Biometrics by Arun Ross and Anil K Jain.
[6]. Filterbank based Fingerprint matching by Anil Jain , Salil Prabhakar, Lin Hong and Sharath Pankanti