Pic using Biometric Active Touch Finger Print in ATM Machine

V.Raghunath
Ece Department,
Trp Engineering College,
Irungalur, Trichirappalli, Tamil Nadu-621105

N.Saravanakumar
Ece Department,
Trp Engineering College,
Irungalur, Thiruchirappalli, Tamil Nadu-621105

ABSTRACT: **A secure model is proposed using fingerprint biometrics to transfer funds to another location. The user selects a person from the network and sends a message to the system stating the amount to be transferred. The system generates an OTP PIN to the receiver. The receiver should enter the PIN along with his fingerprint to get the money. If the fingerprint stored does not match then the sender will receive an alert and money is not transferred. If both the OTP PIN and the fingerprint match then the money is given and the sender receives a message alert .If any unauthorized user tries to detect such activities the ATM door is locked.**

Keywords—fingerprint ,PIC IC ,MP LAB

I.INTRODUCTION

Security has always been a major concern and goal of all organization. There is no such object which can be considered as completely secure especially if it is about money. Security is not only confined to network but also includes Physical security. When talking about ATM machines or EDC we are mainly concerned with Physical security which aims at ensuring Access control, Identification and Authentication. Access control is another consideration of Information System security to confirm the identity of individual so that only authorized entity is accessible to the system. With the development of banking technology the way of banking has changed. On the other hand where it has free us from standing in long queues to carry out cash withdrawal, depositing money, transferring money and many more on the other it has also increased the risks of theft. ATM (Automatic Teller Machine) has proved to be an easy and convenient way to carry out all our banking tasks in just few minutes. An ATM card or debit card authenticates person after verification of card number, Expiry date, card holders name and the PIN. But what in case your card is stolen, or PIN is known to an unknown entity. For this we require a higher level of security which coined up an idea of adding Biometric to the current technology. Biometric has emerged as a measure for highly secure identification and personal verification. Biometric system, to conduct the verification requires a sensor every time to collect the biometric sample.

This sensor is exposed to dusty, sweaty and oily hands depending on person to person thus effects the sensitivity of sensor to gather the accurate sample for verification. There can be a chance when a person needs to withdraw only a low amount or want the mini-statement and behind him is a long queue. So, just to debit a little cash, being the first transaction, waiting for biometric identification is simply time-consuming. To skip this problem it is proposed to use a concept of introducing a cash and day transaction limit with the biometric, where one has to present one's biometric only if one wants to withdraw above the defined cash limit OR if the number of transactions are more than specified "k" times (let k=3) or both condition is found to be true else cash withdrawal without biometric is permitted. It also guarantees security as each ATM has its cash limit and bank has its transaction limit. So, in case of card misuse, will prevent withdrawal of large cash in one transaction or even restrict to debit low cash multiple times by making multiple transactions. It will also limit the maximum amount that can be withdrawn by unauthorized person in case of card misuse.

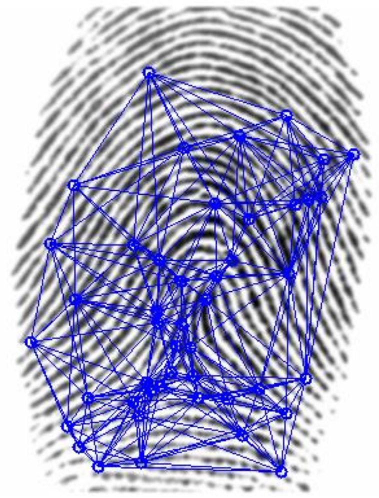
II.RELATED WORK

The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use personal identification numbers (PIN's) for identification and security clearances. Biometrics based authentication provides various advantages over other authentication methods, it has replaced the password based authentication and token based authentication. Biometrics plays a major role in Automated Teller Machine (ATM) system, E-Commerce, Online banking, Passports. The growth in electronic transactions has been increased tremendously; there is a greater demand for fast and accurate user identification and authentication. Sending information from one person to other person encounters a lot of problems due to many types of attack on the communication network. Apart from these attacks on communication network, attackers attacks on the physical access medium. Physical access includes access control, authentication, and verification. An attacker can read the information of the magnetic strip of a credit or debit card by installing a skimming device on electronic data capture machine (or swipe machine).

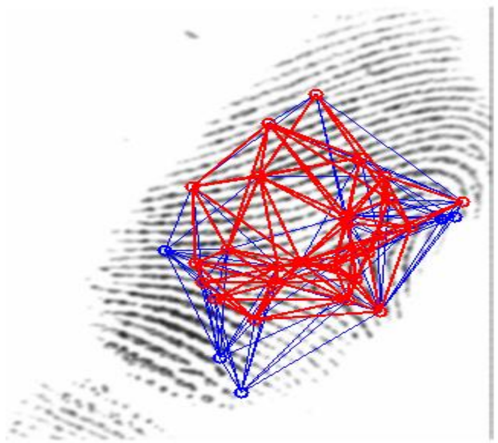
A fingerprint biometric technique is embedded with PIN (personal identification number) to authenticate a customer and for enhancing the security of electronic fund transfer via EDC. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor. Biometric recognition, or, simply, biometrics, refers to the automatic recognition of individuals based on their physiological and/or behavior characteristics.

III.MINUTIAE ALGORITHM

This is the most popular and widely used in commercial applications, because of its good performance and low computation time, specially for good quality images. This method tries to align the minutiae of the input image (query template) and stored templates (reference template) and find the number of matched minutiae. After alignment, two minutiae are considered in matching if the spacial distance and direction difference between them are smaller than a given tolerance. A correct aligning of fingerprint is very important in order to maximize the number of matched minutiae, this requires the computing of the translation and rotation information, as well as other geometrical transformations such as scale and distortion. In order to compute efficiently aligning information there has been proposed many approaches. In this section we present a method that uses segments (formed by minutiae) instead of isolated minutiae. A segment is formed by two pair of minutiae of the same fingerprint, the way how the set of segments are constructed may vary (e.g., nearest neighbor… etc). The figure below shows the segments constructed from the set of minutiae.



Minutiae nodes



query template

IV.EXPERIMENTAL SETUP

PIC16F877A is the heart of this system. It consists of clock circuit and power on reset circuit. Clock circuit is build around crystal oscillator and ceramic capacitor. Purpose of crystal oscillator is to stabilize the frequency and the capacitor is to stabilize the amplitude if the clock. This circuit determines the operating speed. Here we use 4MHz crystal oscillator, so the microcontroller will work at the speed of 1uSec. Purpose of the microcontroller is to control the speed of the DC shunt motor according to the load. It uses internal ADC and complete one port for reading load and control the speed. That is it reads voltage output and produces the digital output according to this input voltage. This microcontroller will set the load limit and terminate the DC shunt motor to prevent from over load

V.EXPERIMENTAL RESULT AND ANALYSIS

Technical evaluation must also access whether the existing systems can be upgraded to use the new technology and whether the organization has the expertise to use it. Once is a technical performance aspects and the other is acceptance within the organization. Technical performance includes issues such as determining whether the system can provide the right information for the organization's personnel, and whether the system can be organized so that it, always delivers this information at the right place and on time. Acceptance revolves around the current system and its personnel. The evaluation must then determine the general attitudes and skills of existing personnel and whether any such restructuring jobs will be acceptable to the current user. It determines whether the investment needed to implement the system will be recovered.

VI.PROPOSED SYSTEM

The proposed system works on authentication with fingerprints. All the accounts of the person are bought to a single screen after verification of the fingerprints. The transactions of any account can be done. To preserve security a Random OTP PIN is generated and sent to email in smart phone. If the PIN is successfully entered the transaction is processed.

VII.CONCLUSION

The sudden growth in electronic transaction and banking technology has demanded for higher level of security. Traditional methods of PIN or I-Cards can be forged or stolen and many times are too easy to be cracked as mostly these PIN are birth dates, security number, contact number or as such which can be easily guessed, but Biometric measures provide a hard-core security which neither can be stolen or forged. It provides a high level security by authentication and access permission to only genuine card holder. Thus the project has implemented for the user to get access multiple bank accounts and do transactions in a safe and secure manner.

VIII.REFERENCES

[1] S.S, Das and J. Debbarma, "Designing a Biometric Strategy(Fingerprint) Measure for Enhancing ATM Security in Indian e-bankingSystem", International Journal of Information and Communication Technology Research, vol.1,no.5,pp.197-203,2011.
[2] W.W.N. Wan, C.L. Luk, and C.W.C. Chow, "Customers Adoption of Banking Channels in Hong Kong", International Journal of Bank Marketing, vol. 23, no. 3, pp. 255-272,2005.
[3] Wikipedia the free encyclopedia, "Biometrics", Downloaded March20,2012 from http://en.wikipedia.org/wiki/Biometrics.
[4] B. Richard and M.Alemayehu, "Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons. Journal of Internet Banking andCommerce,vol.11,no.2,2006.DownloadedMarch15,2012 From http://www.arraydev.com/commerce/jibc/
[5] P.K.Amurthy and M.S.Redddy, "Implementation of ATM Security by Using Fingerprint recognition and GSM", International Journal of Electronics Communication and Computer Engineering vol.3,no.1,pp.83-86,2012.
[6] N.K.Ratha , J.H. Connell, and R.M. Bolle ,"Enhancing Security and Privacy in Biometrics-based Authentication Systems, IBM Systems Journal, vol. 40, no. 3,pp.614-634,2001.
[7] N.K.Ratha , S. Chikkerur, J.H. Connell and R.M.Bolle. "Generating Cancelable Fingerprint Templates", IEEE Transaction on Pattern Analysis and Machine Intelligence, vol.29,no.4,2007.
[8] B, Schouten and B. Jacobs, "Biometrics and their use in e-passport",
Image and Vision Computing vol. 27, pp. 305–312.2009,
[9] S.A. Shaikh and J.R. Rabaiotti,. "Characteristic trade-offs in designing large-scale biometric-based identity management systems". Journal of Network and Computer Applications vol. 33,pp.342–351,2010.
[10] C.A.Oyeka, An Introduction to Applied Statistical methods. Enugu, Nigeria: Modern Avocation Publishing Company. Pp.4, 36, 56. 1990.