Dogo Rangsang Research Journal
ISSN : 2347-7180

UGC Care Group I Journal
Vol-09 Issue-01 No. 01 : 2022

Biometrically Secured ATM Vigilance System

VELALA SURESH [1], J.GEETHA [2],

[1] **PG Research scholar**, Department of ECE, Jogaiah Institute Of Technology And Sciences college Of Engineering, Palakol, West Godavari. A.P.

[2] **Research Supervisor & Assistant professor**, Department of ECE, Jogaiah Institute Of Technology And Sciences college Of Engineering, Palakol, West Godavari. A.P.

----------***----------

Abstract:

The main purpose of our system to make online transaction more secure and user-friendly. Now days Biometric technology is increasing rapidly. Biometric is used for personal identification. Here we are using Fingerprint scanning biometric to provide access to ATM machine. Data of a fingerprint is stored in database using the enrollment process through the Bank. Bank provide authentication to the customer that can be access while performing transaction process. If fingerprint match is found in data base then transaction take place. After verification if fingerprint does not match transaction will be cancelled. Using fingerprint based ATM system user can make secure transaction.

KEYWORDS: **ATM, Accessing, Authentication, Embedded System, Biometrics, Verification, Fingerprint, Security**.

I. INTRODUCTION

Biometric can be used to identify physical and behavioral characteristics of user fingerprints. There are many biometric devices like iris detection, face recognition, fingerprint. In our Project, we are using fingerprint biometrics. Users fingerprint are scanned using biometric trait and stored in database. All fingerprints have unique characteristics and patterns. A normal fingerprint pattern is made up of lines and spaces. These lines are called ridges while the spaces between the ridges are called valleys. Fingerprint biometrics are easy to use, cheap and most suitable for everyone. Characteristics of fingerprint vary from person to person. Fingerprint are unique identity of user.

1.1 Fingerprint Scanning

Fingerprint scanning is one of the type of biometrics system .We are using finger for accessing the ATM machine for transaction. We are using this system because its easy to install. We don't have to remove the current ATM machine. The working process of ATM fingerprint deal with accessing the data from server.

Before accessing process we need to get authentication from bank. Bank employee scan fingerprint using biometric machine. Biometric machine extract the feature of fingerprint and store in to database this complete process is called enrolment process.

When customer want to use the ATM machine with Biometric Scanned first he have to place his finger at Biometric scanner will scan his feature and compare that extracted feature with stored Feature, if feature matches than the person is allowed for transaction otherwise it not process.

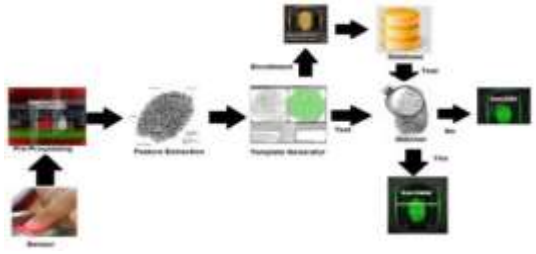


Fig-1: Fingerprint Scanning

II. OBJECTIVES

To propose authentication and verification process on the existing , ATM machine to make a successful and secure transaction.

The main objective of this project is to provide fingerprint as authorized identity and to design a more secure ATM system .In this, ATM machine work as when the customer place finger on biometric scanner of ATM and if the finger match is found it will display the name of customer on ATM machine. If Fingerprint match not found, it does not allow any transaction.

The objective of this study is as follow:-

1. To propose the authentication system on the existing ATM process for withdrawal after the entry of a correct pin.
2. To propose second level authentication system in a scenario where customer specified withdrawal limit.

III. LITERATURE REVIEW

In future ATM will have biometric authentication techniques to verify the owner of ATM card at the time of transaction. To provide such type of facility we have studied different research papers and found some vital information.

For ATM system we can use fingerprint biometrics scanner that capture the fingerprint and then follow certain algorithm for fingerprint matching.

Crime at ATM has become a notion wide issue that faces not only customer but also bank operators and the financial crime case rises repeatedly.

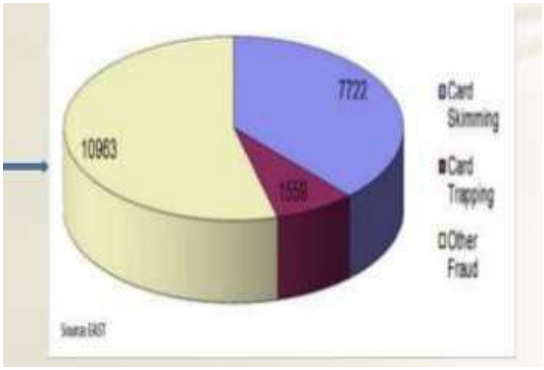


Fig -2: Pie chart of ATM card frauds

ATM Fraud's	Card Skimming	Card Trapping	Other Fraud
Fraud ratio	7722	1559	10963
Overall fraud ratio	20244	20244	20244

Table -1: sample table to estimate card fraud ratio

Criminal steal customers card, after stealing the card criminal use detail of card by illegal means. The fraud include like card Skimming and card Trapping and many more way included in ATM fraud. Above table and Pie chart gives the approximate Ratio of ATM card related Fraud. We can Say that card Skimming is most common type of Fraud.

Once a customer card is lost and the password is stolen, the user's account is able to hack. we can provide authentication of ATM system by using card like debit , credit and smart card and password or pin. For preventing and

to protect our account from hacking some privileging techniques are used for authentication. When customer's credit card get stolen there may be a chance that unauthorised user can often come with the correct personal code to choose easily guessed pins and password that can be birthdays, phone number and social security numbers.
The work done in the development of Fingerprint Based ATM system before with different and similar ideas are as follow:
1) Fingerprint is dependable biometric trait as it is an idiosyncratic and dedicated. It is a technology that is increasingly used in various fields like forensics and security purpose. The vital objective of our system is to make ATM transaction more secure and user friendly. This system replaces traditional ATM cards with fingerprint. Therefore, there is no need to carry ATM cards to perform transactions.
The money transaction can be made more secure without worrying about the card to be lost. In our system we are using embedded system with biometrics i.e r305 sensor and UART microcontroller. The Fingerprint and the user_id of all users are stored in the database. Fingerprints are used to identify whether the Person is genuine. A Fingerprint scanner is used to acquire the fingerprint of the individual, after which the system requests for the PIN (Personal Identification Number). The user gets three chances to get him authenticated. If the fingerprints do not match further authentication will be needed. After the verification with the data stored in the system database, the user is allowed to make transactions.
(Fingerprint based ATM System By Nisha Bhanushali, Meghna Chapaneria ,Krishani Mehta, Mansing Rathod).

2) The main objective of this system is to develop an system, which is used for ATM security applications. In these systems, Bankers will collect the customer finger prints and mobile number while opening the accounts then customer only access ATM machine. The working of these ATM machine is when customer place finger on the finger print module when it access automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer should be entered by pressing the keys on the screen. After entering it checks whether it is a valid one or not and allows the customer further access.

(ATM Transaction Using Biometric Fingerprint Technology By Mr. Mahesh A. Patil Mr.Sachin P.Wanere Mr.Rupesh P.Maighane Mr.Aashay R.Tiwari).

3) The main objective of this system is to develop a system that will increase the ATM security. However, despite the numerous advantages of ATM system, ATM fraud has recently become more widespread. In this paper, we provide an overview of the possible fraudulent activities that may be perpetrated against ATMs and investigates recommended approaches to prevent these types of frauds..Biometrics technology is rapidly progressing and offers attractive opportunities. In recent years, biometric authentication has grown in popularity as a means of personal identification in ATM authentication systems. An 8-bit ATmega16 microcontroller developed by Microchip Technology is used in the system. The necessary software is written in AVR studio programmer and the system is
tested.

(RBI 3X-Fingerprint Based ATM Machine By Bharti Patil1 , Bhagwan S. Chandrekar2, Mahesh P. Chavan3, Bhavesh S. Chaudhri4 E&TC Dept, PVPIT, Bavdhan, Pune1,2,3,4).

4) The existing ATM machine uses PIN-Card as a security which is very weak and easy to contravene. This paper tries to find a solution to the above problems by introducing fingerprint authentication into the existing ATM machine. A program prototype was designed to imitate a typical ATM system that uses fingerprint identification to enhance the security of the ATMs. The proposed system demonstrated a three-tier architectural structure. The verification system which centered on the enrolment, enhancement, feature extraction and matching of fingerprints. The backend database system that serves as warehouse of the templates of all ATM account holders' pre-registered fingerprints. The system's platform creates related transactions such as withdrawals, bill payment, buying of credit cards and balance enquiries etc. The results obtained confirm that the current approach could significantly reduce ATM fraud if not totally eradicate

it.(Fingerprint Authentication System: Toward Enhancing ATM Security By Awotunde, Joseph B. James, Tolorunloju R. Fatimoh T. Adewunmi-Owolabi. Abdulkadir, Suhurat I.).

IV. METHODOLOGY

Fingerprint verification is to verify the authenticity of one person by his fingerprint and PIN code and Fingerprint identification is by matching the information of user such as pin code and fingerprint matching.
Basically we can explain complete Fingerprint base ATM system in two phases:
1) Enrolment Phase
2) Authentication phase

1. Enrolment phase:

In the robust fingerprint application, 3-4 fingers should be enrolled. This enables the system to set high security threshold and still be able to cope with everyday real life issue like skewed finger placement dirty, wet dry, cut or worn fingers. Biometric reference data is collected enrolment and stored in database or in portable data carrier such

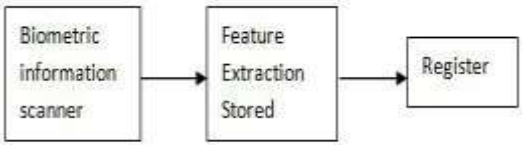
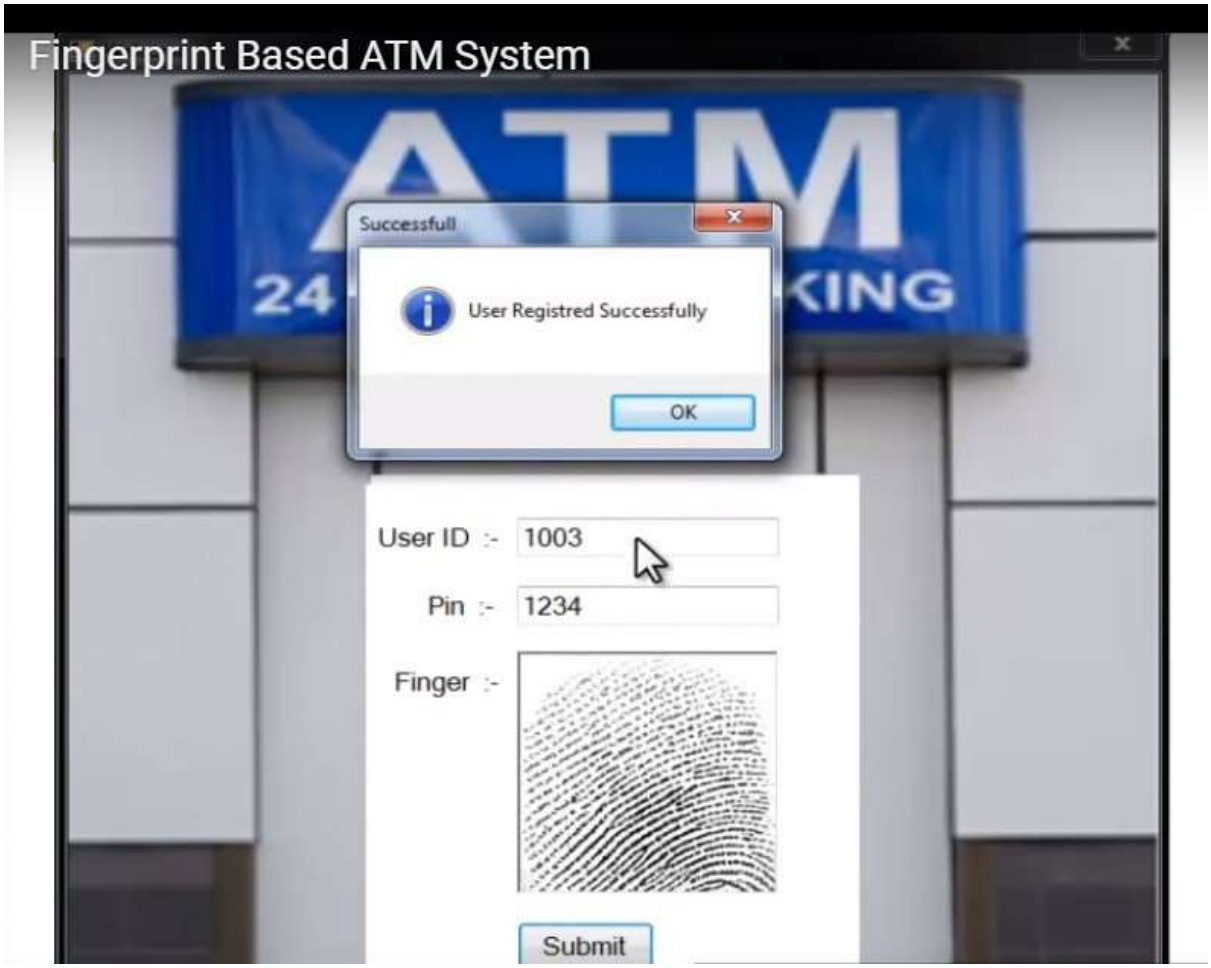


Fig-3: Enrolment Phase

The Enrolment is crucial because the once recorded reference data will normally be used over the active lifetime of user or his/her biometric hardware device.

Multiple Finger enrolment: It is strongly recommended enrolling more than one finger. During daily life injuries can happen that turn a registered fingerprint currently unusable while minor cuts not affect a robust sized sensor system.

1.1 Biometric information scanner:



2. Authentication Phase

In these phase user can make transaction by using their fingers. User can place finger on the Biometric scanner and user's finger scan can be matched through database, where all authenticated user's fingerprints are stored .If User wants to do transaction they simply place their finger on biometric scanner and get their money in few seconds. If user's fingerprint cannot matched by database due to some accidental cuts on their fingers than they can used their other fingers and we will also provide a 4 pin code option ,user can also use this option with their convinces.

Feature extraction:

Feature extraction from a fingerprint image is generally categorized into three levels. Feature can used to categorize into major pattern type such as loop or whorl.

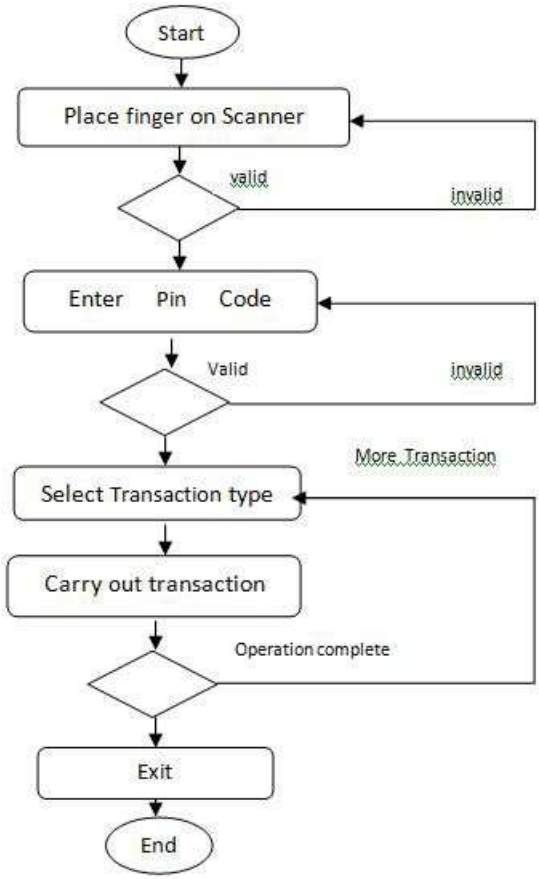


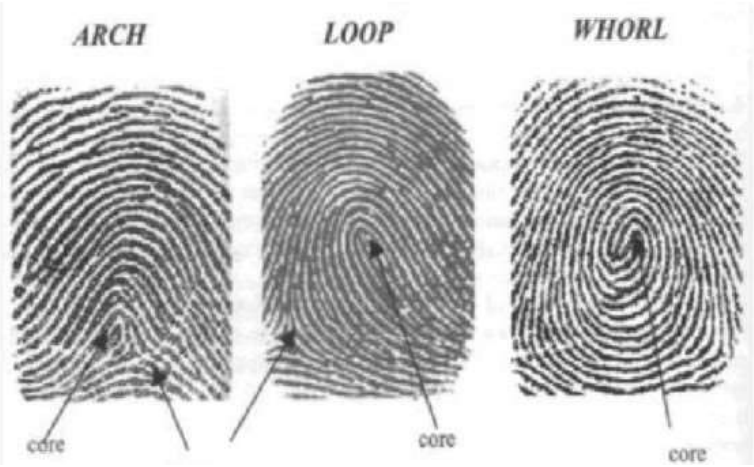
Fig-4: Authentication Phase

V. IMPLEMENTATION

Matching algorithms are used to compare previously stored templates of fingerprints against candidate fingerprints for authentication purposes. In order to do this either the original image must be directly compared with the candidate image or certain features must be compared.The next step is to locate these features in the fingerprint image, using an automatic feature extraction algorithm. Each feature is commonlyrepresented by its location (x, y) and the ridge direction at that location ().Pattern based algorithms compare the basic fingerprint patterns (arch,whorl, and loop) between a previously stored template and a candidatefingerprint. This requires that the images be aligned in the same orientation.To do this, the algorithm finds a central point in the fingerprintimage and centers on that. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match.In the final stage, the matcher subsystem attempts to arrive at a degreeof similarity between the two sets of features after compensating for therotation, translation, and scale. This similarity is often expressed as a score.Based on this score, a final decision of match or no-match is made.A decision threshold is first selected. If the score is below the threshold, thefingerprints are determined not to match; if the score is above the threshold,a correct match is declared.Often the score is simply a count of the numberof the minutiae that are in correspondence.

VI. PATTERNS

The three basic patterns of fingerprint ridges are the arch, loop,and whorl.An arch is a pattern where the ridges enter from one side of thefinger, rise in the center forming an arc, and then exit the other side of thefinger. The loop is a pattern where the ridges enter from one side of a finger,form a curve, and tend to exit from the same side they enter. In the whorlpattern, ridges form circularly around a central point on the finger.



VII. CONCLUSION

ATM machine increase the reliability of the bank organization by providing the easy access to the cash transaction. We can withdraw the cash anywhere and anytime without waiting in queue. Hence, ATM card is used wildly but we have to face the fraud related to the ATM transaction . To make ATM transaction more secure we are using biometric scanning machine to identify the account holder. Finger is unique identity of each person so the use of Biometric Fingerprint scanner we can avoid ATM related fraud. The Security feature enhanced stability and reliability of owner recognition .The whole system designed by using technology of embedded system which makes the system more secure, reliable and easy to use.

REFERENCES

[1] Dr. V. Vijayalakshmi, R.Divya and K. Jaganath, "Finger and Palm print based Multibiometric Authentication System with GUI Interface"
International conference on Communication and Signal Processing, April 3-5, 2013, India, 978-1- 4673-4866-9/13/$31.00 ©2013 IEEE

[2] O.A.Esan and S.M.Ngwira "Bimodal Biometrics for Financial Infrastructure Security" I.O.Osunmakinde School of Computings, College of Science, Engineeringand Technology, University of South Africa, UNISA Pretoria, South Africa, 978-1-4799- 0808-0/13/$31.00 ©2013 IEEE.

[3] Rishigesh Murugesh, "ADVANCED BIOMETRIC ATM MACHINE WITH AES 256 AND STEGANOGRAPHYIMPLEMENTATION", IEEE-Fourth International Conference on Advanced Computing, ICoAC 2012 MIT, Anna University,Chennai. December 13-15, 2012, 978-1- 4673-5584-1/12/$31.00©2012 IEEE.

[4] Rajesh. V and Vishnupriya. S, "IBIO-A New Approach/or ATM Banking System" 2014 International Conference on Electronics and Communication Systems (ICECS-2014), Feb.13-14, 2014, Coimbatore, INDIA.

[5] G. Renee Jebaline and S. Gomathi , "A Novel Method to Enhance the Security of ATM using Biometrics" , 2015 International Conference on Circuit, Power and Computing Technologies [ICCPCT], 978-1- 4799-7075- 9/15/$31.00 ©2015 IEEE

[6] A.Muthukumar and N.Sivasankari,"A Review on Recent Techniques in Multimodal Biometrics", 2016 International Conference on Computer Communication and Informatics (ICCCI -2016), Jan. 07 – 09, 2016, Coimbatore, INDIA ,978-1-4673-6680- 9/16/$31.00 ©2016 IEEE

[7] Umma Hany and Lutfa Akter,"Speeded-Up Robust Feature Extraction and Matching for Fingerprint Recognition", 2nd Int'l Conf. on Electrical Engineering and Information & Communication Technology (ICEEICT) 2015.Jahangirnagar University, Dhaka-1342, Bangladesh, 21-23 May 2015, 978-1- 4673-6676- 2115/$31.00 ©20151EEE.

[8] Ms. Archana S. Shinde and Prof. Varsha Bendre, "An Embedded Fingerprint Authentication System", 2015 International Conference on Computing Communication Control and Automation, 978-1- 4799-6892- 3/15 $31.00 © 2015 IEEE DOI