

IMPLEMENTATION OF ENHANCED FINGERPRINT BASED AUTHENTICATION ON ATM SYSTEM

¹Prof. Shweta Patil, ²Ravi kumar Yadav, ³Pritam Patil, ⁴Harshal Phanse

¹Assistant Professor, ²Student, ³Student, ⁴Student,

¹Department of Computer Engineering,

¹Shivajirao S. Jondhale College of Engineering, Dombivali, India.

Abstract : Our main aim is to develop the technique for fingerprint authentication in ATM. This target can be mainly decomposed into image preprocessing, feature extraction and feature match. For each sub-task, some classical and up-to-date methods in literatures are analyzed. Based on the analysis, an integrated solution for fingerprint recognition and authentication is developed for demonstration.

For the program, some optimization at coding level and algorithm level are proposed to improve the performance of my fingerprint authentication system. These performance enhancements are shown by experiments conducted upon a variety of fingerprint images. Also, the experiments illustrate the key issues of fingerprint recognition that are consistent with what the available literatures say

The underlying principle is the phenomenon of biometric "AUTHENTICATION". In this paper we propose a method for fingerprint matching based on minutiae matching.

IndexTerms - Enhancing ATM security, Security System for ATM, Biometric Base ATM, Fingerprint Based ATM, Minutiae feature extraction..

I. INTRODUCTION

Biometric ATMs are self-service automated teller machines (ATMs), or cash machines, that use a biometric measure to identify customers and allow them to withdraw cash. The biometric check may be the only customer identifier used, or it may be used in conjunction with another format, such as a payment card, a mobile device or an additional security credential, such as a PIN. The biometric measures used will generally include palm or finger vein print biometrics, although they may also include other functionalities such as iris recognition.

But here in our project we are going to implement Enhanced Fingerprint Authentication on ATM System,

Fingerprint based security system is the most secured **system** as compared to other **systems**. Reason is that Card or Keys of lock can be stolen, password may be leaked. However thumbnail of every human being is unique, so no one will get the access unless the same person is present to give the impression. of **fingerprint**.

II. LITERATURE REVIEW

1. Fingerprint Based ATM System

This paper proposes the authentication system on the existing ATM process for withdrawal after the entry of a correct pin. In short this paper proposes an extra layer of security for the ATM by asking fingerprint authentication to the customer, if the entered 4 digit pin was correct.

2. Fingerprint Recognition Using Minutiae Extraction Method

In this paper, minutiae extraction based fingerprint detection was applied with gradient detection as a step, to find the reference point. The reliability of any automatic fingerprint recognition system strongly relies on the precision obtained in the minutiae extraction process.

The minutiae based matching is highly sensible, as, if the finger is moved even a little bit that gives us a different set of minutiae.

3. A Survey on Cardless Cash Access Using Biometric ATM Security System

This research paper implements the Advance Encryption Algorithm to encrypt the customer password, AES (256 bit) cryptographic technique provides high security then previous method currently in use.

4. Fingershield ATM – ATM Security System Using Fingerprint Authentication

This research paper presents the development of The database server subsystem is comprised of two main processes: fetch data and update data. This function was used to communicate with the database using an SQL query. Fetch data is a function to fetch the current database record values into the client machine. It has 2 modes: fetch all data field of a record identified by card code; and fetch a name field of a record identified by account number for transfer purposes.

5. A Review on Securing ATM System Using Fingerprint:

This paper presents a review on challenges of ATM transaction by presenting a literature survey of recent biometric system using fingerprint technique. The Fingerprint based ATM is an application where Fingerprint of the customers is used as an authentication. The Fingerprint minutiae features are different for each human being so the customer can be identified uniquely. The fingerprint and customer detail are stored into the database. The input fingerprint images are used to verify the customer using the database. The main objective of the system is to make ATM transaction more secure and user friendly.

III. PROBLEM DEFINATION

In present scenario, traditional ATM system accepts only on the PIN CODE security system, enabling the other person rather than the owner to access the account very easily.

This ensures that the Traditional ATM system is not fully secured.

IV. EXISTING SYSTEM

Previously Customers were used to be in queue waiting for an hour to do a transactions like deposit money ,withdraw money from the bank. Therefore banks introduces an ATM(Automated Teller Machine) system for customers to withdraw the money. One of biggest merit of ATM system is providing the quick cash. But it has some demerits as well like smart cards can be stolen, lost, replicated, or left behind; passwords can be shared, forgotten, hacked or accidentally observed by a third party and there are so many ATM related frauds are happening in all over the country, while an innocent person tries to withdraw his/her own money from the ATM, where criminals already planted a skimming device in the atm to get the card information.

V. PROPOSED SYSTEM

The proposed system enhances the overall security of the ATM system by providing the fingerprint based authentication system, the system contains two layer of security which includes the old traditional 4digit PIN(Personal identification number) and fingerprint authentication.so it reduces the chance of password to be shared as it require compulsory fingerprint authentication and that is only possible when customer is present at the moment.

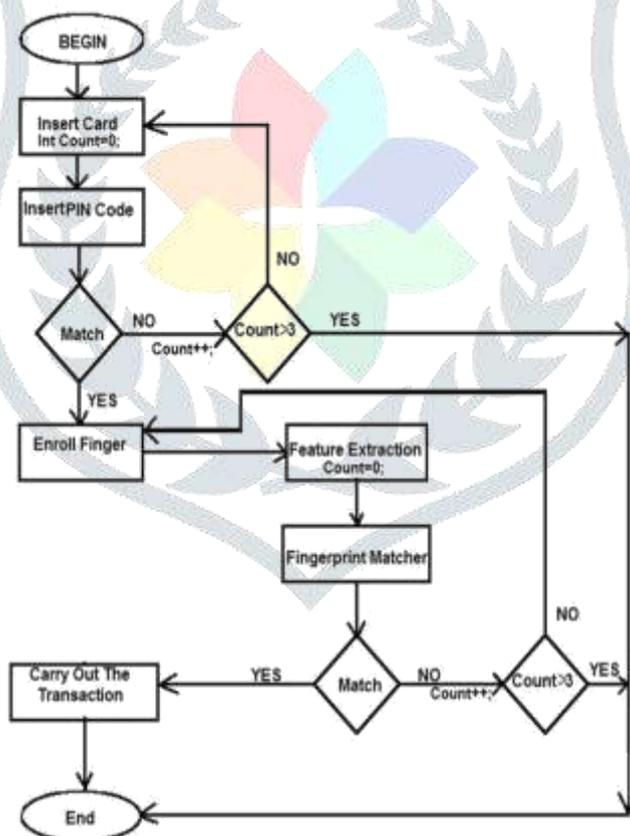


Figure:Proposed System

In figure IV.1 user initiates the transaction process by inserting the ATM card and then user have to enter his/her 4-digit PIN, if pin didn't match then system will ask user to reenter his/her 4 digit PIN and if the entered PIN Password got mached then system will asks user to enroll his finger to the fingerprint scanner after enrolling the finger feature extraction will be performed with the help of minutiae feature extraction algorithm then it will compare if it didn't match it will ask user to re-enroll his/her finger again and it will happen 3 times if fingerprint didn't match, if it got matched then the traction can be carried out.

VI. REQUIREMENT ANALYSIS

Hardware Requirement

- I3 Processor
- Minimum 512 MB RAM
- Internet Connection
- Fingerprint scanner

Software Requirement

- Windows 7 or above Operating System
- Visual Studio
- MySql
- Java

VII. MINUTIAE FEATURE EXTRACTION ALGORITHM

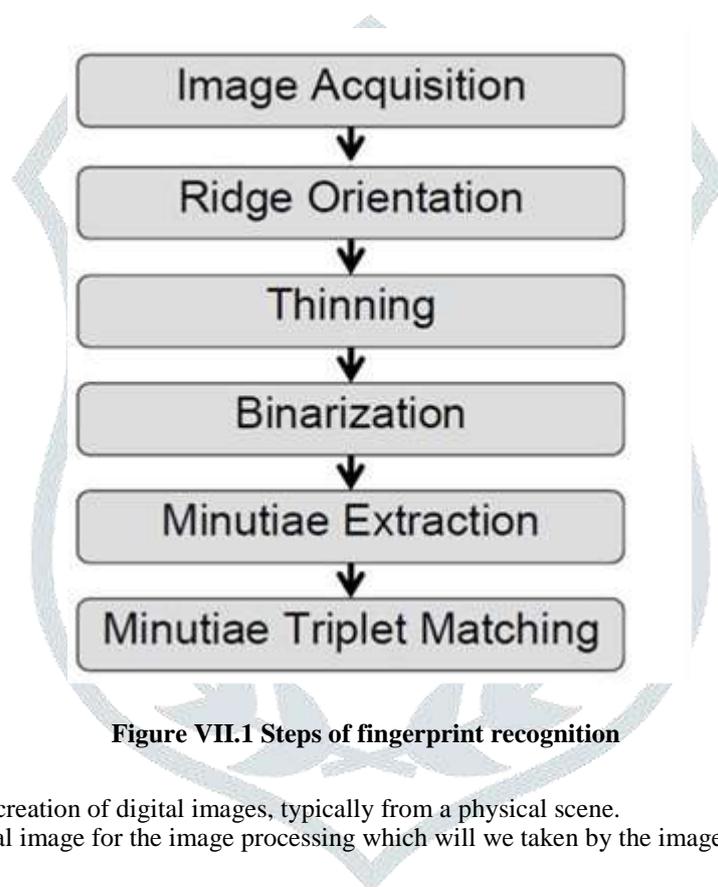


Figure VII.1 Steps of fingerprint recognition

1. Image Acquisition

Image Acquisition is the creation of digital images, typically from a physical scene.

Here, we are using the digital image for the image processing which will be taken by the image scanners and image sensors.

2. Ridge Orientation

Ridge orientation is the process of obtaining the angle of the ridges throughout the image. Ridge orientations are calculated on a block-basis for a $W \times W$ block, where, W is generally equal to 16 i.e. 16×16 block.

3. Thinning

In this step two consecutive fast parallel thinning algorithms are applied, in order to reduce to a single pixel the width of the ridges in the binary image. These operations are necessary to simplify the subsequent structural analysis of the image for the extraction of the fingerprint minutiae. The thinning must be performed without modifying the original ridge structure of the image. During this process, the algorithms cannot miscalculate beginnings, endings and or bifurcation of the ridges, neither ridges can be broken. Minutiae extraction from a perfectly thinned ridge-map of a fingerprint image is a trivial task.



Figure VII.3.(a) before thinning (b) After thinning

4. Binarization

Fingerprint binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black colour while furrows are white.

A locally adaptive binarization method is performed to binarize the fingerprint image. Such a named method comes from the mechanism of transforming a pixel value to 1 if the value is larger than the mean intensity value of the current block (16x16) to which the pixel belongs.

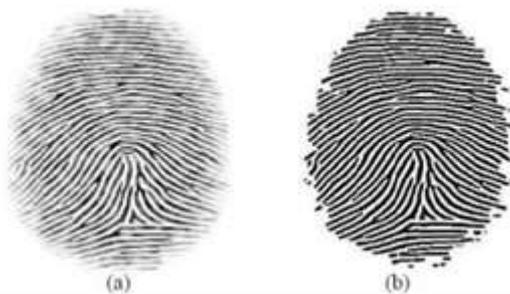


Figure VII.5(a) original Fingerprint (b)Binarized Fingerprint

5. Minutiae Extraction

Our implementation of fingerprint identification and verification is based the topological structural matching of minutiae points. We only consider two kinds of minutiae; ridge endings and bifurcations as shown in the following figure:

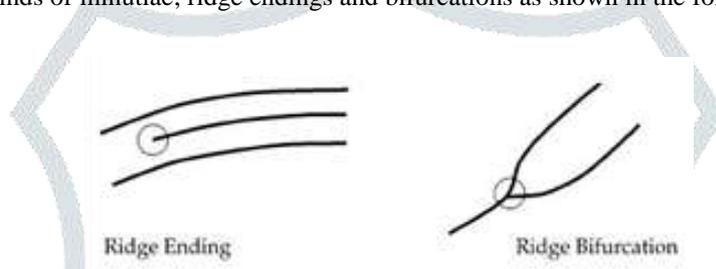


Figure VII.6 Ridge ending & ridge bifurcation

is to count the number of ridge pixels, every ridge pixel on the thinned image is surrounded by it.

However, due to noise, limitation on image acquisition, skin deformations etc the fingerprint image obtained is never ideal. As a result there are a lot of spurious minutiae that crop up if we simply follow the above approach to minutiae detection. To solve the problem, various heuristics have been proposed and we have implemented the following rules to remove most of the spurious minutiae, resulting from noise in the thinned image:

- If several minutiae form a cluster in a small region, then remove all of them except for the one nearest to the cluster centre.
- If two minutiae are located close enough, facing each other, but no ridges lie between them, then remove both of them. In addition to the noise in the fingerprint image, the thinned image may not be ideal. If such is the case, minutiae extraction may not yield the correct results.

In addition to the noise in the fingerprint image, the thinned image may not be ideal. If such is the case, minutiae extraction may not yield the correct results.

6. Minutiae Triplet Matching

Minutiae triplet matching are the step which comes after minutiae extraction and it is here that we match the minutiae obtained from two sample fingerprint images and test whether they are from the same fingerprint or not.

However, a crucial step that needs to be carried out before we can use brute force and match minutiae on two images is alignment of the images. Alignment is necessary so that we correctly match the images. We also need to take care of difference in positioning of minutiae due to plastic deformations in the finger. The algorithms prevalent for minutiae-matching either include the use of details of ridges on which minutiae are present, or use the Hough transform. Both these methods and most other methods are difficult to implement and several complicated functions need to be implemented.

Hence, we decided to implement a minutiae matching algorithm which was inspired by the techniques involving computation of local and global minutiae features.

As the name suggest, it check and compare the three main component of the image during the image processing. It simultaneously check for the ridges-ending, bifurcation, and ridges-pixels. So, the accurate matching could be achieved by eliminating the risk of unnecessary matching.

VIII. RESULTS

APPLICATION FORM NO : 1544

PAGE 1 : PERSONAL DETAILS

NAME :

FATHER NAME :

DATE: DATE: MONTH: YEAR:

GENDER: MALE FEMALE

EMAIL ADDRESS:

MARRIED STATUS: MARRIED UNMARRIED OTHER

ADDRESS:

PIN CODE:

CITY:

STATE:

next

PAGE 2 : ADDITIONAL DETAILS :

PAGE 1. RELI...

CATEGORY:

INCOME:

EDUCATIONAL QUALIFICATION:

OCCUPATION:

PAN NUMBER:

ADHARCARD NUMBER:

SENIOR CITIZEN: yes no

EXISTING ACCOUNT: yes no

next

8.1. Application form page 1

8.2. Application Form Page 2

PAGE 3 : ACCOUNT DETAILS :

ACCOUNT TYPE

saving account fixed deposit ACCOUNT

current account recurring deposit account

CARD NUMBER: XXXX-XXXX-XXXX-4104
YOUR 16 DIGIT CARD NUMBER (CHECK BOOK AND STATEMENTS)

PIN: XXXX
4-DIGIT PASSWORD

SERVICES REQUIRED:

ATM CARD INTERNET BANKING

CHEQUE BOOK EMAIL ALERTS

E-STATEMENT

I hereby declare that the above entered details correct to the best of my knowledge.

submit next

8.3. Application Form Page-3

WELCOME TO ATM

LOGIN ID:

ENTER PIN NO:

8.4. Login page

please select your transaction

8.5. Select Transaction

ENTER AMOUNT YOU WANT TO DEPOSIT

Enter pin

8.6. Deposit

Enter pin

ENTER AMOUNT YOU WANT TO WITHDRAWL

WITHDRAW
BACK

EXIT

CHANGE YOUR PIN

CURRENT PIN

NEW PIN

RE-ENTER PIN

SAVE
BACK

8.7. Withdrawl

8.8. Pin Change

IX. CONCLUSION

The main reason for introducing fingerprint authentication system is to increase overall security. By using Fingerprint based ATM we will be able to establish identity based on who we are rather than what we possess or what we remember. Much as the system may be costly to a financial institution on an ATM may be increase but safety of people's money should be considered as first priority.

X. ACKNOWLEDGEMENT

Firstly We would like to thank the open source community for providing solutions to various problems we faced in our project. We sincerely wish to thank the project guide **Prof.Shweta Patil** for her encouraging and inspiring guidance helped us to make our project a success. Our project guide made sure we were on track at all the times with her expert guidance, kind advice and timely motivation which helped us to determine our project. We would like to thank our project coordinator **Dr. Uttara Gogate** for all the support she provided with respect to project. We also express our deepest thanks to our **HOD Prof. Pramod Rodge** whose benevolent helped us by making the computer facilities Available and making it true success. Lastly, we would like to thank our college principle **Dr. J.W.Bakal** for providing lab facilities and permitting to go with our project. we would also like to thank our colleagues who helped us directly or indirectly during our project.

REFERENCES

- [1] Prof. Ranjit Mane¹, Sagar Chavan², Trushali Birambole³, Asmita kamble⁴, "Fingerprint Based ATM System", International Journal for Research Trends and Innovation (IJRTI) , ISSN:2456-3315, Volume 4, Issue 4, 2017.
- [2] SaimaRafat Bhandari¹, ZarinaBegum K Mundargi², "A Review on Securing ATM System Using Fingerprint", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN:2456-3307, Volume 3, Issue 2, 2018.
- [3] Christiawan¹, Bayu Aji Sahar², Azel Fayyad Rahardian³, Elvayandri Muchtar⁴, "Fingershield ATM – ATM Security System Using Fingerprint Authentication". Issue 4.
- [4] Vijayraj A, "A Survey on Cardless Cash Access Using Biometric ATM Security System", Scholars Journal of Engineering and Technology(SJET), ISSN 2347-9523, Issue 2.
- [5] Moses Okechukwu Onyesolu, Ignatius M. Ezeani, "ATM Security Using Fingerprint Biometric Identifier : An Investigative Study", International Journal of Advanced Computer Science and Applications(IJACSA), 030412, 2012.
- [6] Samayita Bhattacharya and Kalyani Mali," Fingerprint Recognition Using Minutiae Extraction Method", (International World Wide Web Conference Committee) © 2011 IW3C2, published under Creative Commons CC by 4.0 January, 2011.