An Approach to Authentication of Fingerprints in ATM

Sri Sachidananda S. Joshi[1], Bhavana. Desai[2], Dr. J. L. Kalyan[3]

[1]Assistant Professor, Dept of Information Science and Engineering
SDM College of Engineering and Technology, Dharwad- 580001, Karnataka
sachinjoshi055@gmail.com

[2]Research Scholar, Dept of Criminology and Forensic Science
Karnatak Science College, Dharwad- 580001, Karnataka
bhavanadesai19@gmail.com

[3]Associate Professor, HOD, Dept of Criminology and Forensic Science
Karnatak Science College, Dharwad- 580001, Karnataka
drjagdeeshkalyan@gmail.com

Abstract: ***This paper mainly deals with the authentication of the user by his fingerprint in ATM. In Conventional ATM system we use a card and a pin associated with it to authenticate ourselves. In traditional method of using card and pin to authenticate the user has many potential disadvantages, one such is the misuse of card by the third person. But by using fingerprint of the user to authenticate him, we can assure 100% security to the user. This paper contains the following modules: registering the user of the system in bank, storing the fingerprints of user with all details of him, scanning and matching of fingerprints in ATM. So this system provides a user a safe and convenient way to access their accounts in ATM without giving any chances to security issues.***

Keywords: fingerprint authentication, ATM, fingerprint verification

1. Introduction

With the increasing threat on security of ATMs the older method of using the smart card and password is not completely risk free. So, in order to overcome this drawback the proposed approach aims at authenticating a person to use the ATM through fingerprint as his identification. The main objective of the approach is:

1. To develop a application which helps to withdraw a money from ATMs
2. To store the images of FINGERPRINTS in database and match them.
3. Should be efficiently able to match the fingerprints up to cent percent accuracy without any discrepancies.

Finally end user should be given convenient and easy interface to perform the transaction.

2. Proposed System

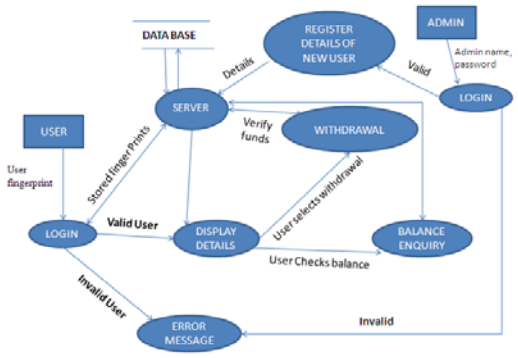

Figure 1: Data flow diagram

Here first the user gives his fingerprint as an input to the system. The system matches his fingerprint with the fingerprint images present in the database and if a match is not found, then an error message will be displayed to the user. In case, the fingerprint matches then a menu will be displayed to the user. Now the user has been authenticated and he can perform his transactions like withdrawal, balance enquiry etc. The admin logs in through his username and password. Once he has logged in his work is to register the details of the users along with their fingerprint images which uniquely identifies each of the users.

3. Implementation

Module description with its input and output:

1) ADMIN LOGIN MODULE

INPUT: Admin username and password

OUTPUT: Admin is redirected to the fingerprint enrollment page.

DESCRIPTION: The module authenticates the admin through his username and password and if he is the authorized administrator he is allowed to proceed further.

2) ENROLLMEMT MODULE

INPUT: USER NAME, PASSWORD, INITIAL BALANCE

OUTPUT: After entering all the details, it enters the enrollment process.

DESCRIPTION: The main function of the module is to enter the username, password, and initial balance according to user specified details. Once all the entries

have been given these details are being entered into the database.

3) FINGERPRINT CAPTURING MODULE

INPUT: User fingerprint.

OUTPUT: Once the user fingerprint is given he is successfully enrolled.

DESCRIPTION: The main function is to capture the fingerprint of the user and then sore them in the memory. This module captures four fingerprint samples of the user with the help of the scanner and this mainly done because each time the user enters one fingerprint sample it captures some of the features of the fingerprint and when all four samples of fingerprints are given, It combines all the features and then converts them into hexadecimal format and stores them in one file.

4) FINGERPRINT VERIFICATION SYSTEM

INPUT: User enters his username and password and gives appropriate option according to his needs.

OUTPUT: According to the option specified by the user the result is displayed.

DESCRIPTION: This main function is to prompt the user to enter his username and password after he enters into the system. Once he enters his username and password then user has two options to choose from either he can view his balance or he can transact the required amount from his account.

5) BALANCE ENQUIRY

INPUT: User enters his username and password.

OUTPUT: Once the user clicks on the balance enquiry button his account balance is displayed.

DESCRIPTION: This main function is to prompt the user to enter his username and password, once the password is entered the balance enquiry button becomes active till then which was inactive. Once the user clicks on this button the module authenticates the user through his username and password and if both are correct then the user's account balance is been displayed.

6) TRANSACTION

INPUT: User enters his username and password and specifies the required amount which he wants to withdraw from his account.

OUTPUT: If the user is authorized user then he is allowed transacting the amount.

DESCRIPTION: This main function is to prompt the user to enter his username and password, and then specify the amount which he wants to withdraw from his account. Once the user clicks on this button the module prompts the user through his fingerprint sample on the scanner and then it authenticates the user through his fingerprint sample by matching it with the one which is present in the memory. Incase if the fingerprint doesn't match, the user is given another two chances for verifying his fingerprint and then he is not to transact the amount and his account is being blocked. If the fingerprint matches then the user is allowed to transact the required amount.

4. Results

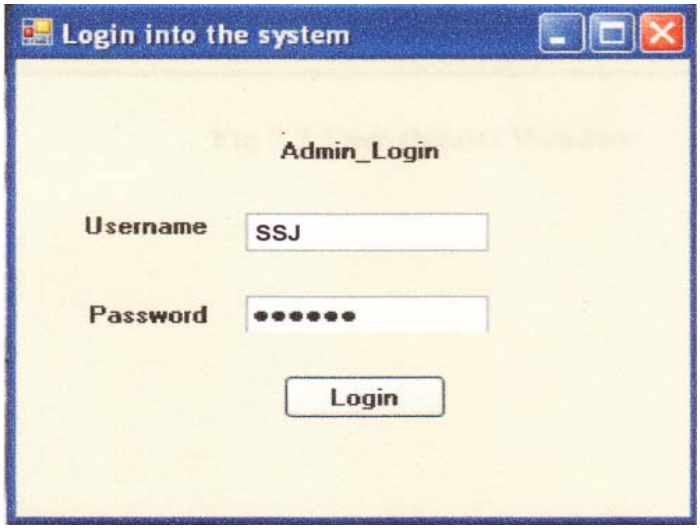

Figure 2: Admin Login

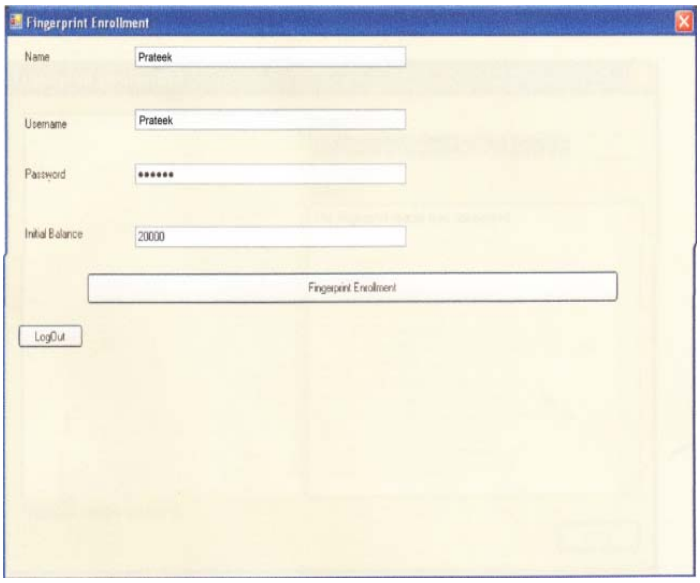

Figure 3: Fingerprint Enrollment process

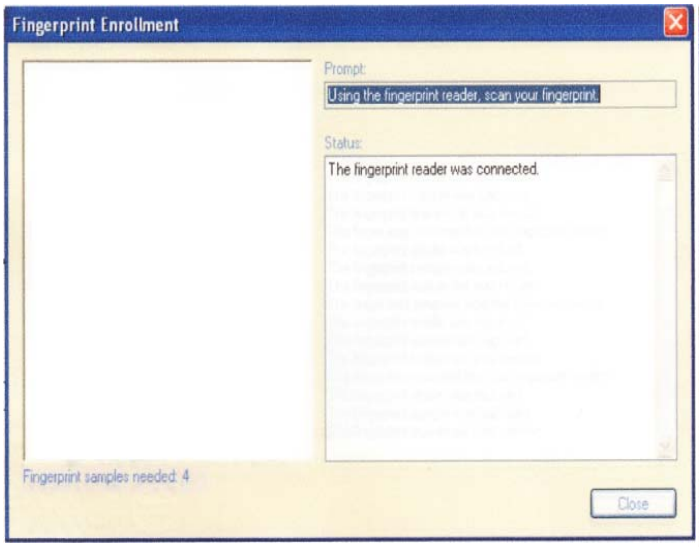

Figure 4a: Finger print Capturing process

Figure 4b: Finger print Capturing process

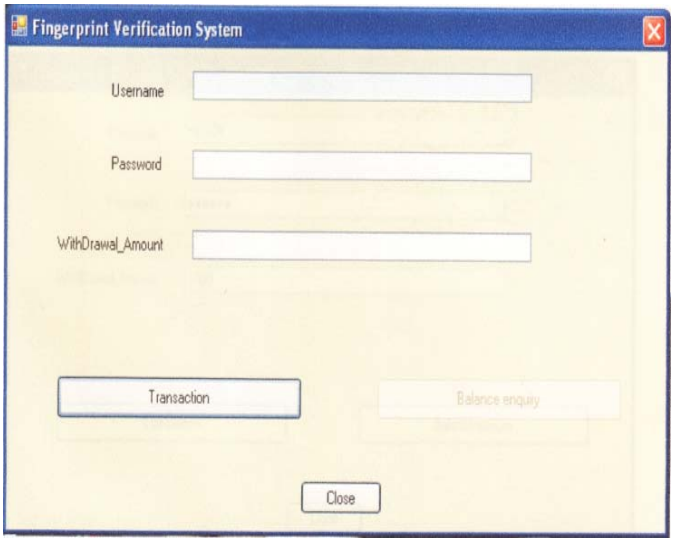

Figure 5: Transaction window for User

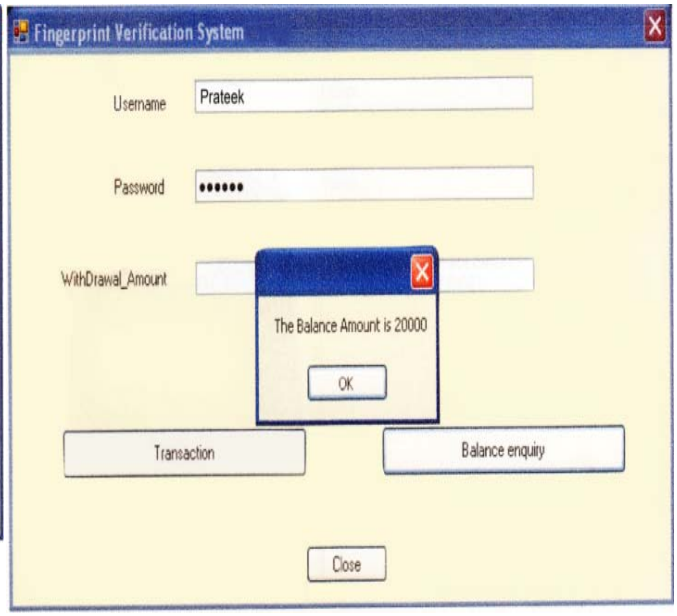

Figure 6: Balance Enquiry window for user

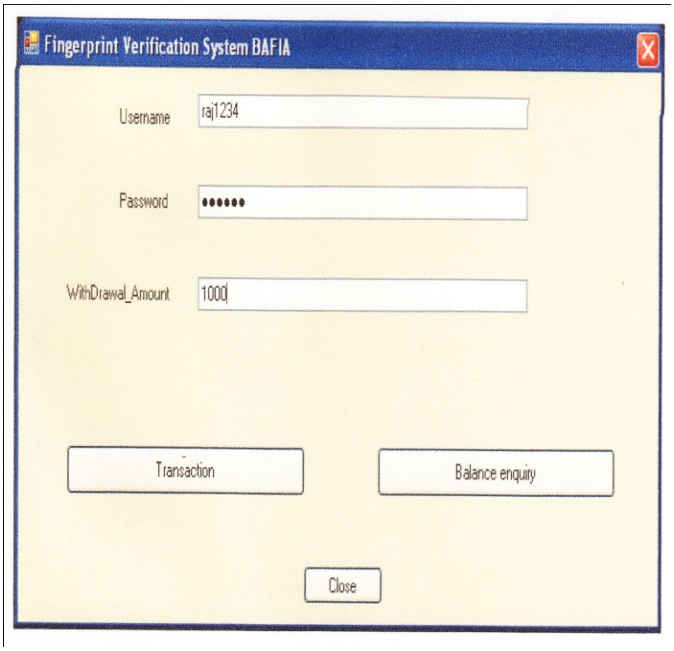

Figure 7: Withdrawal window for User

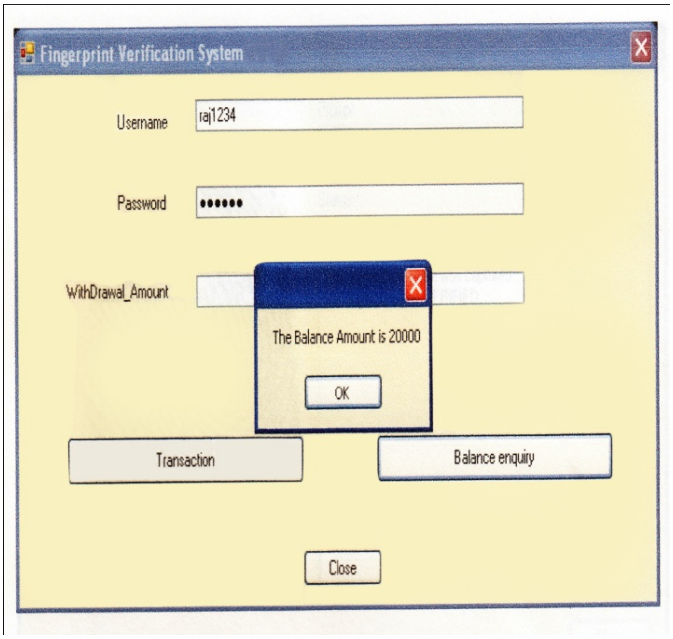

Figure 8: Verification window for user

5. Conclusion and future Scope

This approach is a simple matching algorithm for sets of fingerprint minutiae. The purpose of this approach provides a simple algorithm for comparing with and black box analysis of other, typically commercial, undisclosed fingerprint matching algorithms. However, there are still some issues left for possible future work: it might be desirable to have the algorithm output a degree of likeliness that two given minutiae sets stem from the same finger instead of just a plain positive/negative output, although the utility of this functionality probably depends on the application. The future scope will be to extend the facility of joint account.

References

[1] L.C.Jain, I Hayashi, S.B.Lee "Intelligent Biometric Techniques in Finger Print", CRC Press, 1999(book style)

[2] Anil K. Jain, "Fundamentals of Digital Image Processing", Prentice Hall, U.S.A, 1989 (book style)

[3] Simon Haykin,Bart Kosko, "Intelligent Signal Processing" IEEE Press 2002(journal style)

[4] P.J.Phillips, A.Martin, C.Wilson and M. Przybocki, " An Introduction to Evaluating Biometric Systems ", IEEE Computer, February 2000 (journal style)

Author Profile

Sri Sachidananda S Joshi, Assistant professor at SDM College of Engineering and Technology from Dharwad Karnataka, areas of interest are Network Security, Computer Networks.

Bhavana Desai, Research scholar, pursuing PhD in Forensic Science from Karnataka University, Dharwad, Karnataka. Her areas of interest are Finger Prints, Questioned Document Verification, and Toxicology

Dr. J L Kalyan, Associate professor HOD of Criminology and Forensic Science in Karnataka Science College Dharwad. His areas of interest are Finger Prints, Questioned Document Verification.