ATMIYAUNIVERSITY

RAJKOT

A

ReportOn

FINGERPRINT AUTHENTICATION FOR ATM

Undersubjectof

PROJECT

B.TECH,Semester– VII

(Computer Engineering)

Submittedby:

1.	NIRAV HIRANI	190002041
2.	AHREY VEGAD	190002122

Prof. Nirali Borad

(FacultyGuide)

Prof. Tosal M.Bhalodia

(Head of the Department)

AcademicYear

(2021-22)

CANDIDATE'SDECLARATION

We hereby declare that the work presented in this project entitled "FINGERPRINT AUTHENTICATION FOR ATM**"** submitted towards completion of project in **7th Semester** of B.Tech. (Computer Engineering) is an authentic record of our original work carriedout under theguidance of "**Prof. Nirali Borad".**

We have not submitted the matter embodied in this project for the award of anyotherdegree.

Semester:
7thPlace:Rajot

Signature:
Nirav Hirani (190002041)

Ashrey Vegad (190002122)

ATMIYA

UNIVERSITYRAJKOT

CERTIFICATE

Date:

This is to certify that the “FINGERPRINT AUTHENTICATION FOR ATM” has been carried out by **Nirav Hirani** under my guidance in fulfillment of the subject Project in COMPUTER ENGINEERING (7thSemester) of Atmiya University, Rajkotduringtheacademic year 2021.

Prof. Nirali Borad

(Project Guide)

Prof.Tosal M.Bhalodia

(Head oftheDepartment)

ATMIYA

UNIVERSITYRAJKOT

CERTIFICATE

Date:

This is to certify that the “**The Fingerprint Authentication for ATM**” has been carried out by **Ashrey Vegad** under my guidance in fulfillment of the subject Project inCOMPUTER ENGINEERING (7th Semester) of Atmiya University, Rajkot duringtheacademicyear 2021.

Prof. Nirali Borad Prof.Tosal M.Bhalodia

(Project Guide) **(Head of the Department)**

ACKNOWLEDGEMENT

We have taken many efforts in this project. However, it would not have been possible withoutthe kind support and help of many individuals and organizations. We would like to extend oursincerethanks to all of them.

We are highly indebted to Prof. Nirali Borad for their guidance and constant supervision aswellasforprovidingnecessaryinformationregardingtheMiniProjecttitled **“**FINGERPRINT AUTHENTICATION FOR ATM**”.** We would like to express our gratitude towards staff members of Computer Engineering Department, Atmiya University for their kind co- operation and encouragementwhichhelped us in completion of this project.

We even thank and appreciate to our colleague in developing the project and people who havewillinglyhelped us out with theirabilities.

Nirav Hirani (190002041)

Ashrey Vegad (190002122)

ABSTRACT

Our Project 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. The underlying principle is the phenomenon of biometric “AUTHENTICATION”. In this project we propose a method for fingerprint matching based on minutiae matching.

CHAPTER 1: INTRODUCTION

1.1 PROBLEM STATEMENT

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.

1.2 OBJECTIVE

The objective of our project is to provide biometric security through fingerprint authentication in ATM application. 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 biometrics “AUTHENTICATION”, in this project we propose a method for fingerprint matching based on minutiae matching.

1.3 DESCRIPTION OF FINGERPRINT

The fingerprint is arguably a person’s most unique physical characteristic. While humans have had the innate ability to recognize and distinguish different fingerprints for millions of years, computers are just now catching up…

The twist of this software is that it can pick someone's fingerprint out of crowd, extract that fingerprint for the rest of the scene and compare it with database full of stored images.

In order for this software to work, it has to know what a basic fingerprint looks like. Fingerprint recognition software is based on the ability to first recognize fingerprint, which is a technological feat in itself, and then measure the various features of each fingerprint.

Figure 1.1

1.4 WHAT IS A FINGERPRINT?

A fingerprint is the feature pattern of one finger (Figure 1.2.1). It is believed with strong evidences that each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have being used for identification and forensic investigation for a long time.

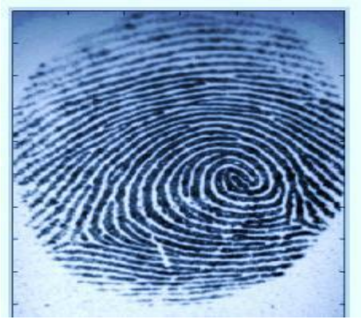


Figure 1.2.1

A fingerprint is composed of many ridges and furrows. These ridges and furrows present good similarities in each small local window, like parallelism and average width. However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by Minutia, which are some abnormal points on the ridges (Figure 1.1.2). Among the variety of minutia types

1.5 WHAT IS FINGERPRINT AUTHENTICATION

The fingerprint authentication problem can be grouped into two sub-domains. One is fingerprint verification and the other is fingerprint identification (Figure 1.3). In addition, different from the manual approach for fingerprint authentication by experts, the fingerprint authentication here is referred as FAA (Fingerprint Authentication in ATM), which is program based.

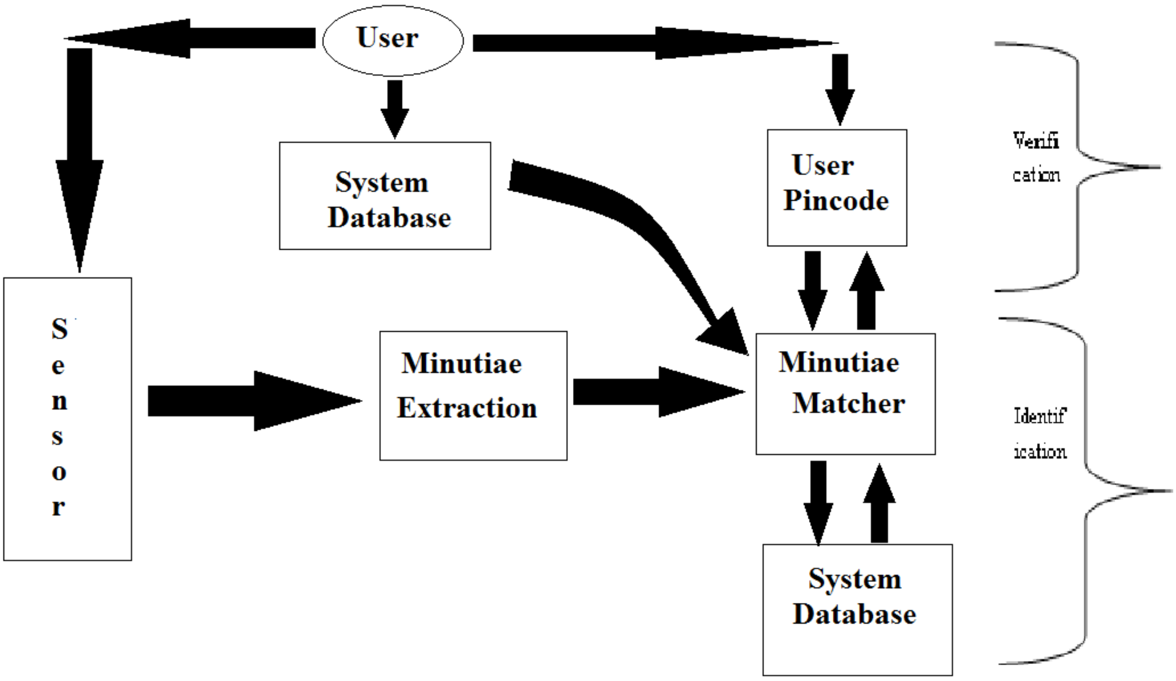


Figure 1.3 Verification vs. Identification

Fingerprint verification is to verify the authenticity of one person by his fingerprint. The user provides his fingerprint together with his identity information like his PIN-CODE. The fingerprint verification system retrieves the fingerprint template according to the PIN-CODE and matches the template with the real time acquired fingerprint from the user. Usually it is the underlying design principle of AFAS (Automatic Fingerprint Authentication System). Fingerprint identification is to specify one person's identity by his fingerprint(s). Without knowledge of the person's identity, the fingerprint identification system tries to match his fingerprint(s) with those in the whole fingerprint database. It is especially useful for criminal investigation cases. And it is the design principle of AFIS (Automatic Fingerprint Identification System). However, all fingerprint recognition problems, either verification or identification, are ultimately based on a well-defined representation of a fingerprint.

1.6 APPROACHES FOR FINGERPRINT RECOGNITION

Two representation forms for fingerprints separate the two approaches for fingerprint recognition.

1. Minutia - based: The first approach, which is minutia-based, represents the fingerprint by its local features, like terminations and bifurcations. This approach has been intensively studied, also is the backbone of the current available fingerprint recognition products. We also concentrate on this approach in our project.

2. Image-based: The second approach, which uses image-based methods, tries to do matching based on the global features of a whole fingerprint image. It is an advanced and newly emerging method for fingerprint recognition. And it is useful to solve some intractable problems of the first approach. But our project does not aim at this method, so further study in this direction is not expanded in our thesis.

CHAPTER 2: SOFTWARE REQUIREMENT SPECIFICATION (SRS)

2.1 INTRODUCTION

- **Purpose**

This Software Requirements Specification provides a complete description of all the functions and specifications of the ATM system of bank. The purpose is to provide extra security to the ATM systems.

- **Scope**

The ATM system is designed to run for 24 hours and to allow bank clients to carry out transactions in a secured way. The data will be held in a bank database. The system is connected to the bank database using a modem.

- **Document Overview**

The remainder of this document is two chapters, the first providing a **full description** of the project for the bank's ATM with fingerprint security. This SRS gives the details about the various **requirements** & about the various hardware & software interfaces.

2.2 OVERALL DESCRIPTION

The ATM system encompasses various GUI menus including the SENSOR, to provide high security. It provides secure access to the account of a customer. The ATM must be able to provide the following **services** to the customer:

Enter Pin: A customer is allowed to enter the PIN Code for his/her Account.

Change Pin: A customer must be able to change the pin linked to the card.

Enroll Finger: A customer is allowed to enroll the fingerprint impression which has been used to provide security to the Account**.**

Change Fingerprint: A customer is allowed to change the fingerprint impression.

2.3 FUNCTIONAL REQUIREMENT

The software to be designed will control a simulated automated teller machine (ATM) having:-

- A sensor to enroll and detect fingerprint.

- A customer console (keyboard and display) for interaction with the customer.(for entering PIN Code)

- **Facility of Aborting transaction**

A customer must be able to abort a transaction in progress by pressing the Cancel key instead of responding to a request from the machine.

- **PIN Code format**

Pin should be of exactly 4 digit.

- **Facility of PIN Re-entering**

If the customer's PIN is invalid, the customer will be required to re-enter the PIN before a transaction can proceed.

- **Denial of service, if PIN goes wrong.**

If the customer is unable to successfully enter the PIN after three tries, the service would be denied for particular card.

- **Enroll finger**

Enroll your finger from first joint to the tip.

- **Facility of Re-enrolling the finger**

If the customer's Fingerprint is invalid, the customer will be required to re-enroll the Fingerprint before a transaction can proceed.

- **Denial of service, if fingerprint goes wrong**

If the customer is unable to successfully enroll fingerprint after three tries, the service would be denied for that particular card.

2.4 NON FUNCTIONAL REQUIREMENT

There are requirements that are not functional in nature. Specifically, these are the constraints the system must follow. They are often called qualities of a system. Other terms for non-functional requirements are “constraints”,” quality attributes”,” quality goals”,” quality of service requirements” and “non-behavioral requirements”.

□ **Scope:** The scope of this project is to allow the user to get access to their account through the ATM using fingerprinting functionality.

□ **Functionality:** One customer at a time can process their account in the ATM machine.

□ **Usability:** The desktop user interface shall be Windows XP/Vista/7 complaint.

□ **Reliability:** The ATM machine must be able to scan or read the card and the fingerprint properly and identify the customer account.

□ **Performance:** The ATM machine support only one customer at a time. The speed and accurate transaction decides the performance factor. The screen must be clearly visible to the user.

□ **Security:** The pin number and the fingerprint in the card guarantee the security of a customer’s account. The ATM system must not store any of this data in its database. The customer with a pin number and a valid card with valid fingerprint impression is allowed to do all transactions.

2.5 FRONT END DESCRIPTION

For developing the front – end interface, we have decided to use ASP.NET platform, with C# as the programming language, due to the following reasons:-

□ Easy to use and flexible interface.

□ A number of options for customizability.

 Proven to provide good performance and high reliability.

 Attractive and visually pleasing interface.

2.6 BACK END DESCRIPTION

For the Image Processing (Minutiae Matching), we have decided to use MATLAB R2012b, due to the following reasons:-

 Full compatibility with various different databases.

 Easy to use and flexible interface.

 Word wide product for the image processing.

 Used by market-leading companies worldwide.

 Easy to code, and easy to convert the files In Dynamic Link Library (DLL) format.

For developing the database (back – end), we have decided to use MS-SQL Server 2008 R2 database, due to the following reasons:-

 Native support and full compatibility with ASP.NET platform.

 Flexible, scalable and robust database architecture.

 Used by market-leading companies worldwide.

 Strong data protection and ease of management.

2.7 DATABASE DESCRIPTION

Tools Used:

Interface	-	Visual Studio 2010 Ultimate
Database	-	MS SQL Server 2008 R2

- Image Processing - MATLAB R1012b

2.8 HARDWARE REQUIREMENT

- Processor - Pentium 4
- Hard Disk - 20GB
- RAM - 256 MB
- Sensor - Fingerprint Recognizer

2.9 SOFTWARE REQUIREMENT

- Operating System - Windows XP/Vista/7
- Database System - MS SQL Server 2008 R2
- Front End - Visual Studio 2010 Ultimate
- Framework - .Net Framework 4.0

CHAPTER 3: DIAGRAMS

3.1 FLOW CHART

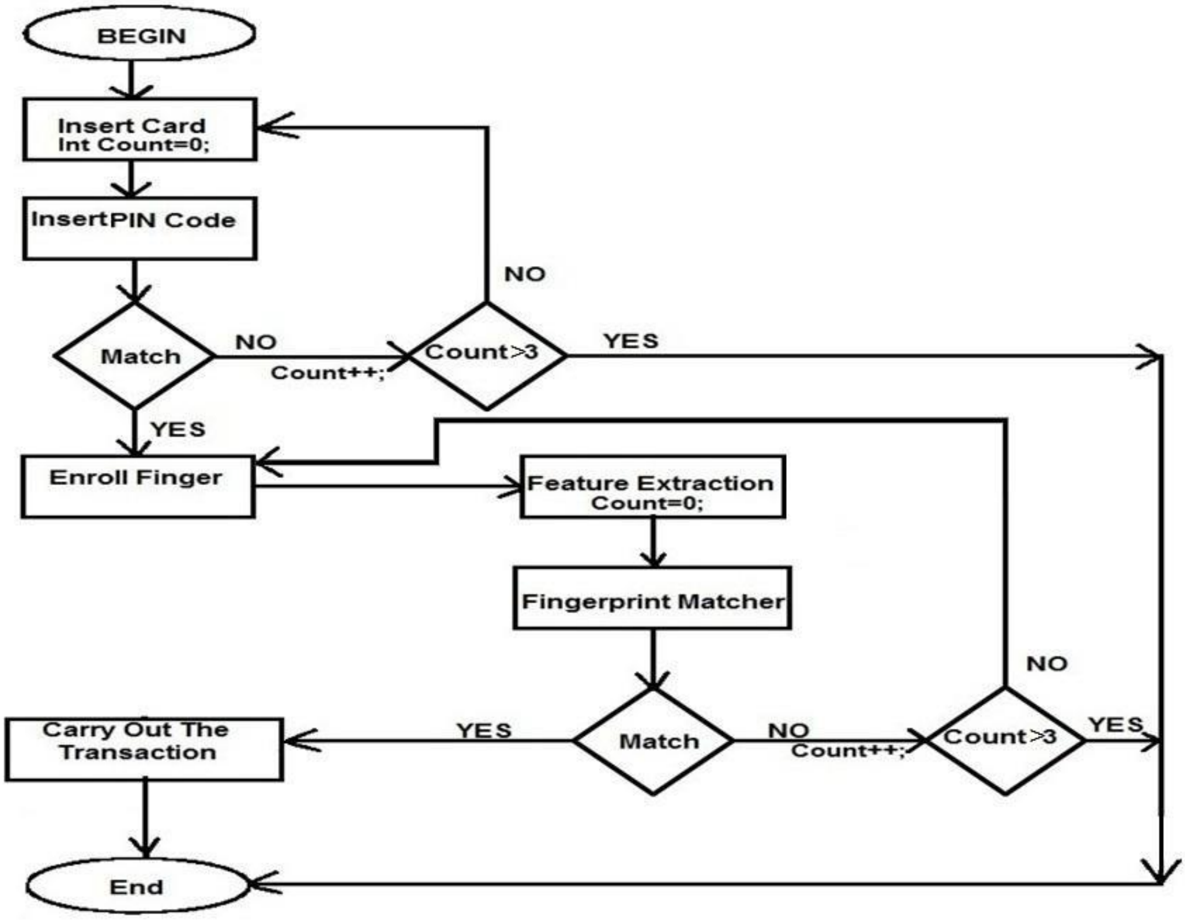


Figure 3.2 Flow chart diagram

3.2 USE CASE DIAGRAM

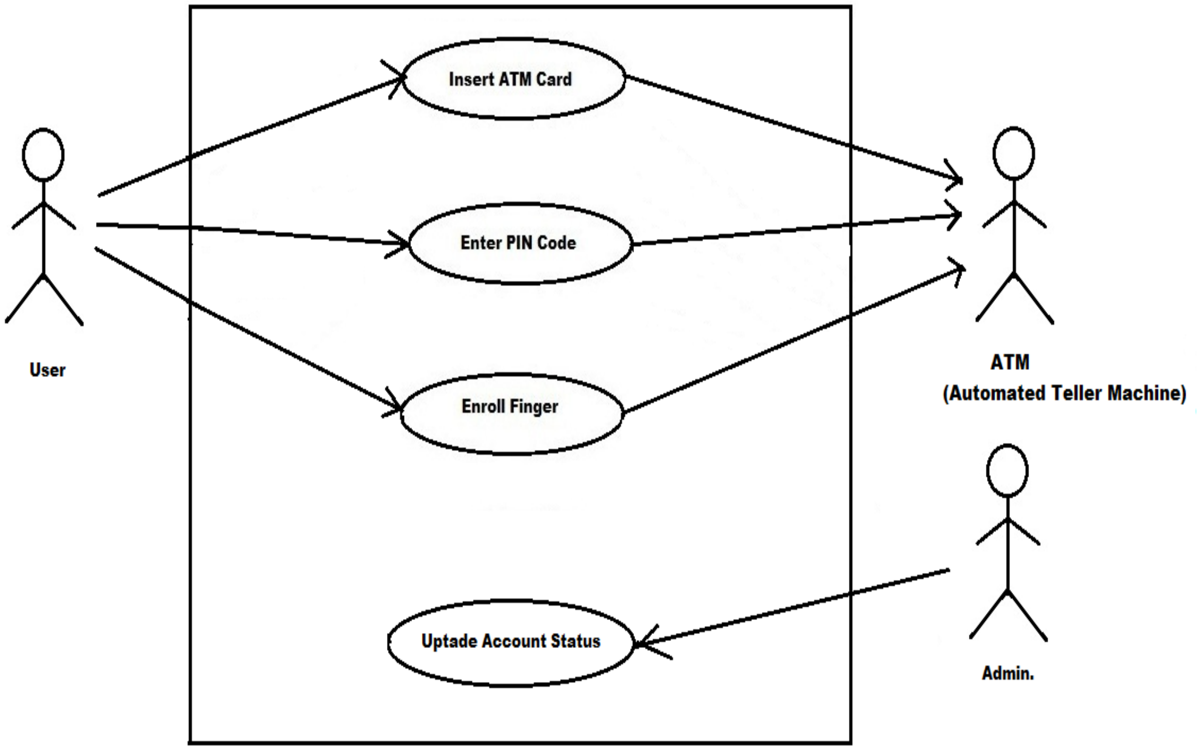


Figure 3.4 Use case diagram

3.4 SEQUENCE DIAGRAM

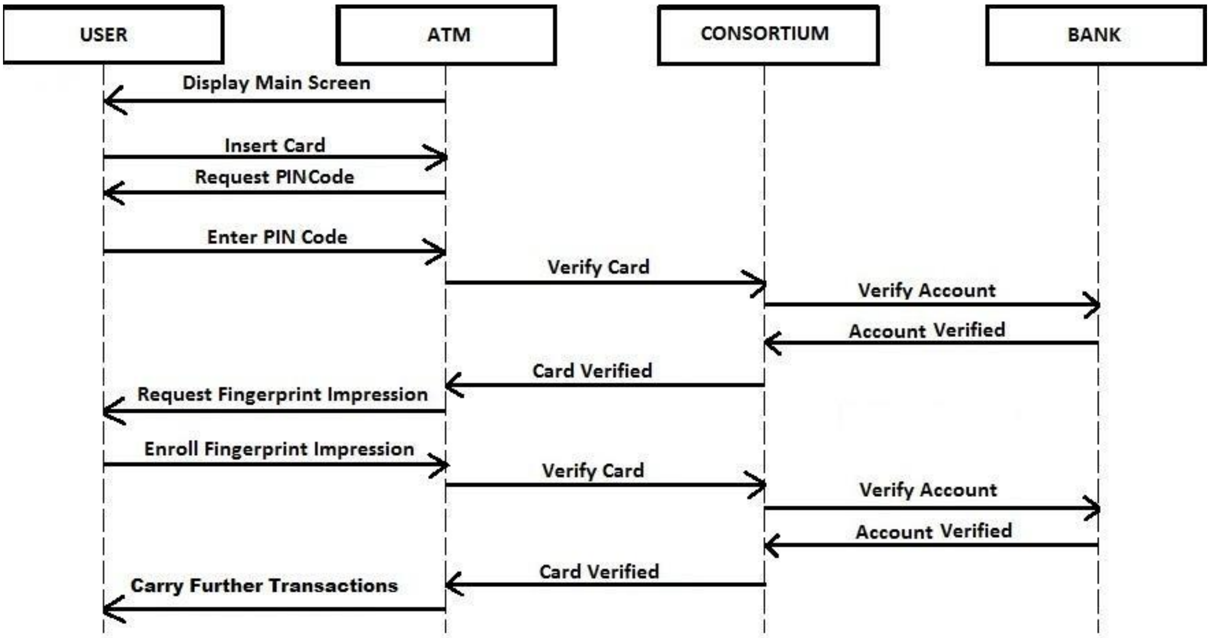


Figure 3.7 Sequence diagram

3.3 E-R DIAGRAM

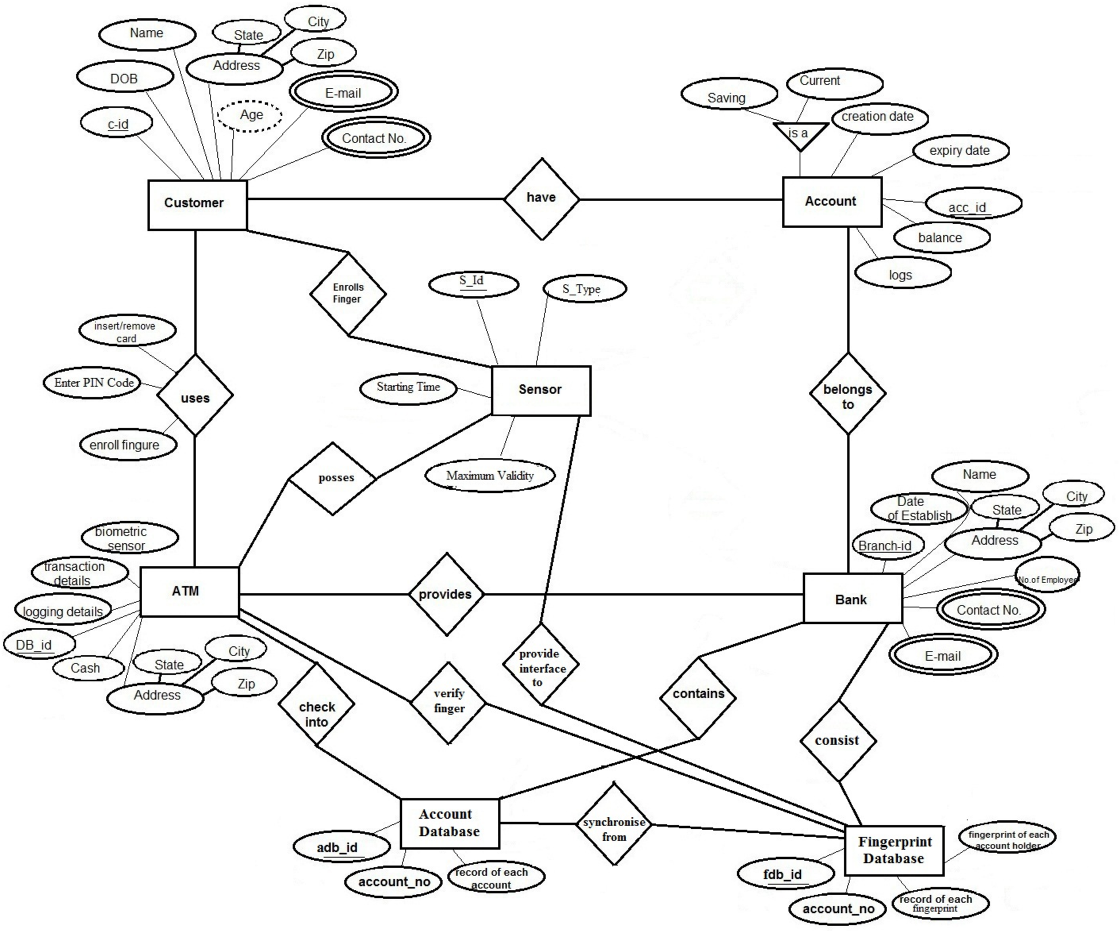


Figure 3.6 Entity Relationship Diagram

3.5 ACTIVITY DIAGRAM

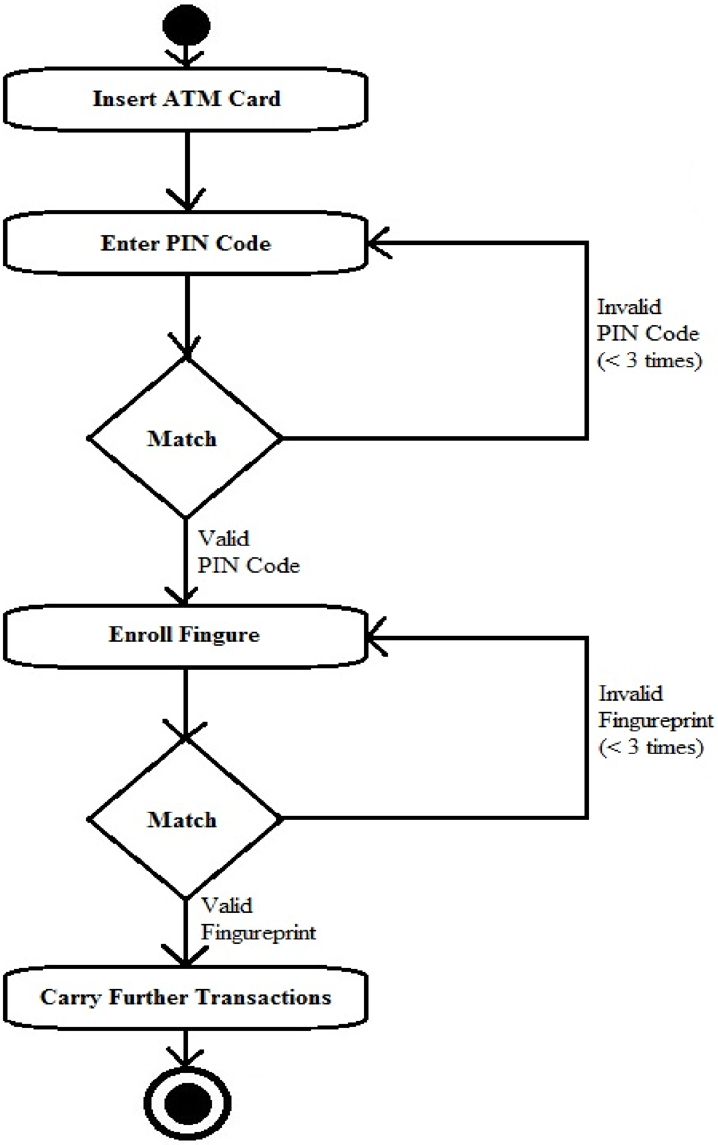


Figure 3.9 Activity Diagram

3.6 DATA FLOW DIAGRAM

3.6.1 DATA FLOW DIAGRAM LEVEL 0

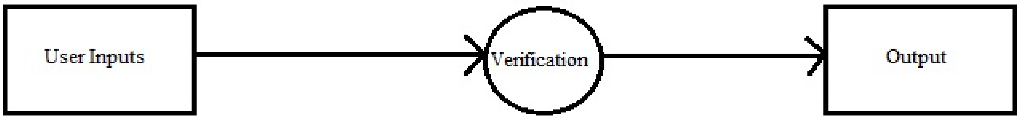


Figure 3.11 DFD Level 0

3.6.2 DATA FLOW DIAGRAM LEVEL 1

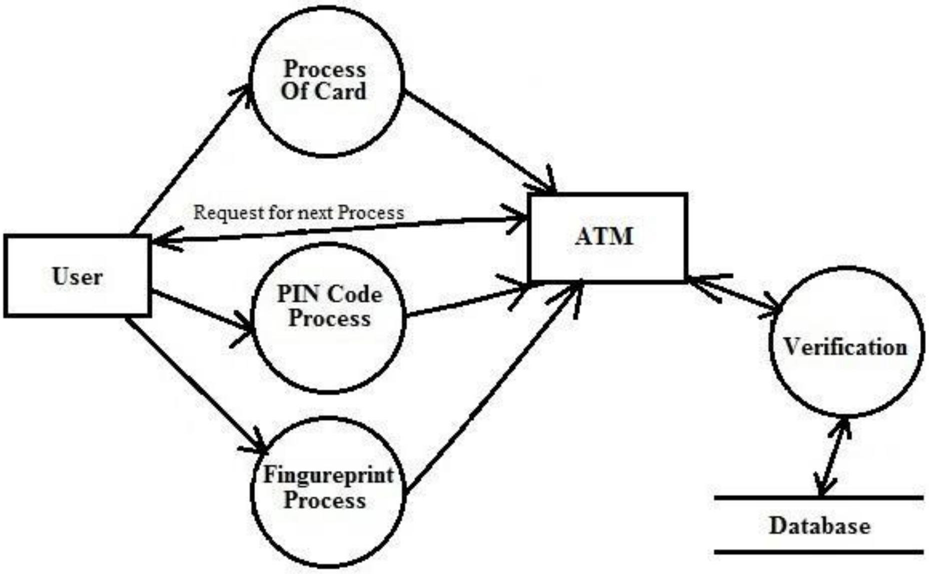


Figure 3.12 DFD Level 1

3.6.3 DATA FLOW DIAGRAM LEVEL 2

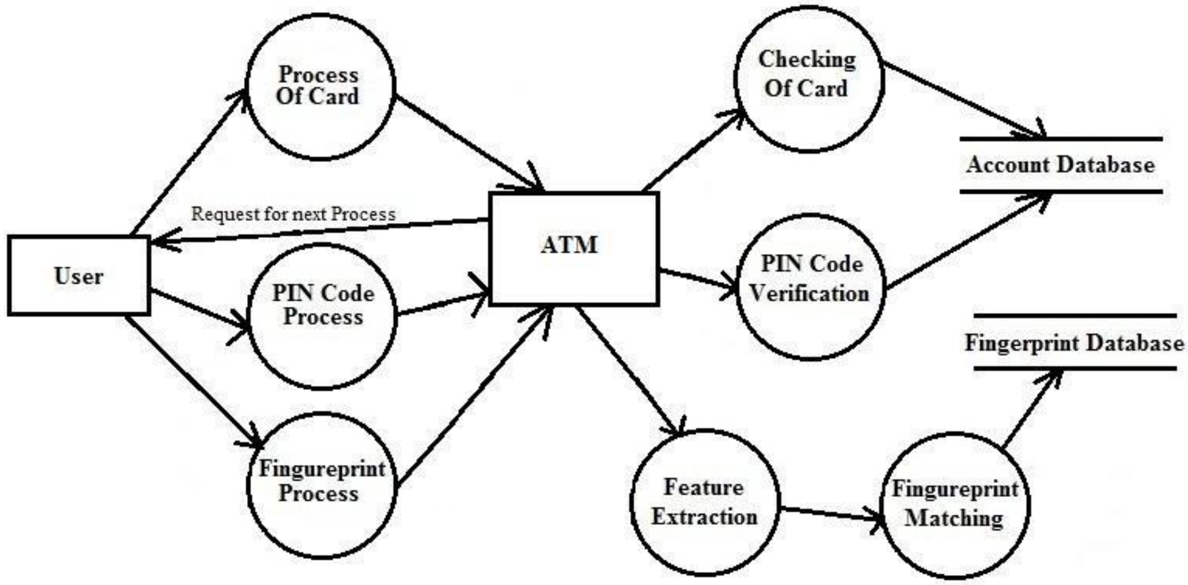


Figure 3.13 DFD Level 2

CHAPTER 4: SYSTEM DESIGN

4.1 OVERVIEW OF SYSTEM DESIGN

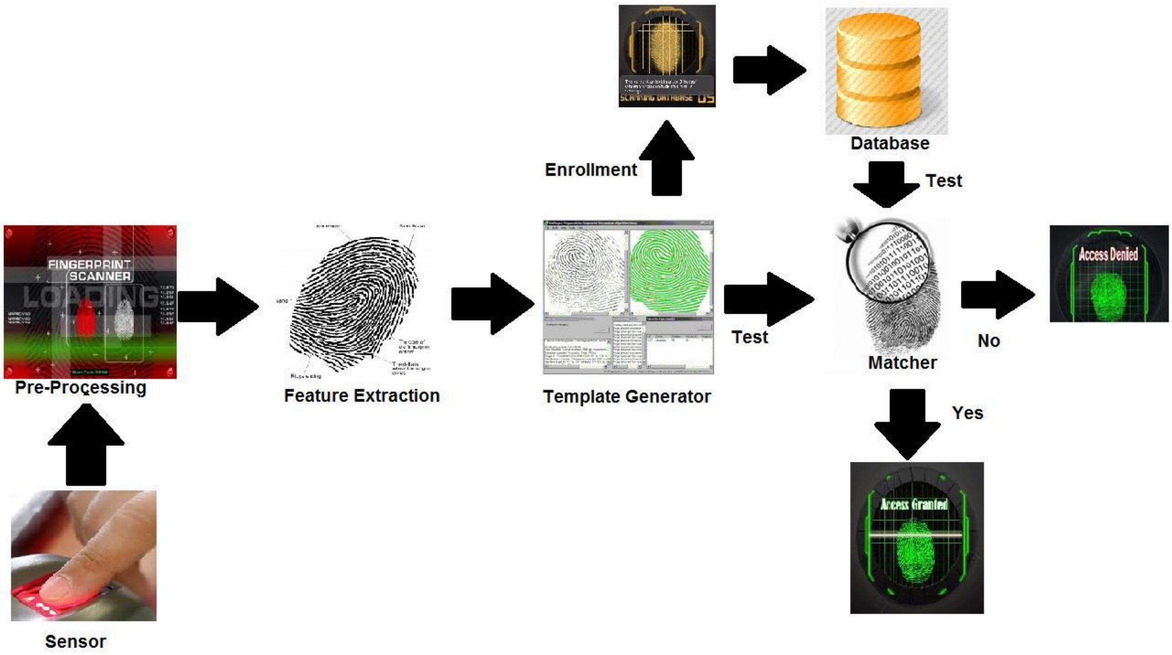
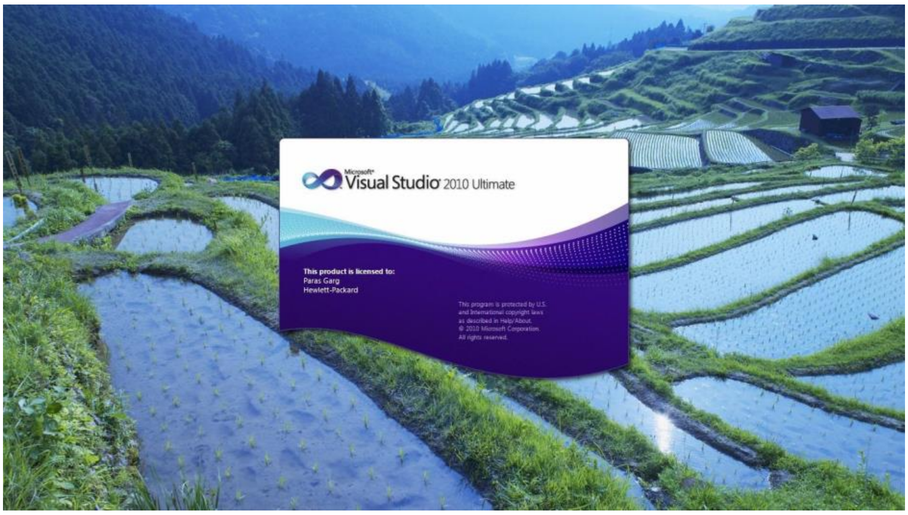


Figure 4.1 System design overview

4.2 INTERFACE SOFTWARE

The front end or the interface of our project is created on the Microsoft Visual Studio 2010 Ultimate. The following snapshots are use to aware from the software environment, how to use it and how to modify the application interface and utility of project by the software functionality.

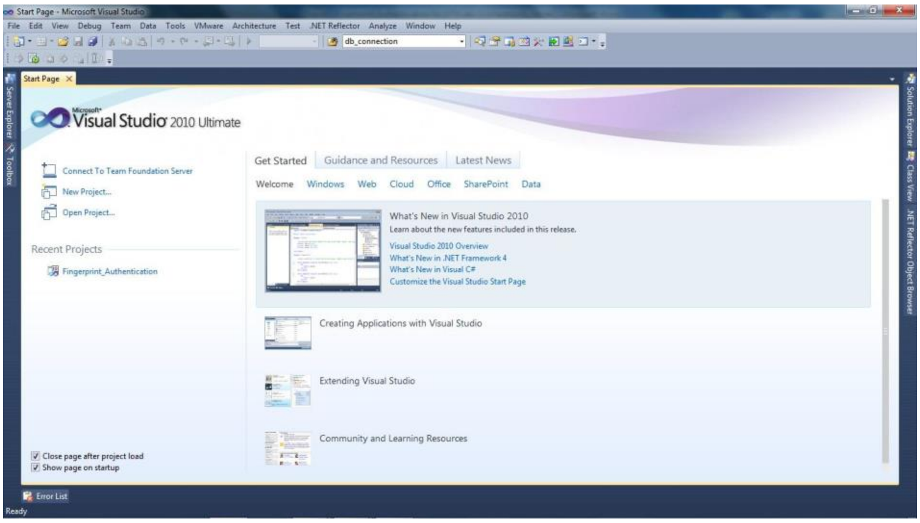
STEP 1 – Start Microsoft Visual Studio 2010 Ultimate.



This product is licensed to:
Paras Garg
Hewlett-Packard

This program is protected by U.S. and International copyright laws as described in Help/About.
© 2010 Microsoft Corporation.
All rights reserved.

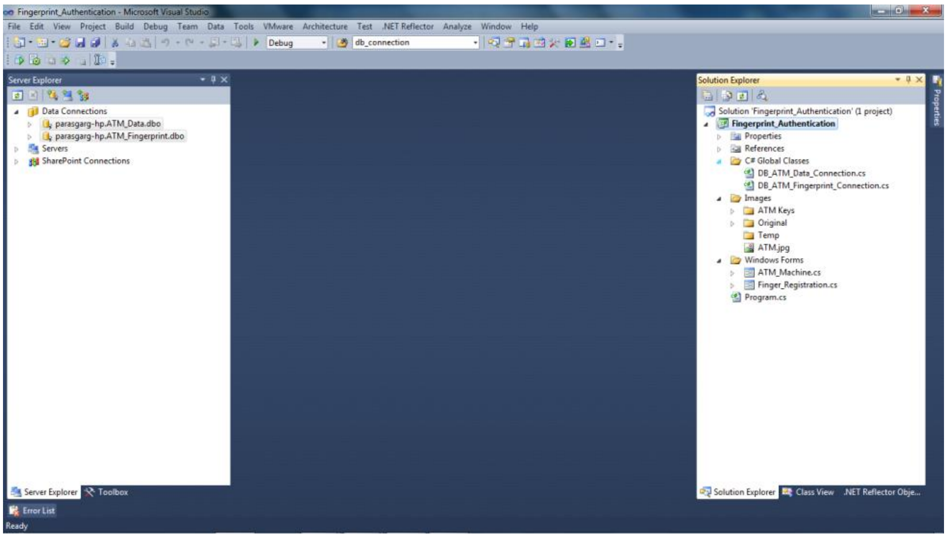
STEP 2 – Choosing the project from the Recent Project List.


Start Page - Microsoft Visual Studio
File
Edit
View
Debug
Team
Data
Tools
VMware
Architecture
Test
.NET Reflector
Analyze
Window
Help
db_connection
Start Page
Server Explorer
Toolbox
Solution Explorer
Class View
.NET Reflector Object Browser
Microsoft® Visual Studio 2010 Ultimate
Connect To Team Foundation Server
New Project...
Open Project...
Recent Projects
Fingerprint_Authentication
Get Started
Guidance and Resources
Latest News
Welcome
Windows
Web
Cloud
Office
SharePoint
Data
What's New in Visual Studio 2010
Visual Studio 2010 Overview
What's New in .NET Framework 4
What's New in Visual C#
Customize the Visual Studio Start Page
Creating Applications with Visual Studio
Extending Visual Studio
Community and Learning Resources
Error List
Ready

Learn about the new features included in this release.

☑ Close page after project load
☑ Show page on startup

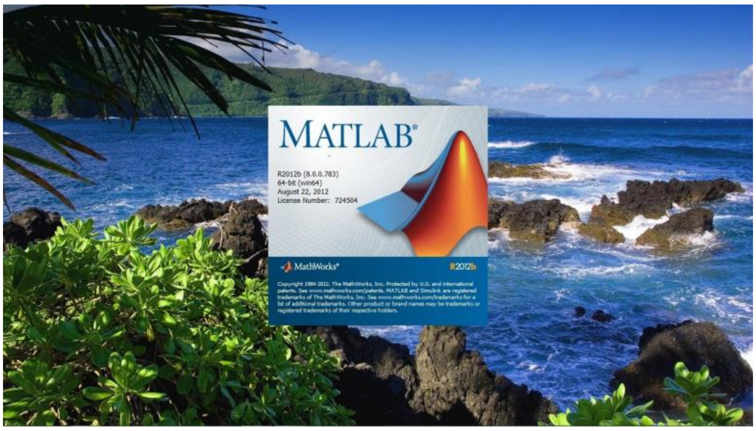
STEP 3 – Checking the database connectivity from Server Explorer in the left and checking the Solution Explorer in the right to modify the project interface**.**


Fingerprint_Authentication - Microsoft Visual Studio
File Edit View Project Build Debug Team Data Tools VMware Architecture Test .NET Reflector Analyze Window Help
Debug
db_connection
Server Explorer
Data Connections
parasgarg-hp.ATM_Data.dbo
parasgarg-hp.ATM_Fingerprint.dbo
Servers
SharePoint Connections
Solution Explorer
Solution 'Fingerprint_Authentication' (1 project)
Fingerprint_Authentication
Properties
References
C# Global Classes
DB_ATM_Data_Connection.cs
DB_ATM_Fingerprint_Connection.cs
Images
ATM Keys
Original
Temp
ATM.jpg
Windows Forms
ATM_Machine.cs
Finger_Registration.cs
Program.cs
Server Explorer
Toolbox
Solution Explorer
Class View
.NET Reflector Obje...
Properties
Error List
Ready

4.3 IMAGE PROCESSING SOFTWARE

The back end functionality of our project is created on the Mathworks Matlab R2012b. The following snapshots are use to aware from the software environment, how to use it and how to modify the back end functionality of project for the image processing and the database connectivity related to information sharing by the software functionality.

STEP 1 - Start Mathworks Matlab R2012b.

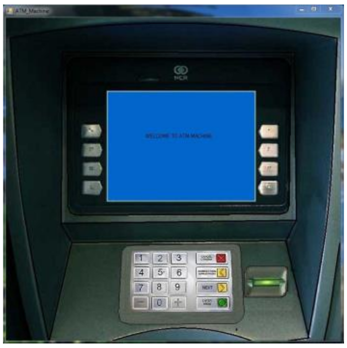


R2012b (8.0.0.783)
64-bit (win64)
August 22, 2012
License Number: 724504

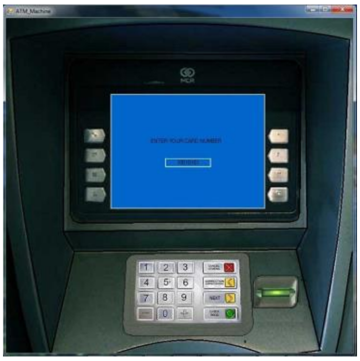
Copyright 1984-2012. The MathWorks, Inc. Protected by U.S. and international patents. See www.mathworks.com/patents. MATLAB and Simulink are registered trademarks of The MathWorks, Inc. See www.mathworks.com/trademarks for a list of additional trademarks. Other product or brand names may be trademarks or registered trademarks of their respective holders.

4.4 PROJECT MODEL

4.4.1 GRAPHICAL USER INTERFACE (GUI)



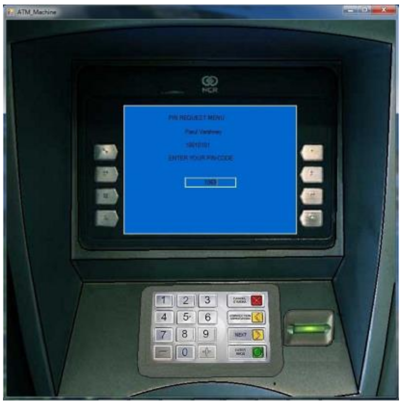
WELCOME TO ATM MACHINE



ENTER YOUR CARD NUMBER

STEP 1 STEP 2

Snapshot is showing the welcome page *Snapshot is showing the card request page*

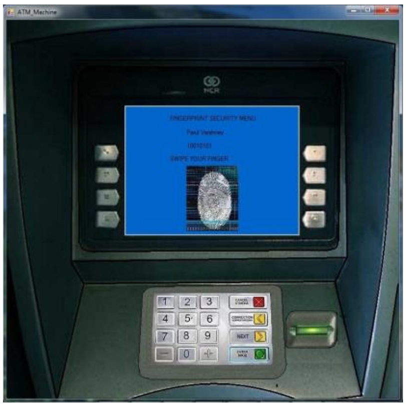


PIN REQUEST MENU

[illegible]

[illegible]

ENTER YOUR PIN CODE



FINGERPRINT SECURITY MENU

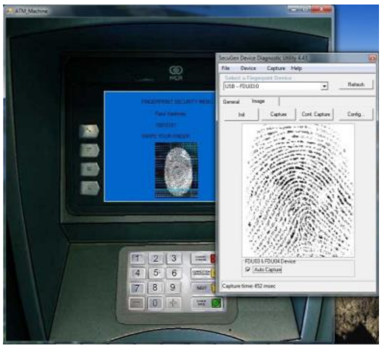
[illegible]

[illegible]

SWIPE YOUR FINGER

STEP 3 *STEP 4*

Snapshot is showing the pin request page Snapshot is of request for enrol finger



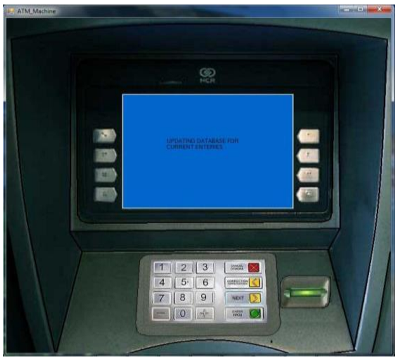
FINGERPRINT SECURITY MENU

SWIPE YOUR FINGER

Capture time: 452 msec

STEP 5

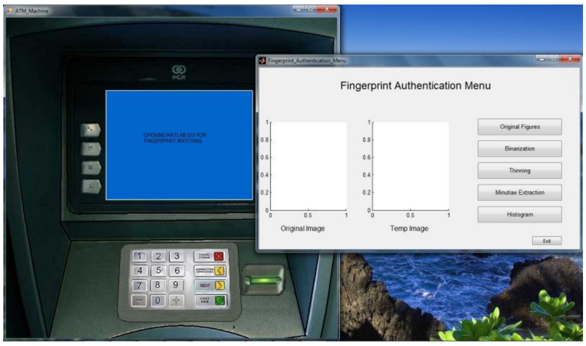
Snapshot is of request for fingerprint



UPDATING DATABASE FOR
CURRENT ENTERIES

STEP 6

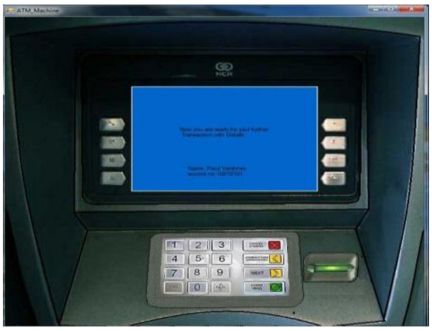
Snapshot is of updating current entries in db



OPENING MATLAB GUI FOR
FINGERPRINT MATCHING

STEP 7

Snapshot is of request for matlab gui



Now you are ready for your further
Transaction with Details

STEP 8

Snapshot is showing the end of process

4.5 METHODOLOGY

4.5.1 STEP-BY-STEP DESIGNING

In this project following steps are taken for the designing of the system:

a. A biometric sensor performs scanning of the fingerprint of intended user.

b. Minutiae algorithm performs matching of that image with the images stored in database.

c. Generating matlab data with the help of MATLAB.

d. Creating database for the storage of data.

e. Developing interface as a connecting medium of the user & machine.

f. Fetching required information needed for proper security check from user side.

4.5.2 ADVANTAGES

1. Very high accuracy and security

    - Identification (Do I know who you are?)

    - Verification (Are you who you claim to be?)

2. Is the most economical biometric PC user authentication technique.

3. It is one of the most developed biometrics.

4. Easy to use.

5. Small storage space required for the biometric template, reducing the size of the database memory required.

6. It is standardized.

7. Replace traditional methods (PINs, Passwords).

4.5.3 DISADVANTAGES

- General Limitations

1. Misidentification

   – False Acceptance

   – False Rejection

2. Privacy

3. Image captured at 500 dots per inch(dpi). Resolution: 8 bits per pixel. A 500 dpi fingerprint image at 8 bits per pixel demands a large memory space, 240 KB approximately □ Compression required (a factor of 10 approximately).

- **Limitations for individual**

1. Dry, wet or dirty hands.

2. For some people it is very intrusive, because it is still related to criminal identification.

CH 5: CONCLUSION

A smartcard based ATM fingerprint authentication scheme has been proposed. The possession (smartcard) together with the claimed user's Biometrics (fingerprint) is required in a transaction. The smartcard is used for the first layer of mutual authentication when a user requests transaction. Biometric authentication is the second layer. The fingerprint image is encrypted via 3D map as soon as it is captured, and then is transmitted to the central server via symmetric algorithm. The encryption keys are extracted from the random pixels distribution in a raw image of fingerprint.

The stable features of the fingerprint image need not to be transmitted; it can be extracted from the templates at the central server directly.

After this, the minutia matching is performed at the central server. The successful minutia matching at last verifies the claimed user. Future work will focus on the study of stable features (as part of encryption key) of fingerprint image, which may help to set up a fingerprint matching dictionary so that to narrow down the workload of fingerprint matching in a large database.