

Fingerprint Recognition System(FRS) for the Perak Loan/Scholarship System

by

Jannatul Aliah Binti Abdullah

Supervisor:

MRS. AMY FONG OOI MEAN

Dissertation submitted in partial fulfilment of
the requirements for the
Bachelor of Technology (Hons)
(Business Information System)

JUNE 2006

**Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan**

t

TK

7862

B56

F677

2006

1) Biometric Identification

TABLE OF CONTENTS

CERTIFICATION.....	i
ACKNOWLEDGEMENT.....	iii
ABSTRACT	iv
CHAPTER 1: INTRODUCTION.....	1
1.1 Background of Study	1
1.2 Problem Statement.....	2
1.3 Objectives and Scope of Study.....	3
CHAPTER 2: LITERATURE REVIEW.....	5
CHAPTER 3: METHODOLOGY.....	9
3.1 Procedure Identification.....	9
3.2 Tools.....	14
CHAPTER 4: RESULT AND DISCUSSION.....	15
CHAPTER 5: CONCLUSION AND RECOMMENDATION.....	18
5.1 Conclusion.....	18
5.2 Recommendation.....	18
REFERENCES	18
APPENDICES.....	22

List of Figures

Figure 1.0	Figure shows the system architecture	10
Figure 1.1	Figure shows the flow chart of the project	13
Figure 2.1:	Shows the table comparison of minutiae matching and FRS.....	16
Figure 2.2:	Shows the graph comparison of minutiae matching and FRS.....	16
Figure 3.1:	Figure shows FRS landing page.....	54
Figure 3.2:	Figure shows FRS administrator's page.....	54
Figure 3.3:	Figure shows FRS user's page.....	55
Figure 3.4:	Figure shows FRS identified administrator's page.....	55
Figure 3.5:	Figure shows FRS identified user's page.....	56
Figure 3.6:	Figure shows FRS enrollment page.....	56
Figure 3.7:	Figure shows FRS delete page.....	57

CERTIFICATION OF APPROVAL

Fingerprint Recognition System(FRS) for the Perak Loan/Scholarship System

by

Jannatul Aliah Binti Abdullah

A project dissertation submitted to the
Business Information System Programme
Universiti Teknologi PETRONAS
in partial fulfilment of the requirements for the
BACHELOR OF TECHNOLOGY (Hons)
(BUSINESS INFORMATION SYSTEM)

Approved by,

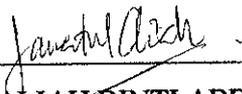
(Mrs. Amy Fong Ooi Mean)

**UNIVERSITI TEKNOLOGI PETRONAS
TRONOH, PERAK**

June 2006

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgments, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.



JANNATUL ALIAH BINTI ABDULLAH

ACKNOWLEDGEMENT

First and foremost, I want to praise the Al-Mighty Allah s.w.t for giving me the chance to finish the project. Thank you very much to my family for supporting me for the whole five years of my study in Universiti Tecknologi Petronas (UTP). I want to give my greatest gratitude to my supervisor, Mrs. Amy Foong Ooi Mean for supervising, helping and guide me all this time from the project is zero until it has become a product. I would also like to thank Mr. Mohd. Sabri Bin Abdul Latiff for giving me the chance to collaborate with the company for this project and for assisting me throughout the project development. I am also grateful to have friends that support me with this project. Last but not least, I would like to express my gratitude to the University Technology Petronas that has given me the chance to study here. Thank you.

ABSTRACT

Creating a biometric verification system in an energy and area constrained embedded environment is a challenging problem. This paper gives results for using triangulation process to improve performance of minutiae matching. Triangulation process is the process of aligning the two fingerprints and compares the fingerprint minutiae with minutiae in the database. Human has almost 50 minutiae in their fingerprints. The fingerprint recognition system (FRS) will test the fingerprint and allows the Perak Loan/Scholarship system to be access when 13 minutiae match with the stored fingerprint data. However, as many data in the database, there are problems of acquiring the data. The time taken to retrieve data may increase due to this large volume of data stored. In a real application, the sensor, the acquisition system and the variation in performance of the system over time is very critical. Therefore the system improves the minutiae matching performance by achieving data retrieving in within 3 seconds. A set of 30 fingerprints from 10 individuals were used to test the system. As the result of the proposed approach, the author achieved 2.68 seconds of average fingerprint matching time and 80% of correct fingerprint matching accuracy for FRS.

CHAPTER 1

INTRODUCTION

1.1 Background of the study

A biometric is any measurable, robust, distinctive, physical characteristic or personal trait of an individual that can be used to identify, or verify the claimed identity of, that individual. Measurable means that the characteristic or trait can be easily presented to a sensor and converted into a quantifiable, digital format.

Identification differs significantly from verification. Identification is when the device asks and attempts to answer the question, "Who is X?" When biometrics is used to identify an individual, the biometric device reads a sample and compares that sample against every template in the database. This is called a "one-to-many" search (1: N). The device will either find a match and subsequently identify the person or not find a match and fail to identify the person.

All biometric systems consist of three basic elements: enrollment, templates, and matching. Enrollment is the process of collecting biometric samples from a person and the subsequent generation of a template. Typically, the device takes three samples of the same biometric and then averages them to produce an enrollment template. The templates are the data representing the enrollee's biometric. They are created by the biometric device, which uses a proprietary algorithm to extract "features" appropriate to that technology from the enrollee's samples. These features are also referred to as minutiae points for some technologies, such as fingerprint systems. Because templates are only a record of distinguishing features of a person's biometric characteristic or trait (and not an image or complete record of the actual fingerprint or voice), the template is usually small and allows for the near-instantaneous processing time characteristic of biometric authentication. Matching is the process of comparing a submitted biometric

sample against one (verification) or many (identification) templates in the system's database.

An important issue in designing a practical system is to determine how an individual is identified. Depending on the context, a biometric system can be either a verification system or an identification system. Various types of biometric systems are being used for real-time identification; the most popular are based on face, iris and fingerprint matching. However, the author's project is focusing on the verification system of the Perak State Government Loan/Scholarship System by using the finger print recognition.

1.2 Problem Statement

1.2.1 Problem Identification

Most current system are using password as the method of identification. But, there are many problems that exist due to the usage of password as the identification. Firstly, password can be traced by other party. Fraudulent can easily be spread without anyone even realized it. Secondly, password can simply be forgotten.

For various reasons finger print recognition are suitable to be used for the Perak State Government Loan/Scholarship System because:

- (i) the person to be identified is required to be physically present at the point-of-identification;
- (ii) password do not have to be remembered. Therefore it reduced the problem of could not enter the system due to password lost.
- (iii) the unique pattern in the person finger print cannot be copied by others.

1.2.2 Significance of the Project

Basically, this project and the development of the application would bring some importance, which are listed as follows:

- ◆ This entire project aimed in applying the finger print biometrics concept as one of biometric concept is also used for the approval/rejection of the payment that will be given to the scholars. The higher officers do not have to sign any later of approval/rejection as the system will help them by using the finger print concept. This will help to prevent the forging of signature by other parties.
- ◆ This project would be regarded as significant, as this project helps in enhancing the ability of the system in receiving the payback loan transaction and issuing the payment for the scholars.

1.3 Objective and scope of the study

1.3.1 Objective of the Study

The objectives of the project are:

- (i) To develop the fingerprint verification system.
- (ii) To speed up the fingerprint matching time.

1.3.2 Scope of the study

Looking into the scope of the entire study, it would be focusing upon the usage of finger printing recognition in helping to develop a secure accounting system for Perak State Government Loan/Scholarship System. Basically, the project involved with the authentication module.

In the authentication module, the finger print will be used in 2 purposes.

- a.) To verified the registered user.
- b) To give access page for user according to their position and responsibility.

1.3.3 Feasibility of the Project within the Scope and Time Frame

These projects is feasible for the two semester's final year project as time will be spent on the research on the triangulation process of fingerprint matching, developing the fingerprint source code and algorithm and also in testing the whole system when it has been completed.

CHAPTER 2

LITERATURE REVIEW

Biometrics-based personal authentication systems that use physiological (e.g., fingerprint, face) or behavioral (e.g., speech, handwriting) traits are becoming increasingly popular, compared to traditional systems that are based on tokens (e.g., key) or knowledge (e.g., password) [1]. Traditional authentication systems cannot discriminate between an impostor who fraudulently obtains the access privileges (e.g., key, password) of a genuine user and the genuine user herself. Furthermore, biometric authentication systems can be more convenient for the users since there is no password to be forgotten or key to be lost and a single biometric trait (e.g., fingerprint) can be used to access several accounts without the burden of remembering passwords.

A typical biometric system operates in two distinct stages: the enrollment stage and the authentication stage. During enrollment, a user's biometric data (e.g., fingerprints) is acquired and processed to extract a feature set (e.g., minutiae points) that is stored in the database. The stored feature set, labeled with the user's identity, is referred to as a template. In order to account for variations in the biometric data of a user, multiple templates corresponding to each user may be stored. During authentication, a user's biometric data is once again acquired and processed, and the extracted feature set is matched against the template(s) stored in the database in order to identify a previously enrolled individual or to validate a claimed identity. The matching accuracy of a biometrics-based authentication system relies on the stability (permanence) of the biometric data associated with an individual over time [2].

Transaction Security Bank of Central Asia (BCA), Indonesia, uses biometrics to protect the interests of their customers, staff and the bank by ensuring that only authorized personnel handle bank transactions. Existing methods of authorizing transactions by the bank's tellers and supervisors through the use of PINs and passwords could be open to fraud and misuse. Replacing traditional passwords, Identix'

biometric system verifies the identity of employees who authorize withdrawals, deposits and electronic transfers over a certain amount and records an irrefutable audit trail. BCA has deployed Identix technology in more than 700 branches throughout Indonesia. The Bank of Cairo is installing a similar system to that used by BCA. To date some 1,000 units have been put into operation. Transaction Verification for Commodities Traders. The Brazilian Mercantile & Futures Exchange (BM&F) is the world's first stock market to implement fingerprint biometrics security for authentication and access to its electronic Global Trading System. The solution requires traders to access the electronic Global Trading System via fingerprint biometric authentication. Traders are required to verify their identity via the fingerprint readers periodically at defined time intervals throughout the period of time they are logged-on to the system. This helps to guarantee the security and exclusiveness of access by authorized traders to the electronic Global Trading System by verifying that an individual placing a trade was actually the one authorized to make the trade.[3].

When the security system was introduced, many different verification methods were considered; the result of these considerations was the decision to adopt a Fingerprint Authentication System - one of the authentication methods based on biological characteristics that are unique to each individual - for its low cost and extremely high level of safety. No two persons have the same fingerprints, and these prints do not change throughout the individual's life. By authenticating these fingerprints, it is possible to reliably identify the individual. The Fingerprint Authentication System makes use of these unique features of the fingerprint. The term "fingerprints" refer to the pattern of interwoven protuberances and hollows in the skin of the fingertips created in the womb. The protuberances that make up the lines in these patterns are called "ridges"[4].

The inadequacies of traditional authentication and identification processes, coupled with more stringent security requirements and an increasingly global economy and mobile population, have in recent years contributed to the increased focus on the development of biometrics. Biometrics is the automated use of unique physiological

characteristics of individuals, such as fingerprints, palm prints, faces or irises, to determine or verify an individual's identity. The individual's biometric characteristic is captured and encoded and then compared against previously encoded biometric data stored in an electronic database to determine or verify the individual's identity. Because biometrics technology utilizes an unchanging, unique characteristic of a person that cannot be lost, stolen, shared or forgotten, it has the capability to be more accurate, convenient and cost-effective than traditional methodologies. Fingerprints have been the most widely used biometric because they are relatively simple to capture, either voluntarily or from latent at crime scenes, are relatively non-intrusive and benefit from a substantial existing infrastructure that employs fingerprints for identification[5].

The problem of resolving the identity of a person can be categorized into two fundamentally distinct types of problems with different inherent complexities: (i) verification and (ii) recognition. [6]. Accurate identification of a person could deter crime and fraud, and save critical resources. Here are a few mind boggling numbers: about one billion dollars in welfare benefits in the United States are annually claimed by double dipping welfare recipients with fraudulent multiple identities [10, 11]. Herschel asserted that he had practiced fingerprint identification for about 20 years [7]. This discovery established the foundation of modern fingerprint identification. In the late century, Sir Francis Galton conducted an extensive study of fingerprints[8].

Thebaud [9] has also proposed a method of locally warping fingerprints to make two fingerprints look more similar. In the case where the prints are from the same finger, this will tend to remove distortion. Frustrated total internal reflection and other optical methods [12] are the oldest livescan methods. The CMOS capacitive [13] sensors and other technologies made it possible to shrink the sensor size to the area of a postage stamp so that the sensors fit in laptops, cellphones and personal digital assistants.

Triangulation is a process that takes a region of space and divides it into subregions. The space may be of any dimension, however, a 2D space is considered here since we are dealing with 2D points (minutiae). In this case, the subregions are simply triangles. Triangulation

has many applications in finite elements simulation, surface approximation and nearest neighbor identification[14].

CHAPTER 3

METHODOLOGY

3.1 Procedure Identification

Fingerprint recognition is an extremely useful biometrics technology since fingerprints have long been recognized as a primary and accurate verification method. It is as a direct result of this recognition, that large fingerprint databases can be found within law enforcement agencies the world over. Fingerprint technology can be used for both verification (1:1) matching as well as for Identification (1:n) matching. Electronic Fingerprint matching can be achieved through one of two methodologies. The first uses the ridge endings and bifurcation's on a person's finger to plot points known as Minutiae (Minutiae based approach). These Minutiae allow for the comparison of two fingerprints to be achieved electronically .The second methodology uses a pattern based approached. The methodology for this system uses a Minutiae based approach which uses the triangulation process. This Minutiae based approach is performed in 2 fundamental blocks:

1. Enrollment
2. Identification

Generally, all biometrics system contains two parts: enrollment and identification. The enrollment part function is to have a user's characteristic registered so that it can be used as a criterion when identification is performed. The identification provides the user interface to have the end users characteristics capture and verified.

System architecture of the system

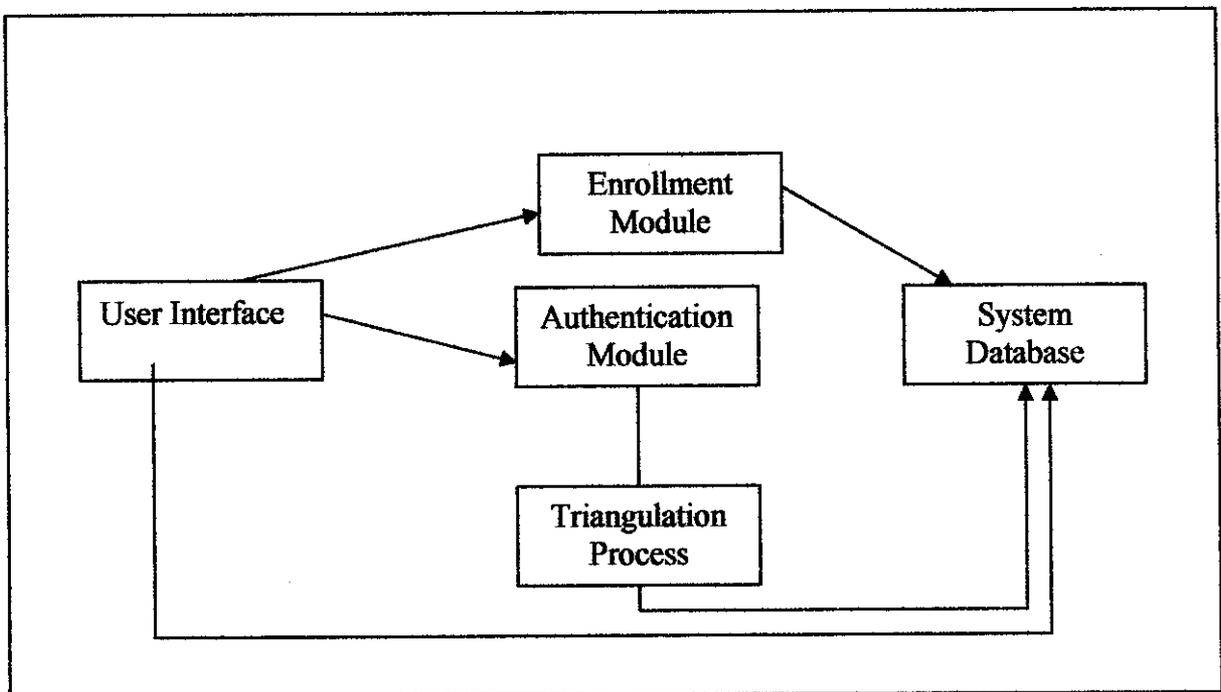


Figure 1.1: Figure shows the system architecture

There are 4 steps that should be taken in order to complete the two fundamental blocks. The steps are:

1. Fingerprint enrollment.
2. Preprocessing of a fingerprint image.
3. Extraction of the fingerprint features.
4. Classification of the fingerprint.

In each steps, there are a few sub steps so that the fingerprint matching can be done and the result will be accurate.

1. Fingerprint enrollment.

1. The fingerprint is scan by using the fingerprint scanner.
2. The image scanned will be stored into the Microsoft Access database. The image is stored in binary format.

2. Preprocessing of a fingerprint image.

1. Background Detection – the background detection is made by removing the white background. The image will be in black and white as the background will be in black and the fingerprint ridge will be in white areas. The image block size and threshold also is set up at this phase so that all the images will be equally in size.
2. Rotation – Rotation tolerance defines the maximum acceptable angle variation (in degrees) between two matching fingerprints being compared that will result in a match response. This value is valid in both clockwise and counter-clockwise directions, so the maximum value set is 180°

3. Extraction of the fingerprint features

1. Fingerprint data are extracted from the sample and a template is created
2. This template is compared to the binary fingerprint data stored in the database before.
3. The template is the joining of all the minutiae in a person's hand.

4. Decision stage.

1. The extracted fingerprint is compared to the binary fingerprint data from the database. The verification is made by a triangulation process between the minutiae only, not the entire image. Triangulation process is performed by aligning the two fingerprints. A list of fingerprints which possibly match query fingerprints is generated. If a large number of minutiae from the sample fingerprint are close, then it is very likely that the two fingerprints come from the same fingerprint.
2. One regular human being has some 50 minutiae. For this system, 13 of them are needed to assure the identification.
3. This stage is the process that the system decides whether the template extracted from the new samples matches the registered fingerprint in the database.

This system will be able to identify the owner of a fingerprint with reasonable accuracy and will have the ability to reject a fingerprint when the system is unsure of its results.

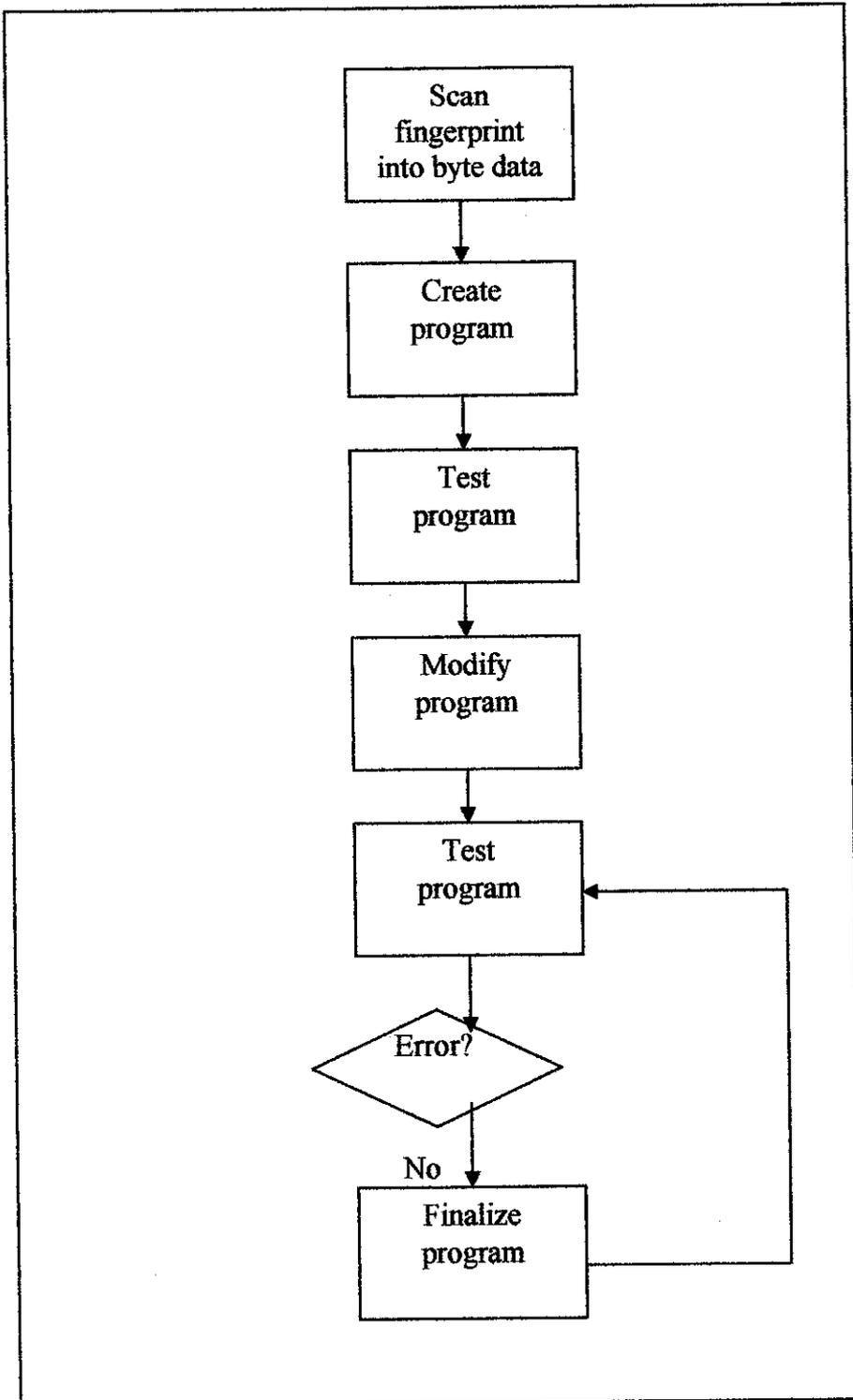


Figure 1.2: Figure shows the flow chart of the project

3.2 Tools

During the development of this particular system, it will be needing and requiring a number of software and tools as what would be described as follows:

3.2.1 Software Requirements

Basically, the software which is needed in completing this particular project would be:

- ◆ Visual Basic 6
- ◆ Microsoft Access(it is used to store all the data regarding the system)
- ◆ Grfinger .dll files (for the fingerprint image capture and extraction)

3.2.2 Hardware Requirements

The hardware description needed in completing this particular project would be as follows:

- ◆ Intel ® Pentium ® III, IV or AMD-K6 ® III based PC, 450MHz or higher
- ◆ Microsoft ® Windows ® XP Professional, Windows 2000 Professional or Windows NT ® 4.0 (SP6 or later)
- ◆ 128MB RAM
- ◆ 1 GB free disk space
- ◆ Mouse or other pointing device
- ◆ CD-ROM drive

CHAPTER 4

RESULT AND DISCUSSION

Basically, what is being expected from the system in the end would be the ability for the system to search for the matching fingerprint from the database in a small amount of time. The system can compare the scanned fingerprint with the stored fingerprints in the database. It will allow the access of the matched user and rejected the wrong matched fingerprint. The system also can process a fingerprint so that the fingerprint can reduce error in the system. Besides, the system also should be able to eliminate the problem being stated earlier. The interface for this particular system is developed by using Visual Basic 6.

As for the current progress, the author is working enhancing the performance time for the system in order to make sure that the system is really reliable and secure for users. The fingerprint is now has been through five phases of analyzing which is

1. Capture fingerprint image
2. Extract the fingerprint template
1. Set identify threshold.
2. Set rotation tolerance.
3. Match the fingerprint template and staff id with the database.

Below are the results that have been achieved by the author for the FRS:

CATEGORIES	Minutiae Matching	FRS
CORRECT	72.00%	80.00%
FAR	0.40%	0.01%
FRR	27.60%	19.99%
TIME	4.7 secs	2.6 secs

Figure 2.1: Shows the table comparison of minutiae matching and FRS

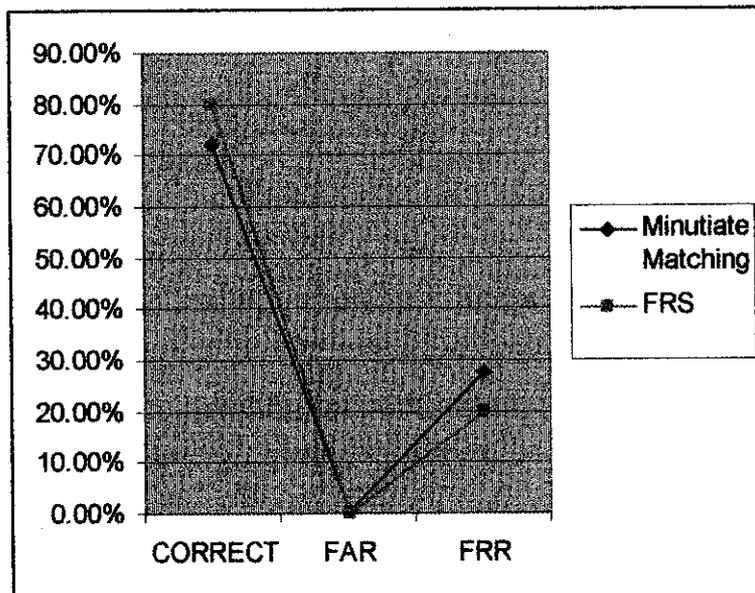


Figure 2.2: Shows the graph comparison of minutiae matching and FRS

The fingerprint images used in this study have been captured using Microsoft Fingerprint Reader. The author's database contains 30 fingerprints, captured from 10 individuals. To characterize system's performance, the author has conducted two experiments. In the first experiment, the author varies the number of imprints stored in the database for each person. Thus, a subset of the 30 fingerprint images was used to build the database. The author have experimented with storing 3 images per person in the database

The author classifies the results in three categories:

1. Correct:

The query fingerprint has been correctly matched to one or more fingerprints from the same person,

2. The false acceptance rate (FAR)

The false acceptance rate (FAR) is the probability that a impostor presenting its verification data is falsely recognized as the lawful owner of the reference data.

3. The false acceptance rate (FRR)

The false rejection rate (FRR) indicates the probability for the lawful owner of the reference data to be falsely rejected when presenting his verification data.

In this case, recognition accuracy improved more than the minutiae fingerprint matching. However, the results indicate that there are certain finger- prints that are very difficult to identify. The main reason for this is that the query fingerprint does not have many minutiae in common with the rest of the finger prints (e.g., two fingerprints might correspond to different poses of the finger on the scanner or the minutiae.

For the second experiment, the author has evaluated the performance of the fingerprint by taking the average time of the fingerprint matching. The speed of the fingerprint is less than 3.0 seconds in which is within the objective. The author plans to reduce the matching time for his/her future work.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1 Conclusion

From the research that has been conducted, it could be seen that, finger print recognition is one of the high level security identification method for an accounting-based system nowadays. This had been proven through many successful projects and development of this particular application, which mainly could be seen rapidly happening in the western countries and also in the Asian country for example Japan and Indonesia. It is low in cost and recommended by other companies who are implementing the concept in their system.

The problem of fraudulent, forging signature and also forgetting password can be eliminated so that the users can use the system effectively. Besides, all the data in the system is guaranteed secure. Basically, the advantages of this project is that no one can hack the system as the unique pattern from the finger print will prevent anyone from accessing the system easily.

The usage of finger print in approving/ rejecting the issued payment will prevent anyone from stealing the money from the Perak state fund. The system function is mainly to minimize the human error. Therefore, the idea of improving the security of the system is finally achieved.

5.2 Recommendation

Basically, the objective of this Final Year Project is reached. The objective of the system is to allow the specific registered user to view the page in the Perak Loan Scholarship system. Besides, the fingerprint matching speed also is attained within of 3 seconds. Although the objective has been reached, the programs still have its own flaws.

The program can be modified to ensure that it is really secure for the user. As a recommendation for future enhancement, distortion elements can be added for the system. Distortion involves the usage of filters in order to reduce noise and distortion in fingerprint data. This could give a better quality fingerprint image and a more reliable result for the fingerprint verification process.

REFERENCES

1. A.K. Jain, R. Bolle, and S. Pankanti, (Eds.), *Biometrics: Personal Identification in Networked Society*, Kluwer Academic Publishers, 1999.
2. Anil Jain, Umut Uludag and Arun Ross, *Biometric Template Selection: A Case Study In Fingerprints*, Retrieved on 17 October 2005, (URL:(http://www.citer.wvu.edu/members/publications/files/19_RossTemplate_AVBPA03.pdf)
3. *Banking: Biometric Solutions for Identity Theft*, Retrieved on 18 October 2005, URL: (<http://www.ibia.org/membersadmin/casestudy/pdf/9/Banking.pdf>.)
4. Kaminoyama City Office, Yamagata Prefecture, *Protecting the property and privacy of citizens with the most reliable Fingerprint Authentication system available*, Retrieved on 17 October 2005, (URL:(www.sw.nec.co.jp/english/library/jirei/)
5. *Automated Fingerprint Identification Systems 2005 Computerworld Honors Case Study*, Retrieved on 18 October 2005, URL :(<http://www.cwhereoes.org/laureates/Business/cogent.pdf>)
- 6.C.L. Wilson, C.I. Watson, E.G. Paek, “Combined Optical and Neural Network Fingerprint Matching”, *Optical Pattern Recognition VIII, SPIE Proceedings* Vol. 3073, p. 373-382, April 1997.
7. G. Ravichandran and D. Casasent, “Minimum Noise and Correlation Energy Optical Correlation Filter”, *Applied Optics*, Vol. 31, p. 1823-1833, April 1992.
8. D. Casasent and S. Ashizawa, “Synthetic Aperture Radar Detection, Recognition and

Clutter Rejection with new Minimum And Correlation Energy filters”, *Optical Engineering*, Vol. 36, no. 10, p. 2729-2736, October 1997.

9. Andrew Senior and Ruud Bolle, *Improved Fingerprint Matching by distortion removal*, Retrieved on 18 November 2005, URL:(<http://www.research.ibm.com/people/a/aws/documents/papers/SeniorDistortionRemovalportion.pdf>)
10. A.Stoinav, C.Soutar,and A.Graham, “High-speed fingerprint verification using an optical correlator”, *SPIE*, 3386:242-252,1998.
11. Nalini Ratha, Ruud Bolle, ”Automatic Fingerprint Recognition System”, Springer, p. 249, 2004.
12. S. E. Schuster, Fingerprinting method, *IBM Technical Disclosure Bulletin*: 12-70, p. 1852. Dec. 1970.
13. C. Tsikos, “Capacitive fingerprint sensor,” US Patent 4353056, 1982.
14. S. Skiena, *The algorithm design manual*, Springer-Verlag, NY, 1998.

APPENDICES

SOURCE CODE

Form Mainpage

Private Sub cmdExec_Click() ' cmdExec is the name of the command button on any form.

Dim RetVal

RetVal = Shell("D:\MIX STUFF\FYP PROGRAMMES\FINGERPRINT\FINGERPRINT\FINGERPRINT 3\GrFinger 4.1
FREE\samples\source\FINGERPRINT RECOGNITION SYSTEM\FINGERPRINT USER\GrFingerSampleVB6.exe", 1)

Unload Form1

End Sub

Private Sub Command1_Click()

Dim RetVal

RetVal = Shell("D:\MIX STUFF\FYP PROGRAMMES\FINGERPRINT\FINGERPRINT\FINGERPRINT 3\GrFinger 4.1
FREE\samples\source\FINGERPRINT RECOGNITION SYSTEM\FINGERPRINT ADMIN 2\GrFingerSampleVB62.exe", 1)

Unload Form1

End Sub

Form Main

Option Explicit

Private Sub about_Click()

frmAbout2.Show

End Sub

Private Sub btnRefresh_Click()

img.Picture = LoadPicture()

img2.Picture = LoadPicture()

formMain.lblName = ""

formMain.lblName2 = ""

formMain.lblLog.Visible = True

```
formMain.lbLog = ""
```

```
End Sub
```

```
Private Sub cmdBack_Click()
```

```
Dim RetVal
```

```
RetVal = Shell("D:\MLX STUFF\FYP PROGRAMMES\FINGERPRINT\FINGERPRINT\FINGERPRINT 3\GrFinger 4.1  
FREE\samples\source\FINGERPRINT RECOGNITION SYSTEM\MainPage.exe", 1)
```

```
Unload formMain
```

```
End Sub
```

```
Private Sub cmdClose_Click()
```

```
cmdClose = True
```

```
Me.Hide
```

```
End Sub
```

```
' Application startup code
```

```
Private Sub Form_Load()
```

```
Dim err As Integer
```

```
' Initialize GrFinger Library
```

```
err = InitializeGrFinger()
```

```
' Print result in log
```

```
If err < 0 Then
```

```
writeError (err)
```

```
Exit Sub
```

```
Else
```

```
writeLog ("**Welcome y'all**")
```

```
End If
```

```
End Sub
```

```
' Application finalization code
```

```
Private Sub Form_Terminate()
```

```
' disable timers
```

```
tmrFinger.Enabled = False
```

```
tmrImage.Enabled = False
```

```
tmrStatus.Enabled = False
```

```
' wait all events to be consumed
```

```
While fireFinger Or fireStatus Or fireImage
```

```
Wend
```

```

' finalize GrFinger
Call FinalizeGrFinger
End Sub

' Add a fingerprint to database
Private Sub btEnroll_Click()
    Dim id As Integer
    Dim g As String

    ' add fingerprint
    id = Enroll

    ' write result to log
    If id >= 0 Then
        ' writeLog ("Fingerprint enrolled with id = " & id)
        'writeLog ("Fingerprint is successfully enrolled")
    Else
        'writeLog ("Error: Fingerprint not enrolled")
    End If

End Sub

' Identify a fingerprint
Public Sub btIdentify_Click()
    Dim ret As Integer, score As Long
    Dim handle As Long

    score = 0
    ' identify it
    ret = Identify(score)
    ' write result to log
    If ret > 0 Then
        writeLog ("Fingerprint identified.")
        'ID = " & ret & ". Score = " & score & ".

        'DB.getTemplates3 (ret)
        'DB.getTemplates4 (ret)
        'Call PrintBiometricDisplay2(True, GR_DEFAULT_CONTEXT)
        ' formMain.img.Picture = PictureFromHandle(Handle)

```

```

    btEnroll.Visible = True
    btClearDB.Visible = True
    btClearLog.Visible = True
    btnRefresh.Visible = True
Elseif ret = 0 Then
    writeLog ("Fingerprint not Found.")
Else
    writeError (ret)
End If
End Sub

' Check a fingerprint
Private Sub btVerify_Click()
    Dim id As Integer
    Dim ret As Integer
    Dim score As Long
    Dim sid As String

    ' ask target fingerprint ID
    score = 0
    sid = InputBox("Enter the ID to verify", "Verify", "")
    If sid <> "" Then
        ' compare fingerprints
        ret = Verify(Val(sid), score)
        ' write result to log
        If ret < 0 Then
            writeError (ret)
        ElseIf ret = GR_NOT_MATCH Then
            writeLog ("Did not match with score = " & score)
        Else
            writeLog ("Matched with score = " & score)
            ' if they match, display matching minutiae/segments/directions
            Call PrintBiometricDisplay(True, GR_DEFAULT_CONTEXT)
        End If
    End If
End Sub

```

OUTPUTS

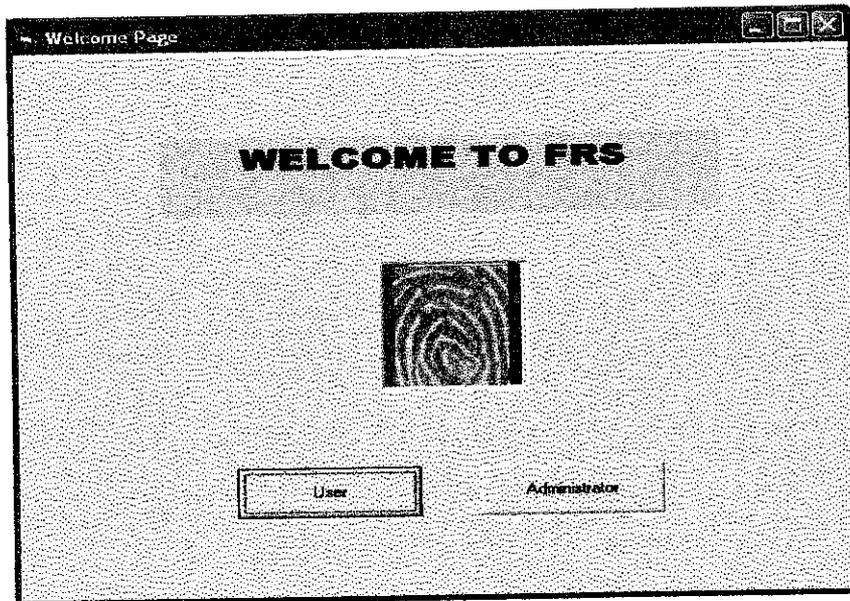


Figure 3.1: Figure shows FRS landing page

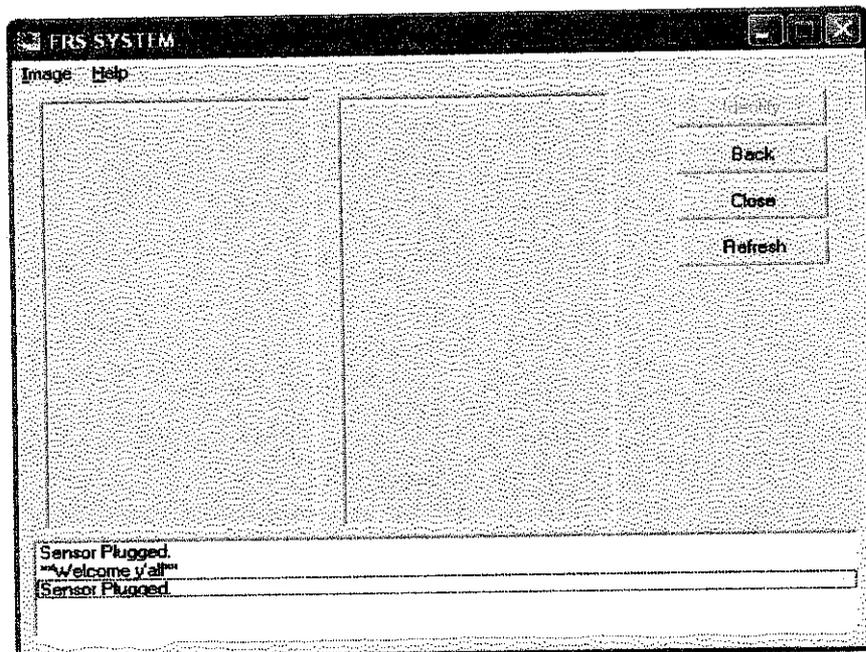


Figure 3.2: Figure shows FRS administrator's page

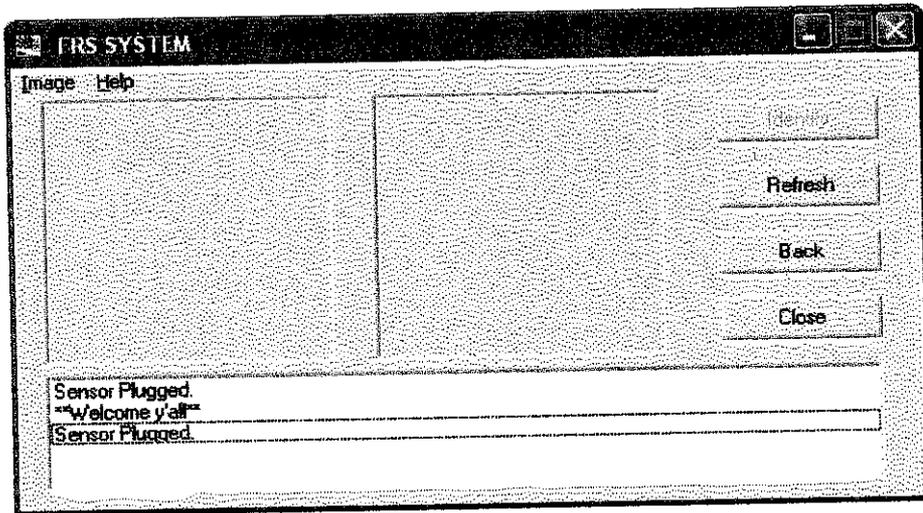


Figure 3.3: Figure shows FRS user's page

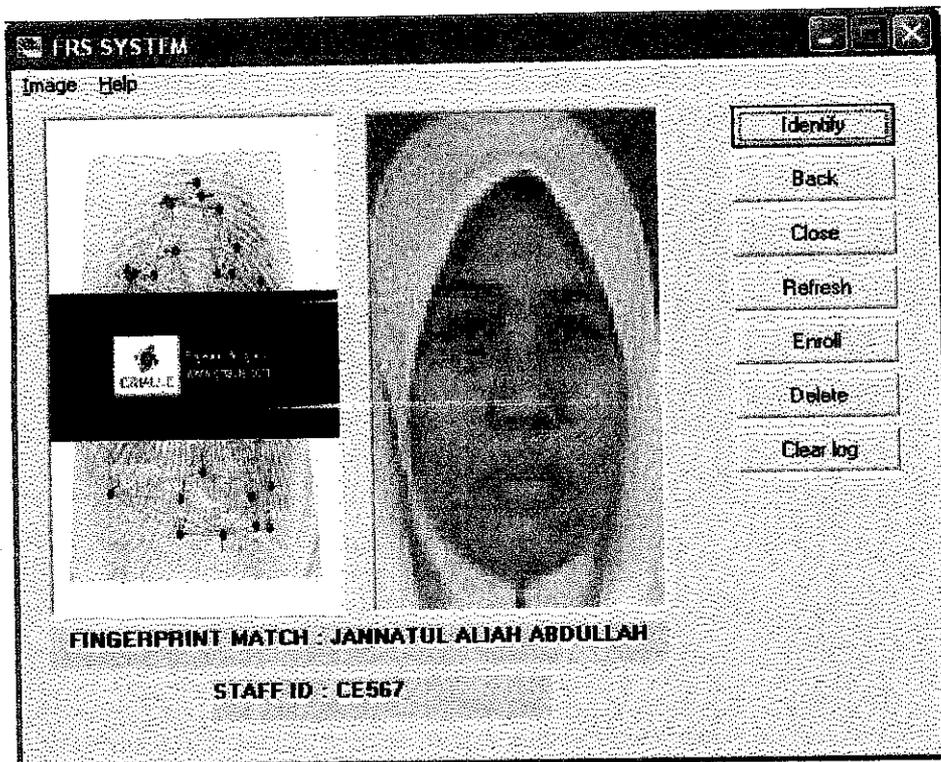


Figure 3.4: Figure shows FRS identified administrator's page

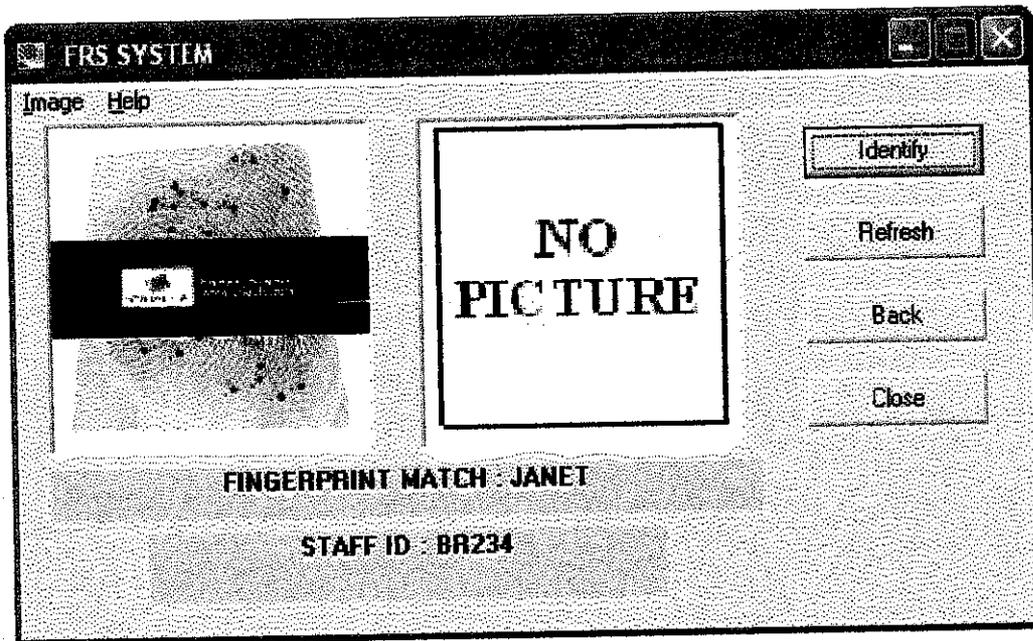


Figure 3.5: Figure shows FRS identified user's page

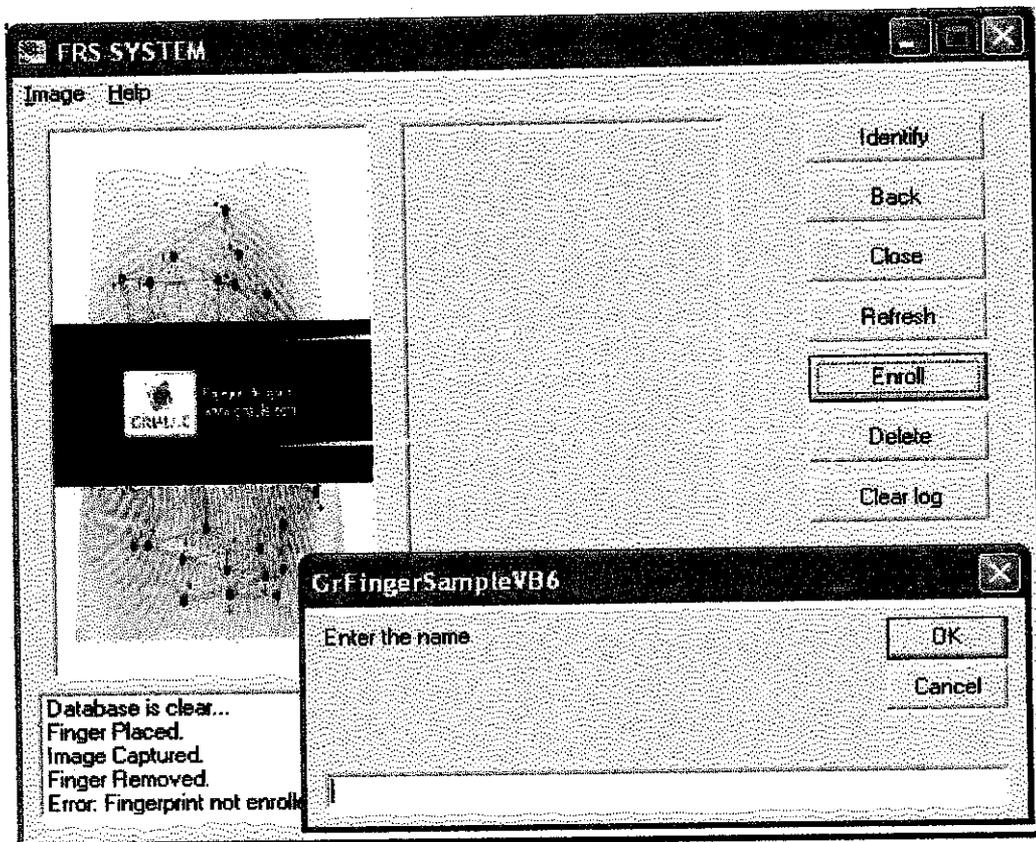


Figure 3.6: Figure shows FRS enrollment page

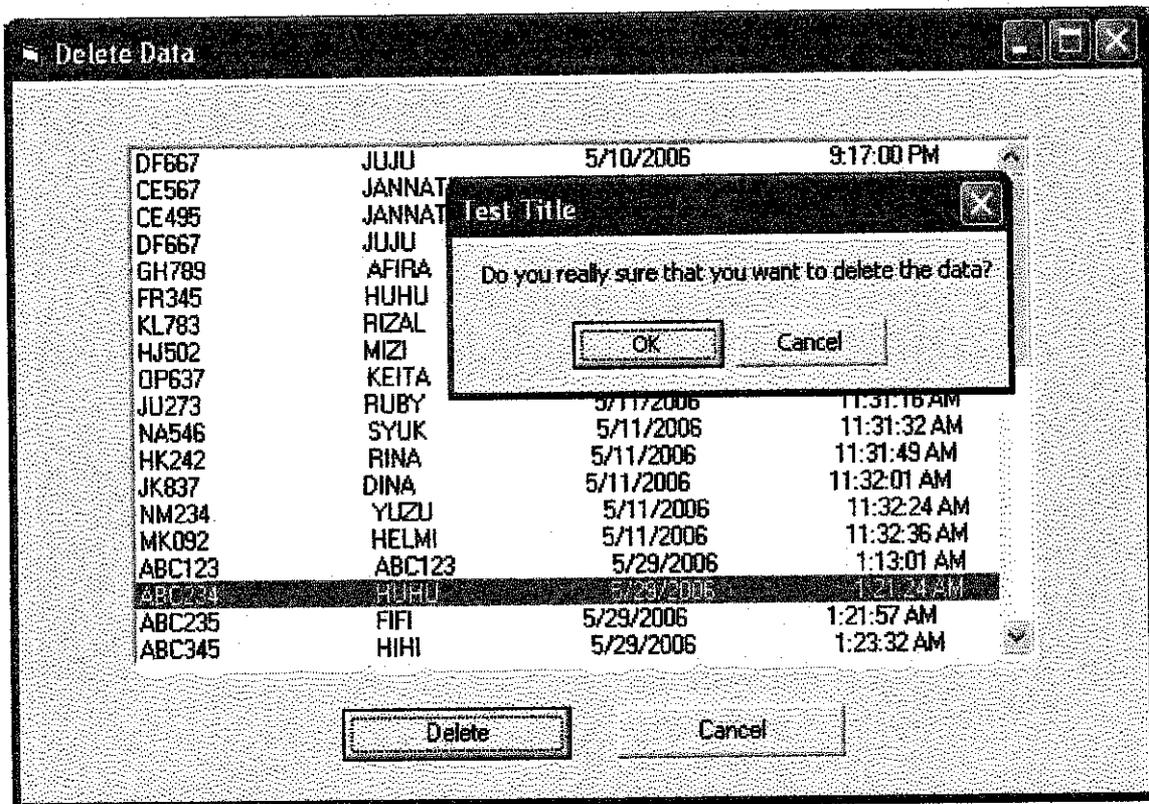


Figure 3.7: Figure shows FRS delete page