

PERFORMANCE EVALUATION OF BIOMETRIC SYSTEM

YOUNIS ELMADANY HAMED

A project report submitted in partial  
fulfillment of the requirement for the award for the Degree of  
Master of Engineering  
(Electrical-Electronics & Telecommunications)

Faculty of Electrical Engineering  
Universiti Teknologi Malaysia

APRIL 2007

## UNIVERSITI TEKNOLOGI MALAYSIA

**BORANG PENGESAHAN STATUS TESIS<sup>♦</sup>**JUDUL : PERFORMANCE EVALUATION OF BIOMETRIC SYSTEMSESI PENGAJIAN: 2006/2007Saya YOUNIS ELMADANY HAMED

(HURUF BESAR)

mengaku membenarkan tesis (~~PSM/Sarjana/Doktor Falsafah~~)\* ini disimpan di Perpustakaan Universiti Teknologi Malaysia dengan syarat-syarat kegunaan seperti berikut :

1. Tesis adalah hakmilik Universiti Teknologi Malaysia.
2. Perpustakaan Universiti Teknologi Malaysia dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. \*\* Sila tandakan (✓ )

SULIT

(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

TERHAD

(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

TIDAK TERHAD

Disahkan oleh

\_\_\_\_\_  
(TANDATANGAN PENULIS)\_\_\_\_\_  
(TANDATANGAN PENYELIA)

Alamat Tetap :

KG. BANGGOL STOL,  
16800 PASIR PUTEH,  
KELANTAN

PROF. IR. DR. SHEIKH HUSSAIN SHAIKH SALLEH  
Nama Penyelia

Tarikh : \_\_\_\_\_

Tarikh : \_\_\_\_\_

CATATAN: \* Potong yang tidak berkenaan.

\*\* Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh tesis ini perlu dikelaskan sebagai SULIT atau TERHAD.

∪ Tesis dimaksudkan sebagai tesis bagi Ijazah Doktor Falsafah dan sarjana secara penyelidikan, atau disertai bagi pengajian secara kerja kursus dan penyelidikan, atau Loporan Projek Sarjana Muda (PSM).

“I hereby declare that I read this project report, and in my opinion this project report is sufficient in terms of scope and quality for the award of the degree of Master of Engineering (Electrical-Electronics & Telecommunications)”.

Signature : .....  
Supervisor : PROF. IR. DR. SHEIKH HUSSAIN SHAIKH SALLEH  
Date : .....

I declare that this thesis entitled “*Performance Evaluation of Biometric System*” is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : .....

Author's name : YOUNIS ELMADANY HAMED

Date : 07-May-2007

*Dedication to my parents my Dad, Elmadany Hamed*

*Mum, Amina Haid*

*Brothers and sisters*

*Thank you for your love, support, prayers,  
and encouragement.*

## **ACKNOWLEDGEMENTS**

By the name of ALLAH and precious prayer on his profit Mohamed, I grateful ALLAH to give me the ability to reach this level of knowledge by making good people helps me, support me, and guide me in this work and gave me the advices to make this work as good as possible my supervisor: Prof. Ir. Dr. Sheikh Hussain Shaikh Salleh and Amar K. Arief, and all my lecturers during my master course.

I acknowledge sincerely with thanks the many contributions of all those who have helped in the preparation of this thesis.

## ABSTRACT

Since biometrics may be used to ensure that a person accessing information is authorized to do so, interest in biometrics for information assurance has increased recently. New biometric applications are constantly being announced while at the same time new spoofing technology is being developed to defeat them. One approach to overcoming the problem of spoofing is the use of multimodal biometric fusion. Most current research is focused on overcoming the deficiencies of a single biometric trait or reducing the false acceptance rate, both without any emphasis on the false rejection rate. Multimodal biometric fusion combines measurements from different biometric traits to enhance the strengths and diminish the weaknesses of the individual measurements. In this project we considered three types of biometrics techniques: fingerprint, hand-scan, and voice-scan. This project examines the use of a cost function to set the threshold point such that an optimization of false acceptance and false rejection rate can be achieved. Other minimum cost thresholds with different settings of FA and FR prior probabilities and costs are also shown to be better than EER in terms of total cost. The experimental results for voice-scan show that the minimum cost is better than EER in terms of combination digits, also the experiments also show that by using a cost function the new threshold can be more accurate and by that one could be able to find new FR and FA which provide a new EER, for example the EER=5.29% for 6 digits in normal case and by using a cost function the EER became 5.28%. The experimental results on the digits combination show that the cost becomes less whenever the number of combination digits becomes bigger. For 2 digits combination the min-cost is 12.5 while it is 5.287 for 6 digits combination. On the hand-scan and fingerprint-scan the experimental results were perfect by the methods used in these tasks. Hence, by considering the cost

function as one way to calculate the cost for any multimodal biometric system, the different costs depending on the application, become easier to provide.

## ABSTRACT

Sejak teknologi biometrik telah diterimapakai dalam memastikan pengguna yang mendapatkan sesuatu maklumat adalah pengguna yang sah, minat terhadap teknologi ini sentiasa meningkat. Aplikasi baru teknologi ini sentiasa muncul dan dalam masa yang sama, teknologi untuk mengalahkannya turut dibangunkan oleh sesetengah pihak. Salah satu cara untuk mengelakkan usaha ini ialah dengan menggunakan gabungan biometrik. Kebanyakan penyelidikan terkini tertumpu pada usaha mengatasi kelemahan sistem biometrik tunggal atau mengurangkan 'false acceptance rate' (FAR), tanpa memberi penekanan pada 'false rejection rate' (FRR). Dalam projek ini, 3 sistem biometrik telah digunakan iaitu pengesanan jari, pengesanan tangan dan pengesanan suara. Projek ini mengkaji penggunaan fungsi kos untuk menetapkan nilai ambang ('threshold') bagi membolehkan FAR dan FRR yang optimum diperolehi. Nilai ambang daripada kos minimum dengan pelbagai kos dan kebarangkalian awalan FA dan FR memberikan keputusan yang lebih baik dari EER dari segi jumlah kos. Keputusan eksperimen untuk pengesanan suara menunjukkan kos minimum adalah lebih baik daripada EER untuk kombinasi digit. Eksperimen juga menunjukkan bahawa dengan menggunakan fungsi kos, nilai ambang yang diperolehi adalah lebih tepat. Seterusnya nilai FR dan FA yang baru boleh diperolehi, yang memberikan EER yang baru. Sebagai contoh, EER bagi kombinasi 6 digit ialah 5.29% manakala menggunakan fungsi kos, nilai EER yang baru ialah 5.28%. Nilai kos akan semakin berkurang apabila bilangan kombinasi digit bertambah. Untuk kombinasi 2 digit, kos minimum ialah 12.5 manakala bagi kos minimum bagi kombinasi 6 digit ialah 5.287. Keputusan bagi pengesanan tangan dan jari memberikan keputusan yang sempurna berdasarkan kaedah yang digunakan dalam projek ini. Oleh itu, dengan menggunakan fungsi kos sebagai cara

mendapatkan kos bagi mana-mana sistem gabungan biometrik, kos yang berbeza berdasarkan aplikasi boleh ditetapkan dengan mudah.

## TABLE OF CONTENTS

<b>CHAPTER</b>	<b>TITLE</b>	<b>PAGE</b>
	<b>TITLE PAGE</b>	i
	<b>ADMISSION PAGE</b>	ii
	<b>DEDICATION</b>	iii
	<b>ACKNOWLEDGEMENT</b>	iv
	<b>ABSTRACT</b>	v
	<b>ABSTRAK</b>	vi
	<b>TABLE OF CONTENTS</b>	vii
	<b>LIST OF TABLES</b>	xiii
	<b>LIST OF FIGURES</b>	xiv
	<b>LIST OF ABBREVIATIONS</b>	xvi
	<b>LIST OF APPENDICES</b>	xix
<b>1</b>	<b>PROJECT BACKGROUND</b>	<b>1</b>
	1.0 Introduction	1
	1.1 Problem statement	2
	1.2 Project Objectives	3
	1.3 Project Scope and Methodology	3
	1.3.1 Methodology	4

1.4	Thesis Organization	5
<b>2</b>	<b>LITERATURE REVIEW</b>	<b>6</b>
2.0	Background of Research Problem	6
2.1	Previous Work on Speaker Verification and Identification	8
2.2	Voice Scan	10
2.2.1	Overview of Voice Scan	10
2.2.2	Voice Scan Biometric: How it Works	11
2.2.3	Voice Scan Biometric Strengths and Weaknesses	12
2.2.4	Voice Scan Biometric Applications	13
2.2.5	Pattern Matching	13

<b>3</b>	<b>PROJECT METHODOLOGY</b>	<b>15</b>
3.0	Introduction	15
3.1	Project Outline	15
3.1.1	Overview of Speaker Recognition	16
3.1.2	Overview of Mel-Frequency Cepstral Coefficients (MFCC) Algorithm	18
3.1.3	Overview of Vector Quantization	20
3.1.4	Overview of Hidden Markov Models (HMM) Algorithm	20
3.1.5	Threshold Setting	22
3.2	Identification	22
3.3	Verification	23
<b>4</b>	<b>FINGERPRINT BIOMETRIC</b>	<b>24</b>
4.0	Introduction	24
4.1	Types of Fingerprint	25
4.2	Fingerprint Recognition System	27
4.3	The History of Fingerprints	27
4.3.1	Why Fingerprint Identification	28
4.4	Fingerprint Processing	30
4.4.1	Image Processing Stage	30
4.4.2	Feature Extraction Stage	30
4.4.3	Minutiae Extraction	31
4.4.4	Minutiae Validation	32
4.4.5	Matching Stage	33
<b>5</b>	<b>HAND-SCAN GEOMETRY BIOMETRIC</b>	<b>34</b>

5.0	Introduction	34
5.1	How Hand-Scan Works	35
5.2	Past Projects	36
5.2.1	A Hand Geometry-Based Verification System	36
5.2.2	Deformable Matching of Hand Shapes for Verification	37
5.2.3	Web-Access using Biometrics	37
5.3	Template Generation and Matching	37
5.4	Applications	37
5.5	Strengths and Weakness	38
5.5.1	Strengths	38
5.5.2	Weaknesses	38
5.6	Hand Geometry vs Fingerprints	39
5.7	Combining Biometric Methods	39
5.8	Registering the Hand	40
5.9	Security	40
5.10	Environment	41
<b>6</b>	<b>ACCURACY PERFORMANCE ANALYSIS OF MULTIMODAL BIOMERIC SYSTEM</b>	<b>42</b>
6.0	How the Biometric System is Evaluated	42
6.1	Introduction	42
6.2	Information Fusion in Biometric	43
6.3	False Acceptance and False Rejection Rates	44
6.4	Multi-Modal Error Rate (MMER)	45
6.5	Failure to Enroll Rate (FTE, also FER)	47
6.6	False Identification Rate (FIR)	48

6.7	Equal Error Rate (EER)	48
6.7.1	EER Threshold	49
6.8	Cost Function	50
6.9	Hit-Rate	51
6.10	Receiver Operation Curve (ROC)	52
6.10.1	How Does One Determine The Receiver Operating Characteristic (ROC) of a Biometric System?	53
6.10.2	What Is Essential When Comparing The ROC Performance Of Biometric Systems?	54
6.11	Cost Function and ROC	56
6.12	Separability of a Biometric	56
6.13	Detection Error Trade-off Curve (DET)	58
6.14	Advantages and Disadvantage of Some Biometrics	58
6.15	Combination of Multibiometric	61
6.16	Conclusion of Using Multi-Biometric System	61
<b>7</b>	<b>DATABASE DESIGN</b>	<b>63</b>
7.0	Introduction	63
7.1	TIDIGIT Database Concept	63
7.2	Description of speakers	64
7.3	Description of Database in this Project	66
7.3.1	Vocabulary Definition	66
7.3.2	Database engine	69
7.4	Speaker Errors	70

<b>8</b>	<b>RESULT DISCUSSION</b>	<b>71</b>
	8.0 Introduction	71
	8.1 Analysis for Single Digit	71
	8.1.1 Single Digit Verification	71
	8.1.2 Hit-Rate Curve	75
	8.1.3 ROC in Verification stage	76
	8.1.4 DET in Verification Stage	78
	8.1.5 Identification	80
	8.2 Analysis of Digit Combination	81
	8.2.1 Digital Combination Identification	81
	8.3 ROC Curve in Digit Combination	84
	8.4 Hit-Rate in Digit Combination	86
	8.5 DET Curve in Digit Combination	86
	8.6 Hand-Scan Results	87
	8.7 Optimization of Threshold Decision	89
	8.8 Conclusion	91
<b>9</b>	<b>CONCLUSION</b>	<b>93</b>
	9.0 Project Summary	93
	9.1 Benefits of the Project	95
	9.2 Suggestion of Future Work	95
	<b>REFERENCES</b>	<b>98</b>
	<b>APPENDIX A-F</b>	<b>102</b>

## **LIST OF TABLES**

<b>TABLE NO.</b>	<b>TITLE</b>	<b>PAGE</b>
6.1	Decisions Matrix	46
6.2	Advantages and disadvantages in multi-biometric system	59

7.1	Distribution of speakers	64
7.2	Distribution of Job and Speakers	65
8.1	FA and FR with different threshold	72
8.2	shows some values of threshold in negative position	76
8.3	Shows FA, FR, TA and EER for single digit	81
8.4	Comparison of EER	82
8.5	Testing of combination digit for clients and impostors	83
8.6	Total cost in digit combination	85
8.7	Hand-scan result (Clients vs. Impostors)	89
8.8	Hand-scan result (Clients vs. Clients)	89
8.9	New FAR, FRR and new threshold point for seven Digits.	90
8.10	New FAR, FRR and new threshold point for eight Digits	91
8.11	New FAR, FRR and new threshold point for five Digits	91
8.12	Min cost and EER	92

## LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
1.1	Multi-modal method	4
2.1	Speech processing	7

2.2	Pattern matching	14
3.1	Methodology	16
3.2	Identification	17
3.3	Verification	18
3.4	MFCC transaction	19
3.5	Identification and Verification	23
4.1	Ridge ending and ridge bifurcation	26
4.2	Main process in identify a fingerprint	26
4.3	Image processing stage	30
4.4	Feature extraction stage	31
4.5	Minutia extraction	32
4.6	False minutiae structures	33
5.1	Hand-scan at the biometric center UTM entrance	38
5.2	Biometric Sensory Access	40
6.1	EER point	48
6.2	EER/CER	49
6.3	$Q_0$ is FA and $Q_1$ is FR	51
6.4	Hit-Rate	52
6.5	ROC (Receiver Operation Curve)	52
6.6	DET curve	58
7.1	Example of two tokens list	67
7.2	List of six tokens to find the first digit in digit stream	67
7.3	10 transition lists as resource to the engine	68
7.4	Database engine	69
8.1	FA/FR vs. Threshold	72
8.2	Comparison between different Costs with EER by using cost function	74
8.3	Different cost to one client depends on level of security required	74
8.4	EER by using cost function vs. threshold	75
8.5	Hit-rate (threshold vs. 1-FR)	75

8.6	Relationship between (Hit-rat and FA) i. e ROC curve	76
8.7.a	Standard ROC Curve	77
8.7.b	Standard ROC Curve	77
8.8	ROC Curve can cross	78
8.9	FR vs. FA (DET)	79
8.10	Shows Standard shape of Hit-rate	79
8.11	Different settings to threshold	81
8.12	EER in Combination Digit	83
8.13	Total cost function in digit combination	83
8.14	ROC for digit combination	85
8.15	ROC Digit combinations for 2-Digits	85
8.16	ROC Digit combinations for 1-Digits	85
8.17	Hit rat in digit combination	86
8.18	DET Curve for digit combination 3-digits	87
8.19	DET Curve for digit combination 5-digits	87
8.20	Comparisons EER with Min Cost	91
9.1	Methodology of Multibiometric System	96
9.2	Three Biometric Device in One system	97

## LIST OF ABBREVIATIONS

$\mu/\bar{x}$	-	Mean
B	-	Boy
$B_i/B_k$	-	Biometric Trait
C	-	Codebook
CCD	-	Charge-coupled device, an electronic light sensor used in digital

		cameras
CER	-	Cross-over Error Rate
CM	-	Cross Match
$C_m$	-	Cepstral coefficients
C1&C2	-	Client Cost & Imposter Cost
$\tilde{c}_m$	-	Weighted cepstral coefficients
3-D	-	Three dimension picture
DET	-	Detection Error Trade-off
DFT	-	Discrete Fourier transform
$D_j$	-	Distortion in vector quantization
DTW	-	Dynamic Time Warping
EER	-	Equal Error Rate
$E_n = EER$	-	Square prediction error
FA	-	False Acceptance
FAR	-	False Acceptance Rate
FBAS	-	Full Multibiometric Adaptive System
FIR	-	False Identification Rate
FR	-	False Rejection
FRR	-	False Rejection Rate
FMR	-	False Match Rate
FNMR	-	False Non-Match Rate
FTA	-	Failure to Acquire
FTE/FER	-	Failure to Enroll
G	-	Girl
GFAR	-	Generalized False Acceptance Rate
GFRR	-	Generalized False Rejection Rate
GMM	-	Gaussian Mixture Model
$H_0$	-	Input Biometric Not From the Same Biometric
$H_i$	-	Input From Same Biometric
HMM	-	Hidden Markov Model
$I$	-	claimed identity

L	-	Lengths of frame of speech
LPC	-	Linear Predictive Coding
LPCC	-	Linear Predictive Coding Cepstral Coefficients
$M$	-	Similarity measure between two Fingerprint Images
M	-	Man
MAP	-	Minimum Adapted System
MFCC	-	Mel-Frequency Cepstrum Coefficients
MMER	-	Multi-Modal Error Rate
MS	-	Multiple similarity
MVE	-	Minimum Verification Error
$N_m$	-	Number of Templates of Database
NN	-	Nearest Nighbors
$P()$	-	Probability
Q	-	Number on input vector to be quantized
$Q_{NO}$	-	Prior Probability
QRR	-	=(FTA) Failure to Acquire
ROC	-	Receive Operating Characteristic
ROCA	-	Receive Operating Characteristic Area
RSI	-	Recognition System Inc
$\sigma$	-	Standard deviation
$S_k$	-	Normalized Matching Score
SI	-	Speaker Identification
SV	-	Speaker Verification
th	-	Threshold Parameter
$T_i$	-	EER Threshold
$t_i$	-	Training vector in vector quantization
TV	-	Television
$v_{i,j}$	-	Codebook vectors in vector quantization
VQ	-	Vector Quantization
VQ-CM	-	Combination of Vector quantization and cross match technique
W	-	Women

$\omega_0$	-	True Imposter Class
$\omega_1$	-	True Enrollee Class
$\varpi_0$	-	Corresponding True Imposter Class
$\varpi_1$	-	Corresponding True Enrollee Class
$w_m$	-	Weighting function
$W_k$	-	Weight Associated With a Biometric Trait
$X_i$	-	Score
$Z$	-	Scores
$\eta$	-	Matching Threshold

## LIST OF APPENDICIES

APPENDIX NO.	TITLE	PAGE
A	Client List	102
A	Identification	103

A	Verification	104
B	Database List Sample (Client)	109
B	Database List Sample (Imposter)	110
C	Fingerprint	111
D	Hand-Scan Geometry Biometric	117
E	Identification Curves for Digit Combination Threshold	119
F	Goldwave Software	126

## **CHAPTER I**

### **PROJECT BACKGROUND**

#### **1.0 INTRODUCTION**

On the basis of media hype alone, you might conclude that biometric passwords will soon replace their alphanumeric counterparts with versions that cannot be stolen, forgotten, lost, or given to another person. But what if the performance estimates of these systems are far more impressive than their actual performance? To measure the real-life performance of biometric systems, and to understand their strengths and weaknesses better, we must understand the elements that comprise an ideal biometric system (P. Jonathon *et al.*, 2000).

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent.

Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal,

state and local governments, in the military, and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies.

Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. Trust in these electronic transactions is essential to the healthy growth of the global economy. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures,

Here we focus on biometric applications that give the user some control over data acquisition. These applications recognize subjects from voice recognition, hand-scan geometry, and scanned fingerprints.

The data collection in this project was done by using the set of available devices. For collecting the voice data, we used a Multispeech System (CSL model 4500) with a normal microphone (Shure dynamic 10). In hand-scan experiments, the data was collected by using a Recognition System Handkey II. Lastly, for the fingerprint part, the data was collected by using a FIU81/PERS (Puppy suite from Sony).

## **1.1 Problem statement**

A potentially more serious security concern occurs when someone uses the same biometric in many systems or when many user biometrics are stored on a single system. Specifically, once an attacker acquires the original biometric, he can use it to compromise the security of many different systems. This potential for identity theft is much more serious for biometrics than passwords since if a password is stolen, it can be

easily changed. A biometric such as a fingerprint if is stolen it is difficult or impossible to change. (Emin Martinian *et al.*, 2005).

By using different biometrics, hand-scan and voice-scan together will reduce this chance and make the system more secured.

Under the voice-scan biometric category the best (optimum) threshold setting will be the one that gives the lowest FA or FR rate. Our task will be to solve this problem i.e. optimize the FA and FR as possible by using an expected misclassification cost (Masters, 1993). False acceptance errors are the ultimate concern of high security can be traded off for a higher false rejection rate [Cample, 97]. Since we know the cost of FA or FR error rate, the cost function can be used to find the optimum threshold so that the minimum (lowest) total expected cost will be achieved.

## 1.2 Project Objectives

- To find the threshold which gives the optimum (best ) FR & FA errors rate for speaker recognition task using cost function.
- To compare the performance of the obtained optimum threshold setting with EER threshold setting.
- Analyze the recognition performance when word combinations are used as an input to the speaker recognition system.
- Analyze performance when system is combined with hand-scan and fingerprint biometrics.

### 1.3 Project Scope and Methodology

- The training task will use all digits while one digit or combination of several digits will be used in recognition task.
- Data base which consists of single digit and combination digits are designed based on TIDIGIT data base.
- The recognition system will use MFCC-derived spectrum and HMM algorithm to create client and impostors model in pattern matching process.
- The enrollment and testing sessions are carried out in normal room environment.
- Hand scan data and Fingerprint will be collected from same number of clients and impostors.

#### 1.3.1 Methodology

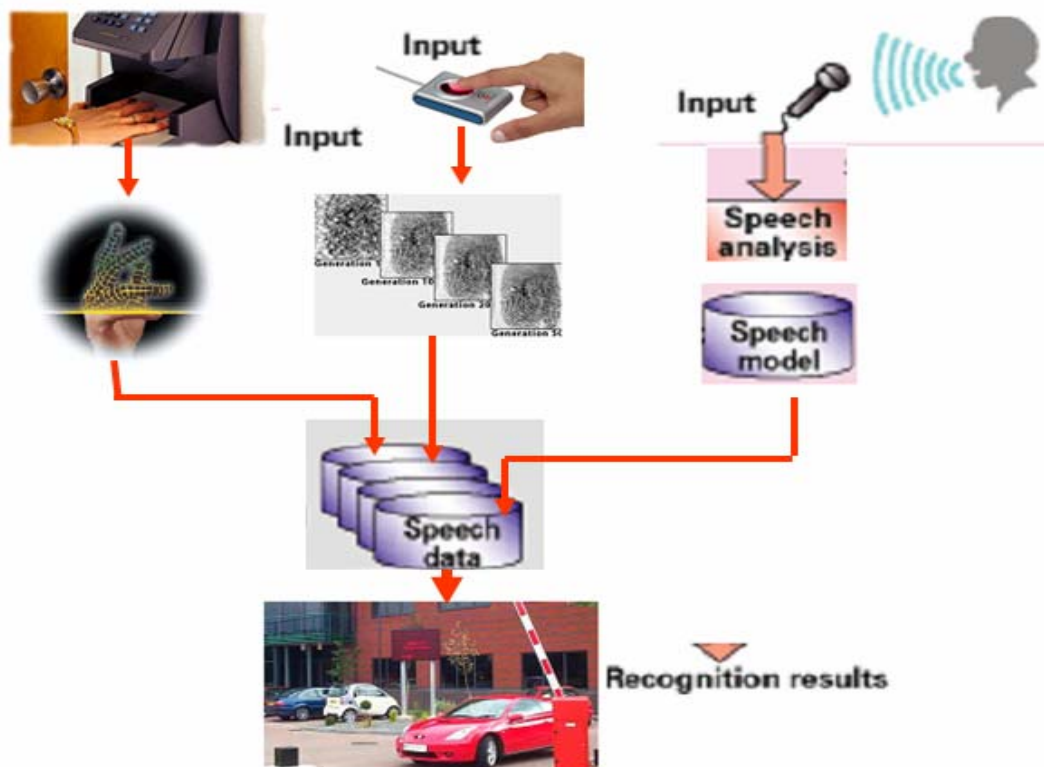


Figure 1.1 Multi-modal method.

Multimodal biometric system is the system which provides a decision depends on different kinds of data, which requires different kinds of processing. The level of security required determines how many methods needed to build the multimodal biometric system, in this project three methods were used as shown e.g. figure 1.1.

#### **1.4 Thesis Organization**

In this thesis we organized the set of chapters to be started with chapter 1 has a biometric introduction, to give definition of the project background to the biometric system and how we could use it in security propose. The problem statement was also mentioned in this chapter as well. Project objectives and scopes of the methodology of this project had been included, at the end of chapter 1 the organization of this thesis had been come.

In the second chapter, the literature review of the project which contains the background of the problem statement and previous works on speaker verification and identification. Voice-scan biometric methods, with some of the voice-scan applications, were included in chapter 2. Chapter 3 has the discussion of the methodology of this project, cepstral coefficients algorithm and Hidden Markov models algorithm was explained in this chapter. Chapter 4 has the finger biometric, which has explanation about types of fingerprint, and the recognition of fingerprint biometric system. The processing of fingerprint had been come in this chapter as well.

Hand-scan geometry biometric was organized to be chapter 5, in this chapter was given full discussion about the methods of hand-scan geometric biometric. Chapter 6 has all the explanations about the accuracy performance analysis of multimodal biometric system. Database design was discussed in the chapter 7. The results of this project had enough explanation in the chapter 8. Chapter 9 was included the summarizing of this project, the benefits of this project and suggestion of future work been mentioned in this chapter. In the end of this thesis the appendixes were organized.

## CHAPTER II

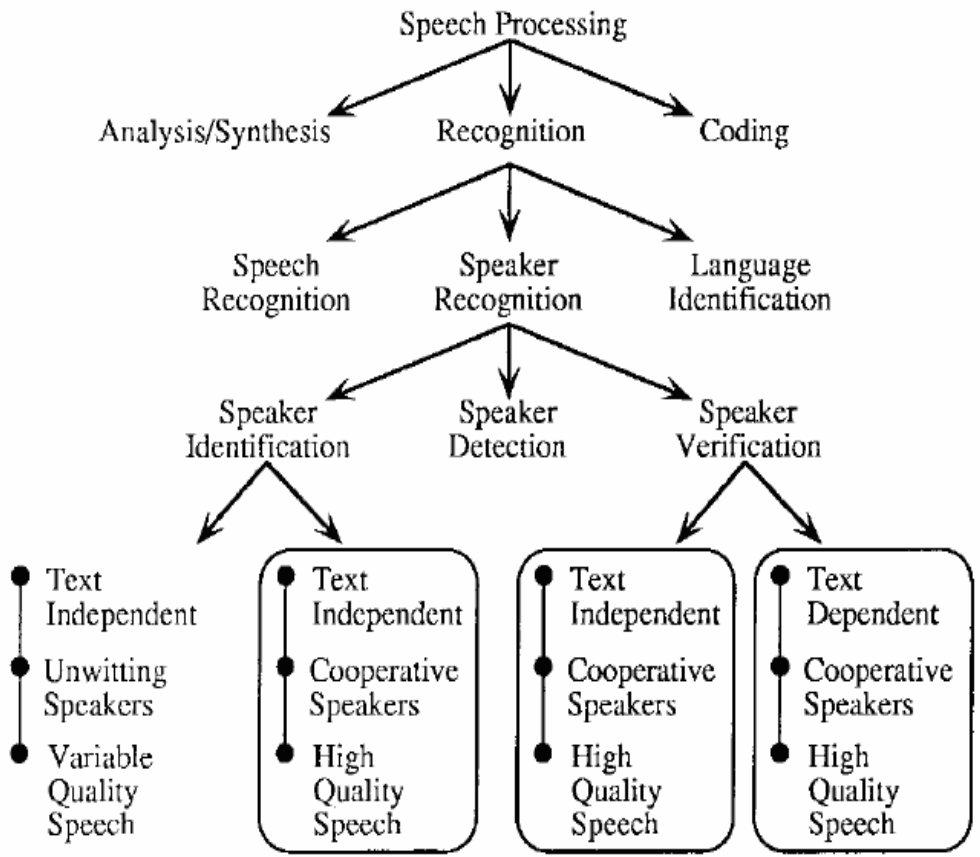
### LITERATURE REVIEW

#### 2.0 Background of Research Problem

Speech has speaker-dependent properties that enable us to recognize our friends without even look at their faces (e.g. through telephone conversation) (Atal, 1976). This has caused scientists to make an extensive research to extract the information in a speech that will enable machine to recognize the spoken word(s) or to recognize the speaker.

The study human speech by a machine is called recognition (Campbell, 1997). Speech processing is a wide field of many different applications such as speech recognition, speech analysis or synthesis, speech coding, and speaker recognition. According to Lee Hetherington (Parson, 1986 and Hetherington *et al.*, 1996), because of the complexity of the research problem, it is not uncommon for a research group to be splintered into separate subgroups, each responsible for a subset of the problem.

Speech processing is a diverse field with many applications. Figure 2.1 shows a few of these areas and how speaker recognition relates to the rest of the field.



**Figure 2.1**Speech processing

In a text-dependent system, a speaker’s identity recognition is based on his pronouncing one or more specific phrases, like a password used in this project. Text-dependent methods are usually based on template-matching techniques – dynamic time warping (DTW) algorithm. The hidden Markov model (HMM) can efficiently model statistical variation in spectral features and have achieved significantly better recognition accuracies than DTW. Therefore, HMM-based method is applied into the word recognition (Rabiner *et.al.*, 1993).

## 2.1 Previous Work on Speaker Verification and Identification

Speaker identification and verification tasks have attracted many industries, national laboratories, and universities over the world to make various researches on those tasks in an attempt to get the perfect system. Among the researches, there are some which use different techniques of decision threshold. In the following will point to some of the previous works are discussed:

**1. Rosenberg *et al.*, (1998)** made an experiment on an HMM-based speaker verification system using a proposed model adaptation – Minimum Verification Error (MVE) training scenario. The training and test database consists of 14 digits verification password utterances collected over the long distance telephone network from 25 female and 24 male speakers. All speeches are parameterized using 12th order LPC derived coefficients and their first derivatives. A comparison was made on a posteriori EER threshold and a priori dynamic threshold setting. The experimental results show that EER threshold gives equal error rate close to 0.6% after model adaptation. However, using dynamic threshold, the MVE adapted system gives 45% lower false rejection and false acceptance rates compared to the MAP adapted system.

**2. Fakotakis *et al.*, (1986)** made a research on speaker verification using optimal decision threshold. The optimal threshold was found by minimizing the sum of the false acceptance and false rejection errors. The speech recording was made by 15 male speakers. Each speaker was required to speak 5 utterances of a continuous three words sentence with an average duration of 1.4 second. The verification test was accomplished using a system based on formant extraction and processing. Experimental results show that the performance of the optimal threshold is better than equal-error threshold by 0.24%.

**3. Pierrot *et al.*, (1998)** made comparison on several a priori threshold settings for speaker verification. Likelihood ratio is used to make adjustment on speaker-

independent and speaker-dependent threshold. All experiments were carried out using telephone speech database

SESP which contains telephone utterances from 21 male and 20 female speakers. The verification system is using 16 LPC cepstral coefficients and Left-Right HMM as its feature extraction and pattern matching method. The experimental results show that the a priori threshold settings are mostly 3 to 5 times larger than the a posteriori EER threshold setting.

**4. Zhongmin Liu *et al.*, (2002)** shows the basic structures of speaker identification and verification systems. The performance of our voice recognition and identification system depends to a large extent on the recording effects of train and test data. Based on the simple equipment we used to record our voices and passwords and small number of speakers in our group for training and testing, our correct rate for the whole identification system is 100% by carefully recording and properly adjusting relevant parameters, such as codebook size, iteration number, etc. VQ tests using a set of 16 downloaded speaker wave files also work perfectly for our system. By plotting the original trained MFCC vectors by two speakers by selecting any two dimensions (e.g. 5th, 6th) of the 13 coefficients and in comparison the codebooks generated by the two speakers using the same two dimensions with a codebook size of 16. Thus we can see that each codeword on the plot exactly represent the corresponding clusters in the original MFCC data points and still accurately represent each speaker's voice characteristics.

**5. A. K. Ariff *et al.*, (2004)** presented the design and implementation of Malay speaker recognition system using discrete hidden Markov model (HMM) and (MFCC) as the classifier, speaker recognition experiments was performed using 99 speakers (13 clients and 86 imposters).

For a seven digit long sequence, 0.96% EER was achieved., as more and more digit being added, the performance is better than using single digit , the overall

performance had an average EER of 8.18% with single digit sequence, while best performance with digit length of 8 digit sequence giving an average EER of 1.67%. The system gave good results, even though there are much more room for improvement.

## **2.2 Voice Scan**

### **2.2.1 Overview of Voice Scan**

Voice scan biometric is a technology which allows a user to use his/her voice as an input device. Voice scan may be used to dictate text into the computer or to give commands to the computer (such as opening application programs, pulling down menus, or saving work).

Older voice scan biometric applications require each word to be separated by a distinct space. This allows the machine to determine where one word begins and the next stops. These kinds of voice scan biometric applications are still used to navigate the computer's system, and operate applications such as web browsers or spread sheets.

Newer voice scan biometric applications allow a user to dictate text fluently into the computer. These new applications can recognize speech at up to 160 words per minute. Applications that allow continuous speech are generally designed to recognize text and format it, rather than controlling the computer system itself.

Voice scan biometric uses a neural net to "learn" recognize your voice. As you speak, the voice scan software remembers the way you say each word. This customization allows voice scan biometric, even though everyone speaks with varying accents and inflection.

In addition to learning how you pronounce words a voice scan biometric system also uses grammatical context and frequency of use to predict the word you wish to input. These powerful statistical tools allow the software to cut down the massive language data base before you even speak the next word.

While the accuracy of voice scan biometric has improved over the past few years some users still experience problems with accuracy either because of the way they speak or the nature of their voice ([www.biometricsinfo.org](http://www.biometricsinfo.org) 2007 ).

### **2.2.2 Voice Scan Biometric: How it Works**

Voice scan biometric technology utilizes the distinctive aspects of the voice to verify the identity of individuals. Voice scan biometric occasionally confused with speech recognition, a technology which translates what a user is saying (a process unrelated to authentication). Voice scan biometric technology, by contrast, verifies the identity of the individual who is speaking. The two technologies are often bundled – speech recognition is used to translate the spoken word into an account number, and voice scan biometric verifies the vocal characteristics against those associated with this account.

During enrollment an individual is prompted to select a passphrase or to repeat a sequence of numbers. The passphrases selected should be approximately 1-3.5 seconds in our project in length very short passphrases lack enough identifying data. The individual is generally prompted to repeat the passphrase or number set a handful of times, making the enrollment process somewhat longer than most other biometrics.

### **2.2.3 Voice Scan Biometric Strengths and Weaknesses**

One of the challenges facing large-scale implementations of biometrics is the need to deploy new hardware to employees, customers and users. One strength of telephony-based voice scan biometric implementations is that they are able to circumvent this problem, especially when they are implemented in call center and account access applications. Without additional hardware at the user end, voice scan biometric systems can be installed as a subroutine through which calls are routed before access to sensitive information is granted. The ability to use existing telephones means that voice scan biometric vendors have hundreds of millions of authentication devices available for transactional usage today.

Similarly, voice scan biometric is able to leverage existing account access and authentication processes, eliminating the need to introduce unwieldy or confusing authentication scenarios. Automated telephone systems utilizing speech recognition are currently ubiquitous due to the savings possible by reducing the amount of employees necessary to operate call centers. Voice scan biometric and speech recognition can function simultaneously using the same utterance, allowing the technologies to blend seamlessly. Voice scan biometric can function as a reliable authentication mechanism for automated telephone systems, adding security to automated telephone-based transactions in areas such as financial services and health care.

Though inconsistent with many users' perceptions, certain voice scan biometric technologies are highly resistant to imposter attacks, even more so than some fingerprint systems. While false non-matching (rejection rate) can be a common problem, this resistance to false matching (acceptance rate) means that voice scan biometric can be used to protect reasonably high-value transactions.

Since the technology has not been traditionally used in law enforcement or tracking applications where it could be viewed as a Big Brother technology, there is less public fear that voice scan biometric data can be tracked across databases or used to monitor

individual behavior. Thus, voice scan biometric largely avoids one of the largest hurdles facing other biometric technologies, that of perceived invasiveness.

#### **2.2.4 Voice Scan Biometric Applications**

Voice scan biometric is a strong solution for implementations in which vocal interaction is already present. It is not a strong solution when speech is introduced as a new process. Telephony is the primary growth area for voice scan biometric, and will likely be by far the most common area of implementation for the technology. Telephony-based applications for voice recognition include account access for financial services, customer authentication for service calls, and challenge-response implementations for house arrest and probation-related authentication. These solutions route callers through enrollment and verification subroutines, using vendor-specific hardware and software integrated with an institution's existing infrastructure.

Voice scan biometric has also been implemented in physical access solutions for border crossing, although this is not the technology's ideal deployment environment.

#### **2.2.5 Pattern Matching**

The pattern matching process involves the comparison of a given set of input feature vectors against the speaker model for the claimed identity and computing a matching score. For the Hidden Markov models discussed above, the matching score is the probability that a given set of feature vectors was generated by the model (www.biometricsinfo.org- 2007). The figure 2.2 below shows the sequence of steps in matching task.

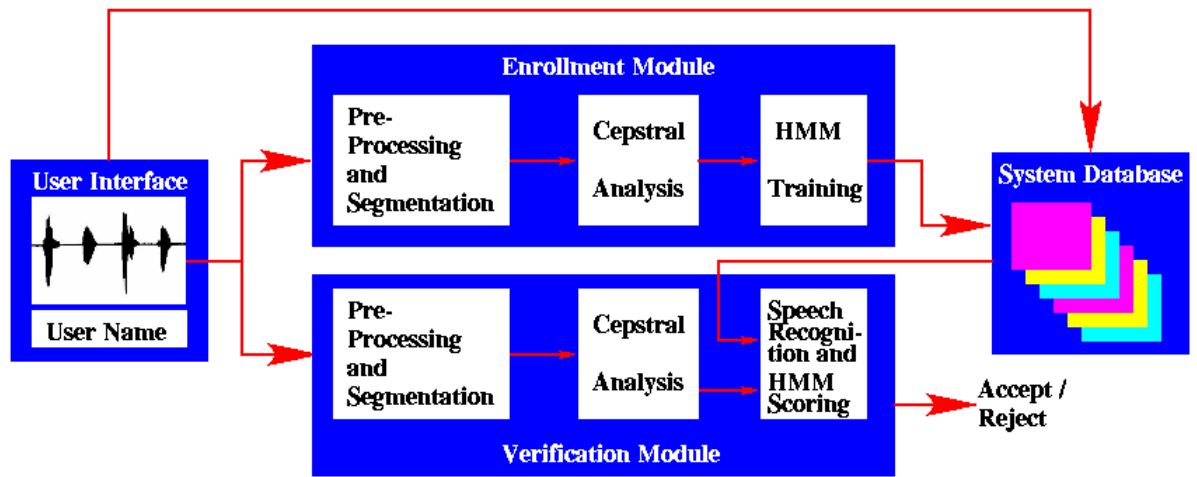


Figure 2.2. Pattern matching

## **CHAPTER III**

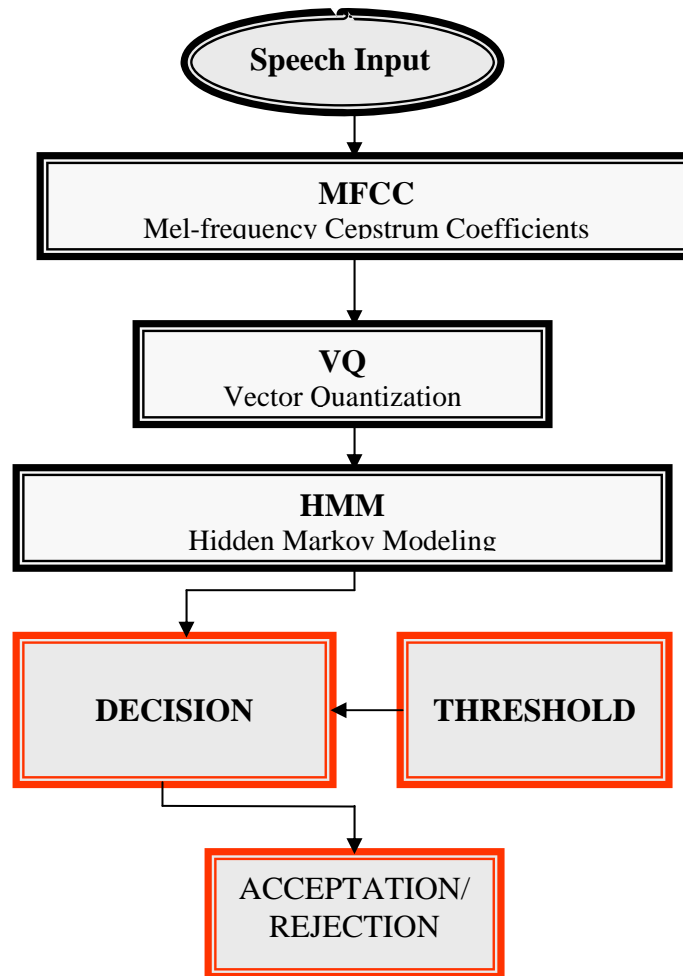
### **PROJECT METHODOLOGY**

#### **3.0 Introduction**

This section shows the methodology or steps taken to carry out the project based on objectives and scope stated in Chapter II. Both speaker identification and speaker verification tasks' methodology will be outlined assuming a text-dependent system based on past research work.

#### **3.1 Project Outline**

This project is carried out using the following methodology in figure 3.1:



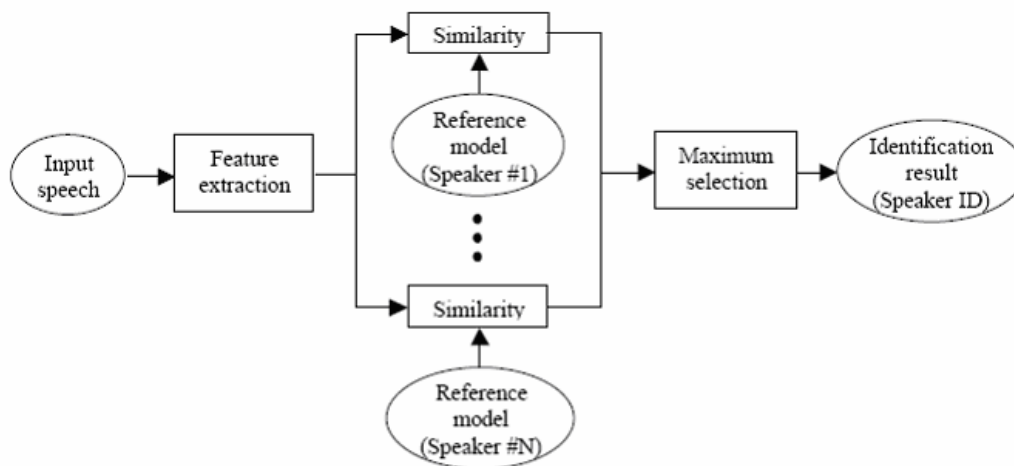
**Figure 3.1** Methodology

### 3.1.1 Overview of voice-scan

All voice-scan biometric systems include an initial signal processing front end that converts a speech waveform into features useful for further processing. The front end is required to extract important features from the original speech waveform that is relatively insensitive to talker and channel variability unrelated to speech message content. The first stage also reduces the data rate into later stages of speech recognizer

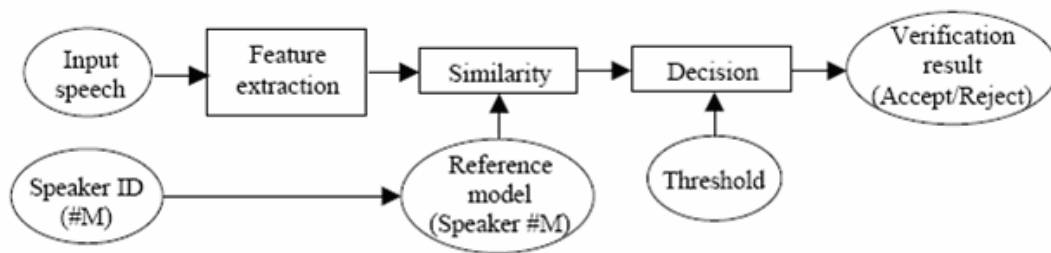
and attempts to decrease redundancy inherent in the speech waveform. This research concentrates only two of speech functions techniques. These techniques are Hidden Markov Models (HMM), and Mel-Frequency Cepstrun Coefficients (MFCC) (Parson, 1987 ).

Another important key question in voice-scan biometric is how speech patterns are compared to determine their similarity. Depending on the requirements of the recognition system, pattern comparison can be done in a wide variety of ways. The people never speak words of exactly the some uniform rate. Words sometime are spoken quickly and in other time are spoken slowly, so some method of time alignment is required in order to compare the test pattern with reference word patterns. Mel-Frequency Cepstral Coefficient (MFCC) technique can handle this problem. Another well-known and widely used statistical method of characterizing the spectral properties of the frames of a pattern is the Hidden Markov Models (HMM) approach. The use of Hidden Markov Models for speech recognition has become increasingly popular in the past few years. This work focuses only on these two modulation comparison techniques, the discussion of (MFCC) and (HMM) can be found later.



**Figure 3.2** Identification

In the figure 3.2 and figure 3.3, show two functions apply over, the first function in figure 3.2 when the speaker sends his speech (key word - which mean here the password) then the system will process the speaker speech and apply the first function as identification then start to apply the second function which is verification of the person speaking and give the last decision. This process of comparison between the input and database is called (1:N). To avoid FA to happen in system, one more step which is verification will be done. This function is called (1:1), see the figure 3.3.



**Figure 3.3** Verification.

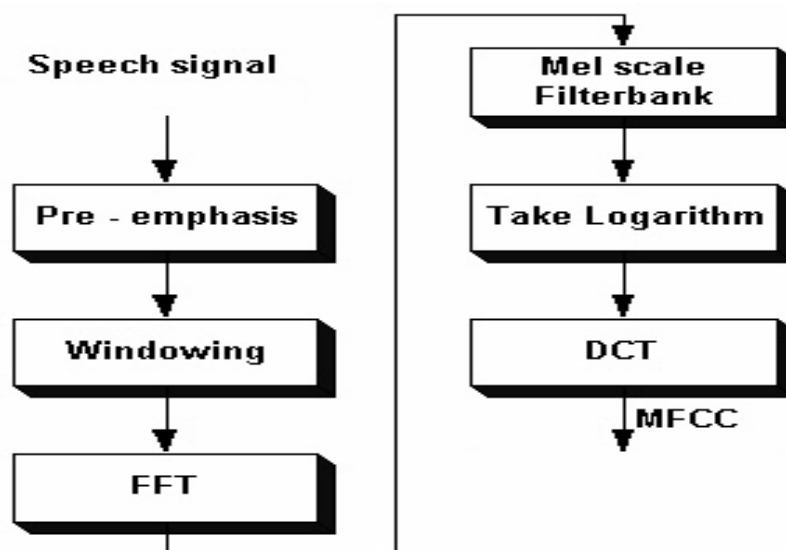
### 3.1.2 Overview of Mel-Frequency Cepstral Coefficients (MFCC) Algorithm

The Mel-Frequency Cepstral Coefficients (MFCC) is commonly used in many speech recognition system. It plays the role of the acoustic feature vectors, extracted by the front-end of the speech recognizer. The pitch frequency may also be used for recognition, especially for tonal languages (e.g. Mandarin Chinese).

Speech recognition technologies are finding their way into client-server applications. In some scenarios, a client compresses the speech during recording using one of the common speech compression techniques. The compressed speech is then stored on the client for future uploading to a speech recognition server (deferred

recognition), or transmitted over bandwidth limited channel to server for real time speech recognition. In addition, the client may also support playback of the compressed speech. However, compressing the speech waveform usually increases recognition errors (especially for dictation tasks), and therefore high quality compression methods should be used. These methods require large processing power or high bit rates which are often not available in client-server system (e.g. when a thin-client is used).

Techniques for speech recognition from Mel-Cepstral or Cepstral like parameters have been previously proposed. However, in both cases the definition of the cepstral parameters rather specific, chosen a priori to allow spectral reconstruction and not in line with the MFCC features used in speech recognition system (Hermansky, 1994). The figure 3.4 below shows the main methods in MFCC category.



**Figure 3.4** MFCC transaction

The accuracy of human speech recognition motivates the application of information processing strategies found in the human auditory system to automatic speech recognition (ASR) (B. Richard C., 1989). The most popular feature extraction method for ASR, Mel-Frequency Cepstral Coefficients (MFCC) and perceptual linear

prediction [PLP], already employ several principles which have known counterparts in the cochlea and auditory nerve frequency decomposition, mel-or bark warping of the frequency axis, and compression of amplitudes. It, therefore, seems natural to consider the next processing step in the auditory periphery-synaptic adaptation in the auditory nerve. Adaptation (also known as synaptic depression) is a principal mechanism of neuronal information processing and is ubiquitous in the brain. Adaptation is strong in the auditory nerve, as has been described in a number of measurements (Hong, K., 2001).

### 3.1.3 Overview of Vector Quantization

Vector quantization (VQ) is used to average out the temporal information of speech. VQ will reduce the dimension of speech vectors into a smaller dimension size (called codebook) using standard clustering methods. Each speaker will have his own codebook created from his speech. In pattern matching process, the match score is obtained by comparing an input vector with code word in the VQ codebook  $C$ . The match score  $z$  for  $L$  frames of speech is given by

$$z = \sum_{j=1}^L \min_{\bar{x} \in C} \{d(x_j, \bar{x})\} \quad 3.1$$

Nearest neighbors (NN) is a new method from a combination of DTW and VQ strengths (Higgins, 1993).

### 3.1.4 Overview of Hidden Markov Models (HMM) Algorithm

The design of a voice-scan biometric system for continuous speech, if the vocabulary size is rather large, needs the definition of recognition unite smaller than

words. Hidden Markov Models provide a way to statistically model such recognition units without hand labeling or segmentation. The cardinality of the unit set must be reasonably low to obtain a good statistical representation and high enough to catch all structural variations of phonetic events (Rabiner *et al.*, 1989) The method is evaluated on an isolated word recognition task using hidden Markov models (HMM's) with Gaussian observation densities and trying at the state level (Becchetti C ,2002).

Our philosophy in the recognition units definition starts from the classical diphones (speech segments between two consecutive stationary portions). The advantage of this choice is that context variations are included in the units, but the cardinality of this set is very high (about 1000). Besides many diphones are necessary in the recognition procedure, in the sense that the information included in the transition is not always significant for the discrimination of the unit itself. On the other side some transition is necessary for the correct recognition of complex phonetic events like plosives.

These considerations suggest the idea of defining the units on the basis of their discriminative capability; if a transition is supposed to help recognition its model is estimated, otherwise “connected-free” models of the phonemes are directly connected (Rabiner *et.al.*, 1993). In recent years, the duration of the recognition phase has emerged as a major problem because of the increasing size of the vocabularies processed by automatic speech recognition systems (Joseph p, 1997 and Becchetti C, 2002). As an alternative approach, note that it is also possible to design procedures that approximate the computation needed during the recognition phase without actually limiting the number of distinct model parameters (Jittiwarakul, N. *et al.* 1998 and Becchetti C, 2002).

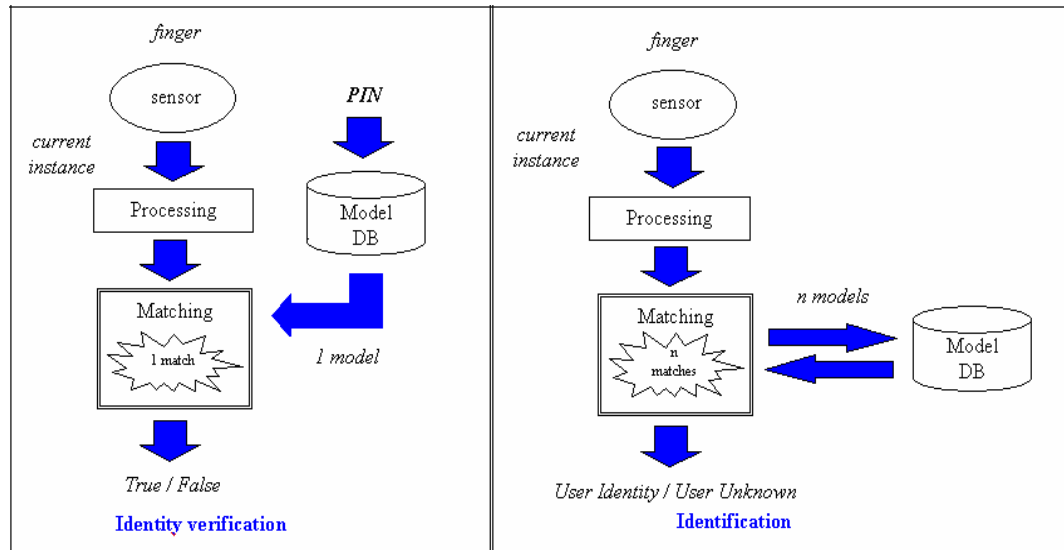
### 3.1.5 Threshold Setting

Threshold basically is the point where the decision will be acceptance or reject in voice-scan biometric system. In order to set a threshold, a probability density function (PDF) for each client, and their corresponding impostors have to be estimated from a set of test samples. In previously to determine the threshold we need to estimate it depends on the FA and FR, but because that make the people in more challenging to decide which design in better, the idea of ERR has come over to solve this problem.

Nowadays there are many techniques are used to set the threshold point in the biometric systems to make the decision more accurate, by using some of those methods in this project for example receiver operation curve (ROC), detection error trade-off curve (DET) and Cost function as well,( in coming chapters will give more details about these criteria's )we could optimize the threshold in our project order.

## 3.2 Identification

With identification, the biometric system asks and attempts to answer the question “Who is X?”. In an identification application, the biometric device reads a sample and compares that sample against every record or template in the database. This type of comparison is called a “one-to-many” search (1:N). Depending on how the system is designed, it can make a “best” match, or it can score possible matches ranking them in order of likelihood. Identification applications are common when the goal is to identify criminals, impostors, terrorists, or other “wolves in sheep’s clothing”, particularly through surveillance. See the figure 3.5.



**Figure 3.5** Identification and verification

### 3.3 Verification

Verification occurs when the biometrical system asks and attempts to answer the question “Is this X?” after the user claims to be X. In a verification application, the biometric system requires input from the user, at which time the user claims his identity via a password, token, or user name (or any combination of the three), which is presented by speaking. This user input points the system to a template in the database. The system also requires a biometric sample from the user. It then compares the sample to or against the user-defined template. This is called a “one-to-one”, search (1:1). The system will either find or fail to find a match between the two verification is commonly used for physical or computer access. See the figure 3.5.

## **CHAPTER IV**

### **FINGERPRINT BIOMETRIC**

#### **4.0 Introduction**

"Yes, We are able to put together in perfect order the very tips of his fingers."  
(The Qur'an, 75:3-4)

As our everyday life is getting more and more computerized, automated security systems are getting more and more important. Today, most of the banking transactions can be performed over the Internet and soon they can also be performed on mobile devices such as cell phones and PDAs. This rapid progress in wireless communication system, personal communication system and smart card technology in our society makes information more susceptible to abuse. Due to the growing importance of the information technology and the necessity of the protection and access restriction, reliable personal identification is necessary.

The key task of an automated security system is to verify that the users are in fact who they claim to be. There are three main methodologies when performing this verification. The security system could ask the user to provide some information known only to the user, it could ask the user to provide something only the user has access to or it could identify some sort of trait that is unique for the user. Identifying some trait that is unique for the user is known as biometric security. A biometrics system is a pattern

recognition system that establishes the authenticity of a specific physiological or behavioral characteristic possessed by a user (Nor., 2006).

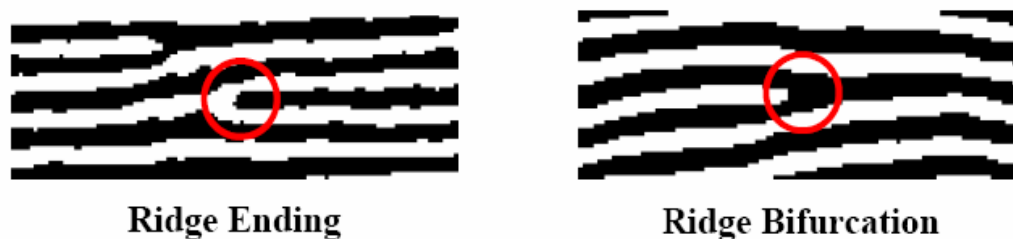
Nowadays, embedded systems have become increasingly popular as advances in IC-technology and processor architecture allow for flexible computational parts and high-performance modules integrated on a single carrier. Embedded system interacts with the physical world. It executes on machines that are not, first and foremost, computers. They are cars, airplanes, telephones, audio equipment, robots, appliances, toys, security systems, pacemakers, heart monitors, weapons, television sets, printers, scanners, climate control systems, manufacturing systems, and so on. They performed function carefully partitioned in software and hardware to strike the balance between flexibility, reusability, performance and cost.

#### **4.1 Types of Fingerprint**

There are two types of fingerprint representations: local and global. Local representations predominantly based on ridge endings or bifurcations (collectively known as minutiae see figure 4.1) are the most common, primarily due to the following reasons:

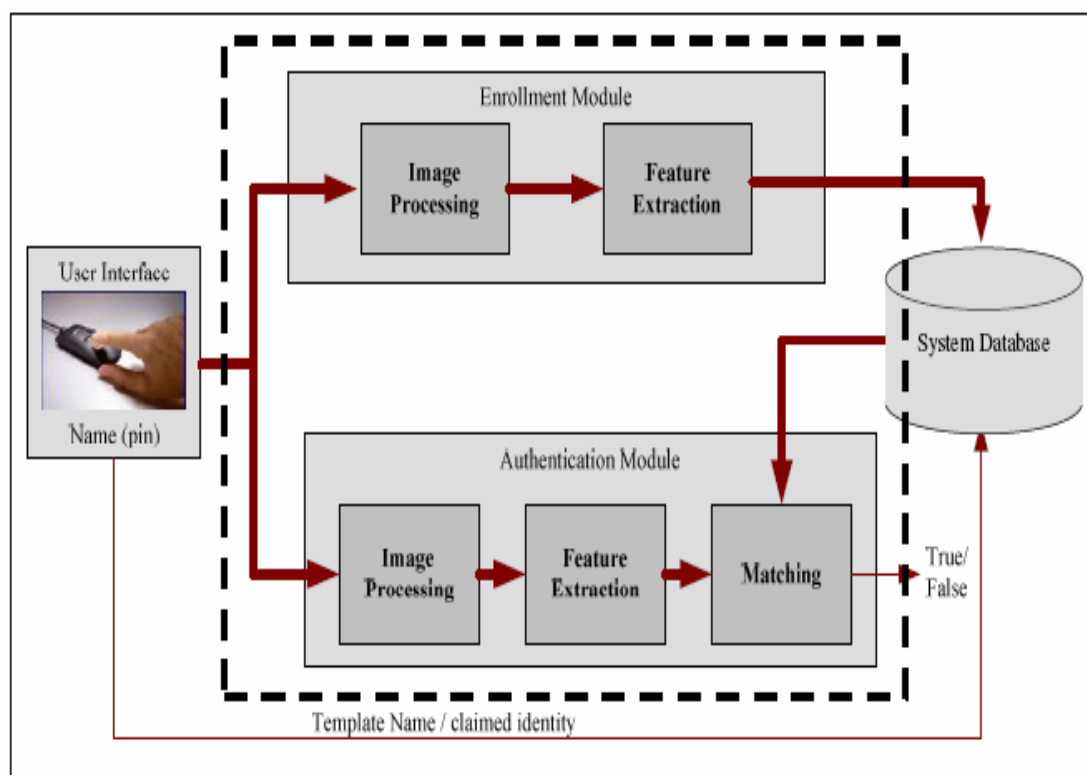
- Minutiae capture much of the individual information
- Minutiae-based representations are storage efficient
- Minutiae detection is relatively robust to various sources of fingerprint degradation.

Typically, minutiae-based representations rely on locations of the minutiae and the directions of ridges at the minutiae location. Cores and deltas are global representation of the fingerprint.



**Figure 4.1** Ridge ending and ridge bifurcation

A fingerprint recognition system involves many process and stages. Figure 4.2 shows the general process to recognize a fingerprint.



**Figure 4.2** Main process in identify a fingerprint

## **4.2 Fingerprint Recognition System**

The architecture of a fingerprint recognition system is shown in figure 4.2. A typical fingerprint recognition system consists of four components: user interface, system database, enrollment module and authentication module.

The user interface provides a mechanism for a user to indicate his/her identity and input his/her fingerprint into the system. The system database consists of a collection of records, each of which corresponds to an authorized person that has access to the system. Each record may contain the minutiae templates of the person's fingerprint and user name of the person or other information such as pin no as an index to the template.

The task of enrollment module is to enroll persons and their fingerprints into the system database. When the fingerprint images and the user name of a person to be enrolled are fed to the enrollment module, the images will be enhanced and thinned at the image processing stage. Then the biometric template will be extracted at the feature extraction stage.

The task of the authentication module is to authenticate the identity of the person who intends to access the system. The person to be authenticated indicates his/her identity and places his/her finger on the fingerprint scanner. The fingerprint images captured is enhanced and thinned at the image processing stage, and at feature extraction stage, the biometric template is extracted. It is then fed to a matching algorithm, which matches it against the person's biometric template stored in the system database to establish the identity.

## **4.3 The History of Fingerprints**

The science of fingerprint Identification stands out among all other forensic sciences for many reasons, including the following ([www.oninonin.com](http://www.oninonin.com)).

- Has served all governments worldwide during the past 100 years to provide accurate identification of criminals. No two fingerprints have ever been found alike in many billions of human and automated computer comparisons. Fingerprints are the very basis for criminal history foundation at every police agency.
- Established the first forensic professional organization, the International Association for Identification (IAI), in 1915.
- Established the first professional certification program for forensic scientists, the IAI's Certified Latent Print Examiner program (in 1977), issuing certification to those meeting stringent criteria and revoking certification for serious errors such as erroneous identifications.
- Remains the most commonly used forensic evidence worldwide - in most jurisdictions fingerprint examination cases match or outnumber all other forensic examination casework combined.
- Continues to expand as the premier method for identifying persons, with tens of thousands of persons added to fingerprint repositories daily in America alone - far outdistancing similar databases in growth.

#### **4.3.1 Why Fingerprint Identification**

Fingerprints offer an infallible means of personal identification. That is the essential explanation for their having supplanted other methods of establishing the identities of criminals reluctant to admit previous arrests.

Outperforms DNA and all other human identification systems to identify more murderers, rapists and other serious offenders (fingerprints solve ten times more unknown suspect cases than DNA in most jurisdictions).

Other visible human characteristics change - fingerprints do not. In earlier civilizations, branding and even maiming were used to mark the criminal for what he was. The thief was deprived of the hand which committed the thievery. The Romans employed the tattoo needle to identify and prevent desertion of mercenary soldiers.

Before the mid-1800s, law enforcement officers with extraordinary visual memories, so-called "camera eyes," identified previously arrested offenders by sight.

Photography lessened the burden on memory but was not the answer to the criminal identification problem. Personal appearances change.

Around 1870, a French anthropologist devised a system to measure and record the dimensions of certain bony parts of the body. These measurements were reduced to a formula which, theoretically, would apply only to one person and would not change during his/her adult life.

This Bertillon system, named after its inventor, Alphonse Bertillon, was generally accepted for thirty years. But it never recovered from the events of 1903, when a man named Will West was sentenced to the U.S. Penitentiary at Leavenworth, Kansas. You see, there was already a prisoner at the penitentiary at the time, whose Bertillon measurements were nearly the same, and his name was William West.

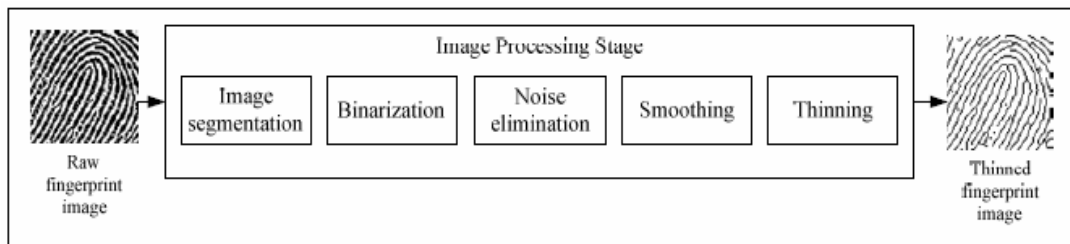
Upon investigation, there were indeed two men who looked exactly alike, but were allegedly not related. Their names were Will and William West respectively. Their Bertillon measurements were close enough to identify them as the same person. However, a fingerprint comparison quickly and correctly identified them as two different people. (Per prison records discovered later, the West men were apparently

identical twin brothers and each had a record of correspondence with the same immediate family relatives) ([www.oninonin.com](http://www.oninonin.com)).

## 4.4 Fingerprint Processing

### 4.4.1 Image Processing Stage

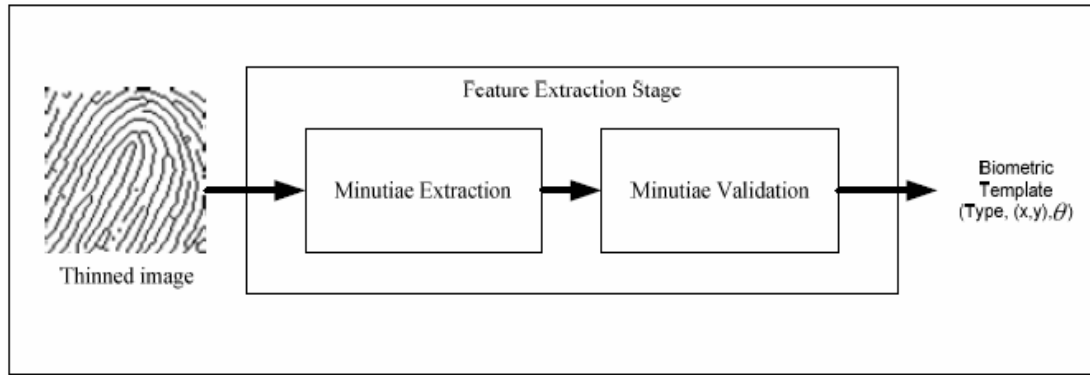
The goal of image processing stage is to filter, binarize, enhance and skeletonized the original gray-level image. Five different processes are sequentially applied to achieve this goal. Figure 4.3 shows the process required in this stage.



**Figure 4.3** Image processing stage

### 4.4.2 Feature Extraction Stage

After the fingerprint image has been binarized, enhanced and thinned, it will be fed to the feature extraction stage. The goal of this stage is to extract the minutiae point from the thinned image. Following the extraction is a minutia validation process that eliminates the false minutiae before storing or using the template for matching process. Figure 4.4 shows the feature extraction stage.

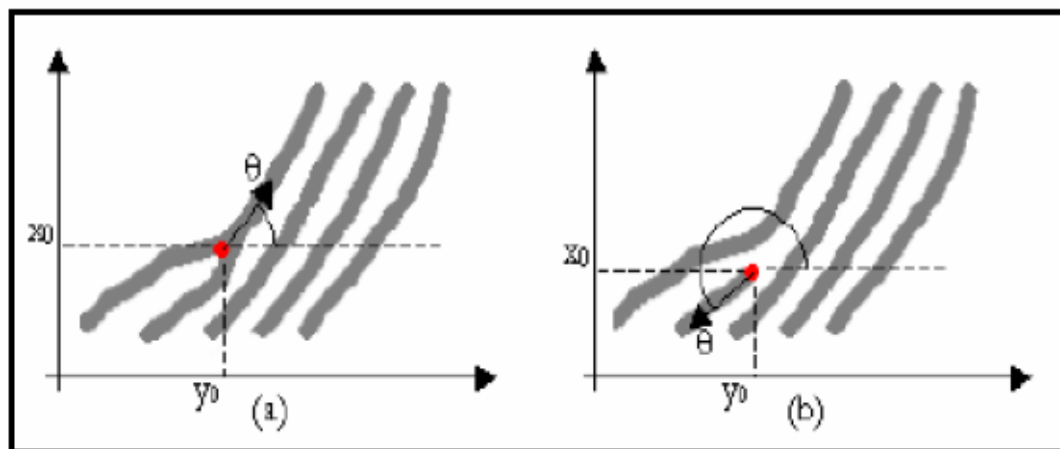


**Figure 4.4** feature extraction stage

#### 4.4.3 Minutiae Extraction.

Minutiae points are essentially the endings and bifurcations of the ridgelines that constitute a fingerprint. The basic properties of a minutia are type, position and direction as shown in figure 4.5. The minutiae type can be either ridge ending or ridge bifurcation. The direction of a minutia is, in this system, defined to be the angle of the vector that starts in the minutia and ends in the eight pixel of the ridge that the minutia belongs to. In the bifurcation case, the vector that has the largest angle to the other two vectors is selected as the direction of the minutia.

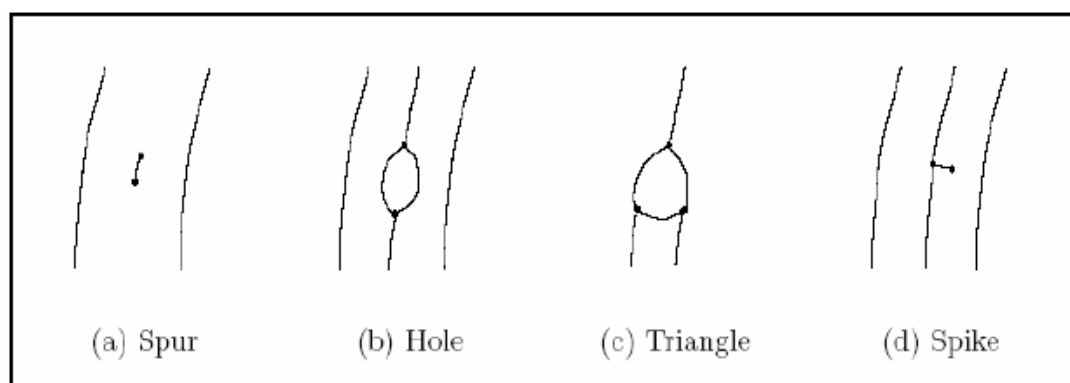
The extraction of minutiae points is a critical step in fingerprint verification systems. This is when the analog fingerprint information captured by the scanning device is transformed to a format that can be matched by an automated system. There are two main methodologies to extract minutia information, binary extraction and direct grayscale extraction



**Figure 4.5** Minutia extraction

#### 4.4.4 Minutiae Validation

False minutiae may be introduced into the image due to factors such as noisy images, and image artifacts created by the thinning process. Hence, after the minutiae are extracted, it is necessary to employ a validation process in order to validate the minutiae. Figure 4.6 illustrates some examples of false minutiae structures, which include the spur, hole, triangle and spike structures.



**Figure 4.6** False minutiae structures

#### 4.4.5 Matching Stage

Reliably matching fingerprint images is an extremely difficult problem, mainly due to the large variability in different impressions of the same finger (i.e., large intra-class variations). The main factors responsible for the intra-class variations are: displacement, rotation, partial overlap, non-linear distortion, variable pressure, changing skin condition, noise, and feature extraction errors. Therefore, fingerprints from the same finger may sometimes look quite different whereas fingerprints from different fingers may appear quite similar.

The similarity measure,  $M$  between two fingerprint images is defined as

$$M = \sqrt{\frac{N_m \times N_m}{N_1 \times N_2}} \quad 4.1$$

Where  $N_1$  and  $N_2$  are the number of templates from database and test fingerprint respectively,  $N_m$  are the number of paired templates in  $S_{\max}$  (Nor. 2006).

The similarity measure  $M$  for two images from the same fingerprint is close to 1. In practice, if the calculated  $M$  is bigger than a predefined reasonable threshold, then it can be said that the two images originated from the same fingerprint.

## **CHAPTER V**

### **HAND-SCAN GEOMETRY BIOMETRIC**

#### **5.0 Introduction**

This biometric approach uses the geometric form of the hand for confirming an individual's identity. Because human hands are not unique, specific features must be combined to assure dynamic verification. Some hand-scan devices measure just two fingers, others measure the entire hand. Features include characteristics such as finger curves, thickness and length; the height and width of the back of the hand; the distances between joints and all bone structure. Although the bone structure and joints of a hand are relatively constant traits, other influences such as swelling or injury can disguise the basic structure of the hand (Bhavani, 2005).

To register in a hand-scan system a hand is placed on a reader's covered flat surface. This placement is positioned by five guides or pins that correctly situate the hand for the cameras. A succession of cameras captures 3-D pictures of the sides and back of the hand. The hand-scan device can process the 3-D images in 5 seconds or less and the hand verification usually takes less than 1 second. Components include: acquisition hardware, matching software, and storage.

## 5.1 How Hand-Scan Works

Hand geometry scanners such as those made by Recognition Systems Inc. take over 90 measurements of the length, width, thickness, and surface area of the hand and four fingers all in just 1 second. The technology uses a 32,000-pixel CCD digital camera to record the hand's three-dimensional shape from silhouetted images projected within the scanner.

The scanner disregards surface details, such as fingerprints, lines, scars, and dirt, as well as fingernails, which may grow or be cut from day to day. When a person uses the scanner, it compares the shape of the user's hand to a template recorded during an enrollment session. If the template and the hand match, the scanner produces an output it may unlock a door, transmit data to a computer, verify identification, or log the person's arrival or departure time.

During enrollment, which takes approximately 30 seconds, the user places the right hand in the reader three times. The unit's internal processor and software convert the hand image to a 9-byte mathematical template, which is the average of the three readings.

The user's template may reside in internal memory (capable of holding over 27,000 users), or on other media such as a hard disk or smart card chip. As opposed to such technologies as fingerprint, voice recognition, and facial recognition, where a multitude of vendors compete via their proprietary technology, hand geometry technology is dominated by one company, Recognition Systems, Inc. (RSI). Finger geometry is led by Biomet Partners.

RSI's method for capturing the biometric sample is as follows: To enroll, the user places his or her hand palm down on the reader's surface. The user then aligns his or her hand with the five pegs designed to indicate the proper location of the thumb, forefinger, and middle finger.

Three placements are required to enroll on the unit; the enrollment template is a representation of the most relevant data from the three placements. RSI's units use a 32,000-pixel CCD (charged coupled device) digital camera, inferring the length, width, thickness, and surface area of the hand and fingers from silhouetted images projected within the scanner.

Over 90 measurements are taken, and the hand and fingers' characteristics are represented as a 9 byte template. Biomet Partners' technology is similar, but draws on the shape and characteristics of the index and middle finger. The data is saved as a 20 byte template.

Hand geometry does not perform 1-to-many identification, as similarities between hands are not uncommon. Where hand geometry does have an advantage is in its FTE (failure to enroll) rates, which measure the likelihood that a user is incapable of enrolling in the system. Fingerprint, by comparison, is prone to FTE's due to poor quality fingerprints; facial recognition requires consistent lighting to properly enroll a user.

## **5.2 Past Projects**

### **5.2.1 A Hand Geometry-Based Verification System**

This project explores the use of hand geometry as a measure of a person's identity. The system consists of an acquisition device that captures the top view and side view of a user's right hand as he places it on the flat surface of the device. A snapshot of the user's hand is taken for processing. A set of features have been identified that could be used to represent a person's hand. These features include the lengths and widths of the fingers at various locations.

### **5.2.2 Deformable Matching of Hand Shapes for Verification**

This project involves designing a mechanism that would align hand shapes prior to verifying a person's identity. Such an approach would enhance the integrity of the feature set made available during the verification stage.

### **5.2.3 Web-Access using Biometrics**

Arun Ross (2007) work's involved securing a website using biometrics. Users are granted access to a set of files in a web-site after their identity has been verified using Biometrics Hand Geometry in particular. We believe biometrics based web-access will add a new layer of security over existing web-security systems. (Arun Ross *et al.*, 2007).

## **5.3 Template Generation and Matching**

Distinctive features include height, width, and thickness of the hand. Distinctive features of the hand and finger are extracted from a series of 3-D images and recorded into a small template.

False matching and false non-matching are possible due to the fact that hands may swell and undergo changes.

## **5.4 Applications**

Hand geometry is currently among the most widely used biometric technologies, most suitable for access control and time and attendance applications. Hand scan is used reliably at thousands of places of employment, universities, apartment buildings, and

airports - anyplace requiring reasonably accurate see the figure 5.1, non-intrusive authentication. The nature of hand geometry technology is such that most projects are fairly small-scale and involve only a handful of readers, but there are some projects which incorporate dozens of readers (Bhavani, 2005).



**Figure 5.1** Hand-scan at the biometric center UTM entrance

## **5.5 Strengths and Weaknesses**

### **5.5.1 Strengths**

1. Easy for use.
2. Resistant to fraud.
3. Template size – using RSI, a template size of 9 bytes is extremely small.
4. User perceptions – non-intrusive.

### **5.5.2 Weaknesses**

1. Cost
2. Static design- largely unchanged for years.

### 3. Injuries to hands.

Accuracy, hand geometry, in its current incarnation, cannot perform 1-to-many searches, but instead is limited to 1-to-1 verification.

## 5.6 Hand Geometry vs. Fingerprints

Unlike fingerprints, the human hand isn't unique. One can use finger length, thickness, and curvature for the purposes of verification but not for identification. For some kinds of access control like immigration and border control, invasive biometrics (e.g., fingerprints) may not be desirable as they infringe on privacy. In such situations it is desirable to have a biometric system that is sufficient for verification. As hand geometry is not distinctive, it is the ideal choice. Furthermore, hand geometry data is easier to collect. With fingerprint collection good frictional skin is required by imaging systems, and with retina-based recognition systems, special lighting is necessary. Additionally, hand geometry can be easily combined with other biometrics, namely fingerprint. One can envision a system where fingerprints are used for (infrequent) identification and hand geometry is used for (frequent) verification (Arun Ross *et al.*, 2007).

## 5.7 Combining Biometric Methods

A system where fingerprints are used for infrequent identification and hand-scanning is used for frequent verification would create a two tiered structure. The hand-scan component used frequently allows identity verification or 1:1 (one to one) verification that ensures the user is who they claim they are. The fingerprint identification component used infrequently, confirms who the user is and accurately identifies the user in a 1:N (one to many).

## 5.8 Registering the Hand

- ▣ To register in a hand-scan system a hand is placed on a reader's covered flat surface.
- ▣ This placement is positioned by five guides or pins that correctly situate the hand for the cameras see the figure 5.2 shows how it uses
- ▣ A succession of cameras captures 3-D pictures of the sides and back of the hand.
- ▣ The hand-scan device can process the 3-D images in 5 seconds or less and the hand verification usually takes less than 1 second.
- ▣ The image capturing and verification software and hardware can easily be integrated within standalone units.



**Figure 5.2** Biometric sensory access

## 5.9 Security

The highest level of security has been implemented in the importance area, which is considered to be the zone of highest importance. Biometric hand scan access control covers all entry points to importance area in some applications and any unprotected

potential paths to importance areas. Outside the importance area access could be controlled by using normal security applications.

### **5.10 Environment.**

- ▣ A house alarm covering general office and circulation areas.
- ▣ A room has air condition should be provided for any hand-scan unit (require close environmental for each unit)
- ▣ Each unit is capable of stand-alone operation.
- ▣ One standby unit is provided per individual area.

## **CHAPTER VI**

### **ACCURACY PERFORMANCE ANALYSIS OF MULTIMODAL BIOMETRIC SYSTEM**

#### **6.0 How the Biometric System is Evaluated**

##### **6.1. Introduction**

Information assurance addresses issues related to authentication, availability, confidentiality, integrity and non-repudiation in information systems. Consequently, there is a need to assure that only authenticated users have access to the system. Interest in biometrics for information assurance has never been greater than it is today. Increasingly, both the public and private sectors are choosing biometrics to secure their physical facilities, electronic data, and computer networks. Biometric technology is being used in a varied array of applications including access control, forensic investigation, identity verification, information protection, and security monitoring. Biometric solutions identify or verify an individual's identity by measuring either physiological or behavioral characteristics. Common physiological biometric measurements include fingerprints, hand geometry, and retina, iris, and facial images, while common behavioral biometric measurements include signatures, voice recordings (which also has a physiological component), and keystroke rhythms. Any one of these biometric measurements can positively identify a person from among hundreds of others. (S. K. Dahel *et al.*, 2003).

However, biometric measurements are inherently varied because of the existence of background noise, signal distortion, biometric feature changes, and environment variations. For instance, facial biometrics can vary with changes in facial expressions and ambient light, and fingerprint biometrics can vary with press pressure and moisture. As a result, recognition based on a single biometric trait may not be sufficiently robust and it has a limited ability to overcome spoofing. Many researchers have proposed multimodal biometric fusion as a solution to this problem (R. Brunelli *et al.*, 1995 and L. Jain *et al.*, 1999).

Multiple samples are taken from multiple biometric traits using multiple sensor technologies and are combined using fusion technology to obtain a more reliable and accurate result.

Biometric systems are designed to make binary decisions-accepting the authorized personnel and rejecting the impostors. Two types of errors accompany biometric systems: false acceptance (FA) errors, letting the impostor in, and false rejection (FR) errors, keeping the authorized personnel out. In this project, we evaluate and compare the false acceptance rate (FAR) and the false rejection rate (FRR) of voice-scan biometric. The system error of a multimodal biometric system is a combination of the FAR and the FRR from hand-scan geometry, fingerprint and voice-scan biometric technologies.

## **6.2 Information Fusion in Biometric**

In recent years, multimodal biometrics has become an important research trend in improving biometric accuracy (Qian *et al.*, 2001)( Frischholz *et. al.*, 2000). For example, multiple biometric traits can be captured by different sensors; a number of biometric procedures can be applied to provide a variety of information; different matching algorithms can be developed to yield independent match scores; and several rules can be

used to make decisions on multimodal biometric outputs. The challenge is in combining separate biometric technologies systematically. To enable a decision based on multimodal biometrics to be superior to that based on a single biometric technology, information fusion technology has been introduced to integrate multiple biometrics to achieve better performance (A. K. Ross *et al.*, 2001)(J. Kittler *et al.*, 2001).

Information fusion is a method for merging the predictions of various sources of information to either generate one presentational format, or to reach a decision. Humans perform acts of information fusion every day: using both eyes; listening to and watching TV; seeing, smelling, and tasting food; etc. All are examples of information fusion. Commonly used decision-making rules in information fusion include the weighted product rule, weighted sum rule, sum rule, min rule, max rule, median rule, and majority voting rule. Information fusion can be applied at different levels of biometrics, such as the sensor, feature, classification, or decision levels, and can be treated in different ways (S. K. Dahel *et al.*, 2003). Depends on voice-scan biometric, hand-scan geometry and fingerprint biometric, we concluded that, in clean conditions, all the non-adaptive approaches provide similar performance, and that the weighted summation method is the most flexible fusion technique.

### **6.3 False Acceptance and False Rejection Rates**

In a real application, a biometric system essentially classifies an individual as either a genuine user (client) (called an enrollee) or an impostor. Thus, the system may make two types of recognition errors: it either falsely accepts an impostor or falsely rejects an enrollee (S. K. Dahel *et al.*, 2003). We prefer to use the following terms to measure these two types of errors. The false acceptance rate is the probability that an unauthorized individual is authenticated. The false rejection rate is the probability that an authorized individual is inappropriately rejected. The false match rate (FMR) is the probability that an enrollee is incorrectly matched to a different user's template. The

false non-match rate (FNMR) is the probability that an enrollee is incorrectly judged not to match with his/her own enrollment template. When multiple attempts are combined to decide acceptance, FAR and FRR are more meaningful at the system level than FMR and FNMR. In practice the true FAR and FRR are seldom known but may be estimated by  $\overline{FAR}$  and  $\overline{FRR}$  respectively, as given by equations 6.1 and 6.2.

$$\overline{FAR} = \frac{\text{Number of False Acceptance}}{\text{Number of impostors attempts}} \quad 6.1$$

$$\overline{FRR} = \frac{\text{Number of False Rejections}}{\text{Number of clients attempts}} \quad 6.2$$

A false acceptance allows an impostor to access high security resources. A false rejection denies an enrollee the ability to use the same resources. A matching threshold “ $t$ ” is used to decide between a genuine user (client) and an impostor.

#### 6.4 Multi-Modal Error Rate (MMER)

The error rates of combining different biometrics can be estimated as follows. Let's assume that, for each biometric, a decision is based on a score  $X_i$ , computed from some user's characteristic and that  $X_i$ , are independent random measurements. Since the decision is either to accept or reject a claimed identity, the null and alternate hypotheses are  $H_0$ : input biometric trait is not from the same biometrics as the template and  $H_1$ : input biometric trait is from the same biometrics as the template.

Then, the accuracy performance of a biometric system can be represented with a confusion matrix, in which the probabilities of all possible situations are as follows in table 6.1.

	$\omega_0$	$\omega_1$
$\varpi_0$	TRR	FAR
$\varpi_1$	FRR	TAR

**Table 6.1** Decisions Matrix

Where  $\omega_0$  is the true impostor class,  $\omega_1$  is the true enrollee class,  $\varpi_0$  and  $\varpi_1$  represent the corresponding assigned classes, TAR is the true acceptance rate, and TRR is the true rejection rate. For a test based on biometric  $i$ , It is assumed (without loss of generality) that  $\omega = \{X_i > t_i\}$  and  $\varpi = \{X_i < t_i\}$  where  $(t)$  is the number of scores.

The false acceptance/rejection probabilities, FAR and FRR, can be computed from the integral of the client and impostor distribution density functions (PDF)  $f(x/\omega_1)$  and  $f(x/\omega_0)$  respectively as follows:

$$FRR = P(\varpi_0/\omega_1) = \int_0^{t_i} f(x/\omega_1)dx \quad 6.3$$

$$FAR = P(\varpi_1/\omega_0) = 1 - \int_0^{t_i} f(x/\omega_0)dx \quad 6.4$$

The probabilities of false acceptance and false rejection for multimodal biometrics can be defined as  $P(FA/X_i)$  and  $P(FR/X_i)$ , for  $i = 1, \dots, n$ , where  $n$  represents the number of biometric traits. The multimodal biometrics test will be based on  $X = (X_1, \dots, X_n)$ . If the purpose of using multimodal biometrics is to enhance the security level – that is lower the FAR - all the biometric traits must pass their own test, so that the decision rule will be the conjunction of the individual rules from each biometric test (S. K. Dahel *et al.*, 2003).

In this project ( $n = 3$ , as we use voice-scan, fingerprint, and hand-scan), so the joint probability of false acceptance can be calculated as:

$$P(FA/X) = P(FA/X_1) P(FA/X_2) P(FA/X_3) \quad 6.5$$

This probability is lower than that of any single biometric test. However, the probability of false rejection will be calculated as:

$$P(FR/X) = P(FR/X_1) + P(FR/X_2) + P(FR/X_3) - P(FR/X_1)P(FR/X_2)P(FR/X_3) \quad 6.6$$

Unfortunately, this probability is higher than that of any individual biometric test. A meaningful operating range needs to be found to balance accuracy with user convenience.

### **6.5 Failure-to-Enroll Rate (FTE, also FER)**

The FER is the proportion of people who fail to be enrolled successfully. FER is a non-stationary statistical quantity which does not only show a strong personal correlation, it can even be determined for each individual feature (called personal FER).

Those who are enrolled yet but are mistakenly rejected after many verification/identification attempts count for the Failure-to-Acquire (FTA) rate. FTA can originate through temporarily not measurable features ("bandage", non-sufficient sensor image quality, etc.). The FTA usually is considered within the FRR and need not be calculated separately ([www.bromba.com](http://www.bromba.com)).

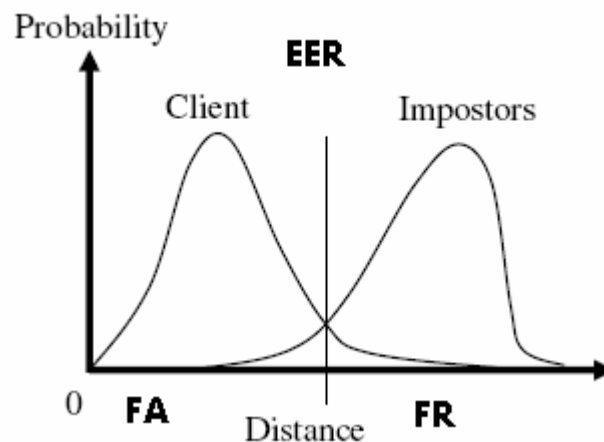
## 6.6 False Identification Rate (FIR)

The False Identification Rate is the probability in an identification that the biometric feature is falsely assigned to a reference. The exact definition depends on the assignment strategy; namely, after feature comparison, often more than one reference will exceed the decision threshold.

## 6.7 Equal Error Rate (EER)

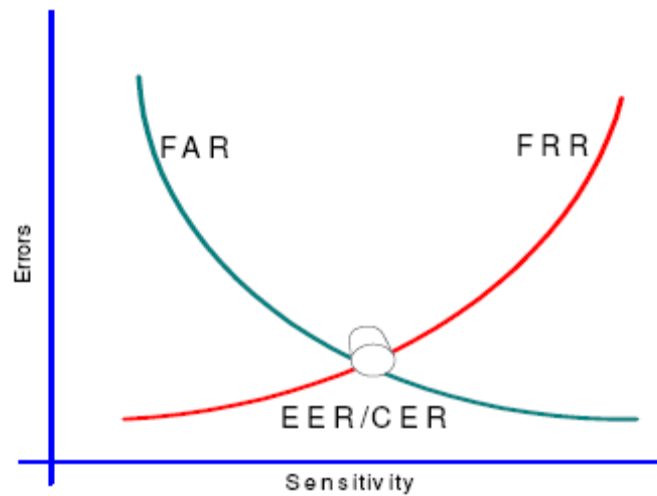
In this thesis the performance of the system is discussed in terms of equal error rate (EER). EER is the point on the receiver operating characteristics curve at which false-acceptance and false-rejection errors are equal.

EER is the common threshold used to evaluate the performance of a speaker recognition system (Joseph P. Campbell, 1997). EER point can be obtained easily by drawing FA and FR probability by threshold.



**Figure 6.1** EER point

The idea of using the EER is to avoid the confusing by using both of FA and FR in obtain the decision of the recognition biometric systems. This is described as the equal error rate (EER), sometimes also known as the cross-over error rate (CER). Low EER/CER scores generally indicate high levels of accuracy. This is illustrated in Figure 6.2 below.



**Figure 6.2 EER/CER**

### 6.7.1 EER Threshold

In order to know the location of intersection whether it is on the left or right of the tested threshold, depends on previous study tests for the difference of FAR to FRR. If FAR is higher than FRR, then the intersection is located on the left of the tested threshold shown above Figure 6.1. The intersection is located on the right of the tested threshold if FRR is higher than FAR.

## 6.8 Cost Function

The performance of a system having two types of decisions such as testing the presence or absence of a condition can be measured using a cost function or called expected misclassification cost (Masters T., 1993). The cost function assumes the existence of prior probability and cost of each condition. For example, in the case of accessing a confidential database, a prior probability of impostors trying to access the databases may be higher than the probability of true user accessing it, and the cost of accepting impostors to access the databases is absolutely very high.

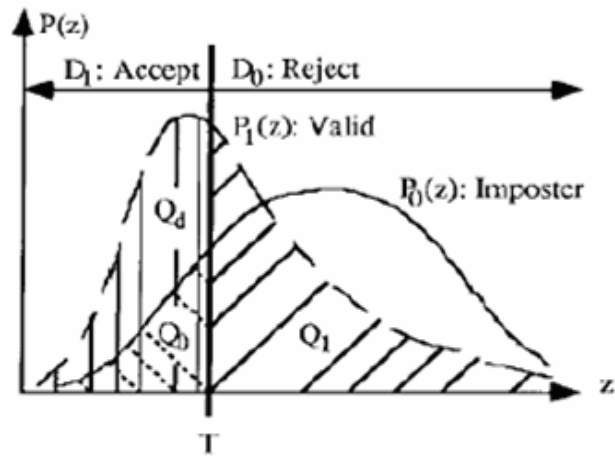
Given a prior probability and cost, the cost function to evaluate a recognition system is given by

$$\text{COST} = (1-q) p_1 c_1 + q p_2 c_2 \quad 6.7$$

Where the first part is the expected cost for false accept (FA) error while the second part is the expected cost for false reject (FR) error.  $(1-q)$  is a prior probability of accepting impostor speaker,  $p_1$  is a measured probability of accepting impostor speaker, and  $c_1$  is the cost of accepting impostor speaker. In the second part,  $q$ ,  $p_2$ , and  $c_2$  are a prior probability, measured probability, and the cost of rejecting true speaker respectively.

A prior probability of FA and FR is summed up to be equal to one since there is only two decisions considered in speaker recognition system. The value of prior probability can be obtained from experience. For example, the prior probability of impostors trying to access a confidential database may be set to 0.6 to 0.8. The cost of each error is usually set by a committee based on certain criteria such as monetary cost. For example, accepting an impostor to access a confidential database may lead a company to go bankrupt. Then, the measured probability of FA and FR denoted by  $P_1$  and  $P_2$  respectively can be obtained from the client-impostor pdf graph as shown in

Figure 6.3. The probability  $P_1$  is shown as an area of  $Q_0$  and  $P_2$  is shown as an area of  $Q_1$  in the graph.



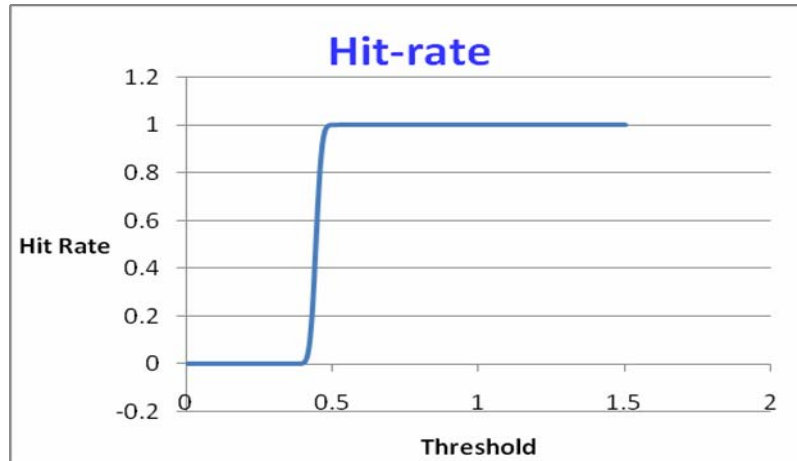
Client and impostor pdf curve

**Figure 6.3:**  $Q_0$  is FA and  $Q_1$  is FR

## 6.9 Hit-Rate

The area under the curve of FRR has relationship with threshold hence the maximum threshold located at the point where the area becomes exact one. Since the FRR equal to zero means all clients will be accepted but the value of FAR also will be increased as well.

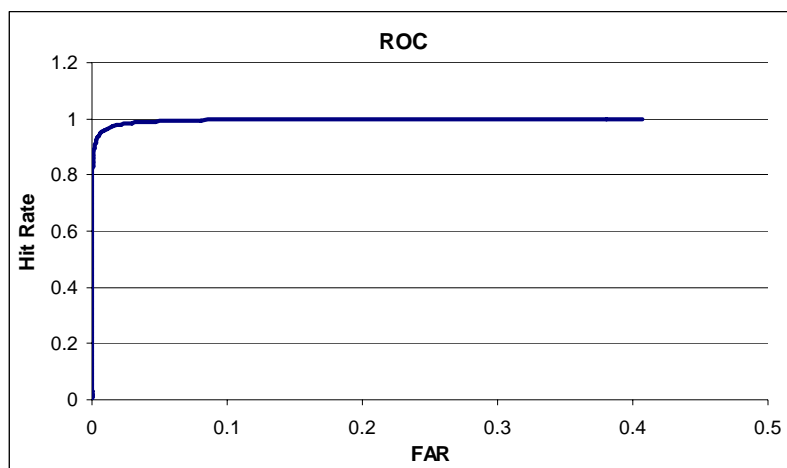
Hit-rate will be at unit value when the FRR at zero value and threshold very big (Masters T., 1993). The graph of hit-rate can be drowning by versus the threshold in horizontal axis and 1-FRR in the vertical axis as shown in figure 6.4 below.



**Figure 6.4: Hit-Rate**

### 6.10 Receiver Operation Curve (ROC)

The graph can help us to understand the relationship between the FA and Hit-rate for all possible thresholds. ROC curve has two endpoints (0,0) at a maximum threshold, (1,1) this corresponds to a threshold zero, where all of FA and Hit-rate are 100% in this point. The ROC curve is FAR vs. Hit-Rate as vertical and horizontal axis. Figure 6.5 shows the ROC curve.



**Figure 6.5 ROC**

Other parameters can also be visualized by means of ROC curve which show the relationship between the hit-rate (true acceptance) and FA error rate (T. Masters, 1993) The point (0,0) on the graph represents the maximum threshold in client-imposter pdf curve Point (1,1) represents the minimum threshold.

### **6.10.1 How Does One Determine The Receiver Operating Characteristic (ROC) of a Biometric System?**

A biometric system test usually starts by determining the similarities of different biometric features and a saved reference feature. After many measurements, one receives a histogram or distribution for authorized users and another for unauthorized users showing the frequency of matches per similarity rating. In an ideal case, the two distribution graphs should overlap as little as possible. When setting a certain similarity rating as a threshold for determination of authorized versus non authorized users, the false acceptance rate (FAR) is the number of non authorized users whose similarity rating happens to fall above the threshold compared to all attempts. On the other hand, a false rejection rate (FRR) is the number of authorized users whose similarity ratings happen to fall below this threshold compared to all attempts. Through integration (in practice, successive summation) of these distribution graphs, FAR and FRR graphs are determined, which are dependent on the adjustable adopted threshold.

If one wants to compare different biometric systems, it is problematic that value "similarities" or, inversely, "distances" are defined very differently, and therefore threshold values often have incomparable meanings. This difficulty is avoided by ROC, in which the similarity threshold parameter is eliminated and FRR is seen as a function of FAR (www.Bromba 2007).

### 6.10.2 What Is Essential When Comparing The ROC Performance Of Biometric Systems?

The accuracy performance of a verification system can be determined by exactly three statistical quantities: FAR, FER, and FRR. Since these three quantities influence each other when parameters (e.g., quality acceptance thresholds for enrollment and authentication) are changed, a comparison of one quantity between two systems makes only sense when the other two quantities are mutually equal. For example, let the FARs of different systems be compared. Then the corresponding FRRs must be equal, and the FERs must be equal, too. Regarding a ROC diagram, this condition can be easily fulfilled for all FRRs for which the curve has been measured, provided that the FERs of all curves are constant and the same. However, this is often violated since the FERs are actually different

A solution to this problem comes from the procedure used, e.g., in the Fingerprint Verification Competition FVC2002 ([www.bromba.com](http://www.bromba.com) 2007), where different algorithms for fingerprint recognition have been tested. The idea is to consider a failure-to-enroll case as a virtual "FTE user" with the properties

- 1-If the virtual FTE user tries a (virtual!) authentication, the result is always a rejection, thus increasing the FRR.
- 2-If an impostor tries an authentication attempt against a virtual FTE user, always a rejection is supposed, thus decreasing the FAR

This way, the FER is eliminated and the ROC curves as well as the FAR/FRR values are forced to become comparable. Mathematically, we implement this method by introducing a Generalized FRR (GFRR) and a Generalized FAR (GFAR). (It will be a matter of standardization to fix these terms. Here they are used until standardization is finalized.) The calculation of GFRR and GFAR is quite simple, if we assume that each authentication trial is preceded by its own enrollment trial. This should make sense because authentication performance is not independent of enrollment: a good enrollment

delivers better FRR values than a worse one. Therefore it seems to be statistically more accurate not to base a whole FRR statistics on a single enrollment.

$$\mathbf{GFAR(th) = (1 - FER) FAR(th)} \quad 6.8$$

$$\mathbf{GFRR(th) = FER + (1 - FER) FRR(th)} \quad 6.9$$

Here (th) denotes the dependency on the decision threshold parameter th which is assumed to range between 0 and K (arbitrary), These formulas show a strong relationship to those derived for FAR and FRR when including the FTA (Failure-to-Acquire).

Similarly, we get for the border values

$$\mathbf{GFAR(0) = (1 - FER)(1 - QRR)} \quad \mathbf{GFAR(K) = 0} \quad 6.10$$

$$\mathbf{GFRR(0) = FER + (1 - FER) QRR} \quad \mathbf{GFRR(K) = 1} \quad 6.11$$

Both formulas are symmetric in QRR (= FTA) and FER (= FTE), showing the strong relationship between Failure to Enroll and Failure to Acquire. In some cases these two values are even equal. This happens when the biometric system uses the same quality rejection mechanisms and levels for enrollment and for authentication. In practice, higher quality requirements during enrollment, leading to a higher FTE, might be quite reasonable to prevent enrollment of nonsense features. Furthermore, too low an enrollment quality will decrease usability of the authentication systems in daily use. In many applications it is better to spend more time during enrollment than losing time by multiple authentication trials (www.bromba 2007).

### 6.11 Cost Function and ROC

The area under the ROC curve can be a deceptive indicator of performance. It is frequently the case when FA is particularly costly. ROC curves emphasize the central portions of the area of confusion. This is further complicated fact that two competing persons may have ROC curves that cross. Thus, the areas may be almost the same, while their actual performance may be dramatically different.

By consider the cost function and  $q, c_1,$  and  $c_2$  are fixed constants and  $p_1,$  and  $p_2$  are dependent on chosen threshold . Look at the following equation.

$$\text{Cost}/[(1-q)*c_1]=p_1+[q*c_2/(1-q)*c_1]*p_2 \quad 6.12$$

If the cost is fixed the relationship will be linearity. More importantly, notice that the relative performance of the persons depends on the cost function through the slope of the line of fixed cost. If different values for the error costs were used, the slope might become more horizontal.

### 6.12 Separability of a Biometric

The Receiver Operating Characteristic (ROC) offers an objective comparison of different biometric systems, in the form of a graph. More practical would be the specification of one single measured value, which forms a kind of average of all the systems settings. Therewith, only a global description of the system would be possible. One must therefore understand that a system can be better overall, despite worse local functioning, for example in an operating point.

Separability is intuitively the ability of a biometric system to differentiate authorized and unauthorized users on the basis of a biometric feature. The higher the

separability, the fewer the errors while differentiating authorized and unauthorized users. The measure of the separability, like that of the ROC, cannot be dependent on implementation specific scales. Additionally, a separability measure should be easy to calculate.

A well known measure for the (inverse) separability is the Equal Error Rate (EER). Unfortunately, the EER describes only one single point of the ROC. While the definition is simple, the calculation is not so easy; the EER point does not exist as a measurement, instead it is derived through decision and approximation.

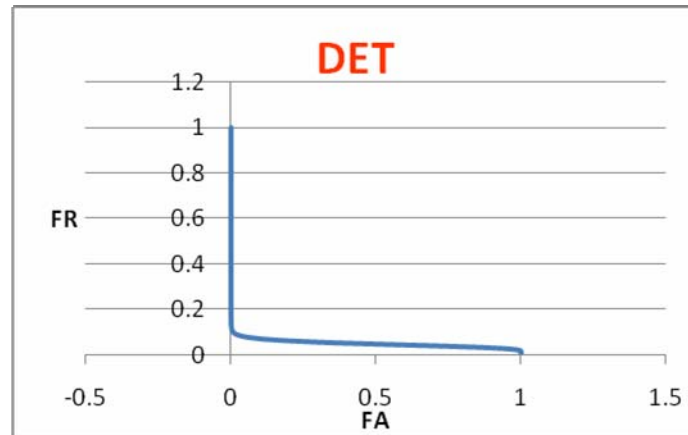
An (inverse) separability measure, which also prevents the EER disadvantages, is the area below the ROC graph. It allows easy calculation of all ROC values through summation. The only difficulty is the fact that the ROC values are not equidistant. Therefore, every y value (FAR) must be weighted by the distance between its corresponding x value (FRR) and the next value. This distance for every ROC point is just the difference (that is the gradient) of two consecutive values in the FAR graph. As a result, the distance is given by the probability distribution graph of non authorized users. (For continuous functions, in which the sum can be replaced by an integral, this would be a consequence of the substitution rule for integrals!) The ROC area, here called ROCA, is ( $K+1$  is the number of similarity ratings considered):

$$ROCA = \sum_{n=1}^k FRR(n)P_N(n-1) \quad 6.13$$

$P_N$ : Probability distribution function for unauthorized users. However, one must assume that no threshold-independent rejections occurs, i.e.,  $FRR = FNMR$  and  $FAR = FMR$ .

### 6.13 Detection Error Trade-off Curve (DET)

The idea behind visualized the relationship between FA vs. FR to see whether there are many similar values at the intersection rezone or not. This case is useful to determine the probability of FA and FR as well as mathematical way. Figure 6.6 shows the DET curve in bellow.



**Figure 6.6** DET curve

### 6.14 Advantages and Disadvantage of Some Biometrics

In normal life procedure we see how the people accept the sequence of security concepts on their body and by that and some practical experience the advantages and disadvantages appear clearly, in coming table we show some of them, see the Table 6.2.

<b>Method</b>	<b>Advantage</b>	<b>Disadvantage</b>	<b>Possible Application</b>	<b>Note</b>
<ul style="list-style-type: none"> <li>• Fingerprint Verification</li> </ul>	<ul style="list-style-type: none"> <li>• High reliability – no two people have ever been found to have identical fingerprints.</li> <li>• Robust.</li> <li>• Highly distinctive.</li> <li>• Proven accuracy – has been used by police forces for more than 100 years to solve crimes.</li> <li>• Advanced technology.</li> <li>• User convenience.</li> <li>• Uniqueness.</li> <li>• Stable over time.</li> </ul>	<ul style="list-style-type: none"> <li>• Some users associate it with a “criminal” stigma.</li> <li>• Functional defects are possible if the fingertips are very dirty or worn.</li> <li>• Hygienic considerations as a result of skin contact with the sensor.</li> <li>• Injury can affect.</li> <li>• Dry skin, grease &amp; sweat can cause recognition difficulties.</li> <li>• Poor environmental conditions can adversely affect collection.</li> </ul>	<ul style="list-style-type: none"> <li>• Access Control (IT, building, physical)</li> <li>• ATM’s</li> <li>• Motor Vehicle access</li> <li>• PC/Laptop access</li> <li>• Identification</li> <li>• Forensics</li> </ul>	Used in this project
<ul style="list-style-type: none"> <li>• Hand Geometry</li> </ul>	<ul style="list-style-type: none"> <li>• Small template</li> <li>• Unaffected by skin condition</li> </ul>	<ul style="list-style-type: none"> <li>• Size of scanner</li> <li>• Hygiene considerations as a result of skin contact with the sensor</li> <li>• Juvenile growth</li> <li>• Injury can affect</li> <li>• Low distinctiveness</li> </ul>	<ul style="list-style-type: none"> <li>• Time and attendance</li> <li>• Access Control (IT, building, physical)</li> </ul>	Used in this project
<ul style="list-style-type: none"> <li>• Face Recognition</li> </ul>	<ul style="list-style-type: none"> <li>• High precision</li> <li>• Efficient process</li> <li>• High acceptance because no physical contact with the sensor is necessary</li> </ul>	<ul style="list-style-type: none"> <li>• The face changes over time.</li> <li>• Can be manipulated by surgery.</li> <li>• Cannot distinguish between twins.</li> <li>• Religious or cultural inhibitions.</li> <li>• Poor environmental conditions can adversely affect collection.</li> </ul>	<ul style="list-style-type: none"> <li>• Access Control (IT, building, physical)</li> <li>• Crowd Control</li> <li>• Border Control</li> <li>• Recognition /identification systems</li> </ul>	
<ul style="list-style-type: none"> <li>• Retinal Scanning</li> </ul>	<ul style="list-style-type: none"> <li>• Uniqueness– no two people have identical retina patterns. - Robust</li> <li>• Stable over time.</li> <li>• Highly distinctive.</li> </ul>	<ul style="list-style-type: none"> <li>• Not user-friendly.</li> <li>• The procedure is often perceived as unpleasant – fear of “eye scans”.</li> <li>• Slow read time.</li> <li>• High user training</li> </ul>	<ul style="list-style-type: none"> <li>• Access Control (IT, building, physical).</li> </ul>	

		<p>requirement.</p> <ul style="list-style-type: none"> <li>• Poor environmental conditions can adversely affect collection.</li> </ul>		
<ul style="list-style-type: none"> <li>• Voice Recognition</li> </ul>	<ul style="list-style-type: none"> <li>• High level of user acceptance because the voice is a natural form of communication.</li> <li>• The voice is a characteristic, individual feature.</li> <li>• Simple and cost-effective technological application.</li> <li>• Low training requirement.</li> </ul>	<ul style="list-style-type: none"> <li>• Voice and language usage change over time (e.g. as a result of age or illness).</li> <li>• Easy to manipulate, can be surgically altered.</li> <li>• Computerized solutions often have low accuracy.</li> <li>• Poor environmental conditions can adversely affect collection.</li> </ul>	<ul style="list-style-type: none"> <li>• Access Control (IT, building, physical).</li> <li>• Mobile 'phones.</li> <li>• Internet banking.</li> </ul>	Used in this project
<ul style="list-style-type: none"> <li>• Iris Scanning</li> </ul>	<ul style="list-style-type: none"> <li>• Uniqueness – no two people have ever been found to have the same iris structure.</li> <li>• Robust.</li> <li>• Very precise and efficient method.</li> <li>• High acceptance because no physical contact with the sensor is necessary.</li> <li>• Stable over time.</li> <li>• Highly distinctive.</li> </ul>	<ul style="list-style-type: none"> <li>• Relatively new technology</li> <li>• Complex procedure</li> <li>• High costs</li> <li>• Protected by patent until 2005, which was hindering technological advancement.</li> <li>• Poor environmental conditions can adversely affect collection.</li> </ul>	<ul style="list-style-type: none"> <li>• Access Control (IT, building, physical)</li> <li>• ATM</li> <li>• Airline check-in</li> </ul>	
<ul style="list-style-type: none"> <li>• DNA Analysis •</li> </ul>	<ul style="list-style-type: none"> <li>• DNA is unique.</li> <li>• Even twins do not have the same DNA structure.</li> </ul>	<ul style="list-style-type: none"> <li>• Sample taking and analysis are time and cost-consuming processes.</li> <li>• Only feasible on a limited basis.</li> <li>• Problems relating to data protection.</li> <li>• Cloning will mean that DNA is no longer unique.</li> </ul>	<ul style="list-style-type: none"> <li>• Criminal forensics.</li> </ul>	

**Table 6.2** Advantages and disadvantages in multi-biometric system

### 6.15 Combination of Multibiometric

Multibiometrics using a single trait reintroduces the problem of non-universality (i.e., failure to enroll) and circumvention (i.e., spoofing). For this reason, it is better to utilize multiple biometric traits for user verification. Suppose  $N$  biometric traits,  $B_1; B_2; \dots; B_N$ , are used to verify the claimed identity,  $I$ . Let  $S_k$  be the normalized matching score provided by  $B_k$ . We define the fused score as

$$S_{fus} = \sum_k^N W_k \cdot S_k \quad 6.14$$

Where  $W_k$  is the weight associated with biometric trait  $B_k$ . If  $S_{fus} \geq \eta$ , where  $\eta$  is the matching threshold, then the claimed identity is true (a genuine user); otherwise the claimed identity is false (an impostor) (Anil K *et al.* 2002). In this project, three different biometric traits have been considered fingerprint (B1), voice-scan (B2) and hand geometry (B3). Data was collected from 98 persons; 12 clients provided 110 samples of voice biometric over two sessions, and the remaining 12 users provided data over a period of approximately three weeks, around 80 samples were collected from the Impostors.

### 6.16 Conclusion of Using Multi-Biometric System

Multimodal biometrics has the potential to overcome the limitations of any individual biometric technology in improving system security level and anti-spoofing. Information fusion technology can be applied at different levels and in different ways to in multimodal biometric applications. The challenge lies in finding a meaningful operation range to not lower the user convenience while increasing the accuracy.

The error rates of a bimodal biometric fusion have been evaluated. The results show that the performance of summation approach is superior to a conjunction method that treats the two modalities independently. Further research need's to be undertaken to extend the result to various approaches on multimodal biometric fusion so that users may evaluate the error rates before integrating different fusion technologies in biometric applications

## **CHAPTER VII**

### **DATABASE DESIGN**

#### **7.0 Introduction**

A large speech database has been collected for use in designing and evaluating algorithms for speaker-independent recognition of connected digit sequences. This dialectically balanced database has capacity of more than 25 thousand digit sequences. The data were collected in a normal laboratory environment and digitized at 16 kHz.

Formal human listening tests on this database provided certification of the labeling of the digit sequences, and also provided information about human recognition performance and the inherent recognizability of the data, this database built depending on TIDIGIT database as stander database known over world by using in many research's.

#### **7.1 TIDIGIT Database Concept**

There are many types of database nowadays are designed and used by several generations to enroll kind of data as we did in this project. However, the big choice today make the database design more common and easier to collect and save the different data which depends on the purpose.

A large speech database has been collected for use in designing and evaluating algorithms for speaker-independent recognition of connected digit sequences by Shochet, E *et al.*, (1981) in USA. This dialectically balanced database consists of more than 25 thousand digit sequences spoken by over 300 men, women, and children. The data were collected in a quiet environment and digitized at 20 kHz. Formal human listening tests on this database provided certification of the labelling of the digit sequences, and also provided information about human recognition performance and the inherent recognizability of the data.

## 7.2 Description of Speakers

The number of speakers and the age range of the speakers for each of the categories Man, Woman, Boy, and Girl are shown in the table 7.1.

Category	Symbol	Number	Age Range (year)
Man	M	111	21 – 70
Women	W	114	17 – 59
Boy	B	50	6 – 14
Girl	G	51	8 - 15

**Table 7.1** Distribution of speakers

In order to obtain a dialectically balanced database, the continental U.S. was divided into 21 dialectical regions (1), and speakers were selected so that there were at least 5 adult male and 5 adult female speakers from each region. In addition, 5 adult black males and 6 adult black females were selected. There was no attempt to dialectically balance the child speakers. Table 7.2 lists the 22 dialect classifications, the

associated metropolitan areas, and the numbers of speakers in categories Man, Woman, Boy, and Girl.

The utterances collected from the speakers are digit sequences. Eleven digits were used: "zero", "one", "two", ... , "nine", and "oh". Seventy- seven sequences of these digits were collected from each speaker.

The table 7.2 shows description of job and distribution of speakers:

City	Dialect	M	W	B	G	
01 Boston, MA	Eastern New England	5	5	0	1	
02 Richmond, VA	Virginia Piedmont	5	5	2	4	
03 Lubbock, TX	Southwest	5	5	0	1	
04 Los Angeles, CA	Southern California	5	5	0	1	
05 Knoxville, TN	South Midland	5	5	0	0	
06 Rochester, NY	Central New York	6	6	0	0	
07 Denver, CO	Rocky Mountains	5	5	0	0	
08 Milwaukee, WI	North Central	5	5	2	0	
09 Philadelphia, PA	Delaware Valley	5	6	0	1	
10 Kansas City, KS	Midland	5	5	4	1	
11 Chicago, IL	North Central	5	5	1	2	
12 Charleston, SC	South Carolina	5	5	1	0	
13 New Orleans, LA	Gulf South	5	5	2	0	
14 Dayton, OH	South Midland	5	5	0	0	
15 Atlanta, GA	Gulf South	5	5	0	1	
16 Miami, FL	Spanish American	5	5	1	0	
17 Dallas, TX	Southwest	5	5	34	36	
18 New York, NY	New York City	5	5	2	2	
19 Little Rock, AR	South Midland	5	6	0	0	
20 Portland, OR	Pacific Northwest	5	5	0	0	
21 Pittsburgh, PA	Upper Ohio Valley	5	5	0	0	
22	Black	5	6	1	1	
Total Speakers		111	114	50	51	326

### 7.3 Description of Database in this Project

In this project, since we were working in voice biometric field therefore the suitable database design in this project is TIDIGIT database which used in long time and achieved success. This kind of database is able to generate random digits in term of single digit as well as stream digit. Particularly in this project had been made some changes on TIDIGIT database to be a suitable in our design system because the Malay language does not has “oh” number which means Zero also in English language which the TIDIGIT was designed on. By using Visual C++ the designing task had been done, and we mentioned the description steps of design task through this chapter.

### 7.3.1 Vocabulary Definition

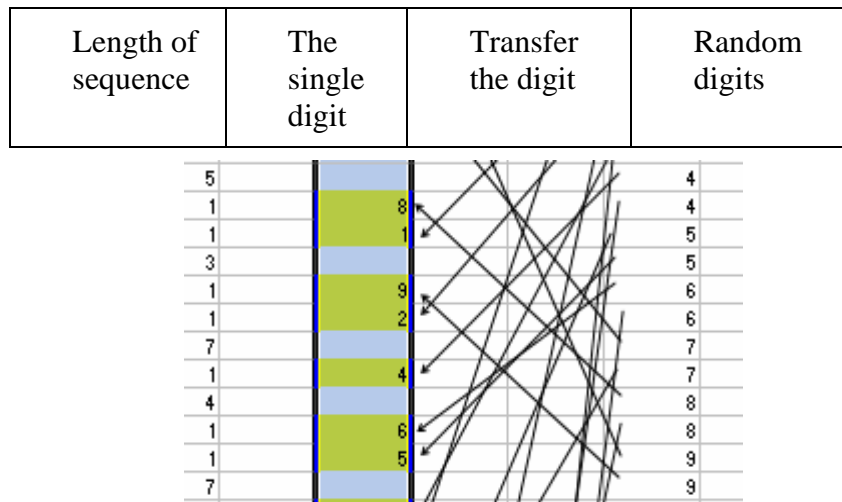
The utterance will be collected from the speaker are digit sequences. Ten digits were used “kosong”, ”satu”,.....,”sembilan”. 80 sequences of digits will be collected from each speaker, and consisted of the following types:

- 20 isolated digits (two tokens of each of the single digits)
- 10 two-digit sequences
- 10 three-digit sequences
- 10 four-digit sequences
- 10 five-digit sequences
- 10 six-digit sequences
- 10 seven-digit sequences

A unique set of prompts prepares for each speaker. The following algorithm will be used to generate a unique list of prompts for a given speaker (Shochet, E *et al.*, 1981).

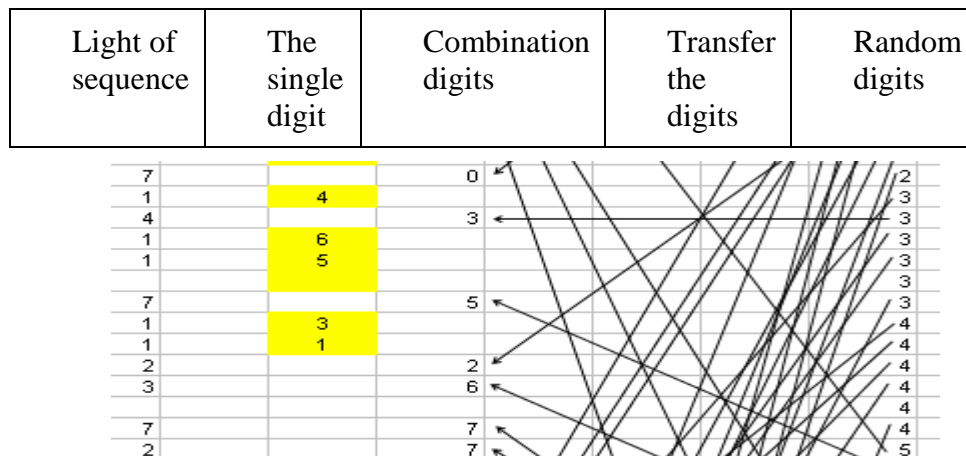
1. Generate a 80-element array containing the digit sequence lengths. (20 elements of this array were 1 and 10 each were 2, 3, 4, 5, and 7.) These 80 elements were then randomized uniformly, and used to determine the position in the prompt list of the sequences of a given length.

2. For the 20 isolated digits, randomly select (without replacement) from a list of two tokens of each of the ten digits. Figure 7.1 shows sample as example.



**Figure 7.1** Example of two tokens list

4. To determine the first digit in each of the 60 sequences of length 2 or more, randomly select (without replacement) from a list of 6 tokens of each of the ten digits. See the example in figure 7.1 to generate the stream digit.



**Figure 7.2** List of six tokens to find the first digit in digit stream

4. To determine succeeding digits in a sequence of length 2 or more, randomly select (without replacement) from the "transition list" corresponding to the previous digit. There are 10 transition lists, one corresponding to each of the 10 digits, and they initially contain 3 tokens of each of the 10 digits, figure 7.3 shows example. Should more than 30 transition tokens from any of the transition lists be required to complete a sequence, then the entire procedure is begun again (go to step (1)).

0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
2	2	2	2	2	2	2	2	2	2
2	2	2	2	2	2	2	2	2	2
2	2	2	2	2	2	2	2	2	2
3	3	3	3	3	3	3	3	3	3
3	3	3	3	3	3	3	3	3	3
3	3	3	3	3	3	3	3	3	3
4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4
5	5	5	5	5	5	5	5	5	5
5	5	5	5	5	5	5	5	5	5
5	5	5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6	6	6
6	6	6	6	6	6	6	6	6	6
6	6	6	6	6	6	6	6	6	6
7	7	7	7	7	7	7	7	7	7
7	7	7	7	7	7	7	7	7	7
7	7	7	7	7	7	7	7	7	7
8	8	8	8	8	8	8	8	8	8
8	8	8	8	8	8	8	8	8	8
8	8	8	8	8	8	8	8	8	8
9	9	9	9	9	9	9	9	9	9
9	9	9	9	9	9	9	9	9	9
9	9	9	9	9	9	9	9	9	9

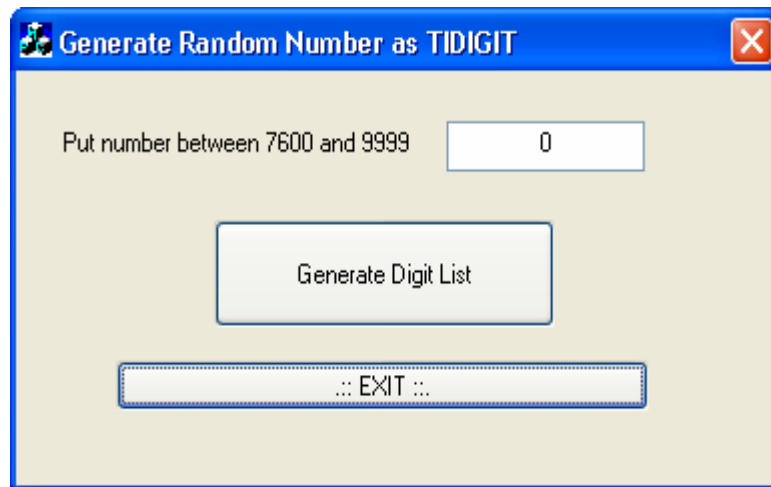
**Figure 7.3** 10 transition lists as resource to the engine

Note: All the steps above are just for impostors, but for clients in this project was considered more date i.e. (made the single digits be 50 rather than 20 as was mentioned above).

The data was collected in Malay language. See appendix "E" shows the lists for clients and impostors.

### 7.3.2 Database Engine

In this project we designed the engine of our database by using Visual C++ on the concepts of tidigit. The figure 7.4 shows the interface of this engine.



**Figure 7.4** Database engine

The following information is stored in the heard of each data file:

1. Speaker's name
2. Speaker's age
3. Speaker's category (M,W,B,G)
4. Speaker's race
5. State / country of birth
6. Occupation
7. Data recorded

## 7.4 Speaker Errors

Distribution of speakers errors according to error type: The 30 speaker errors can be categorized into the following seven types: (1) Omission of a digit; (2) Insertion of a digit; (3) Transposition of two digits; (4) Substitution of another digit for the correct digit; (5) False start, followed by a correction; (6) Sequence spoken as a numeral (e.g., the sequence "4 2" was spoken as "forty-two"); and (7) Pause between digits too long, causing the segmenter to cease digitizing prematurely (Shochet, E *et al.*, 1981).

Note: That the errors are not indicative of actual speaker performance since the number of errors detected by the data collector.

## **CHAPTER VIII**

### **RESULT DISCUSSION**

#### **8.0 Introduction**

In this project we considered much important operations to achieve the task of optimization decision like EER, ROC, DET, Hit-Rate, FA/FR, and MIN-Cost. The analysis data and the calculation parts were done by using Microsoft Excel. To make the result easier for understanding we plotted all the analysis by using Microsoft excels.

As was mentioned in the beginning of this project that we included 12 clients and 86 impostors to run our experiments and we carried out the following result.

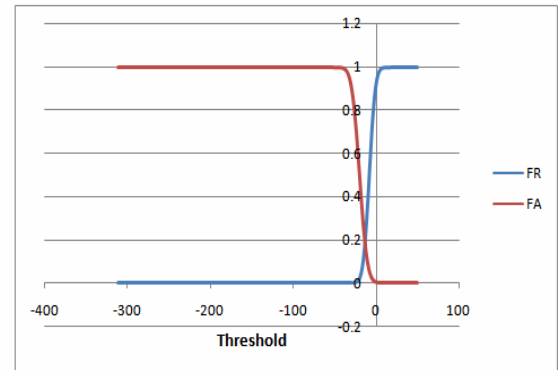
#### **8.1 Analysis for Single Digit**

##### **8.1.1 Single Digit Verification**

Voice verification for single digit is verifying a claimed person from a set of clients in the database. It depends on the comparison with model of claimed speaker by using HMM algorithm. So, by seen to different thresholds (T) for FA and FR, they will be as shown below in table 8.1 and figure 8.1.

In single digit verification stage there are 1200 tests been done for every client (10 samples x 10 single digits x 12 clients). For impostors trials the tests been done in this project database with 516000 which come by easy calculation (10 single digits x 10 test samples for clients x 5 test samples for impostors x 12 clients x 86 impostors) for every 12 clients.

T	FR	FA
-200	6.81E-27	0.9999269
-190	2.00E-24	0.9997743
-180	4.40E-22	0.999356
-170	7.23E-20	0.9983006
-160	8.89E-18	0.9958509
-150	8.19E-16	0.9906187
-140	5.65E-14	0.9803364
-130	2.92E-12	0.9617427
-120	1.13E-10	0.9308043
-110	3.31E-09	0.8834358
-100	7.24E-08	0.8167024
-90	1.19E-06	0.7301941
-80	1.48E-05	0.6270047
-70	0.000139	0.5137454
-60	0.0009887	0.3993584
-50	0.0053517	0.2930565
-40	0.0221702	0.2021555
-30	0.0708514	0.1306304
-20	0.1766777	0.0788447
-10	0.3494812	0.0443444
0	0.5614543	0.0231952
10	0.756797	0.0112655
20	0.8920335	0.0050737
30	0.9623632	0.0021167
40	0.9898342	0.0008172
50	0.9978921	0.0002917
60	0.9996667	9.63E-05
70	0.99996	2.93E-05
80	0.9999964	8.25E-06
90	0.9999998	2.14E-06
100	1	5.13E-07



**Figure 8.1** FA/FR vs. Threshold

**Table 8.1** FA and FR with different threshold.

The experiments for a verification part was carried out for all costs and the threshold was taken for different cost settings as following:

1-Equal error rate.

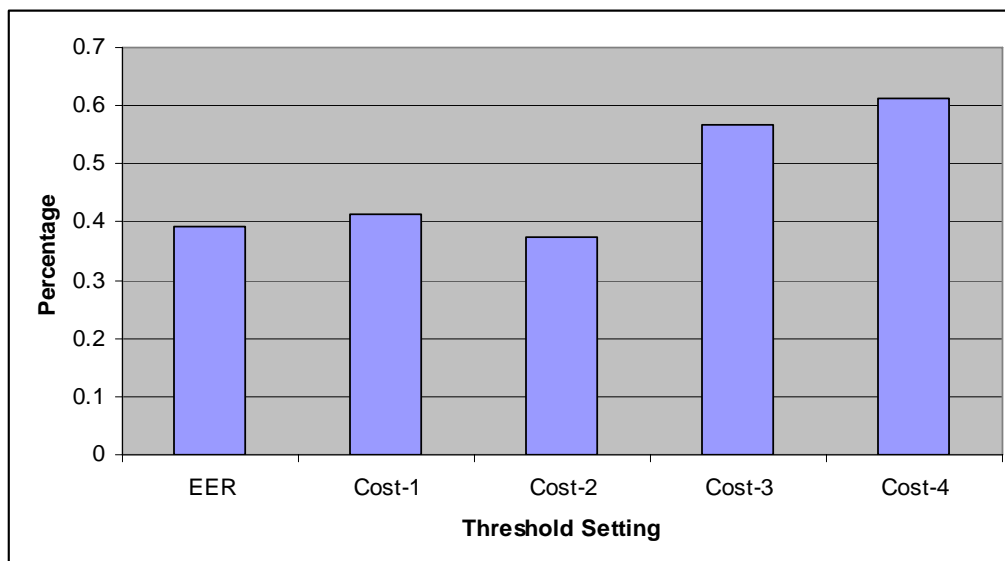
2-Equal error rate by using cost function ( $q=0.5$ ,  $C1=1$ ) in impostor side and ( $q=0.5$ ,  $C2=1$ ) in client side in cost function.

3-Min-Cost-1: by making the parameters in impostor side like ( $q=0.3$ ,  $C1=1$ ) and for client's parameters they will same, i.e. make the cost goes down by using prior probability ( $q=0.3$ ).

4-Min-Cost-2: In order to make the cost quite lower than EER, it is done by making the prior probability goes a bit up than 0.5 to be in this case  $q=0.7$ , and we could see the different as shown in figure 8.3.

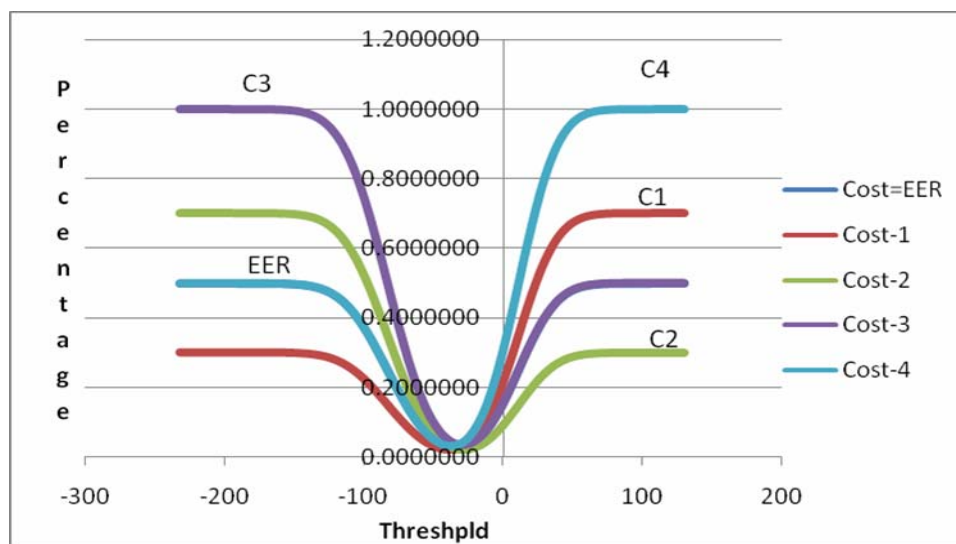
5-Min-Cost-3: to make difference in the cost value it is also can be done buy using cost function but by make difference in the cost itself, in this stage we made the cost in client's side a bit more to be  $C2=2$  rather than  $C2=1$  in the cases above.

6-Min-Cost-4: In order to provide highest level of security in some cases like the bank area, we could make the cost at high level by making the cost of accepting an impostor high, i.e.  $C1=2$  and make the cost of reject the client quiet low, see the figure 8.2.

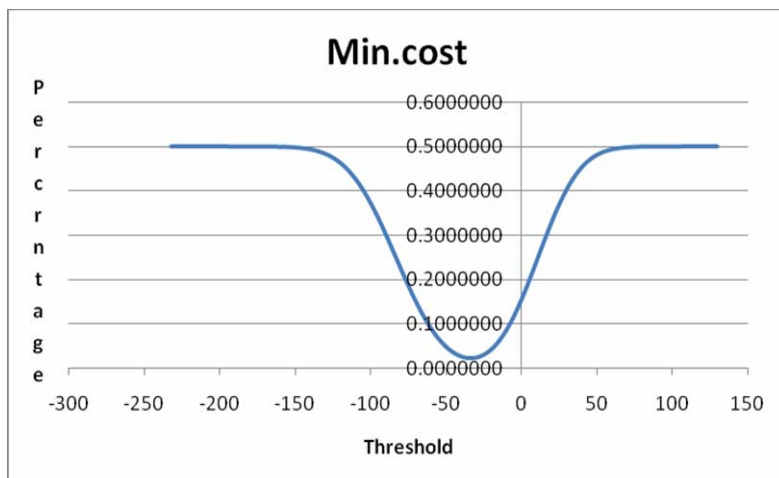


**Figure 8.2** Comparison between different Costs with EER by using cost function

The comparison task between EER and the Cost looks clear when we see the figure 8.3, and figure 8.4 here we could see the different cost to one transaction in both sides (client-and-impostor and also the minimum threshold for this case.



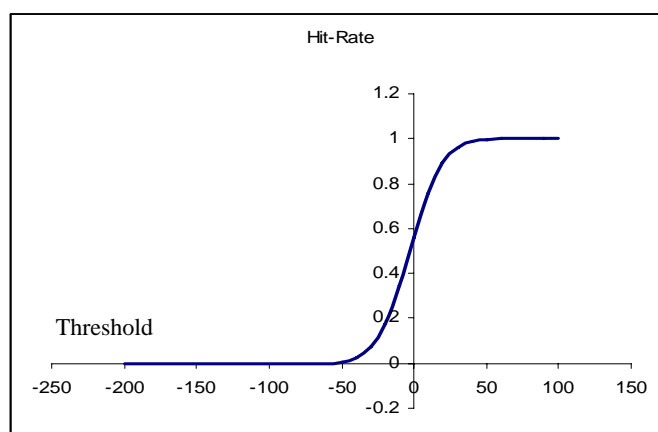
**Figure 8.3** Different cost to one client depends on level of security required



**Figure 8.4** EER by using cost function vs. threshold.

### 8.1.2 Hit-Rate Curve

The graph of hit-rate can be drawn by plotting the threshold in horizontal axis and 1-FRR in the vertical axis as shown in figure 8.5 below, By considering that the HMM makes the scores has some negative values, so the threshold also has negative values in most of cases see table 8.2.



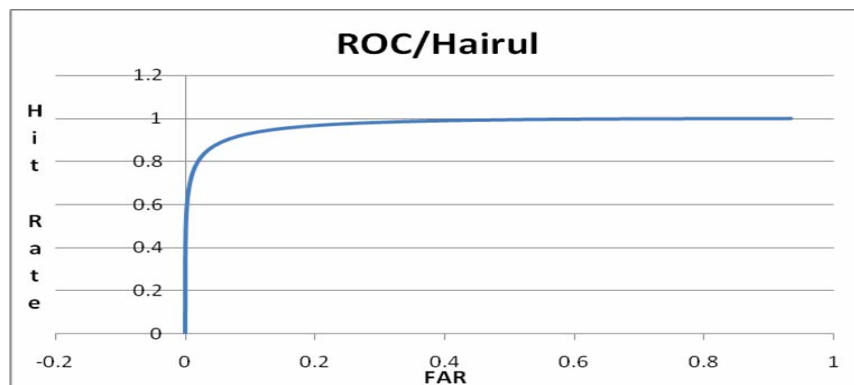
**Figure 8.5** Hit-rate (threshold vs. 1-FR)

Threshold.	Hit-rate
-200	6.81365E-27
-190	2.00142E-24
-180	4.39727E-22
-170	7.22841E-20
-160	8.89341E-18
-150	8.19287E-16
-140	5.65402E-14
-130	2.92472E-12
100	1.13482E-08
110	3.30566E-07
120	7.23685E-06

**Table 8.2** shows some values of threshold in negative position

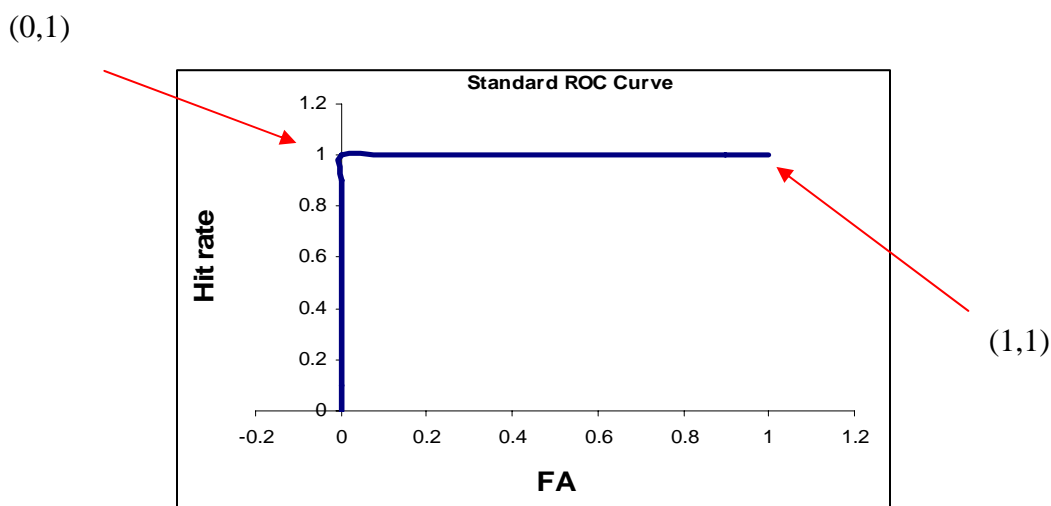
### 8.1.3 ROC in Verification stage

Depends on the Hit-rate values and FA values we concluded that ROC curve has two endpoints (0,0) at a maximum threshold, and (1,1) which corresponds to a threshold zero, where all of FA and Hit-rate are 100% at this point, see the figure 8.6.

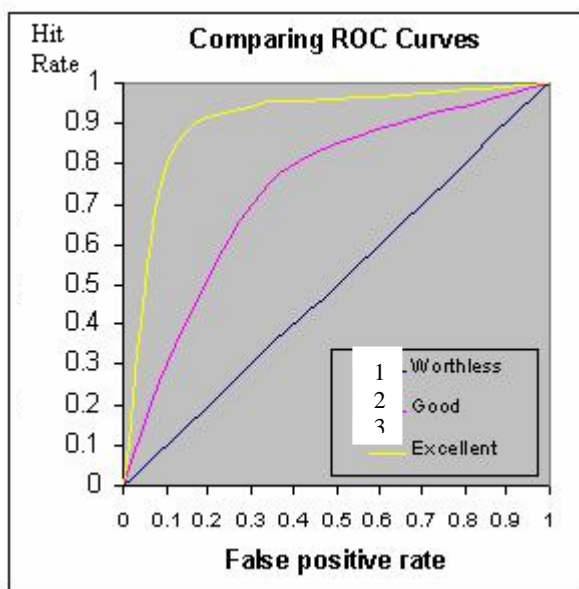


**Figure 8.6** Relationship between (Hit-rat and FA) i. e ROC curve.

By comparing the graph in figure 8.5 by the standard one as in figure 8.6 we could say for this person his ROC curve accepted, i. e. if there were some threshold at which the person could perfectly discriminate, the ROC curve would be a right angle. At magic threshold, the hit rate would be “1” and false acceptance rate would be zero (Masters T., 1993). This point would be plotted at (0,1), the upper left corner for all lesser thresholds, see the figure 8.7(a) and figure 8.7(b) show stander conditions for ROC curve.



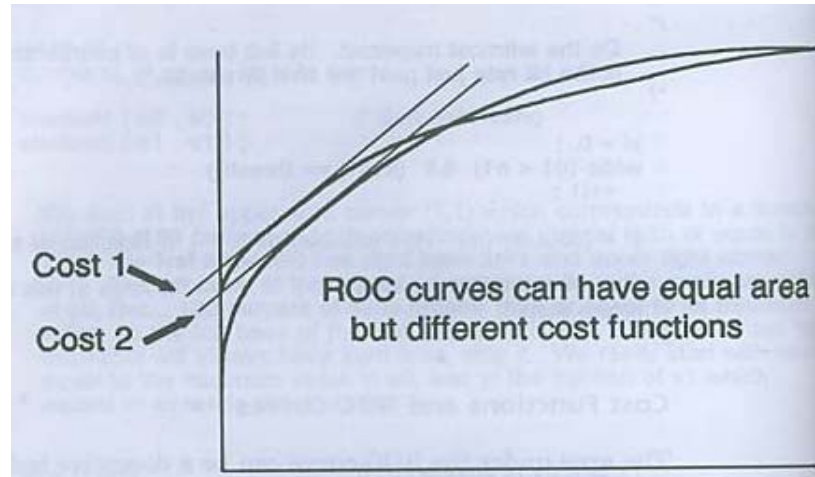
**Figure 8.7.a** Standard ROC curve



**Figure 8.7.b** Standard ROC curve

The worst case for ROC curve when it gets going be a diagonally till it become perfectly diagonal. In this case the ROC curve for a person has corresponding values between Hit rate and FA values. The quality of performance of system is demonstrated by the degree to which the ROC curve pushed upward and to the left corner. This can be quantified by calculate the area under the ROC curve.

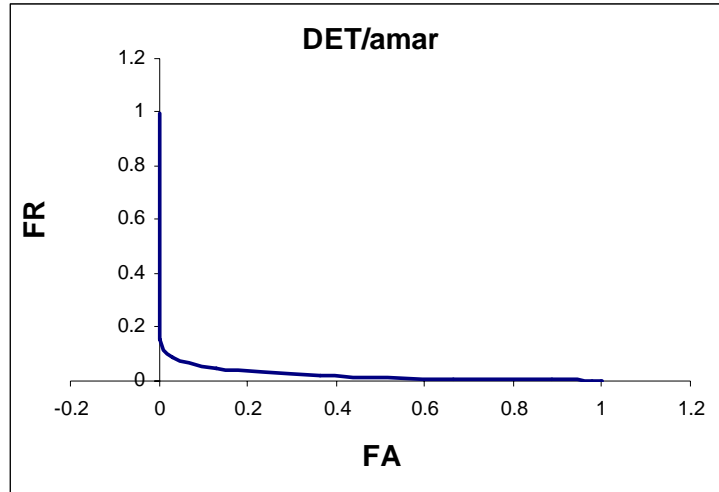
In some practical cases the area under two ROC curve for two persons have similarity but the characteristics of those persons are different completely, to solve this problem the cost function will be used see figure 8.8, thus, we notice that the relative performance of the people on the cost function through the slop of line of fixed cost.



**Figure 8.8** ROC Curve can cross.

#### 8.1.4 DET in Verification Stage

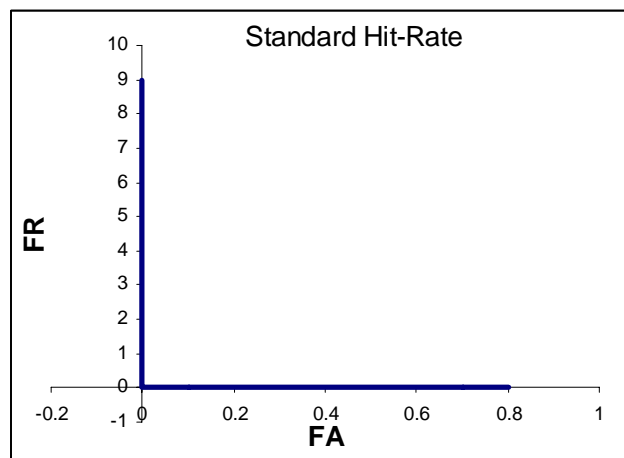
This case is useful to determine the probability of FA and FR as well as mathematical way. Figure 8.9 shows the DET curve in below.



**Figure 8.9** FR vs. FA (DET)

In general some researchers consider that DET is another face to ROC curve, it does by make the Hit-rate ( $1-FR$ ) to be just FR and verses it by FA as we do in DET. So, the difference will be the face of curve and we could see that be seen to the both figures 8.5 and 8.8 above.

Since the perfect shape is like figure 8.10, then the shape in figure 8.9 is almost good as practical result in this project.



**Figure 8.10** Shows Standard shape of Hit-rate.

### 8.1.5 Identification

Identification is a process of identifying the person when he presents his voice to biometric machine from group of clients given speech. When the client presents his voice to the biometric system, the system will do the comparison between the current speaker and the entire database as 1:N. By calculating the scores and compare them by the fixed threshold the system will decide whether accept or reject the speaker. In identification as well as verification every client will have its own threshold point which is different than other client threshold points, and this point will be determined by using EER or different setting of cost function.

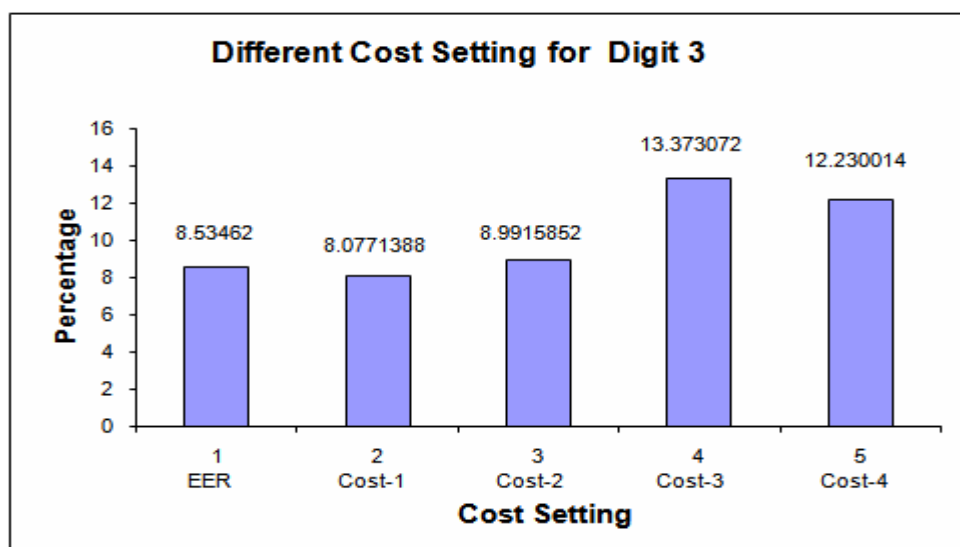
In the experiment, all of FA, FR, and TA calculated as shown in table 8.3, also the threshold for all numbers by using EER in this case.

Name	True Accept	False Reject		False Accept		Threshold	EER%
	TA%	FR	FR%	FA	FA%		
0	80	31	20	36	15.65217	-13.4144	17.69303
1	76.077419	36	23.22581	59	25.65217	-14.5924	24.40886
2	81.93548	28	18.06452	0	0	-0.30959	0
3	79.35484	32	20.64516	51	22.17391	-1.60917	21.39589
4	87.74194	19	12.25806	33	14.34783	0.767789	13.26185
5	85.80645	22	14.19355	29	12.6087	1.173973	13.37767
6	86.45161	21	13.54839	24	10.43478	-6.46106	11.8901
7	87.74194	19	12.25806	24	10.43478	-0.03264	11.30974
8	89.67742	16	10.32258	27	11.73913	-3.08992	11.00809
9	61.29032	60	38.70968	113	49.13043	-10.071	43.6099

**Table 8.3** Shows FA, FR, TA and EER for single digit

In single digit identification the cost for any digit is calculated as in the verification stage. By using cost function we could get different thresholds (cost) for one digit as

shown in figure 8.11. In here we could see that even for EER has reduction value than that one which collected by using normal way, see the table 8.4.



**Figure 8.11** Different settings to threshold

Digit	EER by normal way	EER by use cost function
2	12.7551	12.78451
6	5.29627	5.399718

**Table 8.4** Comparison of EER

## 8.2 Analysis of Digit Combination

### 8.2.1 Digital Combination Identification

In digit combination the identification of client by using a number of samples make the combination samples much more varies each other. In this project we have 12 clients

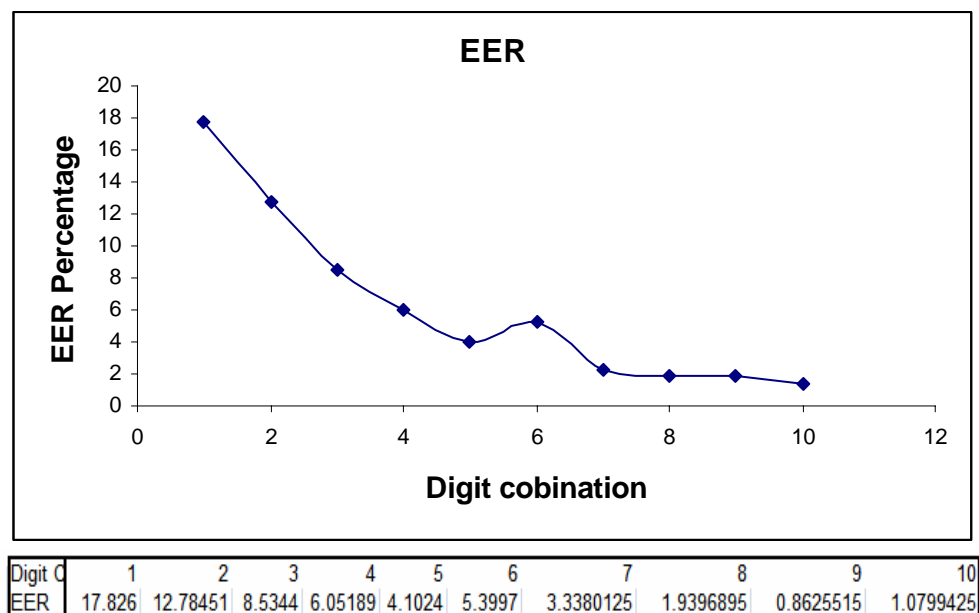
that required to 1200 tests for one digit combination for every client (12 clients x 10 samples x 10 digit combination). For impostors the number of tests will be 4300 for each digit combination for impostor (86 impostors x 5 test time will be 4300 tests and for 10 digit combination) Table 8.5 shows the details of test for each digit combination.

Digit Combinations	Digits Combination Pairs	No. of Test Samples	
		Clients	Impostors
1	10	1200	4300
2	9	1080	3870
3	8	960	3440
4	7	840	3010
5	6	720	2580
6	5	600	2150
7	4	480	1720
8	3	360	1290
9	2	240	860
10	1	120	430

**Table 8.5** Testing of combination digit for clients and impostors

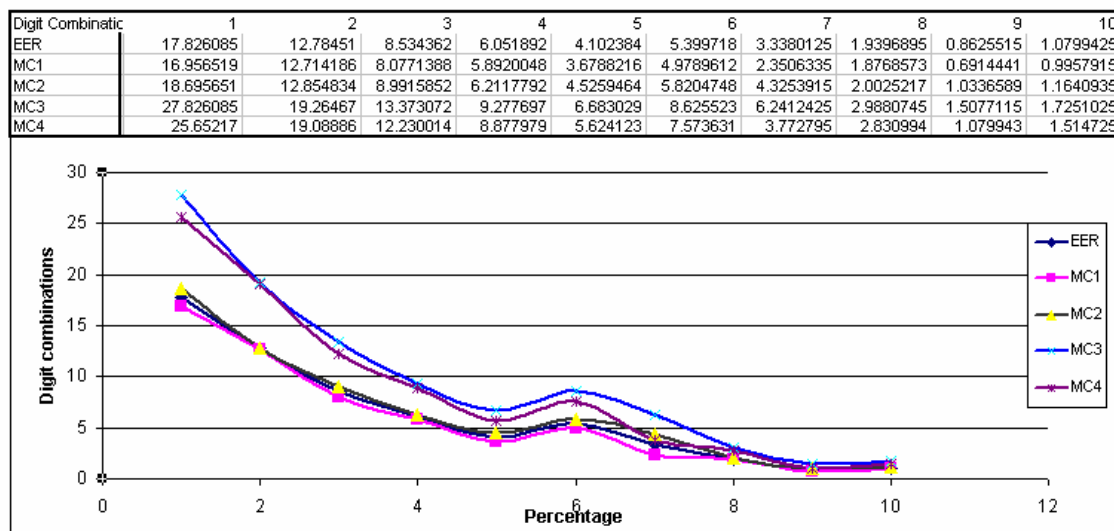
The testing transactions were done for all 86 impostors as well as for 12 clients in the database, and all graphs and results had come depend on this training and testing. Refer to the appendix to see more graphs about the results

For combination digit the EER will be lower for long combination digits as shown in figure 8.12. Depending on that we concluded the combination digit is better in term of reducing the error.



**Figure 8.12** EER in Combination Digit

Total cost of digit combination in this project result had shown the comparison between different cost by using cost function as identification task. Figure 8.13 shows the total cost of each digit combination for each threshold setting.



**Figure 8.13** Total cost function in digit combination.

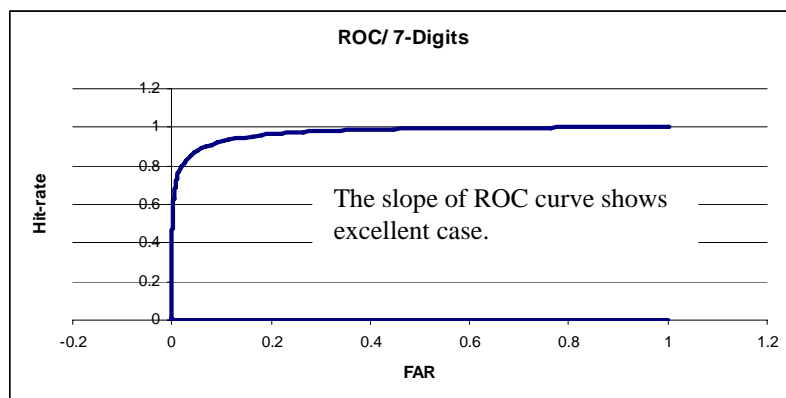
The table 8.6 shows the clear comparison even between the cost values among themselves, in this table we could see how the cost can be change regarding to the application required.

Digit C.	FA	FR	NOR.EER	Cost=EER	Cost-1	Cost-2	Cost-3	Cost-4
1	15.652	20	17.693	17.82609	16.957	18.6957	27.826	25.652
2	12.609	12.96	12.755	12.78451	12.714	12.8548	19.265	19.089
3	7.3913	9.677	8.4575	8.534362	8.0771	8.99159	13.373	12.23
4	5.6522	6.452	6.0387	6.051892	5.892	6.21178	9.2777	8.878
5	3.0435	5.161	3.9634	4.102384	3.6788	4.52595	6.683	5.6241
6	4.3478	6.452	5.2963	5.399718	4.979	5.82047	8.6255	7.5736
7	0.8696	5.806	2.247	3.338013	2.3506	4.32539	6.2412	3.7728
8	1.7826	2.097	5.8259	1.93969	1.8769	2.00252	2.9881	2.831
9	0.4348	1.29	1.865	0.862552	0.6914	1.03366	1.5077	1.0799
10	0.8696	1.29	1.426	1.079943	0.9958	1.16409	1.7251	1.5147

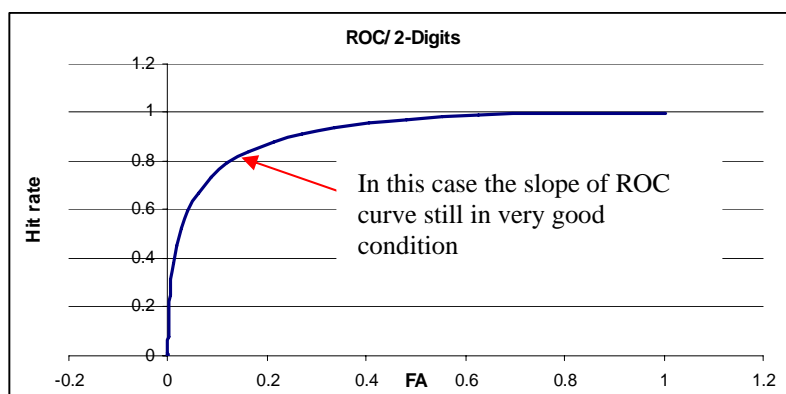
**Table 8.6** Total cost in digit combination

### 8.3 ROC Curve in Digit Combination

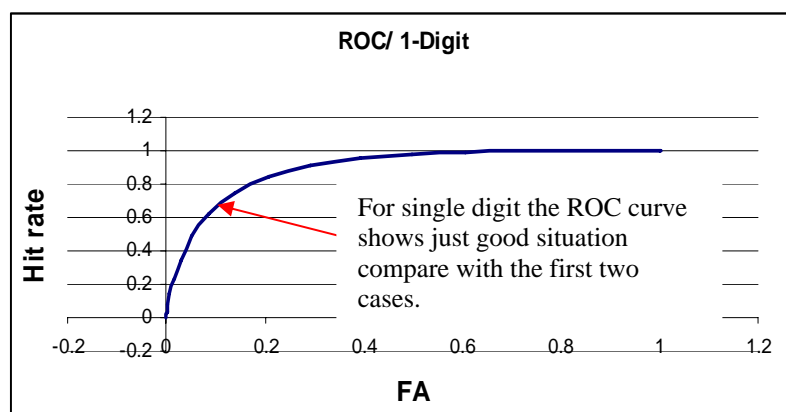
As relation between the Hit rate and FAR which discussed previously in this project, in the experimental result gives us the good shape of ROC curve like in figure 8.14 for seven combination digits. The difference between the ROC for less number of digits is clear in the figure 8.15 and for single digit also in figure 8.16.



**Figure 8.14** ROC for digit combination.



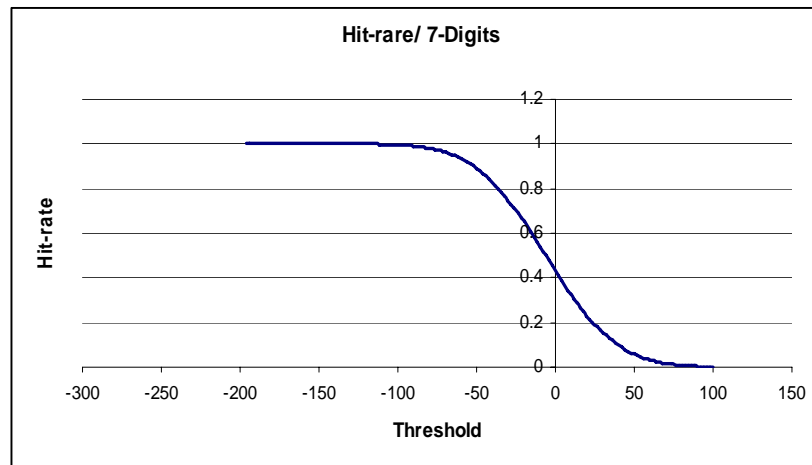
**Figure 8.15** ROC Digit combinations for 2-Digits.



**Figure 8.16** ROC Digit combinations for 1-Digits.

### 8.4 Hit-Rate in Digit Combination

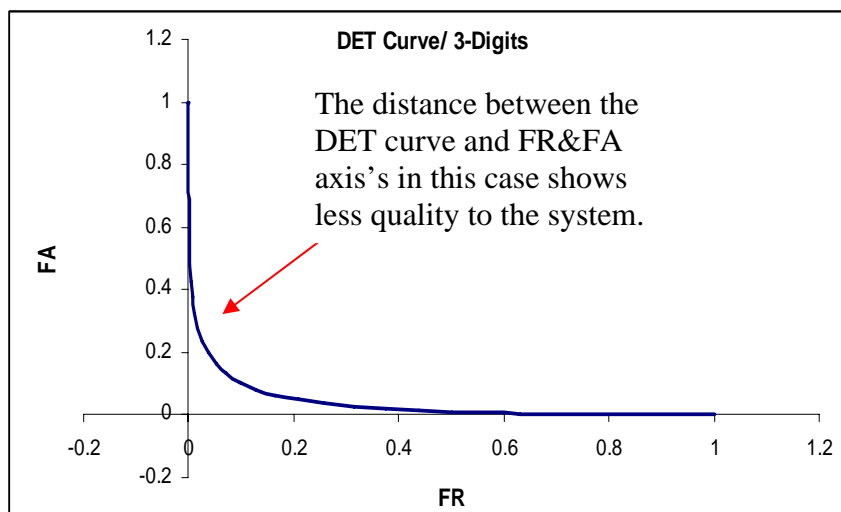
Digit combination give more good result in term of EER values also FA and FR, that gives good values to draw hit rat curve which relation between 1-FRR and threshold as shown in figure 8.17. We could notice that because of the negative threshold that made the face of shape became in inverse case.



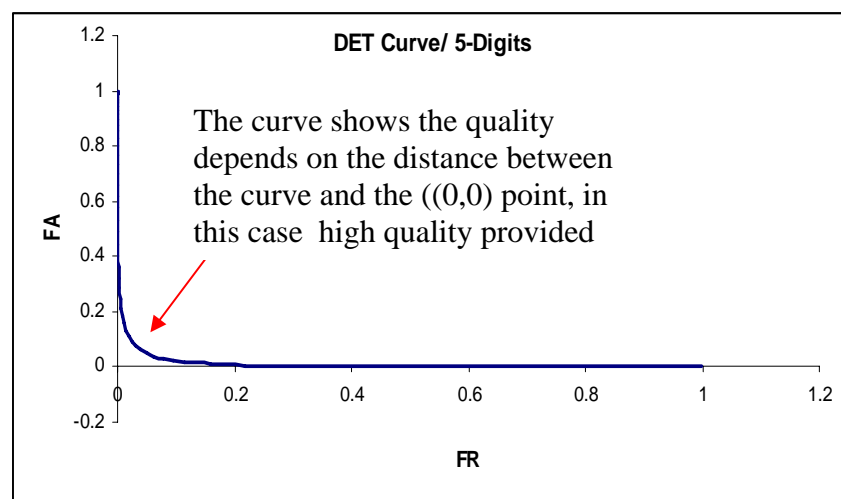
**Figure 8.17** Hit rat in digit combination.

### 8.5 DET Curve in Digit Combination

This case as same as for single digit by drawing the curve of Detection Error Trade-off to see the quality of system when the single digit is used and when combination digit is used. Depending on the shape of the curve, DET in figure 8.18 show how the system quality depends on FR and FA rates. By comparing the figure 8.19 which had drawn for 5-digits we could see the change of system quality by the angle of the curve which low FR and FR be achieved here.



**Figure 8.18** DET Curve for digit combination 3-digits



**Figure 8.19** DET Curve for digit combination 5-digits

## 8.6 Hand-Scan Results

For the hand-scan geometry device, we could collect just YES or NO data as a decision can be get from this device because the geometry machine was produced for

daily life usage but in order to evaluate multimodal it was used to make the final decision more guaranty. In table 8.7 we could see the results were achieved by verses impostors by clients to see how the decision is.

Client Names Impostor Names	Client Pass. Impostor IDs.	Younis	Amar	Kamarul
		1234	11	12
Mohd Dzulfadhli	BE020082	NO	NO	NO
Ling ching shyang	AE040481	NO	NO	NO
Ho ming Kong	AE040077	NO	NO	NO
Mohed Johan Alyas	AE040189	NO	NO	NO
Che Noor Hajizul	AE040044	NO	NO	NO
Mohd Hanan Masrom	BE030351	NO	NO	NO
Heap yee sim	AE040073	NO	NO	NO
kay chee keong	AE040089	NO	NO	NO
Mohamad Nawawi	AE040136	NO	NO	NO
mohd hafriz bin ismail	AE040181	NO	NO	NO
lim choong honn	AE040110	NO	NO	NO

**Table 8.7** Hand-scan result (Clients vs. Impostors)

Client Names	Client Pass.	Younis	Amar	Kamarul
		1234	11	12
Younis	1234	YES	NO	NO
Amar	11	NO	YES	NO
Kamrul	12	NO	NO	YES

**Table 8.8** Hand-scan result (Clients vs. Clients)

In the table 8.8 shows some results by verses the client with other clients the results here also were perfect.

## 8.7 Optimization of Threshold Decision

In order to optimize the FA and FR to provide new threshold as major target in this project we used cost function to achieve that, because of we usually see to the minimum cost, by using this concept, in the calculation of EER by using cost function to find new threshold was done, see the table 8. 9.

Threshold Normal -36.15076851	EER% normal 5.296271413
FAR% 4.347826087	FRR% 6.451612903
Threshold Cost Optimized (New)Threshold -34.5	ERR by Cost function 5.399719495
New FAR% 3.47826087	New FRR% 7.096774194
	Min-cost% 5.287517532

**Table 8.9** New FAR, FRR and new threshold point for seven Digits.

By increasing the number of digit combinations the EER should become lower. That case is shown in table 8.10 for eight digits combination. We notice here the difference between the first threshold and the new one, by this new threshold the FRR has big reduction value from 5.806% to be zero-0% but in normal balancing case the FAR had been increased to be 5.217% rather than 0.869% in the top.

Table 8.11 shows best situation in term of combination digits in this project experiments for all of FRR, FAR and EER have reduction values.

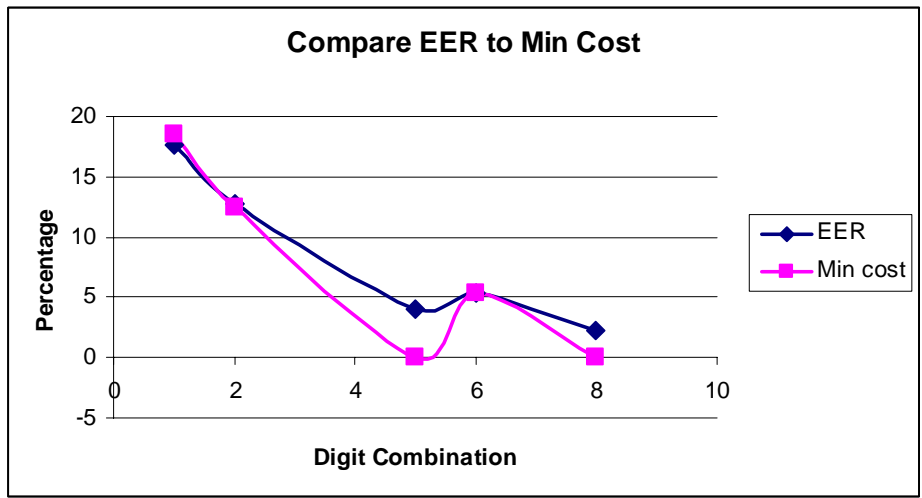
Threshold Normal -32.5758	EER% normal 2.247018
FAR% 0.869565217	FRR% 5.806451613
ERR Cost function 3.338008415	
Optimized (New) Threshold -50.5	
New FAR% 5.217391304	New FRR% 0
	Min-cost% 2.608

**Table 8.10** New FAR, FRR and new threshold point  
for eight Digits.

Threshold Normal -28.12652136	EER% normal 3.963366611
FAR% 3.043478261	FRR% 5.161290323
ERR Cost function 4.102384292	
Optimized (New) Threshold -28.1	
New FAR% 3.0434783	New FRR% 5.1612903
	Min-cost% 3.963366611

**Table 8.11** New FAR, FRR and new threshold point  
for five Digits.

The new EER (Min Cost) can be plotted with normal EER to see the change in the total cost regarding to the number of digits in the combination as show in the figure 8.20, and this figure related to the values in the table 8.12



**Figure 8.20** Comparisons EER with Min Cost.

Digit combination	EER	Min cost	Threshold	New Threshold
1	17.693	18.5	-13.4144	-14.3
2	12.755	12.5	-27.9	-27.96
5	3.9633	0.04958	-28.1265	-28.1
6	5.296	5.287	-36.150768	-34.5
8	2.247018	0	-32.5758	-50.5

**Table 8.12** Min cost and EER.

### 8.8 Conclusion

The quality of any system changes depends on some factors which make it high or low, in here by using cost function to determined the cost of every digit or person we considered three factors the error rate of FA&FR, and the cost C1&C2 as second factor lastly the prior probability Q. By define some standard curves like ROC and DET the

estimation of quality level becomes easier. By seeing to the figure 8.12 above we notice that as long as the number of digits combination increases the slope of cost line will come down and down.

However, to make the idea neat to the understanding we could see to the ROC in figure 8.13 and 8.15 as comparison between seven digits ROC curve and one digit ROC curve alternatively, the distance between the slope of the curve and point (1,0) is changed, the shortest one means high quality of the system in this situation exactly, and in general as well, we could say for DET curve in figures 8.17 and 8.18 same thing but the distance will be between the slope of the curve and point (0,0).

## **CHAPTER IX**

### **CONCLUSION**

#### **9.0 Project Summary**

This project is carried out to evaluate multimodal biometric system and was considered in the way how the decision of the system depending on multi variables which presents all of biometrics devices in this project. The project had analyzed the scores from voice-scan biometric as major part of the work in this project, then hand geometry device and fingerprint biometric as second part of the project by using the decision only without figure out the algorithm is used in those devices. The reason why we couldn't get the numerical scores of the hand geometry and fingerprint is because both of those devices are economy productions where the order to get score need to get the research production which was seems impossible for project period time.

For both identification and verification tasks, it is explained that the use of optimal threshold setting had performed better in terms of total cost compared to EER threshold setting. In terms of digit combination, it is expected that the use of more digit combinations is given a lower cost for both EER and optimal threshold setting. Experimental results were shown that minimum cost threshold outperforms equal error rate (EER) threshold by reduction in total cost for speaker identification task.

This project has shown the results of using several threshold settings in speaker verification and speaker identification tasks. The results of using EER and several cost

function settings had been compared and discussed. We have also briefly touched upon typical applications of biometrics and their particular characteristics as might have been expected.

However, these are very pertinent issues, especially at this stage in the overall development and acceptance of biometric technology in relation to everyday processes.

Multibiometrics using a single trait reintroduces the problem of non-universality (i.e., failure to enroll) and circumvention (i.e., spoofing). For this reason, it is better to utilize multiple biometric traits for user verification. Suppose  $N$  biometric traits,  $B_1; B_2; \dots; B_N$ , are used to verify the claimed identity,  $I$ . Let  $S_k$  be the normalized matching score provided by  $B_k$ . We define the fused score as  $S_{fus} = \sum_k^N W_k \cdot S_k$ , where  $W_k$  is the weight associated with biometric trait  $B_k$ . If  $S_{fus} \geq \eta$ , where  $\eta$  is the matching threshold, then the claimed identity is true (a genuine user); otherwise the claimed identity is false (an impostor) (Anil K *et al.* 2002). In this project, three different biometric traits have been considered fingerprint (B1), voice-scan (B2) and hand geometry (B3). Data was collected from 98 persons; 12 clients provided 110 samples of voice biometric over two sessions, and the remaining 12 users provided data over a period of approximately three weeks, around 80 samples were collected from the Impostors.

Fingerprint images were acquired using a Digital Biometrics sensor (FIU810/PERS-Sony). Minutiae features were used to represent and match fingerprints. Images of a subject's hand were obtained using a Handkey and a CSL Multispeech system (Model 4500).

## 9.1 Benefits of the Project

The project contributes mainly to the development of system that can be used to identify and display both client's and its impostor's using the given data. It then is able to calculate the EER and minimum cost threshold using the expected misclassification cost function. The calculated minimum cost threshold is shown to be better than the EER threshold.

This project also shows that the cost function can be used effectively to calculate other minimum cost threshold using different setting of FA or FR prior probabilities and costs which also gives a lower or higher total cost compared to EER. This result is important to real world applications which often need different settings of false acceptance or false rejection rate.

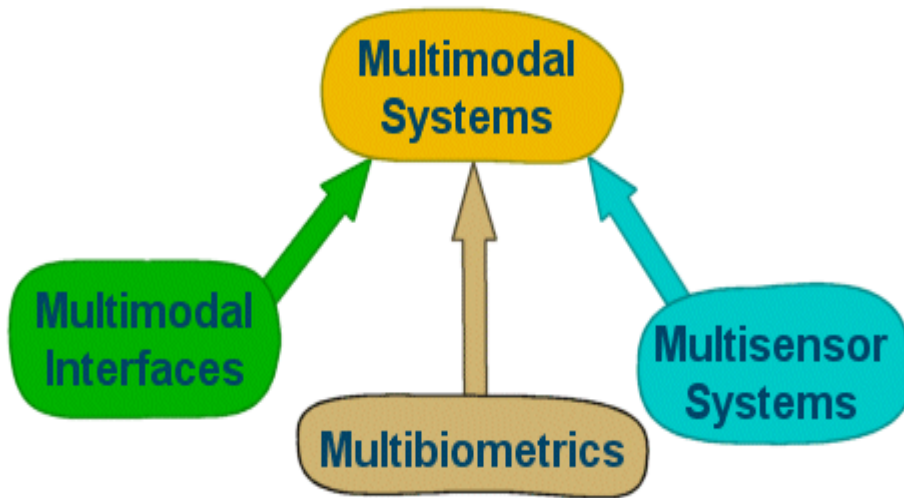
Other than that, in this project the program advanced of MFCC and HMM's software was inadequate, and the database software designed. By working on the Hand-scan scanner we could know that all images needed to be perfectly flat to give more accuracy in processing stage.

The training and testing more focused on this project on voice biometric and they had been helpful. Less theory, more practice, and more information up front of this project made the work successful and much useful for this kind of study.

## 9.2 Suggestion of Future Work

Full Multi-Biometric Adaptive System (FBAS): The term multibiometrics is used to refer to the consolidation of information presented by multiple evidences. These multiple evidences can stem from a single biometric trait or from multiple traits.

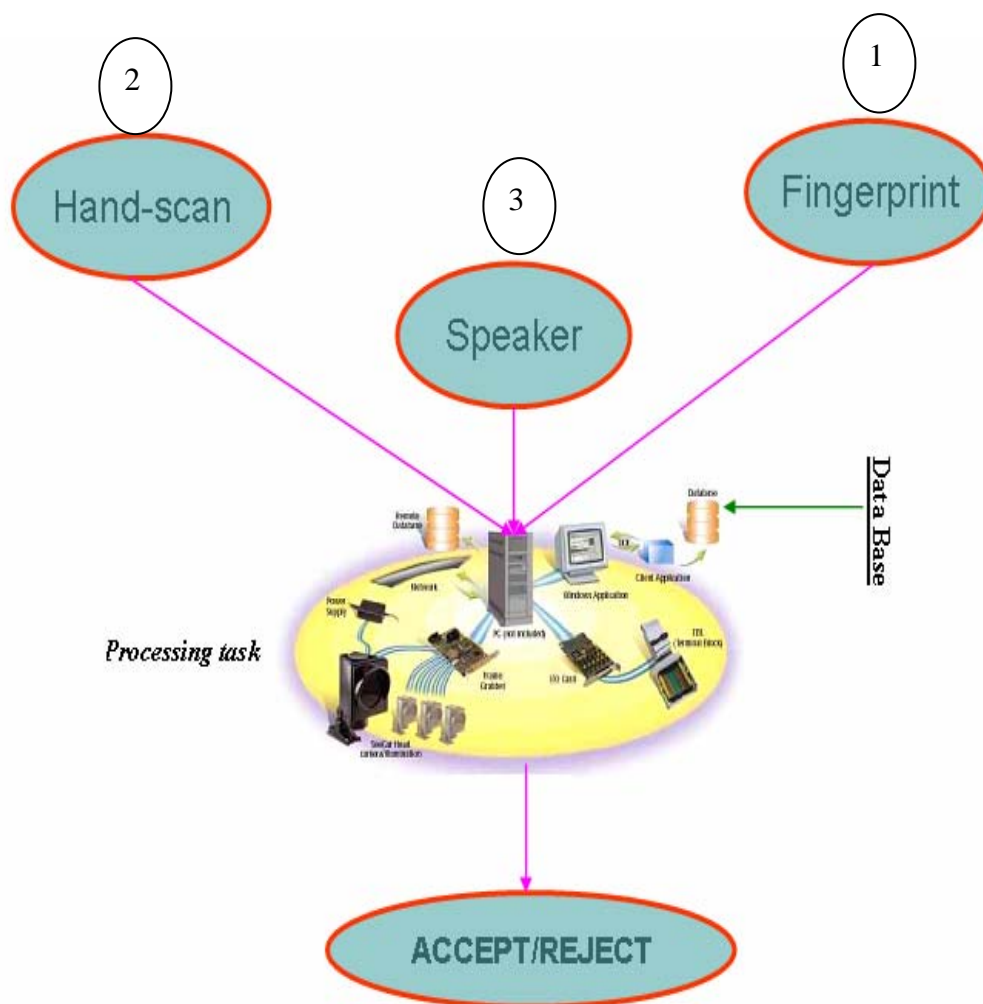
The scores provided by all traits will be converted to similarity measures and normalized in the range. Figure 9.1 shows images of the simple methodology to build a Multibiometric system.



**Figure 9.1** Methodology of Multibiometric System.

The management of input of multimodal system depends on the database of the application required, figure 9.2 shows example of priority of multimodal system as suggestion depended on the this project.

Also for voice scan biometric I suggested in future work, the Digit stream should be used rather than Digit Combination with HMM to provide the adaptation task. The thing should be consider the in the project the behaviour of the humankind to obey to this kind of systems.



**Figure 9.2** Three Biometric Device in One system.

## REFERENCES

- A. .K. J. A. Ross and J. Z. Qian. (2001). “*Information fusion in biometrics,*” ‘in *Proc. 3rd International Conference on Audio- and Video-Based Biometric Person Authentication*, Halmstad, Sweden, pp. 354-359, June 2001.  
<http://citeseer.nj.nec.com/rossOlinformation.html>.
- A. K. Ariff, Arief Ruhullah, M. Alwi, Sh-Hussain,Salleh. (2004) Centre for Biomedical Engineering Faculty of Electrical Engineering Universiti Teknologi Malaysia 81310 Skudai, Johor, Malaysia
- Atal, B.S. (1976). “Automatic Recognition of Speakers from Their Voices”.  
Proceedings of the IEEE. Vol 64, No 4, April 1976. Pp 460-475.
- Anil K. Jain and Arun Ross (2002). Appeared in Proc. International Conference on Image Processing (ICIP), Rochester, New York
- Arun Ross and Anil Jain (2007) [www.biometrics.msc.edu/ Hand\\_proto.html](http://www.biometrics.msc.edu/Hand_proto.html). updated By Feb 2007.
- Becchetti C., Ricotti L. P.(2002). *Speech Recognition Theory and C++ Implementation*. West Sussex: John Wiley & Sons Ltd. 122-301; 2002
- Blight, Richard C. (1989). *An exegetical summary of 1 & 2 Thessalonians*. Dallas: Summer Institute of Linguistics. 291 p.

Dr. Bhavani Thuraisingham (2005). The University of Texas at Dallas Biometric Technologies: Some Physiological Biometrics October 5, 2005

Emin Martinian, Sergey Yekhanin, and Jonathan S.(2005). Yedidia Secure Biometrics Via Syndromes 43rd Annual Allerton Conference on Communications, Control, and Computing, (Monticello, IL) October 2005 28-

Fakotakis, N.; Dermatas, E.; and Kokkinakis, G. (1986). "Optimal Decision Threshold for Speaker Verification", Signal Processing III: Theories and Applications, Elsevier Science Publishers B.V (North-Holland), 1986. Pp. 585-587.

Hong, K. S.( 2001). Implementation of Speech Recognition Using Hidden Markov Models. Bachelor Thesis. Universiti Teknologi Malaysia. 1-120 ; 2001

Higgins, A., Bhaler, L.; Porter, J. (1993). "Voice Identification Using Nearest Neighbor Distance Measure". Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Minneapolis, MN. Pp 375-378.

Hermansky, H., Morgan, N. RASTA processing of speech. IEEE Transactions on Speech and Audio Processing. Oct 1994. 2(4): 578 –589.

J. Kittler and E. F.( 2001). Roli, Decision-level fusion in fingerprint verification. Springer Verlag, 2001.

J. Wang, Q. Zhang, K.( 2001). Ren, Multi-scaling hierarchical structure analysis.

Joseph P. Campbell, Jr., Senior member IEEE.( 1997). Speaker Recognition. A tutorial, 27-June-1997.

Jittiwarakul, N. et al.(1998). Thai Syllable Segmentation for Connected Speech Based on Energy. IEEE Asia-Pacific Conference on Circuits and Systems.

24-27 Nov 1998. Thailand: IEEE, 1998. 169-172.

L. H. A. K. Jain and Y.(1999). Kulkarni, "A multimodal biometric system using fingerprint, face, and speech," in *Proc. 2nd International Conference on Audio- and Video- Based Biometric Person Authentication*, Halmstad, Sweden, pp. 182-187, March 1999. <http://www.cse.msu.edu/cgiuser/web/tech/document?NUM=98-32>.

Master work.(2006). IMPLEMENTATION OF FINGERPRINT BIOMETRIC TEMPLATE SYSTEM University technology Malaysia 2006.

Masters, T. (1993). "Practical Neural Network Recipes in C++", Academic Press Inc., Canada.

Rabiner, L.R. (1989). "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition". *Proc. IEEE*, Vol 77, Feb 1989. Pp 257-286.

Rabiner, L. and Juang, B. H.(1993). *Fundamentals of Speech Recognition*. Englewood Cliffs, N.J.: Prentice Hall. 69-481 ;1993

Rosenberg, A.E.; Siohan, O.; Parthasarathy, S. (1998). "Speaker Verification Using Minimum Verification Error Training". *Acoustics, Speech and Signal Processing, 1998. Proceedings of the 1998 IEEE International Conference on*, Vol:1, 1998. Pp. 105-108.

R. W. Frischholz and U.(2000). Dieckmann, "Bioid: A multimodal biometric identification system," *IEEE Computer*, vol. 33, pp. 64-68, February 2000.

R. Brunelli and D. Falavigna. (1995). "Person identification using multiple cues," *IEEE Transactions on PAMI*, vol. 17, pp. 955-966, October 1995.

P. Jonathon Phillips Alvin Martin C.L. (2000). Wilson Mark Przybocki  
National Institute of Standards and Technology .2000

Paper EEL 6586- Final project. (2002). A speaker identification and Verification  
System. By Zhongmin Lin,. Qizhang Yin , and Weimin Zhang. In 04-24-2002.

Pierrot, J.B; Lindberg, J.; Koolwajj, J.; Hutter, H.P.; Genoud, D.; Blomberg, M.;  
Bimbot, F. (1998). "A Comparison of a Priori Threshold Setting Procedures for Speaker  
Verification in the Cave Project". Acoustics, Speech, and Signal Processing, 1998.  
Proceedings of the 1998 IEEE International Conference on, Vol:1, 1998. Pp. 125-128.

Parsons, T.W. (1987). "Voice and Speech Processing". McGraw-Hill Inc. New  
York, USA.

Quran Karem. Surah Al-Qiyamat (75:3-4).

Shochet, E. and D. Connolly, (Jan., 1981). "An Investigation into the Effects of  
Dialectical Variation on Flight Plan Filing by Machine Recognition", Interim Report,  
FAA-RD-80-115

S. K. Dahel and Q. Xiao .(2003).Accuracy Performance Analysis of Multimodal  
Biometrics Information Assurance United States Military Academy,  
West Point, NY June 2003

[www.bromba.com/faq/biofaq.htm#ROC](http://www.bromba.com/faq/biofaq.htm#ROC) Updated by Mar 2007.

[www.biometricsinfo.org/](http://www.biometricsinfo.org/) copy right Mar 2007

[www.oninonin.com/fp/fmiru\\_.chinese\\_day-seal/jpg](http://www.oninonin.com/fp/fmiru_.chinese_day-seal/jpg) Updated in Sep. 2007

## Appendix A

Clients Table.

No	Name	Age	Gender	Occupation	Race	Native Language	Location	Note
1	DR.SHEIKH	49	Male	Lecturer	Malay	Malay	Penang	No data
2	ASIF		Male	Researcher	Bangladesh	Banguly	Bangladesh	
3	HAIZA	26	Female	Researcher	Malay	Malay	Pahang	
4	AMAR	28	Male	Researcher	Malay	Malay	Terengganu	No data
5	TING	26	Male	Researcher	Chinese	Mandarin	Perak	
6	RONI	30	Male	Researcher	Malay	Malay	Johor	
7	NAJEB	27	Male	Researcher	Malay	Malay	Kedah	
8	DIN	24	Male	Researcher	Malay	Malay	Selangor	
9	KAK MEED	39	Female	Staff	Malay	Malay	Johor	
10	HAIRUL	23	Male	Technician	Malay	Malay	Johor	No data
11	KAMARUL	27	Male	Researcher	Malay	Malay	Terengganu	
12	DR.NASIR	46	Male	Lecturer	Malay	Malay	Kelantan	
13	RUBITA	36	Female	Lecturer	Malay	Malay	Johor	
14	TAN	29	Male	Researcher	Chinese	Mandarin	Johor	House Wife Temporary
15	HAMIDAH	51	Female		Malay	Malay	Penang	
16	YOUNIS	29	Male	Researcher	Libyan	Arabic	Libya	

## Appendix A

## IDENTIFICATION RESULTS

## EER FOR SINGLE DIGIT

Name	False Reject		False Accept		Threshold	EER%
	FR	FR%	FA	FA%		
0	31	20	36	15.65217	-13.4144	17.69303
1	36	23.22581	59	25.65217	-14.5924	24.40886
2	28	18.06452	0	0	-0.30959	0
3	32	20.64516	51	22.17391	-1.60917	21.39589
4	19	12.25806	33	14.34783	0.767789	13.26185
5	22	14.19355	29	12.6087	1.173973	13.37767
6	21	13.54839	24	10.43478	-6.46106	11.8901
7	19	12.25806	24	10.43478	-0.03264	11.30974
8	16	10.32258	27	11.73913	-3.08992	11.00809
9	60	38.70968	113	49.13043	-10.071	43.6099

## Appendix A

## A VERIFICATION RESULTS.

EER for Digit One [1].

Name	False Reject		False Accept		Threshold	EER%
	FR	FR%	FA	FA%		
ASIF	0	0	1	0.232558	-24.8041	0
HAIZA	0	0	2	0.465116	-22.5629	0
AMAR	0	0	7	1.62797	-16.6722	0
TING	0	0	0	0	8.740317	0
NAJEB	0	0	0	0	-2.143853	0
DIN	0	0	0	0	-6.58388	0
KAK MEED	0	0	0	0	-18.582	0
HAIRUL	2	0.53333	8	1.860465	-14.5981	0.99616
KAMARUL	2	0.5333	10	2.325581	-38.2674	1.113692
TAN	0	0	0	0	3.586588	0
HAMIDAH	0	0	0	0	-4.91185	0
YOUNIS	0	0	1	0.434783	-11.5244	0

EER for Digit Two [2].

Name	False Reject		False Accept		Threshold	EER%
	FR	FR%	FA	FA%		
ASIF	0	0	0	0	11.84922	0
HAIZA	0	0	0	0	10.5671	0
AMAR	1	6.6667	2	0.465116	-5.61546	1.760902
TING	0	0	0	0	12.992	0
NAJEB	0	0	0	0	6.735107	0
DIN	0	0	1	0.232558	7.892751	0
KAK MEED	0	0	1	0.232558	11.92448	0
HAIRUL	1	0.26667	0	0	10.453	0
KAMARUL	0	0	0	0	4.962356	0
TAN	0	0	0	0	11.11485	0
HAMIDAH	0	0	1	0.232558	21.99395	0
YOUNIS	0	0	0	0	14.22204	0

EER for three digits  
[3].

Name	False Reject		False Accept		Threshold	EER%
	FR	FR%	FA	FA%		
ASIF	0	0	0	0	-16.9213	0
HAIZA	0	0	5	10162791	-16.3963	0
AMAR	1	6.6667	3	0.697674	-4.96548	2.156655
TING	0	0	0	0	18.41185	0
NAJEB	0	0	0	0	14.03557	0
DIN	0	0	0	0	29.35466	0
KAK MEED	0	0	15	3.488372	-23.6704	0
HAIRUL	0	0	0	0	-18.936	0
KAMARUL	1	0.26667	1	0.232558	-1.98526	0.249029
TAN	0	0	0	0	13.15807	0
HAMIDAH	0	0	0	0	17.55781	0
YOUNIS	0	0	0	0	-11.543	0

EER for four digits [4].

Name	False Reject		False Accept		Threshold	EER%
	FR	FR%	FA	FA%		
ASIF	0	0	0	0	7.176106	0
HAIZA	0	0	0	0	11.7168	0
AMAR	0	0	0	0	8.08438	0
TING	0	0	0	0	10.83559	0
NAJEB	0	0	0	0	3.278356	0
DIN	0	0	0	0	11.58088	0
KAK MEED	0	0	0	0	2.419488	0
HAIRUL	0	0	0	0	11.09185	0
KAMARUL	0	0	0	0	12.07956	0
TAN	0	0	0	0	13.02799	0
HAMIDAH	0	0	0	0	15.56806	0
YOUNIS	0	0	0	0	-0.12019	0

EER for five digits [5].

Name	False Reject		False Accept		Threshold	EER%
	FR	FR%	FA	FA%		
ASIF	0	0	0	0	14.18119	0
HAIZA	0	0	0	0	18.28166	0
AMAR	0	0	1	0.232558	-6.00913	0
TING	0	0	0	0	15.31196	0
NAJEB	0	0	0	0	21.85953	0
DIN	0	0	0	0	32.15897	0
KAK MEED	0	0	0	0	17.28364	0
HAIRUL	0	0	0	0	15.50567	0
KAMARUL	0	0	0	0	26.53101	0
TAN	0	0	0	0	23.73926	0
HAMIDAH	0	0	0	0	35.11519	0
YOUNIS	0	0	0	0	9.601466	0

EER for six digits [6].

12.9056

Name	False Reject		False Accept		Threshold	EER%
	FR	FR%	FA	FA%		
ASIF	0	0	0	0	12.9056	0
HAIZA	1	0.266667	0	0	9.117458722	0
AMAR	0	0	0	0	-5.78987265	0
TING	0	0	0	0	6.716475	0
NAJEB	0	0	0	0	2.2085771	0
DIN	0	0	0	0	7.6630724	0
KAK MEED	0	0	0	0	3.4090959	0
HAIRUL	1	0.266667	1	0.232558	4.8234254	0.24902912
KAMARUL	0	0	0	0	12.905607	0
TAN	0	0	0	0	18.366383	0
HAMIDAH	0	0	0	0	31.607247	0
YOUNIS	0	0	0	0	6.8656471	0

EER for seven digits  
[7].

Name	False Reject		False Accept		Threshold	EER%
	FR	FR%	FA	FA%		
ASIF	1	0.26667	0	0	1.4135151	0
HAIZA	0	0	0	0	0.6539164	0
AMAR	0	0	0	0	-6.550633	0
TING	0	0	0	0	18.005139	0
NAJEB	0	0	0	0	0.87625441	0
DIN	0	0	0	0	2.6089179	0
KAK MEED	0	0	0	0	3.901302711	0
HAIRUL	0	0	0	0	2.85893138	0
KAMARUL	0	0	0	0	9.92998893	0
TAN	0	0	0	0	6.9198136	0
HAMIDAH	0	0	0	0	7.55223217	0
YOUNIS	0	0	0	0	-13.427083	0

EER for eight digits  
[8].

Name	False Reject		False Accept		Threshold	EER%
	FR	FR%	FA	FA%		
ASIF	0	0	0	0	1.3335603	0
HAIZA	0	0	0	0	8.0727379	0
AMAR	1	6.66667	0	0	-13.230484	0
TING	0	0	0	0	12.77167617	0
NAJEB	0	0	0	0	2.891455	0
DIN	0	0	0	0	12.188523	0
KAK MEED	0	0	0	0	2.81291509	0
HAIRUL	0	0	0	0	-1.4379572	0
KAMARUL	0	0	0	0	10.318612	0
TAN	0	0	0	0	10.26201492	0
HAMIDAH	0	0	1	0.232558	-0.9010887	0
YOUNIS	0	0	0	0	-2.3892351	0

EER for nine digits [9].

Name	False Reject		False Accept		Threshold	EER%
	FR	FR%	FA	FA%		
ASIF	1	0.26667	0	0	0.5676873	0
HAIZA	0	0	0	0	16.593438	0
AMAR	1	6.6667	14	3.255814	-6.1160985	4.658908
TING	0	0	0	0	19.965059	0
NAJEB	1	0.266667	0	0	6.7636903	0
DIN	0	0	0	0	6.289365149	0
KAK MEED	0	0	0	0	16.18773769	0
HAIRUL	0	0	0	0	9.1127194	0
KAMARUL	0	0	0	0	16.5035906	0
TAN	0	0	0	0	10.56112734	0
HAMIDAH	0	0	0	0	22.561793	0
YOUNIS	0	0	0	0	11.9296659	0

EER for zero digits [0].

Name	False Reject		False Accept		Threshold	EER%
	FR	FR%	FA	FA%		
ASIF	1	0.266667	1	0.232558	29.39561262	0.24902912
HAIZA	0	0	0	0	38.80617857	0
AMAR	3	20	19	4.418605	25.83480868	9.40064322
TING	0	0	0	0	6.048393141	0
NAJEB	0	0	1	0.232558	6.625458462	0
DIN	0	0	0	0	5.870692937	0
KAK MEED	0	0	13	3.023256	37.03868669	0.89788727
HAIRUL	1	0.266667	26	6.046512	28.66636465	1.26980436
KAMARUL	0	0	0	0	11.27619279	0
TAN	0	0	0	0	5.502898188	0
HAMIDAH	1	0.266667	1	0.232558	5.883859406	0
YOUNIS	0	0	4	1.73913	30.40605286	0

## Appendix B

Database List Sample		<i>Client</i>
Name :	Gender (M/F) :	Race (kaum) :
Age :	State/country of Birth (negeri) :	Date Recorded :
Occupation :		
1 : 4	41 : 7	81 : 4 4 0 6 1
2 : 3	42 : 9	82 : 9 2 2 3 3
3 : 0	43 : 8	83 : 1 1 8 9 8
4 : 2	44 : 8	84 : 6 7 2 7 6
5 : 9	45 : 6	85 : 9 7 2 0 9
6 : 7	46 : 9	86 : 5 3 9 3 8
7 : 0	47 : 5	87 : 4 5 7 0 2
8 : 6	48 : 9	88 : 8 7 5 4 6
9 : 3	49 : 9	89 : 3 4 9 5 2
10 : 2	50 : 5	90 : 3 1 7 9 8
11 : 3	51 : 1 2	91 : 5 8 4 4 2 4
12 : 3	52 : 2 1	92 : 3 4 5 7 4 6
13 : 0	53 : 4 7	93 : 2 4 0 9 5 1
14 : 5	54 : 7 7	94 : 7 0 5 8 5 0
15 : 0	55 : 1 4	95 : 9 1 9 7 6 3
16 : 4	56 : 2 3	96 : 7 7 5 9 4 1
17 : 2	57 : 8 0	97 : 3 8 6 8 2 1
18 : 2	58 : 2 9	98 : 0 0 4 3 5 3
19 : 8	59 : 4 9	99 : 8 6 6 2 2 5
20 : 1	60 : 8 4	100 : 6 9 1 3 7 8
21 : 1	61 : 9 9 2	101 : 6 5 5 6 0 1 9
22 : 7	62 : 9 6 5	102 : 6 1 4 3 0 3 2
23 : 2	63 : 0 4 8	103 : 3 7 3 6 4 9 3
24 : 5	64 : 9 4 8	104 : 3 0 7 8 3 1 5
25 : 0	65 : 5 1 6	105 : 4 4 2 6 2 7 1
26 : 3	66 : 0 8 5	106 : 5 6 9 6 8 9 7
27 : 7	67 : 1 3 2	107 : 1 5 0 7 3 9 8
28 : 5	68 : 7 9 6	108 : 6 3 5 5 0 3 3
29 : 7	69 : 8 1 7	109 : 7 1 0 0 2 8 8
30 : 6	70 : 1 8 7	110 : 5 4 5 7 6 9 0
31 : 8	71 : 0 5 9 0	
32 : 6	72 : 0 6 6 7	
33 : 4	73 : 0 1 1 2	
34 : 1	74 : 4 7 1 0	
35 : 1	75 : 7 4 1 6	
36 : 4	76 : 2 9 9 0	
37 : 6	77 : 2 6 4 2	
38 : 8	78 : 8 2 5 4	
39 : 4	79 : 5 2 8 0	
40 : 1	80 : 6 0 8 3	

Thank you .....

## Appendix B

## Database List Sample

*Impostor*

Name :

Age :

Gender (M/F) :

Race (kaum) :

State/country of Birth (negeri) :

Occupation :

Date Recorded :

1 : 8	31 : 1 6 8	61 : 2 7 3 4 3 8
2 : 4	32 : 4 9 6	62 : 8 5 4 5 6 9
3 : 6	33 : 2 9 2	63 : 9 1 8 3 5 0
4 : 2	34 : 1 9 7	64 : 0 7 5 1 8 4
5 : 8	35 : 0 5 5	65 : 2 6 5 9 4 7
6 : 5	36 : 8 9 5	66 : 8 5 2 4 0 1
7 : 5	37 : 0 6 2	67 : 6 7 7 5 3 1
8 : 4	38 : 7 4 8	68 : 9 5 9 2 7 2
9 : 2	39 : 7 6 6	69 : 8 7 9 3 6 0
10 : 6	40 : 9 6 2	70 : 6 8 2 1 0 1
11 : 1	41 : 9 0 8 7	71 : 6 9 9 1 5 1 5
12 : 9	42 : 4 0 3 9	72 : 6 6 0 5 7 0 4
13 : 7	43 : 3 4 4 4	73 : 8 8 1 2 8 6 1
14 : 3	44 : 0 0 9 3	74 : 5 8 3 6 3 2 0
15 : 0	45 : 9 7 0 2	75 : 6 7 1 6 3 7 8
16 : 0	46 : 2 9 9 8	76 : 5 8 2 0 9 4 9
17 : 1	47 : 1 1 2 5	77 : 6 7 1 7 7 2 3
18 : 3	48 : 7 3 2 6	78 : 5 4 1 7 9 9 3
19 : 9	49 : 7 8 0 0	79 : 5 2 3 9 0 7 3
20 : 7	50 : 8 0 3 3	80 : 5 7 2 1 8 5 7
21 : 7 4	51 : 2 2 4 2 5	
22 : 0 2	52 : 7 6 4 6 4	
23 : 4 1	53 : 3 5 6 5 3	
24 : 1 4	54 : 4 3 1 1 9	
25 : 1 3	55 : 9 8 6 3 9	
26 : 3 8	56 : 0 6 1 3 3	
27 : 4 6	57 : 3 0 8 4 7	
28 : 3 7	58 : 4 8 8 9 0	
29 : 3 0	59 : 5 0 4 5 5	
30 : 1 0	60 : 2 2 8 1 4	

Thank you .....

## Appendix C

## The Fingerprint Processing

1- The main inter-face for fingerprint device when it is activated

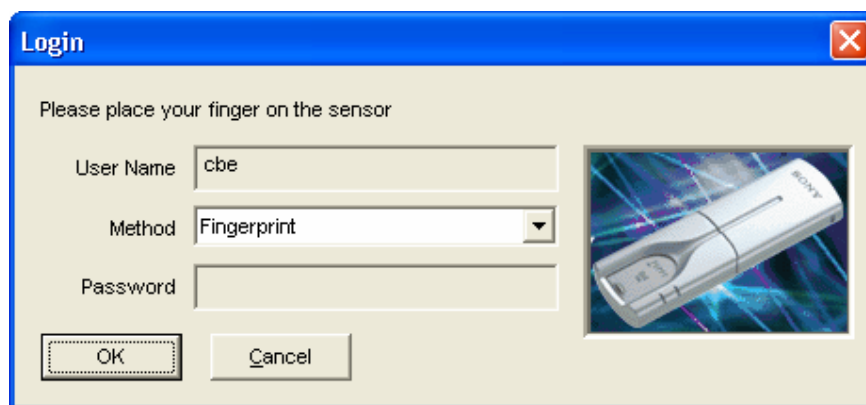


Figure c.1

2- The options in the main inter-face give the way to determine the password type (Key password or Fingerprint password)

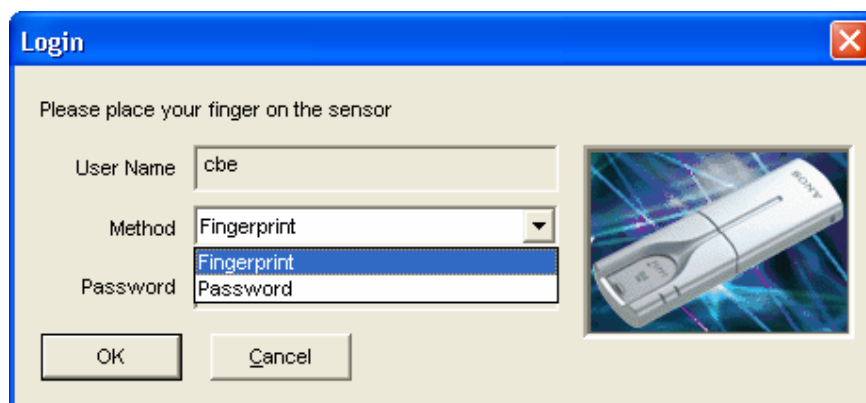


Figure c.2

3- By choose fingerprint then press OK after that scan the finger on the camera, for the client the decision will be as shown in coming figure [c.3] as acceptance.



Figure c.3

For the impostor the result should be as shown in figure [c.4] which mean rejection case.

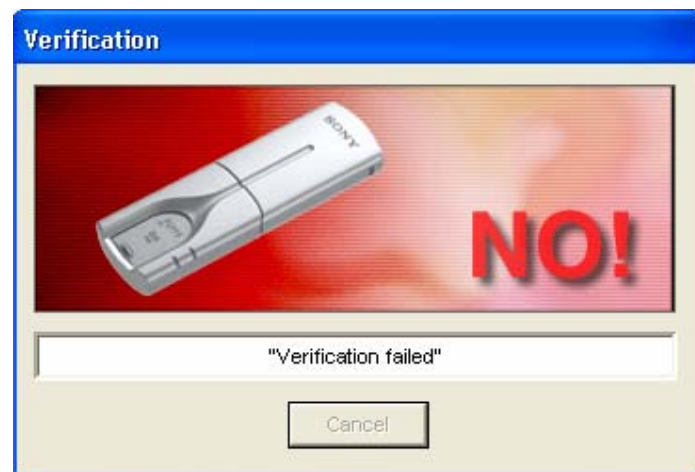


Figure c.4

4- For administrator client will have the options as shown in figure [c.5] to give ability to change and register clients.

In this project the device was used is kind of personal device. Under this case these options will be available to whoever registered his finger as client.

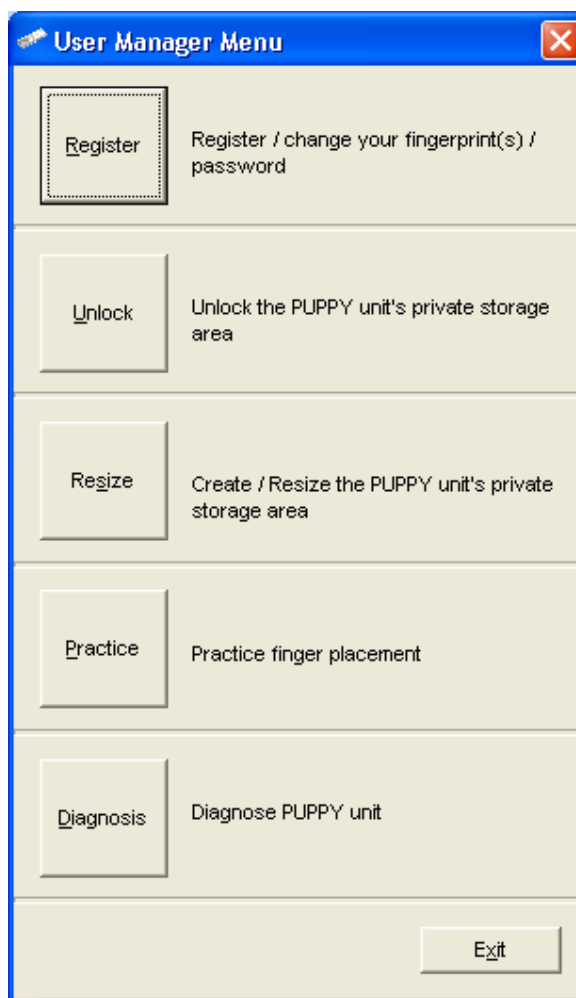


Figure c.5

5- In order to know which finger was registered in the device, it is activated by press over Register button and will be seen as in figure [c.6].

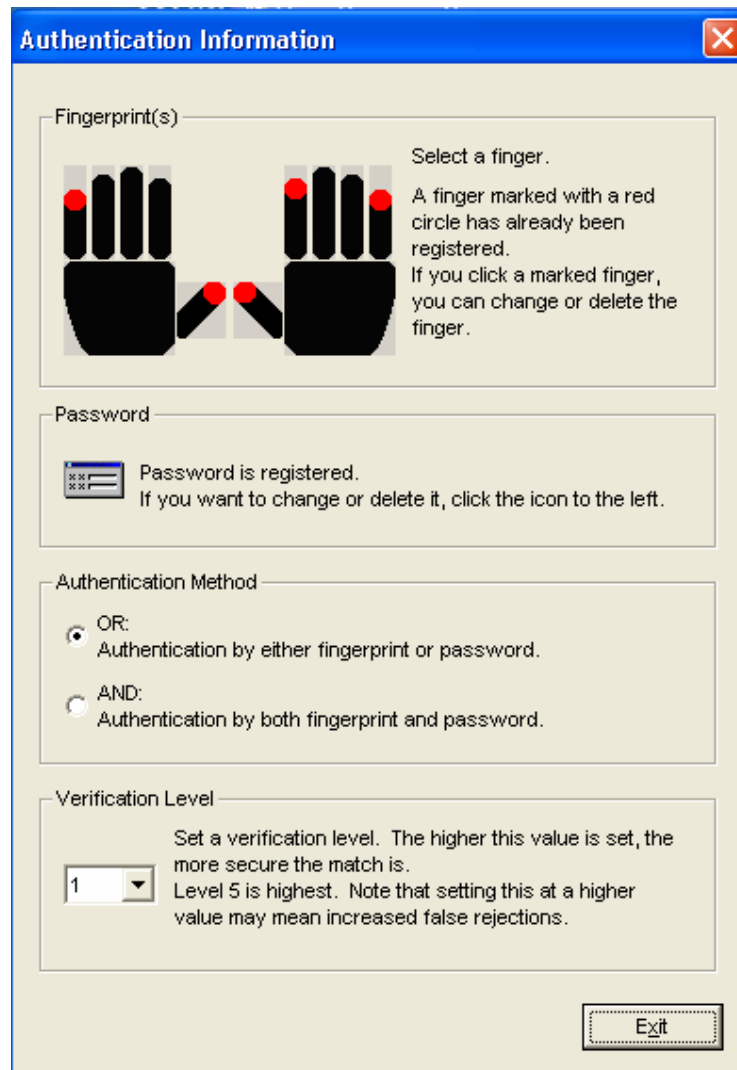


Figure c.6

6- In order to see or scan finger for any one to see or test the accuracy of the device, it could be done by a-press on scan then scan a finger Figure [c.7], b- remove the finger on the camera, c- press the verify button, d- rescan same finger, the result will come out whether is successful as in figure [c.8] or failed as in figure [c.9]



Figure c.7



Figure c.8



Figure c.9

## Appendix D

## The Hand-Scan Geometry Biometric



Figure F.1 Hand-scan geometry

Recognition system handkeyII, use for identify the client to high level of security as clients. See the figure F.2 how it uses.

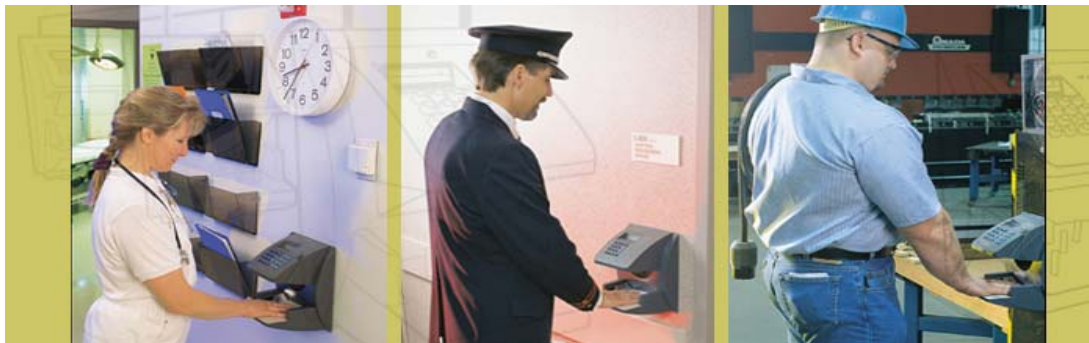


Figure F.2 Hand-scan how it uses

Hand-scan biometric is failed for some hands which are small or short, in figure F.3 shows some characters for the hand the system can scan it.



Figure F.3 Hand characters for hand-scan

Use the network to connect set of hand scan geometrics for nowadays become familiar as shown in the figure F.4 how they connect.

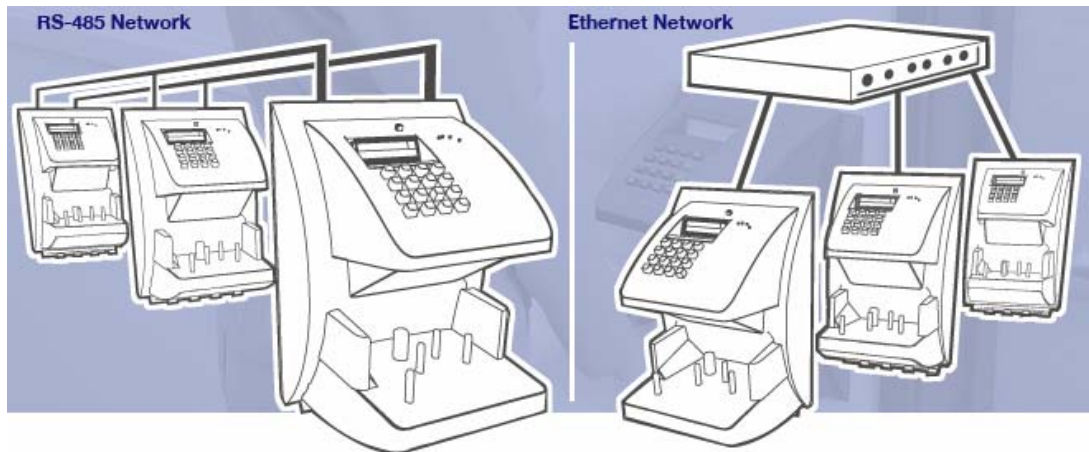


Figure F.4 Hand-scan Ethernet network

## Appendix E

Identification Curves for Digit Combinations Threshold vs. Score.

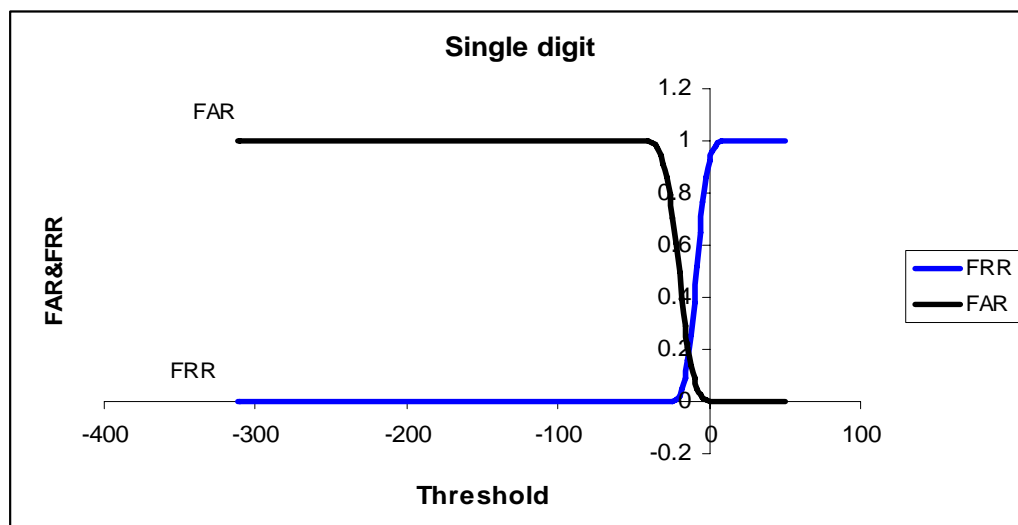
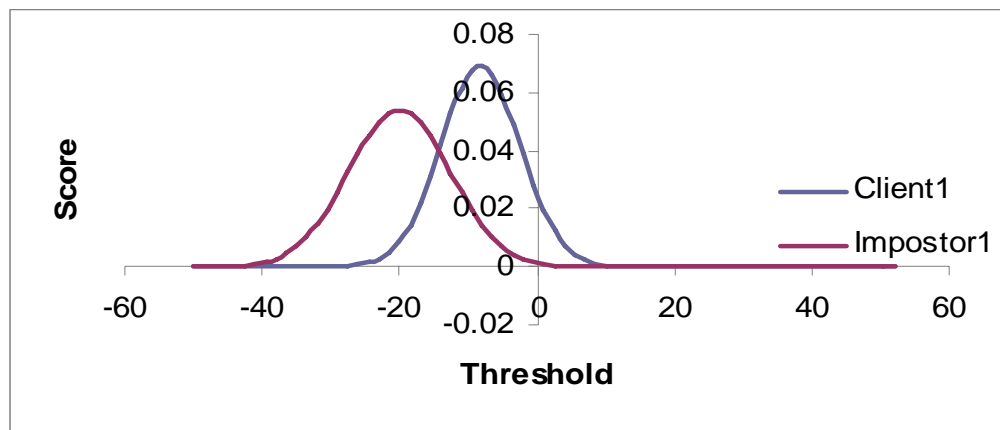


Figure G.1 One Digit

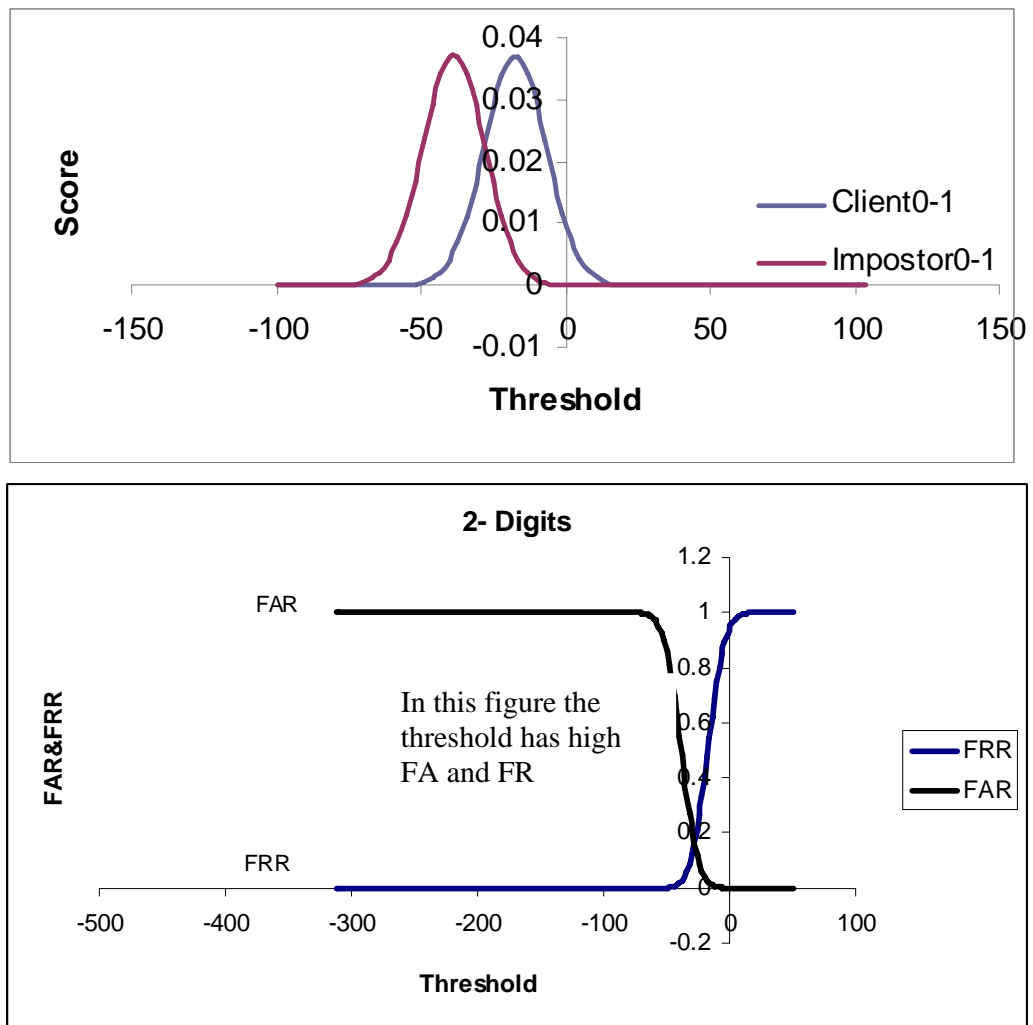


Figure G.2 Two Digit Combinations.

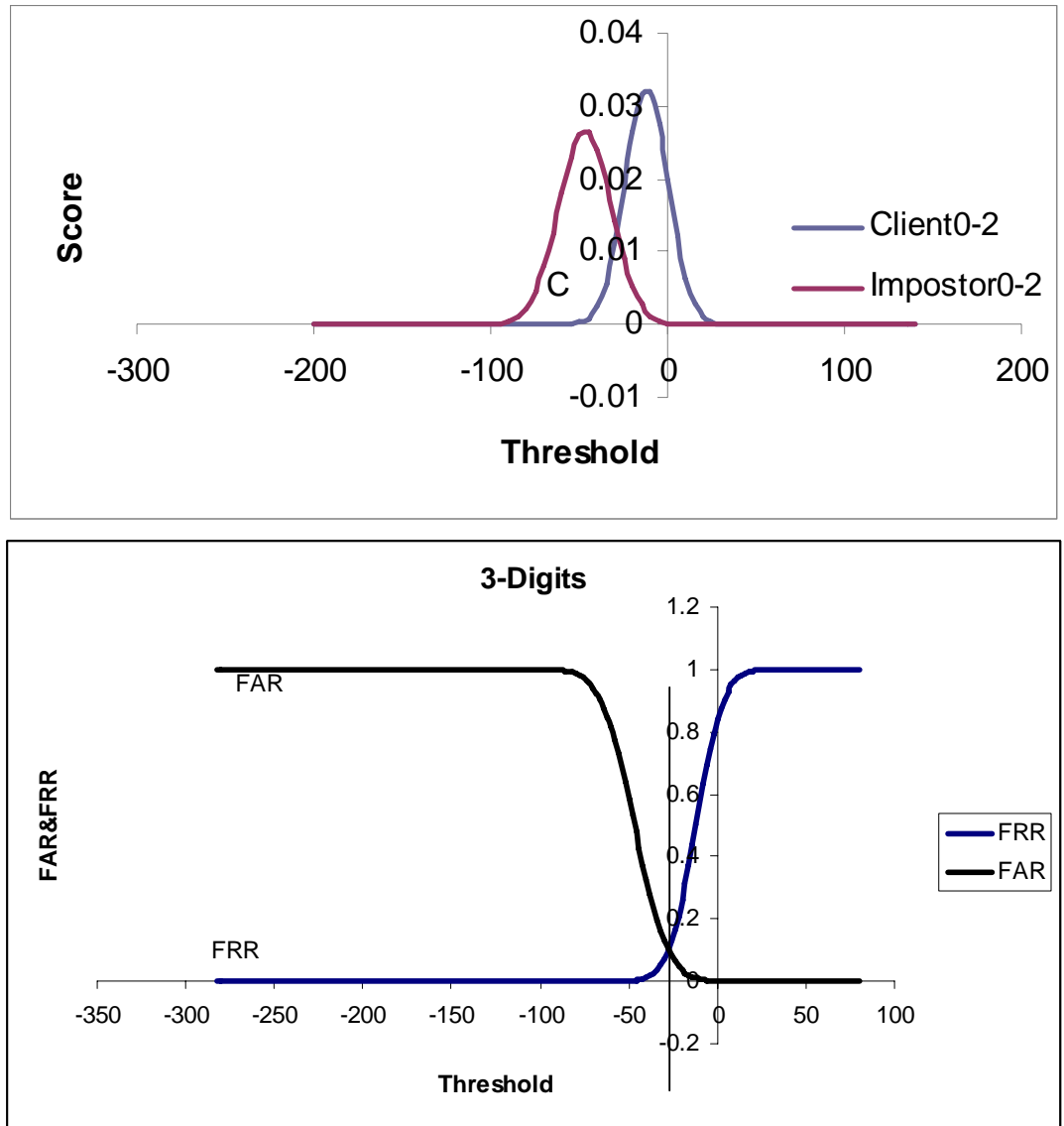


Figure G.3 Three Digit Combinations.

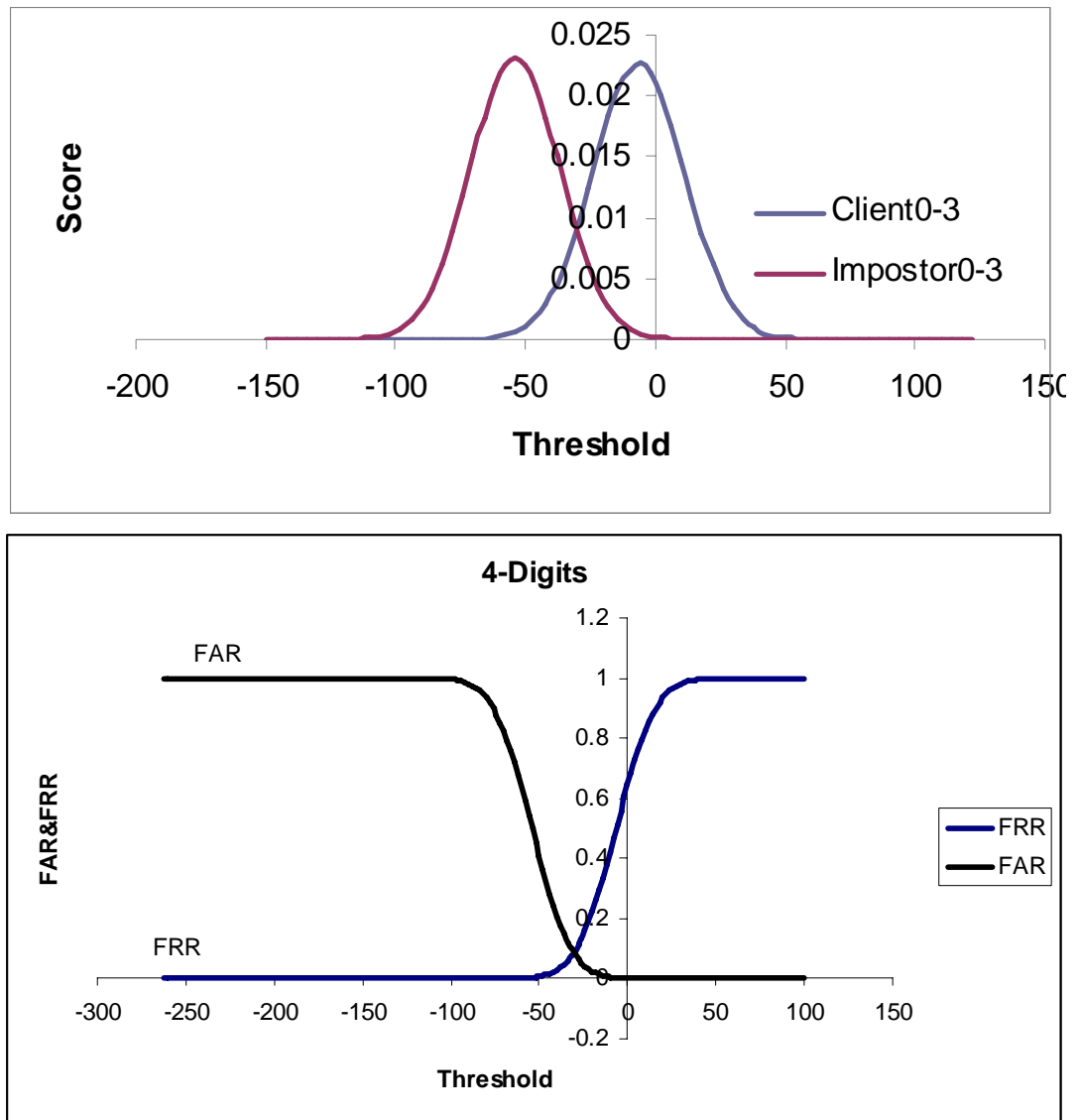


Figure G.4 Four Digit Combinations.

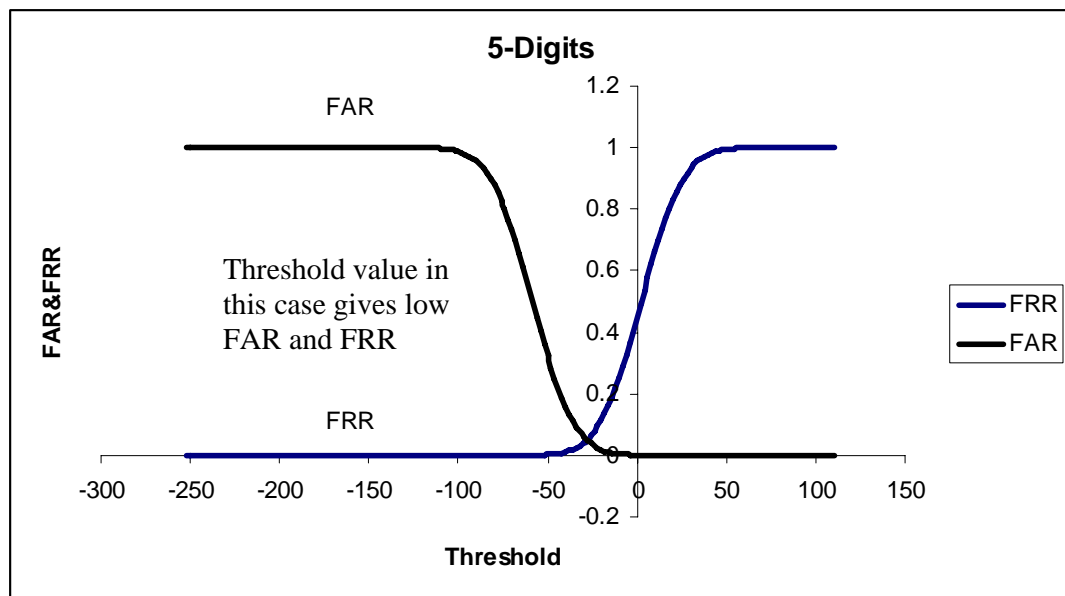
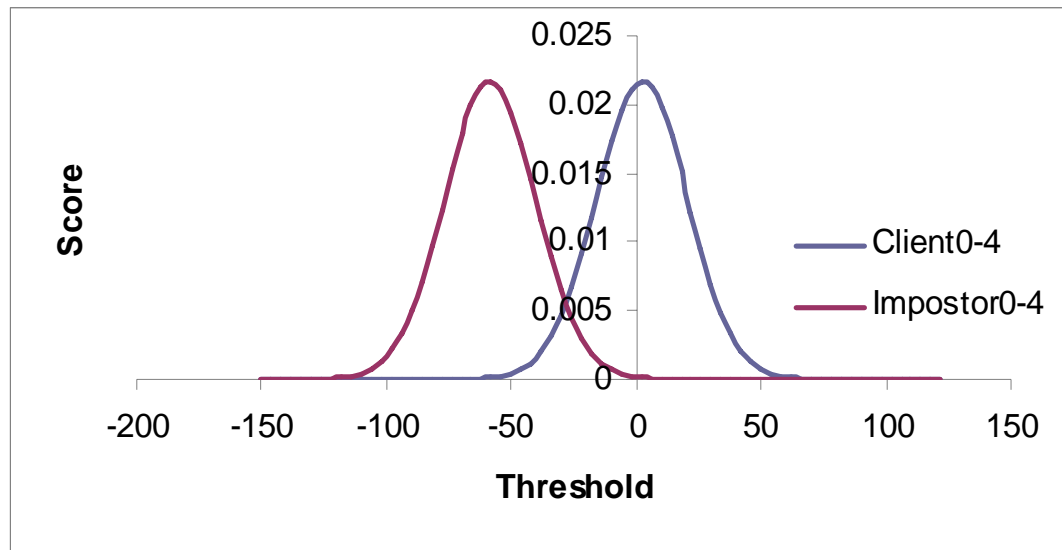


Figure G.5 Digit Combination.

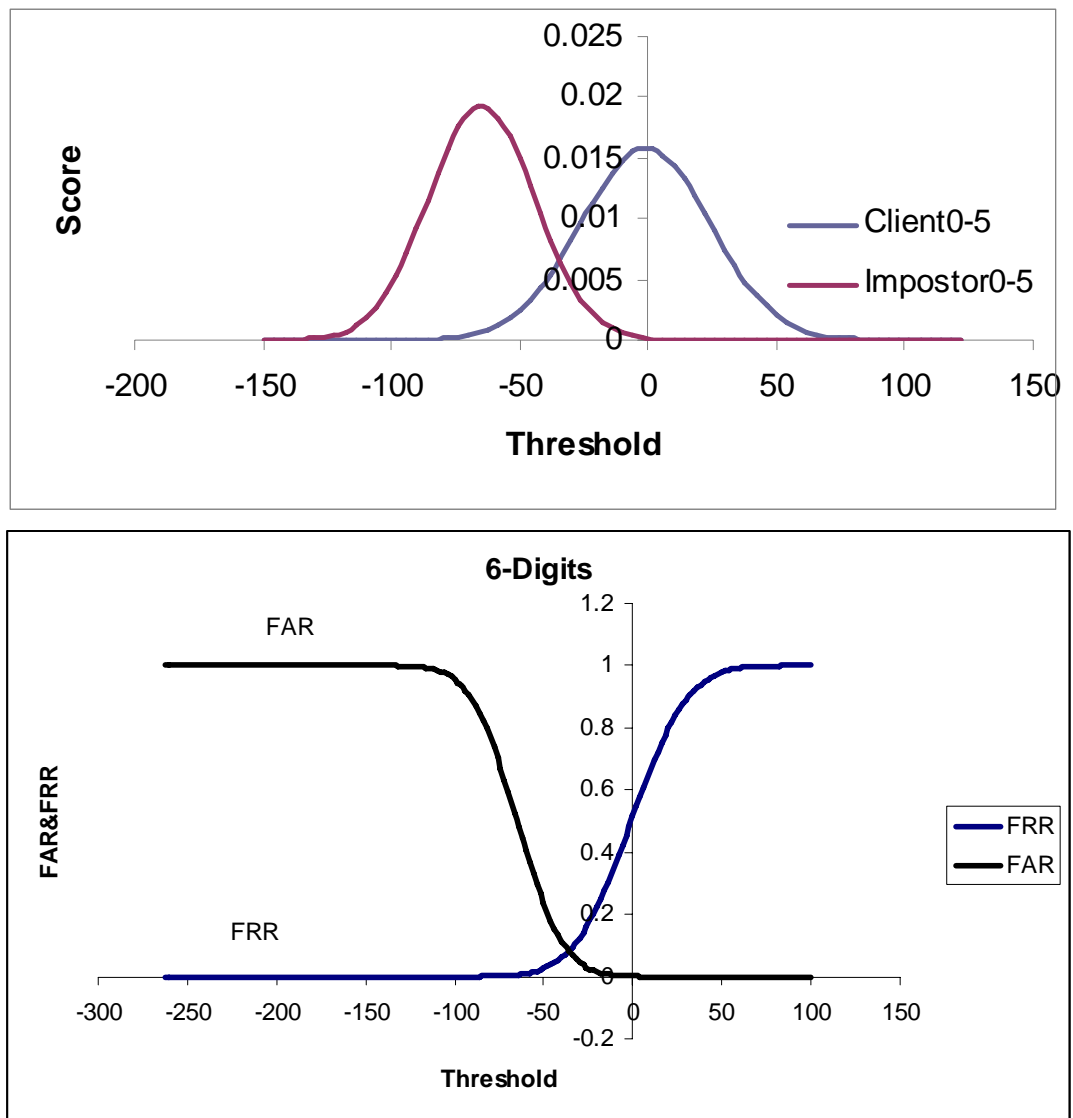


Figure G.6 Digit Combinations.

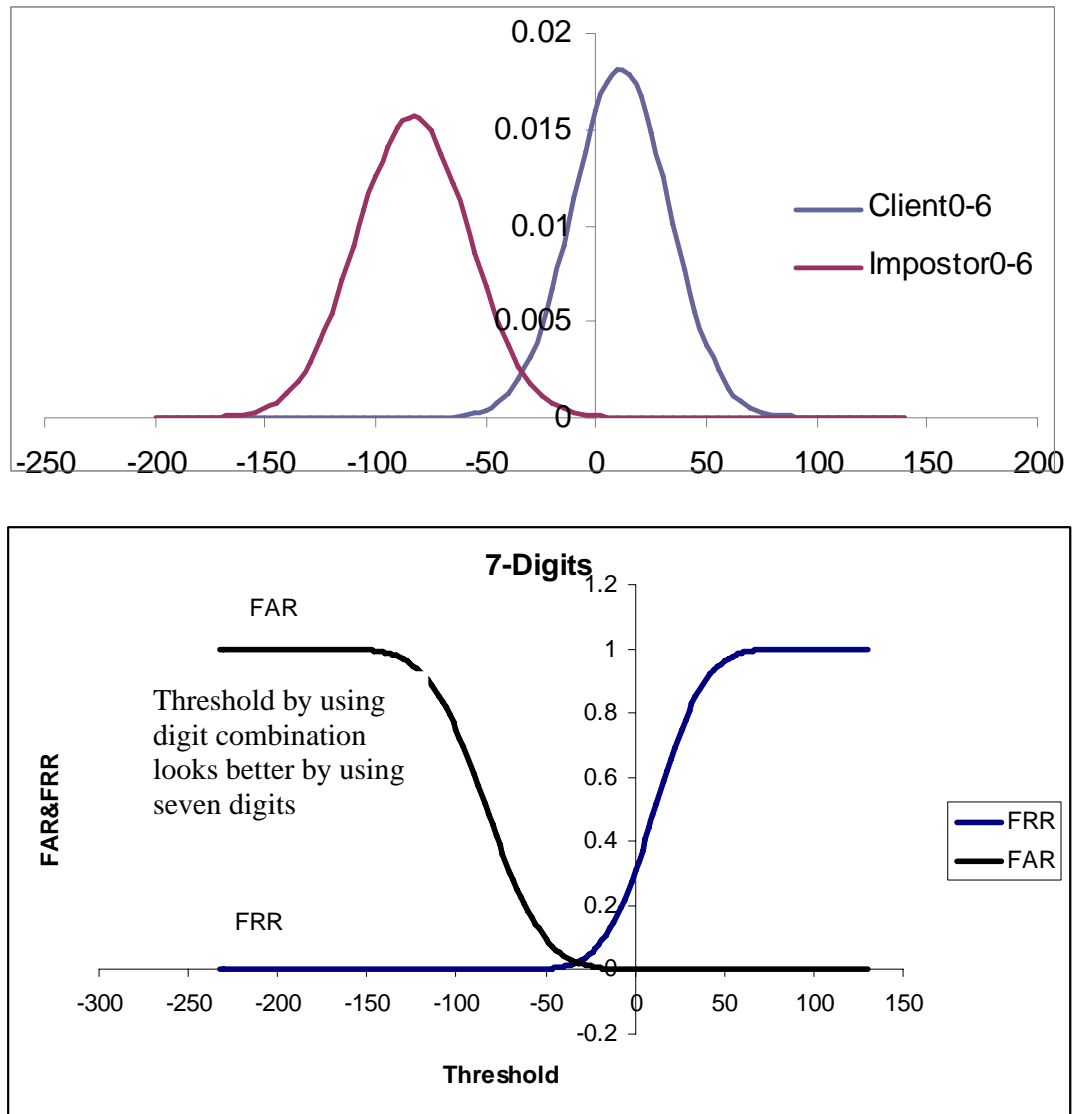


Figure G.7 Digit Combination

## Appendix F

### GOLDWAVE SOFTWARE

The recording software used in this project is GoldWave Digital Audio Editor (4.00 KB on hdd disk). The interface for this software is shown in figure F.1.

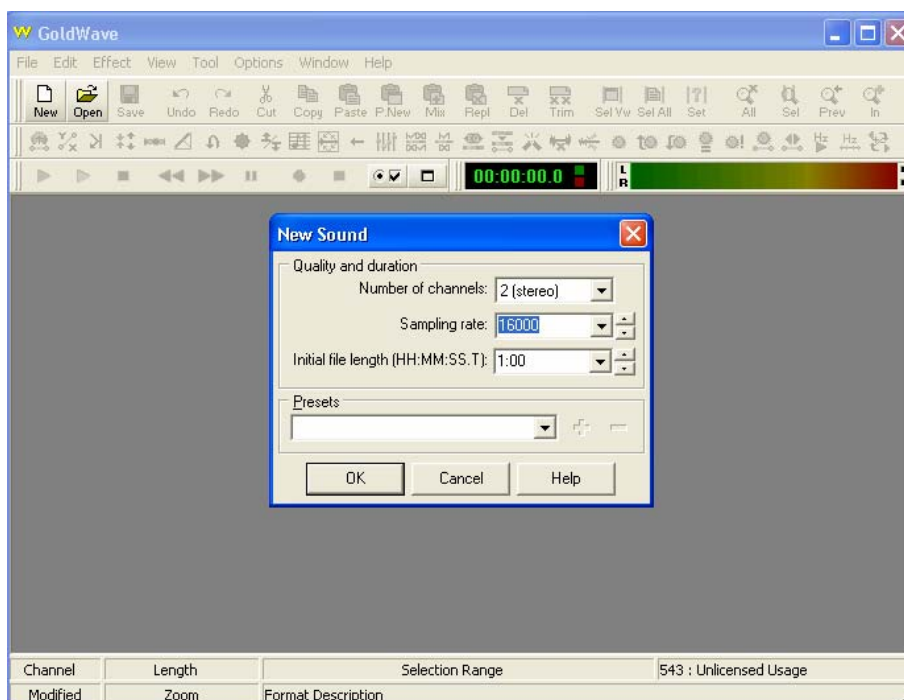


Figure F.1 Interface of goldwave software

#### 1.How GoldWave Works

1. By clicking on the icon of the goldwave the mine interface will appear out, then press on the open icon in the goldwave interface as shown in the figure F.1. Adjust the frequency in sampling rate place, in this project it is 16 KHz, and by adjusting the kind of sound which appears over as stereo, lastly choose the period time for recording task as

single word or sentence. When the software is ready for recording will appear as in figure F.2.

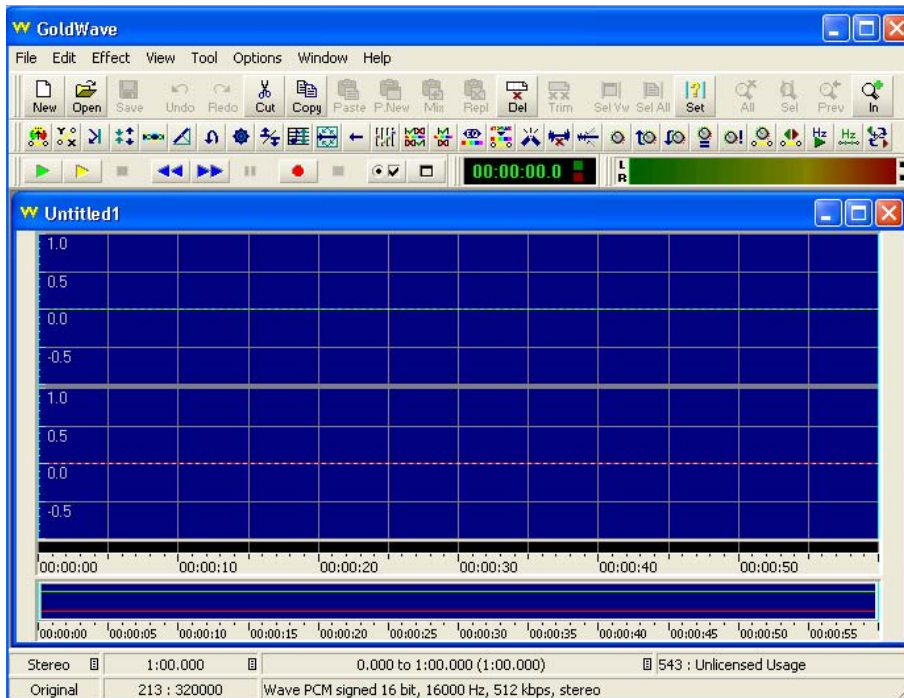



Figure F.2 Ready sample for record

2. The recording task will be needed to the hardware methods as well which the microphone, sound card and computer. To start the recording, click the red button . The recording sample will be appeared as in the figure F.3.
3. In normal situation the time for recording maybe is longer than the speaker time or shorter, to make it properly it done for first case buy cut the empty space as shown in the figure F.4. In second case which happens when the speaker or the word takes long time, this it solved by rerecording or readjust the period recording time.

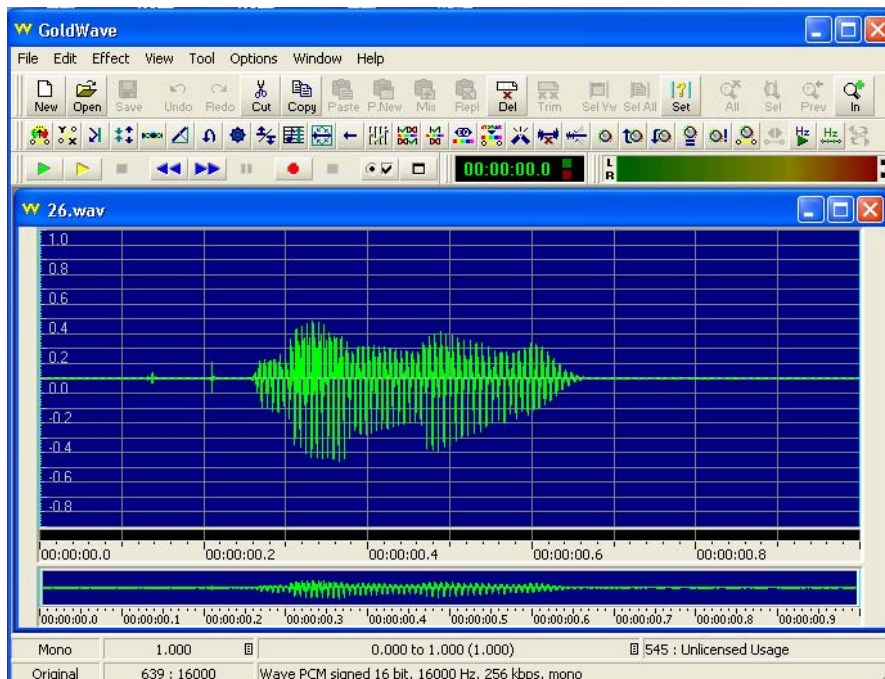


Figure F.3 Sound sample

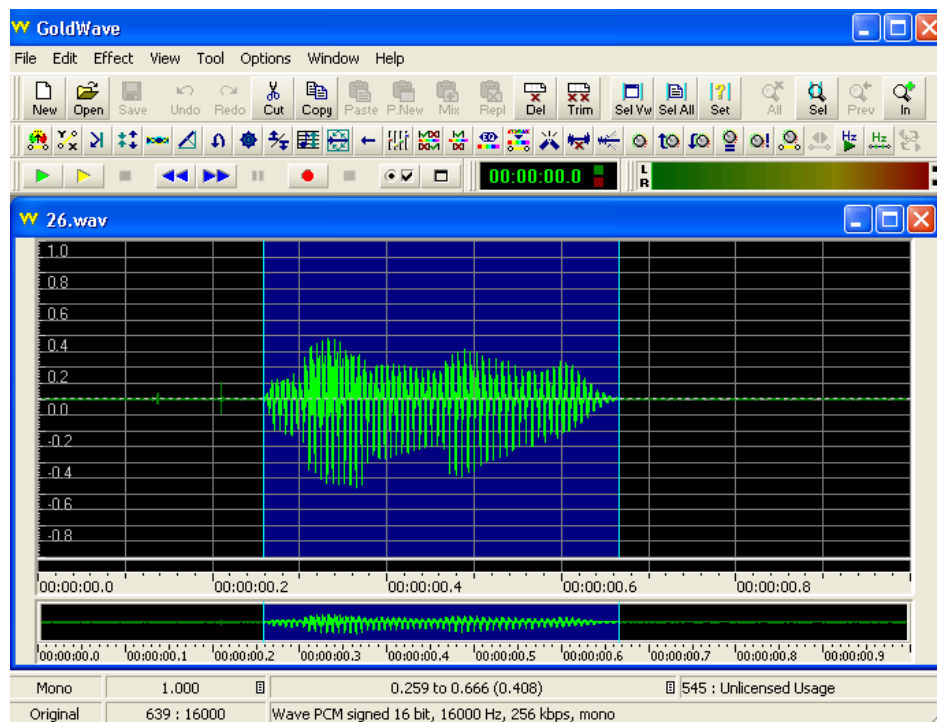


Figure F.4 cut the empty space

The cut sound wave will be appeared as in figure F.5.

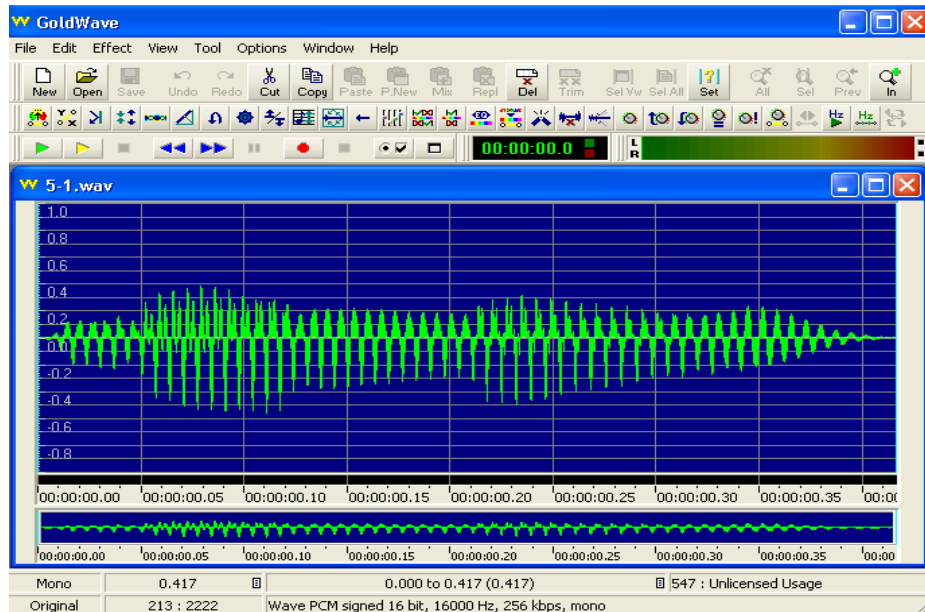


Figure F.5 The sample after cut

4. In order to record a continuous speech the period time should be longer, the combination words are as in the figure F.5

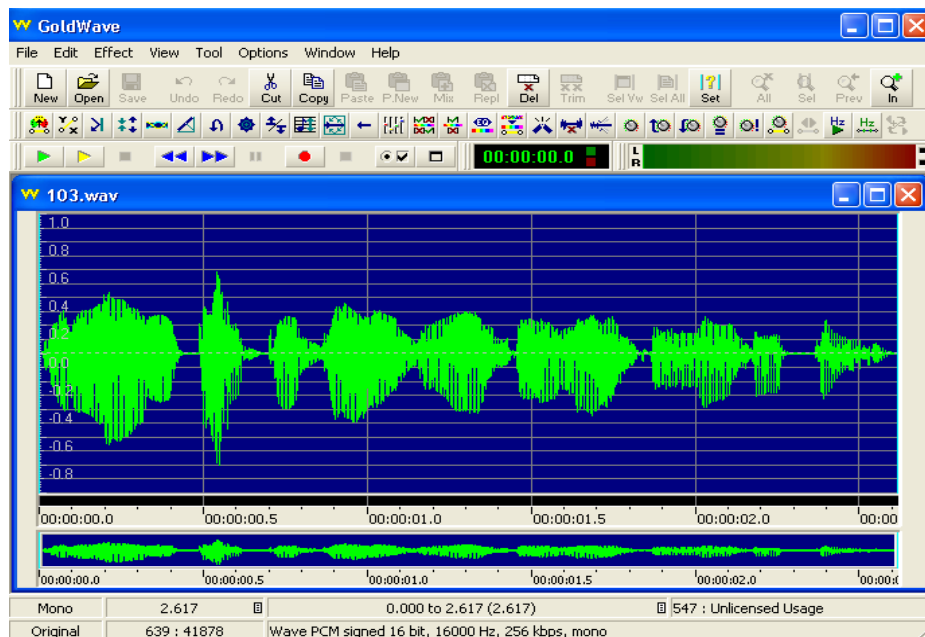


Figure F.5 Sample of continuous speech

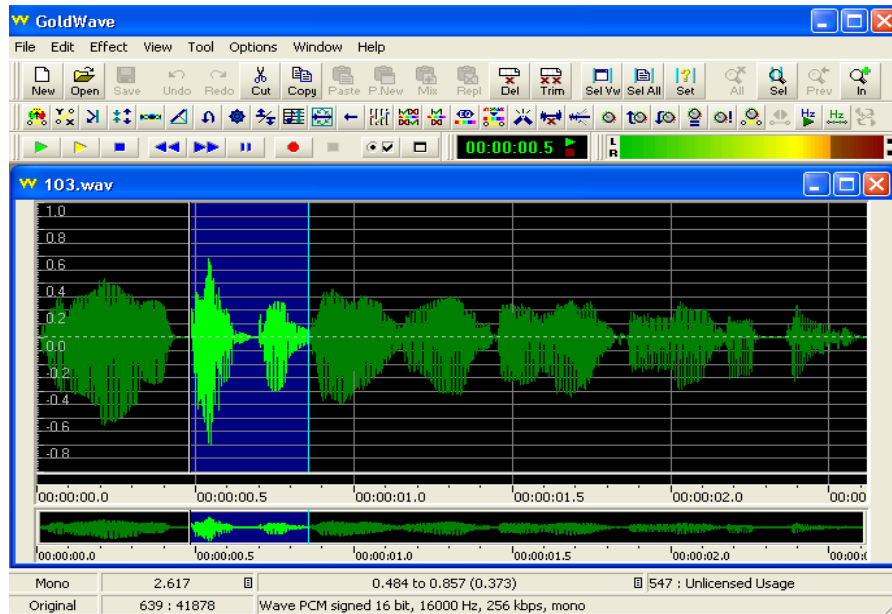


Figure F.6 Cut the continuous voice sample

5. For the continuous samples the cut task will be quite difficult than a single ones. In figure F.6 shows how the cut task does. The word after will be cut by the same way and hear to the sound if it is complete. The cut of samples in continuous voice depends on the experience of the user. See the figure F.7.

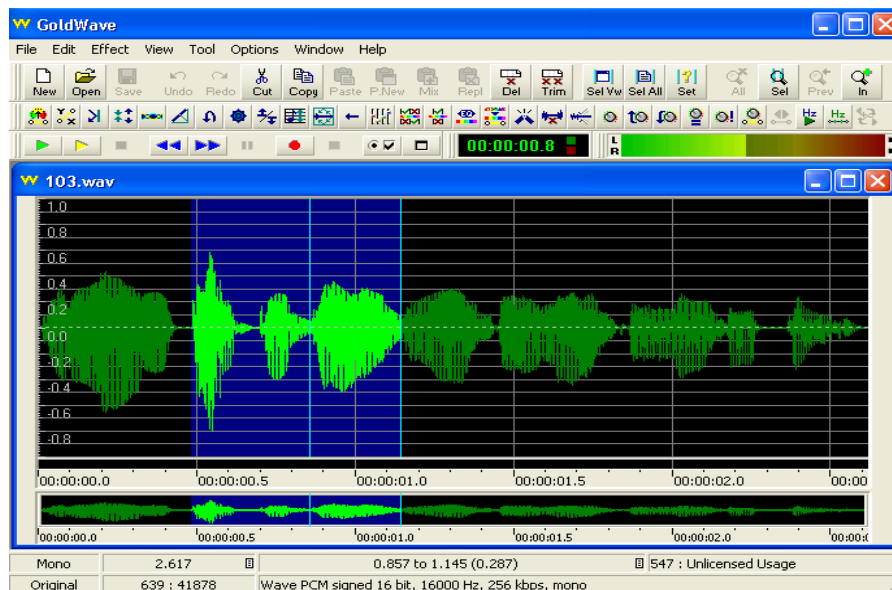


Figure F.7 Determine the end of words

6. The words will have different pronunciation inside of sentences, so the expert user will be able to determine the perfect place to cut as shown in figure F.8. The control method makes the work easier for

user by looking to highest level of sound and low one to know the starting and the end of the words as shown in figure F.9 the testing way by using the controller.

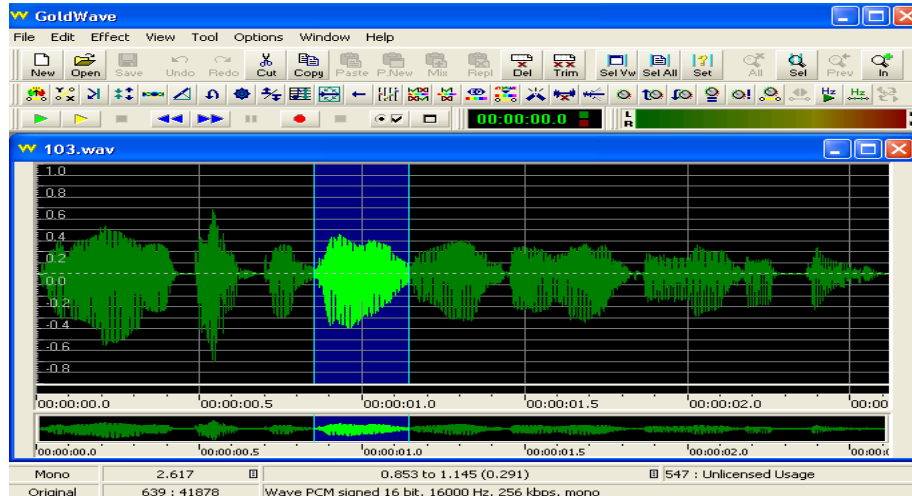


Figure F.8 One word after cut from the sentence

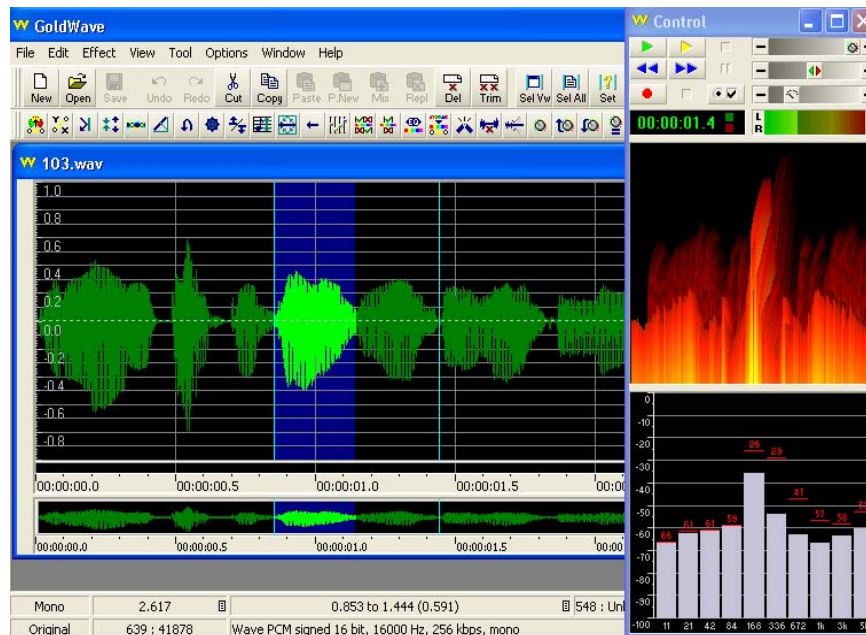


Figure F.9 Using control method for testing

7. Saving the data by pressing on save button, then specify the folder which made for that purpose. For the single words should be counted who many the same word comes, but for the sentences it doesn't matter. See the figure F.10.

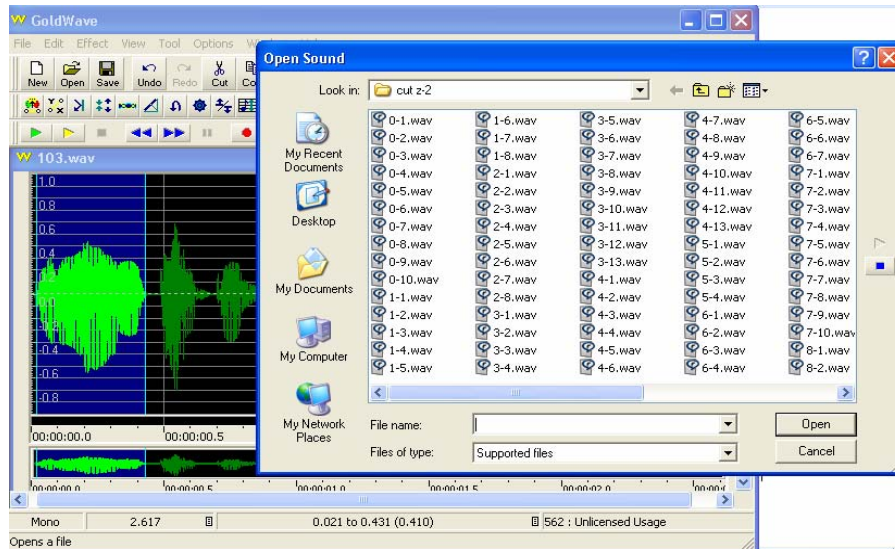



Figure F.10 the saving step how it does

8. Finally to read the data again the same goldwave is used, by adjusting the player as shown in figure F.11. then press the green button .

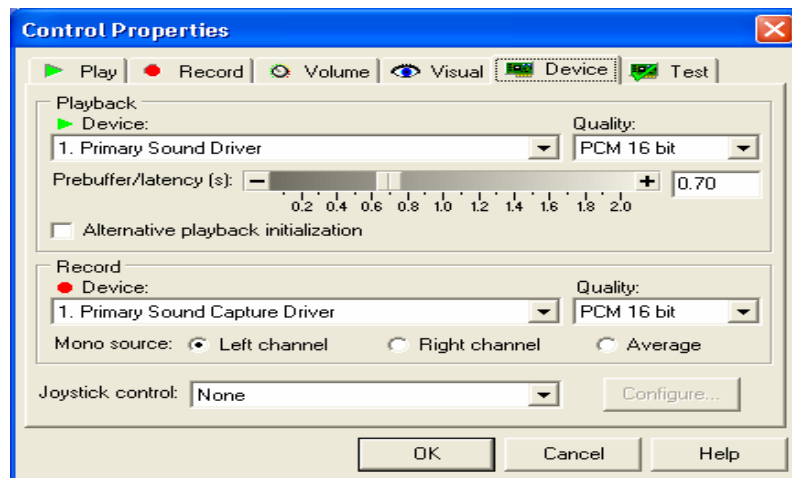


Figure F.11 Adjusting the reader method  
By using the controller, the control in level on the voice is done.  
In the figure F.12 shows the controller.

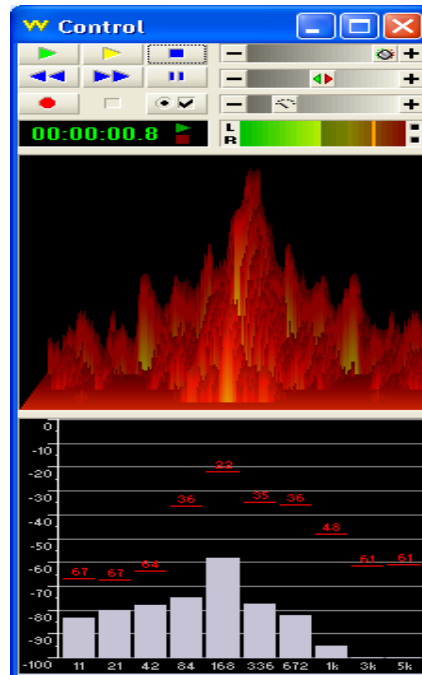


Figure F.12 The controller interface

GoldWave provide some other methods like the reading from the CD it shows in figure F.13, and also for some complex experimental it is qualified also by giving the some method to match some single word to made some phrases as shown in figure F.14 also in figure F.15.

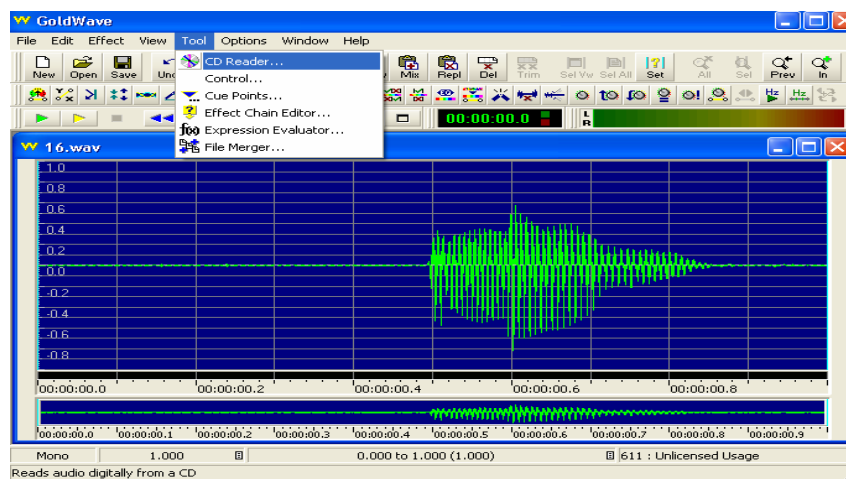


Figure F.13 Read date from CD by using the goldwave

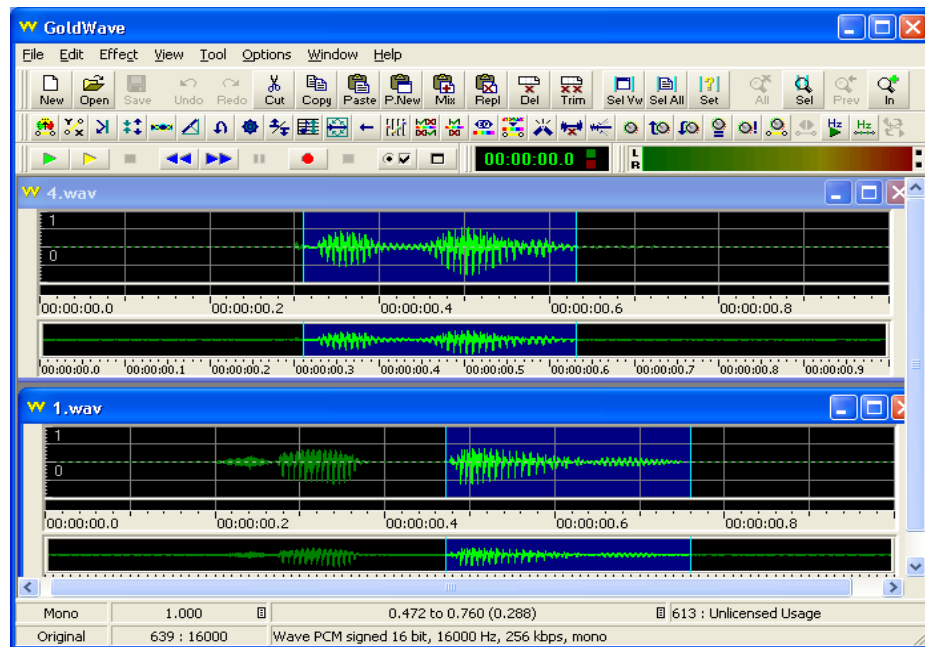


Figure F.14 cut word from one combination to use it in other one

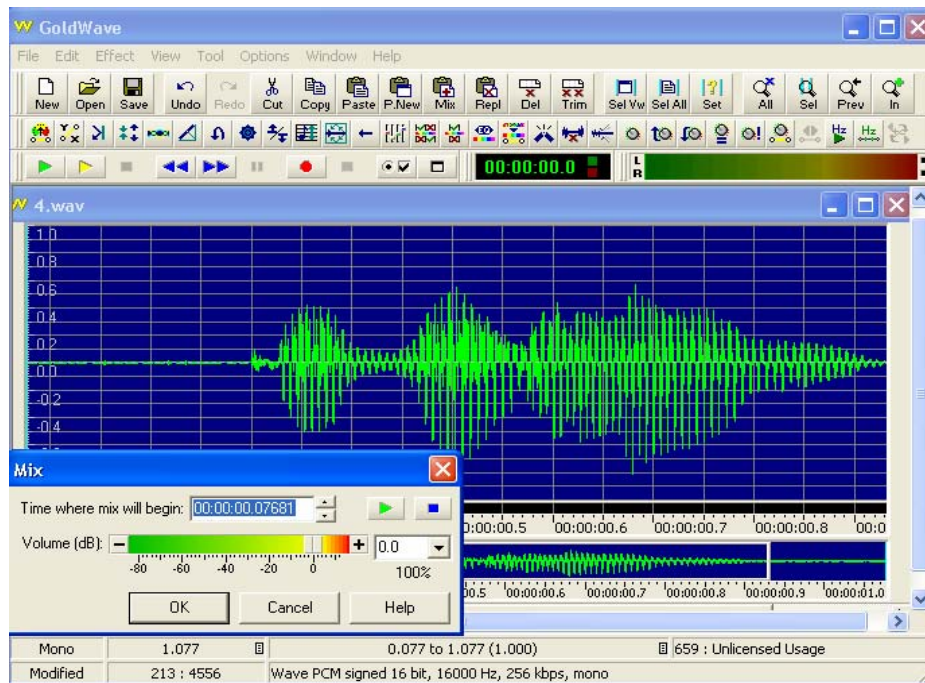


Figure F.15 Matching a word to other one to give a sentence