SECURITY EQUIPMENT USING BIOMETRICS

MUHAMAD FIRDAUS BIN JUSOH

This Report Is Submitted In Partial Fulfillment of Requirement for the Bachelor Degree of Electronic Engineering (Computer) With Honours

Faculty of Electronics and Computer Engineering
Universiti Teknikal Malaysia Melaka

2013

UNIVERSTI TEKNIKAL MALAYSIA MELAKA

FAKULTI KEJURUTERAAN ELEKTRONIK DAN KEJURUTERAAN KOMPUTER

BORANG PENGESAHAN STATUS LAPORAN

PROJEK SARJANA MUDA II

Tajuk Projek	:	SECURITY EQUIPMENT USING BIOMETRICS
Sesi Pengajian	:	SESI 2012/2013

Saya MUHAMAD FIRDAUS BIN JUSOH mengaku membenarkan Laporan Projek Sarjana Muda ini disimpan di Perpustakaan dengan syarat-syarat kegunaan seperti berikut:

1. Laporan adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan laporan 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**	

Ditulis oleh:

_____
(TANDATANGAN PENULIS)

Alamat : No 4, Lorong Air Putih 24,
Jalan Air Putih, 25300, Kuantan,
Pahang Darul Makmur.

Tarikh: ……..

Disahkan oleh:

_____
(COP & TANDATANGAN PENYELIA)

Tarikh: ……..

"I hereby declare that this is the results of my own paper except for quotes as cited in the references."

Signature : _____

Author : MUHAMAD FIRDAUS BIN JUSOH

Date : 10 JUNE 2013

"I hereby declare that I have read this report and in my opinion this report is sufficient in terms of the scope and quality for the award of Bachelor Degree of Electronic and Computer Engineering (Computer) with Honours."

Signature : _____

Supervisor's Name : MR.MUHAMMAD NOORAZLAN SHAH BIN ZAINUDIN

Date : 10 JUNE 2013

This study is dedicated to my parents, Jusoh Che Omar and Zakiah Binti Mohamed Ghazalli. They had taught me the important lessons in life, which one of the lesson is as hard the life gets, it is possible to succeed in it as long as we do the best out of us, does not let bad things to turn us down, having the courage and remember to keep Islam's lesson as main guidance. They also taught me about being independent in achieving something in life.

ACKNOWLEGDEMENT

Alhamdulillahirabbil ‘alamin washolatu wassalamu’ala asrafil anbiyai wal mursalin, wa’ala alihi waaskhabihi ajma’in. praise to Allah S.W.T the most gracious and merciful for giving me the strength and wisdom in completing my Final Year Project (FYP). First and foremost, I want to perform my gratefulness to Allah S.W.T for keeping me in faith and show me guidance throughout the period of this study. I’m also thankful to Him for easing out everything during the hard times.

Secondly, I would like to gratitude my parents, Jusoh Bin Che Omar and Zakiah Binti Mohamed Ghazalli for supporting me emotionally, morally and financially. They are the main catalyser that ignites me to study well and to do my best in my study.

Next, my appreciation to my supervisor, Mr. Muhammad Noorazlan Shah Bin Zainudin. Special thanks to him for giving my guidance in doing this study. He is also responsible in giving me useful and beneficial suggestions, ideas and reference materials.

Last but not least, my appreciation goes to the staff, faculty, lecturers and administration of Universiti Teknikal Malaysia Melaka and not forgetting, my friends and course-mates for indirectly helping my during this study by suggesting me some references as well as giving me constructive critics and comments regarding my study.

ABSTRACT

Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. Biometrics based security systems are far most secure and accurate than traditional password or token based security systems. For example a password based security system has always the threat of being stolen and accessed by the unauthorized user. Furthermore the traditional security systems are always prone to accuracy as compared to biometrics which is more accurate. The biometrics that were used in this project are fingerprints biometric. This biometrics were choose to be used in this project after a deep research. It was the suitable biometrics for this project because of the attributes of the fingerprints itself. The methods of matching technique in this project are image based. It is among the most fastest and reliable method. More importantly, the proposed security system will contribute to the biometric technology application in our daily life.

ABSTRAK

Biometrik adalah sains dan teknologi untuk mengukur dan menganalisis data biologi. Dalam teknologi maklumat, biometrik merujuk kepada teknologi yang mengukur dan menganalisis ciri-ciri badan manusia seperti DNA, cap jari, retina mata dan irises, corak suara, corak muka dan ukuran tangan, untuk tujuan pengesahan. Sistem keselamatan berasaskan biometrik adalah lebih selamat dan tepat berbanding sistem keselamatan tradisional atau sistem keselamatan berasaskan kad. Sebagai contoh, sistem keselamatan berasaskan kata laluan sentiasa digodam dan diakses oleh pengguna yang tidak dibenarkan. Tambahan pula, sistem keselamatan tradisional sentiasa terdedah kepada bahaya berbanding biometrik yang lebih tepat. Biometrik yang digunakan didalam projek ini adalah cap jari. Biometric ini dipilih setelah penyelidikan yang mendalam dilakukan. Ia adalah biotmetrik yang paling sesuai untuk digunakan kerana ia mempunyai ciri-cirinya sendiri. Kaedah yang digunakan untuk teknik padanan cap jari adalah berdasarkan imej. Projek ini bertujuan untuk mereka bentuk prototaip peralatan keselamatan menggunakan biometrik cap jari untuk kegunaan penyimpanan. Lebih penting lagi, sistem keselamatan yang dicadangkan itu akan menyumbang kepada aplikasi teknologi biometrik dalam kehidupan seharian kita.

	PAGE
TITLE	**i**
PROJECT DECLARATION FORM	**ii**
DECLARATION	**iii**
APPROVAL	**iv**
DEDICATION	**v**
ACKNOWLEDGEMENT	**vi**
ABSTRACT	**vii**
ABSTRAK	**viii**
TABLE OF CONTENT	**ix**
LIST OF TABLE	**xii**
LIST OF FIGURE	**xiii**
LIST OF APPENDICES	**xv**

CHAPTER		**PAGE**
I	**INTRODUCTION**	**1**
1.1	Introduction	1
1.2	Introduction Of The Project	1
1.2.1	One Individual, Multiple Ids	3
1.2.2	One Id, Multiple Individual	3
1.2.3	Accuracy And Security	3
1.3	Biometrics Categories	4
1.3.1	Physical Biometrics	4
1.3.1.1	Fingerprints	4
1.3.1.2	Face Recognition	5
1.3.1.3	Hand Geometry	6
1.3.1.4	Iris Scan	7
1.3.2	Behavioral Biometrics	8
1.3.2.1	Gait	9

	1.3.3 Chemical Biometrics	9
	1.4 Multi Biometrics Systems	9
	1.4.1 Multi Sensorial	10
	1.4.2 Multi Modal	10
	1.4.3 Multi Algorithmic	11
	1.4.4 Multi Instance	11
	1.5 Problem Statement	11
	1.6 Project Objectives	12
	1.7 Scope Of Work	12
	1.8 Thesis Outlines	15
II	**LITERATURE REVIEW**	**17**
	2.1 Introduction	17
	2.2 Brief History Of Fingerprint	18
	2.3 Literature Review	19
	2.3.1 Characteristics Of Fingerprints	19
	2.3.2 Fingerprint Image Enhancement	22
	2.3.3 Minutiae Based Matching Technique	23
	2.3.4 Correlation Based Matching Technique	25
	2.3.5 Ridge Feature Based Matching Technique	27
	2.3.6 Image Based	28
	2.4 Fingerprint Scanner	30
	2.4.1 Capacitance Sensor	30
	2.4.2 Optical Sensor	31
	2.5 Visual Studio	31
	2.6 Comparative Studies	33
III	**PROJECT METHODOLOGY**	**34**
	3.1 Introduction	34
	3.2 Project Flowchart	35
	3.3 Biometrics Process	37

IV	**RESULT AND ANALYSIS**	**40**
	4.1 Introduction	40
	4.2 RESULT	40
	4.2.1 The Result Of Stored Database	41
	4.2.2 Hardware	42
	4.2.3 Gui Of Security System Using Biometric	43
V	**CONCLUSION**	**49**
	5.1 Conclusion	49
	5.2 Future Work	50
REFERENCES		52
APPENDICES		54

LIST OF TABLE

TABLE NO.	TITLE	PAGES
1.1	Comparative Study	33
4.1	GUI Description	44

LIST OF FIGURES

FIGURE NO.	TITLE	PAGES
1.1	Types of Biometrics	2
1.2	Image of Fingerprint	5
1.3	Face Recognition	6
1.4	Hand Measurement	7
1.5	Iris Recognition	8
1.6	Stages of Gait Cycle	9
1.7	Multi biometrics Categories	10
1.8	Minutiae based matching technique	13
1.9	Image based matching technique	14
1.10	Correlation Based Technique	14
1.11	Ridge Features Based Technique	15
2.1	Type of Ridge Pattern	20
2.2	Local and Global Features	21
2.3	Fingerprint Distribution	21
2.4	Fingerprint Image	22
2.5	Bifurcation and Ridge Ending	24
2.6	Minutiae Based Workflow	24
2.7	Correlation Technique	26
2.8	Correlation Based Workflow	26
2.9	Ridge features based	27
2.10	Example of Image Matching Technique	28
2.11	Image Based Workflow	29
2.12	Capacitance Sensor	30
2.13	Optical Sensor	31
2.14	Visual Studio	32
3.1	Project Flowchart	35
3.2	Biometric Process	37

3.3	Block Diagram for Fingerprint Reader	38
4.1	Access Database	41
4.2	Hardware Connection	42
4.3	Admin Form	43
4.4	Main GUI of Security System Using Biometric	44
4.5	Admin Mode Interface	46
4.6	Add Record process	47
4.7	Clear Record process	48
5.1	Multimodal Biometrics	51

LIST OF APPENDICES

NO. OF APPENDIX	TITLE	PAGES
APPENDIX A	Database Operation Coding	54
APPENDIX B	Adding and Deleting Fingerprint Coding	60
APPENDIX C	Fingerprint Matching Coding	68
APPENDIX D	Project Picture	73

CHAPTER I

INTRODUCTION

1.1 Introduction

This chapter will cover introduction of the project. To outline the chapter, it is first discussed the introduction if the project then followed by the problem statement of the project that is trying to be improved. Then, the objectives are presented and the remaining section described the work scope and the structure of this report.

1.2 Introduction of the project

Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. Biometrics based security systems are far most secure and accurate than traditional password or token based security systems[3]. For example a password based security system has always the threat of being stolen and accessed by the unauthorized user. Furthermore the traditional security systems are always prone to accuracy as compared to biometrics which is more accurate. Biometrics can be categorized in various

categories such as physical and behavioral biometric. For physical biometrics, it can be classified to fingerprint, face recognition, iris scans and hand geometry meanwhile for behavioral biometrics is gait, handwriting, speech and signature [8]. Figure 1.1 show the example of biometrics types that were discussed earlier.

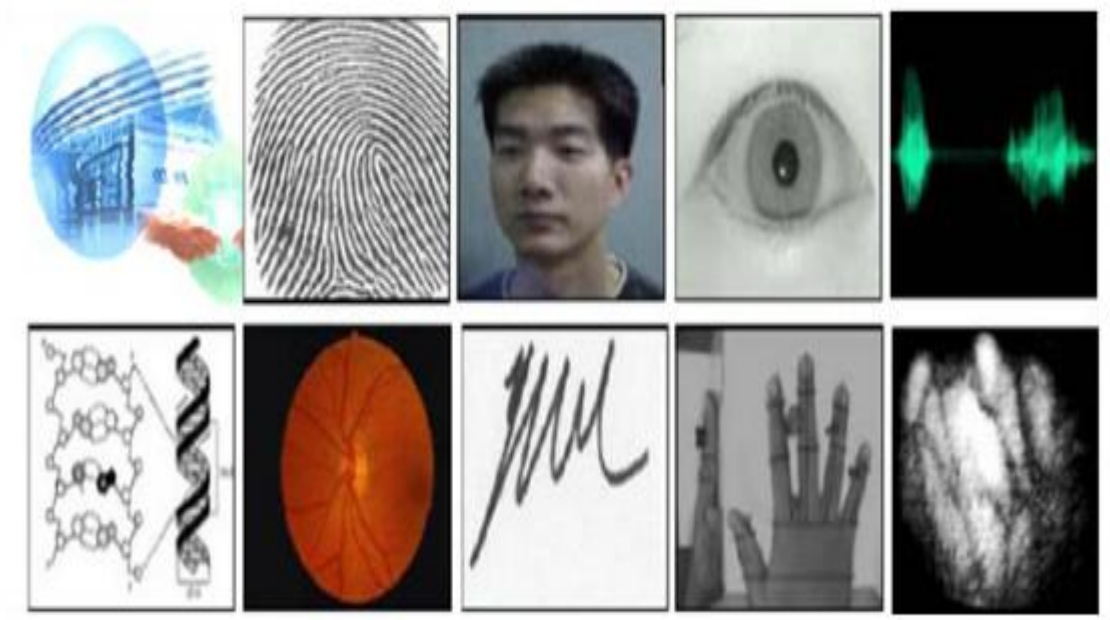

Figure 1.1 Types of Biometrics

Fingerprint based security system is one of the most important biometric technologies which have drawn a substantial amount of attention recently. Fingerprint technology is so common on personal identification has been well established. Each human has unique own fingerprint, even the twin have different fingerprint. So, fingerprint recognition is useful in security and law application

Biometrics offers several advantages over traditional security measures. Some of them are presented below.

1.2.1 One individual, Multiple IDs

Traditional security systems face the problem that they don't give solution to the problem of individuals having multiple IDs. For examples a person having multiple passports to enter a foreign country. Thanks to biometrics, they give us a system in which an individual can't possess multiple IDs and can't change his ID throughout his life time. Each individual is identified through a unique biometric identity throughout the world.[3]

1.2.2 One ID, Multiple Individual

In traditional security systems one ID can be used by multiple individuals. For example in case of a password based security system a single password can be shared among multiple individuals and they can share the resources allotted to a single individual. Biometric based security system doesn't allow such a crime. Here each individual has a single unique ID and it can't be shared with any other individual.[3]

1.2.3 Accuracy and Security

Biometrics based security systems are far most secure and accurate than traditional password or token based security systems. For example a password based security system has always the threat of being stolen and accessed by the unauthorized user. Furthermore the traditional security systems are always prone to accuracy as compared to biometrics which is more accurate.[3]

1.3 Biometrics Categories

Biometrics can be categorized in various categories as follow.

1.3.1 Physical Biometrics

This biometrics involves measurement of physical characteristics of individuals. The most prominent of these include

- Fingerprints
- Face
- Hand geometry
- Iris scans

1.3.1.1 Fingerprints

Fingerprints recognition has been present for a few hundred years. Due to tremendous research this field has reached such a point where the purchase of fingerprint security system is quite affordable. For this reason these systems are becoming more widespread in a variety of applications. Example image of fingerprints are showed in Figure 1.2.

Figure 1.2 Image of Fingerprint

1.3.1.2 Face Recognition

Some facial recognition algorithms identify facial features by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. Other algorithms normalize a gallery of face images and then compress the face data, only saving the data in the image that is useful for face detection. A probe image is then compared with the face data. One of the earliest successful systems is based on template matching techniques applied to a set of salient facial features, providing a sort of compressed face representation. Recognition algorithms can be divided into two main approaches, geometric, which looks at distinguishing features, or photometric, which is a statistical approach that distills an image into values and compares the values with templates to eliminate variances. Popular recognition algorithms include Principal Component Analysis using eigenfaces, Linear Discriminate Analysis, Elastic Bunch

Graph Matching using the Fisherface algorithm, the Hidden Markov model, the Multilinear Subspace Learning using tensor representation, and the neuronal motivated dynamic link matching. Figure 1.3 shows on how the face recognition worked.

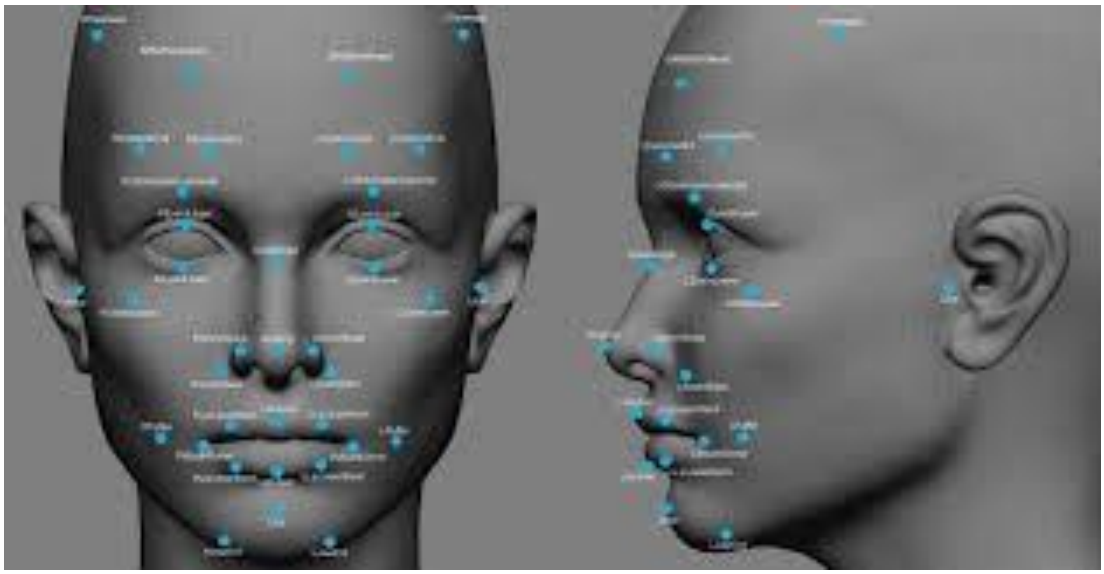

Figure 1.3 Face Recognition

1.3.1.3 Hand Geometry

One way to identify a person is to measure the unique geometry of their hand. This is an attractive biometric because it is minimally invasive and has no criminal stigma associated with it (unlike fingerprints). Feature extraction involves computing the widths and lengths of the fingers at various locations using the captured image. These metrics define the feature vector of the user's hand. It is shown in Figure 1.4. Current research work involves identifying new features that would result in better discriminability between two different hands, and designing a deformable model for the hand.

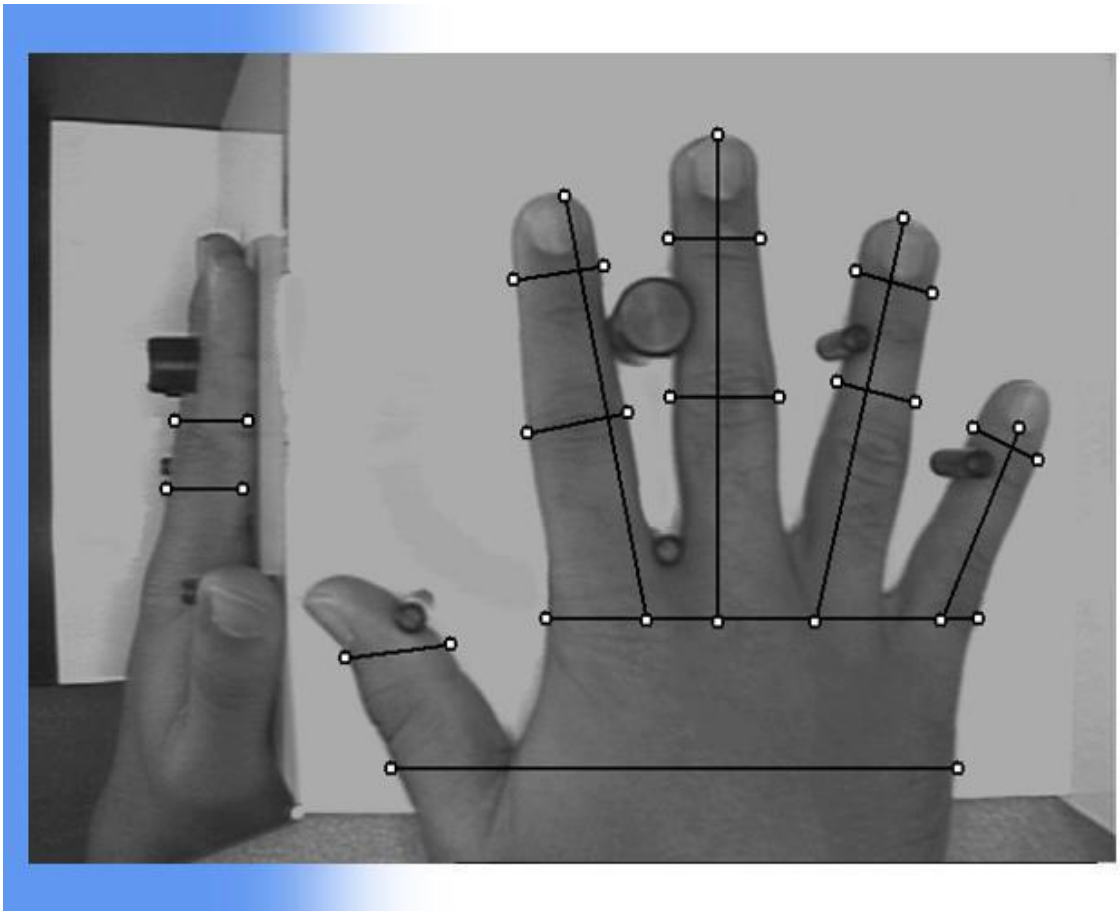

Figure 1.4 Hand Measurement

1.3.1.4 Iris Scan

The colored part of the eye is called the iris. It will control the light levels inside the eye similar to the aperture (the space through which light passes in an optical or photographic instrument, especially the variable opening by which light enters a camera). The round opening in the center of the iris is the pupil. The iris are embedded with tiny muscles that dilate (widen) and constrict (narrow) the pupil size. The sphincter muscle lies around the very edge of the pupil. In bright light, the sphincter contracts, causing the pupil to constrict. The dilator muscle runs radially through the iris, like spokes on a wheel. This muscle dilates the eye in dim lighting. The iris are flat and divides the front of the eye (anterior chamber) from the back of the eye (posterior

chamber). Its color comes from microscopic pigment cells called melanin. The color, texture, and patterns of each person's iris are as unique as a fingerprint.[10] Figure 1.5 show step by step on how iris recognition work. First, the scanner will read from outer iris inward to pupil edge then the scanner plots distinct markings on iris and maps unique shape. After plotting many marks within the iris, all data will be saved to a database. Other scanners will compare this data to verify individual identities.

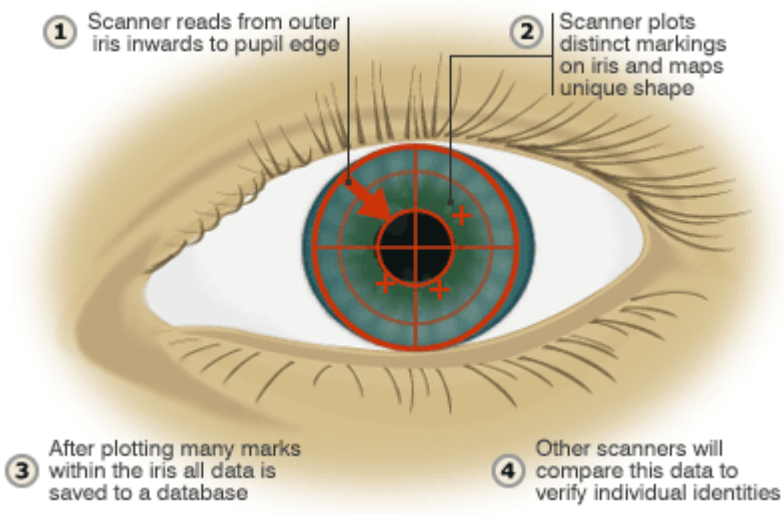

Figure 1.5 Iris Recognition

1.3.2 Behavioral Biometrics

This category of biometrics is temporal in nature. They are evolved during the lifetime of an individual. It involves measuring the way in which an individual performs certain tasks. Behavioral biometrics include

- Gait
- Handwriting
- Speech
- Signature

1.3.2.1 Gait

Gait-based recognition involves identifying a person's walking style. Although these systems are currently very limited, there is a significant amount of research being conducted in this area. Furthermore, studies have shown that gait changes over time and is also affected by clothes, footwear, walking surfaces, and other conditions. Figure 1.6 outlines the various stages of a gait cycle.

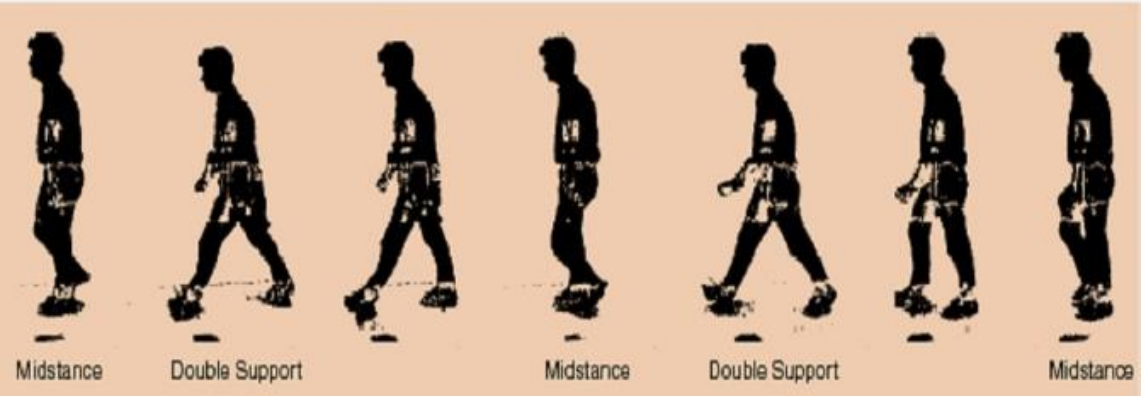

Figure 1.6 Stages of Gait Cycle

1.3.3 Chemical Biometrics

This is a new emerging field. It involves measuring of chemical or biological composition of an individual different body parts such as

- DNA
- Blood glucose

1.4 Multi biometrics systems

There are several other techniques aimed at improving the performance of a biometric system, as outlined in Figure 1.7.