# UNIVERSITI TEKNIKAL MALAYSIA MELAKA

## SYSTEM DEVELOPMENT OF AN INITIATION SEQUENCE USING FACE RECOGNITION TECHNOLOGY

This report submitted in accordance with requirement of the Universiti Teknikal Malaysia Melaka (UTeM) for the Bachelor Degree of Manufacturing Engineering (Robotic and Automation) with Honours.

by

**AHMAD FIRDAUS BIN MOHD AZMI**

FACULTY OF MANUFACTURING ENGINEERING
2010

# UNIVERSITI TEKNIKAL MALAYSIA MELAKA

## BORANG PENGESAHAN STATUS TESIS*

JUDUL: **SYSTEM DEVELOPMENT OF AN INITIATION SEQUENCE USING FACE RECOGNITION TECHNOLOGY**

SESI PENGAJIAN: 2009-2010

Saya AHMAD FIRDAUS BIN MOHD AZMI

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka (UTeM) dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hak milik Universiti Teknikal Malaysia Melaka .
2. Perpustakaan Universiti Teknikal Malaysia Melaka 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 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:

_____ _____

(AHMAD FIRDAUS BIN MOHD AZMI) (AHMAD YUSAIRI BIN BANI HASHIM)

Alamat Tetap: Cop Rasmi:

_____

_____

_____

Tarikh: _____ Tarikh: _____

* Tesis dimaksudkan sebagai tesis bagi Ijazah Doktor Falsafah dan Sarjana secara penyelidikan, atau disertasi bagi pengajian secara kerja kursus dan penyelidikan, atau Laporan Projek Sarjana Muda (PSM).
** 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.

# DECLARATION

I hereby, declared this report entitled "System Development of An Initiation Sequence Using Face Recognition Technology" is the results of my own research except as cited in references.

Signature : .....

Author's Name : AHMAD FIRDAUS BIN MOHD AZMI

Date : .....

# APPROVAL

This report is submitted to the Faculty of Manufacturing Engineering of UTeM as a partial fulfillment of the requirements for the degree of Bachelor of Manufacturing Engineering (Robotic and Automation) with Honours. The member of the supervisory committee is as follow:

……

Supervisor

( En. Ahmad Yusairi Bin Bani Hashim)

Faculty of Manufacturing Engineering

(Official Samp and Date)

# ABSTRACT

Facial recognition had gained increasing interest in the recent decade. Over the years there have been several techniques that being developed to achieve high success rate of accuracy in the identification and verification of individuals for authentication in security systems. This project show the concept of using face recognition technology in order to develop a system of an initiation sequence in a specific application with its own limitations, example security system of industrial machine. The approach of this project is to conceptualize by simulation of the various processes involved in developing an implement able system.

# ABSTRAK

Dalam masa singkat kebelakangan ini pengenalan muka (facial recognition) telah banyak menerima tumpuan. Beberapa teknik atau cara telah dikaji dan dibangunkan untuk mencapai tahap ketepatan dengan kadar kejayaan yang tinggi dalam usaha mengenalpasti seseorang individu untuk diberi kebenaran laluan dalam sistem-sistem keselamatan. Projek ini telah menyelidiki konsep yang menggunakan Face Recognition teknologi untuk menghasilkan sebuah sistem yang mengikut urutan dalam penggunaan yang tertentu yang mempunyai had-hadnya tersendiri, contohnya sistem kawalan keselamatan bagi mesin-mesin industri. Projek ini tertumpu kepada membuktikan konsep tersebut dengan cara simulasi berbagai proses aturcara yang terlibat dalam sesuatu system yang boleh direka.

# DEDICATION

***To my beloved family especially my parents, my supervisor, my friends.***

# ACKNOWLEDGEMENT

Alhamdulillah thanks to ALLAH all mighty with bless and forgiveness I have finished my paper work for Projek Sarjana Muda in the time period with successfully. I also want to dedicate to my supervisor En. Ahmad Yusairi B. Bani Hashim that gives a lot of guidance and opinion until the project finished. And the last but not least to My parents Mohd Azmi Bin Marzuki and Kamilah Binti Ab. Rashid that give full of support and bless for me to do this project. Thanks also to my entire friend that help me in finished this project.

# TABLE OF CONTENT


Abstract i

Abstrak ii

Dedication iii

Acknowledgement iv

Table of Content v

List of Figures viii

List of Tables xi

**1. INTRODUCTION 1**

1.1 Biometrics for Identification and Verification 1

1.2 Verification vs. Identification 2

1.3 Incentives for Facial Recognition Application in Any Security System 2

1.4 Project Background 4

1.5 Overall Objectives 4

1.6 Problem Statement 5

1.7 Scope 5

**2. LITERATURE REVIEW 6**

2.1 Introduction 6

2.2 Security System 6

2.2.1 History 6

2.2.2 Types of security system 7

2.3 Biometrics System 9

2.3.1 Definitions 9

2.3.2 History 9

2.3.3 Biometric Characteristic 10

2.3.4 Biometric Process 12

2.3.4.1 Biometric Process (refer block diagram) 13

2.3.5 Biometric Technologies 14
2.3.6 Biometric Parameters 15
2.3.7 Process Verification of Biometric 17
2.3.8 Performance 18
2.3.9 Failure of Biometric 19
2.4 Combination of biometric security system 23
2.4.1 Biometric Combination Categories 24
2.5 Face Identification Technology 25
2.5.1 History 25
2.5.2 Process Recognition Face 26
2.5.3 User Observation On Face Recognition 28
2.6 VeriLook 3.1 30
2.6.1 VeriLook Standard SDK and Extended SDK 30
2.6.2 VeriLook Algorithm Features and Capabilities 31
2.6.3 VeriLook 3.1 Reliability 32
2.7 Programming 35
2.7.1 Programming Language 35
2.7.2 Visual Basic 36
2.8 RS232 37
2.8.1 RS232 Circuit 39

**3. METHODOLOGY 40**

3.1 Introduction 40
3.2 Project Development Plan 41
3.3 Gantt Chart 44
3.4 Method of Literature Review 46
3.4.1 Flow of Literature Review 47
3.5 General Concept of Manufacturing Security System; Face Detection Technology 49
3.6 Process of Biometric System 51
3.7 Face Detection Process 52

**4. RESEARCH AND DEVELOPMENT** **55**

4.1 Introduction 55

4.2 Develop Data Using MS Access 55

4.2.1 Design Table 55

4.2.2 Design Form 59

4.3 Develop the interface using Visual Basic.Net 64

4.3.1 Design the interface 64

4.3.2 Make the programmed code 67

4.4 Interface RS232 circuit 79

4.5 Relay SRD-5V DC 83

4.6 Omron Sysmax CP1H 84

**5. RESULT AND DISCUSSION** **85**

5.1 Introduction 85

5.2 Result 85

5.3 Discussion 92

**6. CONCLUSION AND SUGGESTION** **93**

6.1 Conclusion 93

6.2 Suggestion for future work 94

**7. REFERENCES** **96**

# LIST OF FIGURE


| NO | TITLE | PAGE |
|---|---|---|
| 2.1 | Phase level of several type of security system | 8 |
| 2.2 | Classifications of some biometric trait | 11 |
| 2.3 | Biometric Process | 12 |
| 2.4 | Biometric Verification Process | 17 |
| 2.5 | Fingerprint | 19 |
| 2.6 | Voice Fequency | 20 |
| 2.7 | Face Recognition | 20 |
| 2.8 | Iris | 21 |
| 2.9 | Retina | 21 |
| 2.10 | Palm Vein Identification | 22 |
| 2.11 | Signature | 22 |
| 2.12 | Widow Peak | 26 |
| 2.13 | Face Position | 31 |
| 2.14 | FRR vs FAR | 33 |
| 2.15 | Active X | 36 |
| 2.16 | VB.Net | 37 |
| 2.17 | Serial Port De-9 | 38 |
| 2.18 | Pin DE-9 | 38 |
| 2.19 | USB-RS232 cable | 39 |
| 2.20 | RS232 Circuit | 40 |
| 2.21 | Omron Sysmax CP1H | 41 |
| 3.1 | Project Development | 44 |
| 3.2 | Method of Literature Review | 48 |
| 3.3 | Flow of literature review | 49 |
| 3.4 | General Concept of Manufacturing Security System; Face Detection Technology | 51 |
| 3.5 | Process of Biometric System | 53 |

| NO | TITLE | PAGE |
|---|---|---|
| 3.6 | Face Detection Process | 54 |
| 4.1 | Wizard | 56 |
| 4.2 | Table Wizard | 56 |
| 4.3 | Rename Field | 57 |
| 4.4 | Data for the table | 58 |
| 4.5 | Database Table | 58 |
| 4.6 | Form Wizard | 59 |
| 4.7 | Form Wizard | 60 |
| 4.8 | Form Selection | 61 |
| 4.9 | Change Form Wizard | 61 |
| 4.10 | Modify Form | 62 |
| 4.11 | Database Form | 63 |
| 4.12 | Database Table | 63 |
| 4.13 | New Project Command Windows | 64 |
| 4.14 | Blank form | 66 |
| 4.15 | Interface Form | 66 |
| 4.16 | Add Existing Item | 67 |
| 4.17 | Starting Form | 67 |
| 4.18 | Coding Form | 68 |
| 4.19 | Form 2 | 69 |
| 4.20 | Coding Form 2 | 70 |
| 4.21 | Modification of Coding | 71 |
| 4.22 | Face detection process | 72 |
| 4.23 | Verification Process | 72 |
| 4.24 | Device Form | 73 |
| 4.25 | Device Form Coding | 73 |
| 4.26 | Enroll Form | 74 |
| 4.27 | Verification Process | 77 |
| 4.28 | RS232 Form | 77 |
| 4.29 | Serial Port Attached | 78 |

| NO | TITLE | PAGE |
|---|---|---|
| 4.30 | Serial Port | 78 |
| 4.31 | Properties of Serial port | 78 |
| 4.32 | USB-RS232 | 79 |
| 4.33 | RS232 circuit | 79 |
| 4.34 | Relay Circuit | 83 |
| 4.35 | Omron Sysmax CP1H PLC | 84 |
| 5.1 | Main Form | 86 |
| 5.2 | Form 2 | 87 |
| 5.3 | Device Form | 87 |
| 5.4 | Matching Form | 88 |
| 5.5 | Enroll Form | 89 |
| 5.6 | Error Message Box | 89 |
| 5.7 | Database | 89 |
| 5.8 | Successful Message box | 90 |
| 5.9 | Matching Process | 90 |
| 5.10 | Verification Success | 91 |
| 5.11 | Verification Success | 91 |
| 5.12 | Verification Success | 91 |
| 6.1 | Combined System | 94 |
| 6.2 | Booth System | 95 |

# LIST OF TABLE


| NO | TITLE | PAGE |
|---|---|---|
| 2.1 | Comparison of various biometric technologies | 16 |
| 2.2 | Specification of VeriLook 3.2 | 34 |
| 2.3 | DE9 Pin | 39 |
| 3.1 | Gantt Chart PSM 1 | 46 |
| 3.2 | Gantt Chart PSM | 47 |

# CHAPTER 1
# INTRODUCTION

This chapter focuses on the introduction of the project. Introduction of the project includes biometrics for identification and verification, verification versus identification, incentives for facial recognition application in any security system, project background, objective, problem statement and scope of this project.

## 1.1 Biometrics for Identification and Verification

Biometrics is an emerging set of pattern-recognition technologies which accurately and automatically identifies or verifies individuals based upon each person's unique physical or behavioural characteristics. Identification using biometrics has advantages over traditional methods involving ID Cards (tokens) or PIN numbers (passwords) in that the person to be identified is required to be physically present where identification is required and there is no need for remembering a password or carrying a token. PINs or passwords may be forgotten, and tokens like passports and driver's licenses may be forged, stolen, or lost. Biometrics methods work by unobtrusively matching patterns of live individuals in real-time against enrolled records. Biometric templates cannot be reverse-engineered to recreate personal information and they cannot be stolen and used to access personal information. Because of these inherent attributes, biometrics is an effective means to secure privacy and deter identity theft. Various biometric traits are being used for real-time recognition, the most popular being face, iris and fingerprint. Other biometric systems which have found their usefulness are based on retinal scan, voice, signature and hand geometry. By using them together with existing

tokens, passwords and keys, biometric systems are being deployed to enhance security and reduce fraud. In designing a practical biometric system, a user must first be enrolled in the system so that his biometric template can be captured. This template is securely stored in a central database or a smart card issued to him. The template is retrieved when an individual needs to be identified. Depending on the context, a biometric system can operate either in verification (authentication) or identification mode (Ritikos, 2007).

## 1.2 Verification Versus Identification

There are two different ways to recognize a person: verification and identification. Verification (answers the question "Am I who I claim I am?") involves confirming or denying a person's claimed identity. In identification, the system has to recognize a person (addressing the question "Who am I?") from a list of *N* users in the template database. Identification is a more challenging problem because it involves 1:N matching compared to 1:1 matching for verification.

## 1.3 Incentives for Facial Recognition Application in Any Security System

Research on automatic face recognition in images has rapidly developed into several inter-related lines, and this research has both lead to and been driven by a disparate and expanding set of commercial applications. The large number of research activities is evident in the growing number of scientific communications published on subjects related to face processing and recognition. Anti-theft devices are not foolproof, but they can a deterrent or to slow down the process.

In a biometric security system, the objective is to authenticate a user being an authorised person to have access to the ignition system. It could be a first step before ignition could commence or it could be an integrated system for auto ignition subsequent to authorisation being cleared. A progression from the now common keyless fob used to open a machine or vehicle, there is a recent successful commercial implementation of

biometric for authorisation, in the form of fingerprint recognition. This, however, does have its own weaknesses, such as the one depicted by a report by BBC News on 31 March 2005 of a local robbery incident where the owner's finger was sliced off the end of his index finger with a machete. Potential applications of biometrics in security system are for private vehicles, industrial machine and other else. (BBC News, 2005)

Because of its many advantages, biometrics is fast being used for physical access control, computer log-in, welfare disbursement, international border crossing (e-Passports) and national ID cards, verification of customers during transactions conducted via telephone and Internet (e-Commerce and e-Banking). For example, in automobiles, biometrics is being adopted to replace keys for keyless entry and keyless ignition. Here are some commercially available products for such vehicle access and starting applications

| **Product name** | **Biometrics method** |
|---|---|
| Identisafe-09 | Fingerprint |
| Retinasafe-18 | Eyeball Recognition |
| Brainsafe-72 | Brain fingerprinting |
| Voicesafe-36 | Voice |
| Think-Start-99 | Brain waves |

There is much interest in using FR for security systems due to it advantages for the above listed methods. These will be explained in the next chapter. Among some advantages of Facial Recognition method for security application are:-

(i) more convenient, no active part of user; sensed as soon as one is seated in position (and facing the camera).

(ii) low risk scenario (failure means loss of one vehicle, compared to loss to company properties & confidential materials, national security and safety).

## 1.4 Project Background

This project is develop in order to make a security system that can identify only a personal person that can operating one machine that have been specific to them. This system will identify the person that want to produce the product, repairing the machine or change the data type of the machine by referring to the database. In this security system, all the data interface between human and machine will be collect in systematic order. All the data that want to identify the person are in biometric type.

In order to simulate this project, we change the machine with PLC. We hope our system can be work and success to trigger the signal at PLC power system. We optimize that these project will become the new project which can be applied to security system industry.

## 1.5 Overall Objectives

The objectives of this project are to:-

- Identify the problem of security system.
- Build an interface system using Visual Basic. Net software
- Design the system that link the interface with verilook3.1 software.
- Test the output to trigger PLC by using RS232.

## 1.6 Problem Statement

Nowadays, all manufacturing product are base on automation system**.** That's means all command or data type of the product must be put into the product in order to make it automatic. Because of that we have to create security system of the product in order to avoid any hackers or person who wants to destroy the data or the machine. In this day and age, existence security systems that are not good enough and not integrate with several others of security system in order to make a security system that was good enough.

With make a system with some security that has been integrated, it will difficult to the person to access by using another person. Using finger print and face recognition will avoid any hackers' activity.

This system will classified the user for some level for some work that is:

- level 1: Operator
- level 2: Repairing the machine
- level 3: Change the data type

All the security level can be suitable with any company.

## 1.7 Scope

The scope of this project includes:-

- Build a security system that use face recognition that can accept the data type.
- Manage the output so that it can been carry by the agent to the database
- Want to prove that this system can be use as security system in order to realize the objective.

# CHAPTER 2
# LITERATURE REVIEW

This chapter focuses on the data collection from various resources for the project. All data was collect and sort in order to make this project run properly.

## 2.1 Introduction

Several literature reviews have been done in order to build this security system. It want to make this project can be done with successfully. All sources from internet and journal from library have been study in order to give illustration how to develop this system. Its also want to choose suitable program and application that want to use.

## 2.2 Security System

### 2.2.1 History

Various types of system security have long existed since a concern over private property has existed. Early security system, despite not advanced compared to modern security systems that use advanced technologies, however effective in getting people and property. For example, a common security measures to palaces and forts is to place buildings on the edge of a high slope. With a building can not be passed three times, it becomes easier to defend against intruders. Defense against attack is only important in

one part of the building, victory more likely for high available. Modern security systems mostly rely on technology to protect their area. Many houses, business buildings, stores, and government offices using electronic security systems to protect against intruders. System security has become more prolific as the technology became more advanced and less expensive to implement. Although security is largely composed of modern defense technology, the system can use several technologies together to maximize the safety of physical defenses (Fillippini, 1998).

### 2.2.2 Types of security system

The types of security systems that are present contain several types:-

a) Keyboard (password) is the type of the most popular and least expensive. It is easy to use but less secure, because users can post code entry or share it with others. Different card systems, the code can not be shared or copied, and your safety is more assured.
b) Smart Card is also famous. The cards, which need to be brought, near the detector to detect and it is divided into several types that have a bar code, magnetic stripe, and the card has a chip. When the card is lost, it is one thing that makes it easy to deactivate them and issue a new card to replace the lost.
c) Biometrics system is a system which includes the fingerprint sensor, sound sensor, and scanner face or eyes. This system is far better safety compared with the control of other security systems. However, this system is also very expensive and intruders can force users to use for coercion. This shows that this system also has some disadvantages compared with other methods.

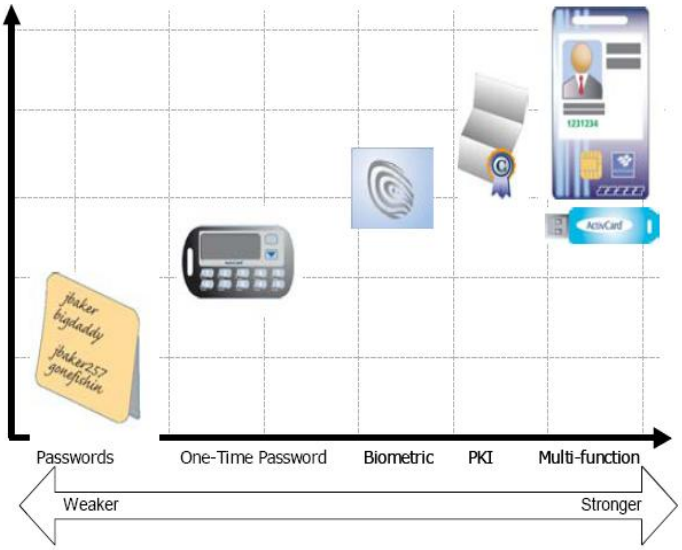


**Figure 2.1:** Phase level of several type of security system (wicker, 2000).

## 2.3 Biometrics System

### 2.3.1 Definitions

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 fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. Biometric physiological are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, hand and palm geometry, iris recognition, which has largely replaced retina, and odor/scent. Biometric behavioral are related to the behavior of a person. Examples include, but are not limited to typing rhythm, gait, and voice. Some researchers have coined the term behavior metrics for this class of biometrics. Strictly speaking, *voice* is also a physiological trait because every person has a different vocal tract, but voice recognition is mainly based on the study of the way a person speaks, commonly classified as behavioral.

### 2.3.2 History

Biometrics comes from ancient Greek: *bios* mean "life" and *metron* mean "measure". It was refers to two very different fields of study and application. The first, which is the older and is used in biological studies, including forestry, is the collection, synthesis, analysis and management of quantitative data on biological communities such as forests. Biometrics in reference to biological sciences has been studied and applied for several generations and is somewhat simply viewed as "biological statistics." More recently and incongruently, the term's meaning has been broadened to include the study of methods for uniquely recognizing humans based upon one or more intrinsic physical