UNIVERSITI TEKNIKAL MALAYSIA MELAKA

The Application Of Voice Verification For Security System

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

MOHD SYAUQEE BIN MOHD

FACULTY OF MANUFACTURING ENGINEERING

2009

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS TESIS*

JUDUL: The Application Of Voice Verification For Security System

SESI PENGAJIAN: 2009-2010

Saya MOHD SYAUQEE BIN MOHD

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:

(MOHD SYAUQEE BIN MOHD) (RUZAIDI BIN ZAMRI)

Alamat Tetap:
NO 65, KAMPUNG HILIR
06200 KEPALA BATAS
ALOR SETAR, KEDAH

Cop Rasmi:
RUZAIDI BIN ZAMRI
Pensyarah
Fakulti Kejuruteraan Pembuatan
Universiti Teknikal Malaysia Melaka
Karung Berkunci 1200, Ayer Keroh
75450 Melaka

Tarikh: 17/5/2010

Tarikh: 17/5/2010

* 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.

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:

....
(Mr. Ruzaidi Bin Zamri)

DECLARATION

I hereby, declared this report entitled “The Application Of Voice Verification For Security System” is the results of my own research except as cited in references.

Signature : ....

Author’s Name : MOHD SYAUQEE BIN MOHD

Date : ....

ABSTRACT

Security system is the most important method to prevent homes from being intruded. Biometrics is applied to this security system as the key because of the increasing popularity. The conventional methods that are currently used for home security system have many weaknesses. Therefore, this project is developed so that the invasion could not be done easily. This project applies the voice verification as the key to home security systems. Matlab software is used for the development of this security system in this project. This project also uses equipment such as servo motor for the system designing.

ABSTRAK

Sistem keselamatan adalah kaedah paling penting untuk mengelakkan rumah daripada diceroboh. Biometrik diaplikasikan pada sistem keselamatan ini sebagai kunci kerana peningkatan popularitinya. Kaedah konvensional yang digunakan pada masa ini sebagai system keselamatan rumah mempunyai banyak kelemahan. Oleh sebab itu, projek ini dibangunkan supaya pencerobohan tidak boleh dilakukan dengan mudah. Projek ini mengaplikasikan pengesahan suara sebagai kunci untuk sistem keselamatan rumah. Perisian MatLab digunakan untuk pembangunan sistem keselamatan di dalam projek ini. Projek ini juga menggunakan peralatan elektrik seperti motor untuk rekaan sistem ini.

DEDICATION

To our beloved parents, thank to all the help and love given. To all my friends and lecturers who always cooperate and help that is not infinite, your support

is greatly appreciated until the end of life.

May Allah bless u all.

ACKNOWLEDGEMENT

First of all I would like to take this opportunity to say millions of thanks to my supervisor Mr. Ruzaidi bin Zamri who had been providing assistance and contribution ideas throughout the process to prepare this project.

In addition, I also want to take this opportunity to thanks to all my friends who have helped in preparing this project from the aspect of ideas, teaching, technical assistance, and anything that allows me to complete this project. And not forgotten to my panel, Mr. Shariman and Mr. Ahmad Yusairi.

Finally, I would also like to thank to my parents, brothers sisters and also to anyone who has been involved in the process to complete this project either directly or indirectly.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Background

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.

Voice is a part of human biometric. Voice pattern is unique for each person. Since voice is a natural phenomenon, it is very easy to be used in a daily life compared to other biometric like iris, fingerprint, and face and to name but a few.

Voice as a biometric can be separated in two parts, namely voice verification and voice recognition. Voice verification and voice recognition are the different voice system although the two are often confused. Voice verification verifies the vocal characteristic from a specific person while voice recognition is used to translate the spoken word into a specific response.

Voice verification is text dependent, meaning the caller must state a specific word, phrase or digit sequence in order to be verified. Voice verification receives spoken keywords/passwords from a specific user through a microphone. Voice verification is conceptually similar to fingerprint. It is common knowledge that each person's fingerprints have unique characteristics that can be used to distinguish one person to another. It has also been proven that each person can be identified by the unique features of his or her vocal characteristic and speaking pattern.

Biometric voice verification is the process of comparing a voice sample with a stored, digital voice model, or voiceprint, for the purpose of verifying identity. A voiceprint is a digital representation of some of the unique characteristics of a caller's voice, including physiological characteristics of the nasal passages and vocal chords, as well as the frequency, cadence and duration of the vocal pattern. A voiceprint is not a recording or sound file – it cannot be played back into a voice biometrics system by an imposter.

Voice recognition is to understand the spoken word and cannot identify the identity of the speaker. A familiar example of voice recognition system is that of an automated call center asking a user to "press number one on his/her phone keypad" or "say the word 'one'." In this case, the system does not verify the identity of the person who says the word "one"; it is only checking that the word "one" was said.

An individual's biometric features such as fingerprints, retinal patterns, and facial features, but an individual's speech pattern has more unique qualities and is often recognized as the most natural form of biometrics. The human voice is also considered the most common form of communication and is an ideal form of personal identification, because your voice can never be lost, stolen or shared without your knowledge.

1.2 Problem Statement

Today, biometric is a popular method used as a security system. Conventional methods for automated personal identification or identity verification mainly rely on something a person must have such as a token, key or a card and something to be memorized like Personal Identification Numbers (PIN) or a password. However, this method brings a certain level of security, users suffer conceptual flaws since tokens can be lost or stolen while PIN and passwords can be forgotten or guessed by unauthorized users.

In today's world, there are always people wanting to steal and copy information. Security system goal is to keep unauthorized users from maliciously destroying and altering resources. Security is not an absolute way to keep these malicious acts from occurring; it simply makes it much more difficult.

The use of voice identification as a 'security key' is more applicable to replace the existing conventional domestic security system.

1.3 Project Aim and Objectives

The objective of this project is:

- To develop security system using voice verification system
- To identify typical plan in designing the system
- To develop a programme for voice verification system by using MatLab software

1.4 Scope

The project will cover the application of voice verification system as the "door key" to the house main entrance.

- using electric equipment such as servo motor
- develop programme using MatLab software

CHAPTER 2

LITERATURE REVIEW

Biometrics is used as an automated security system to determine or verify identity through physiological or behavioral characteristics. This task is done with the use of automated databases that store small and large amounts of biometric records. There are many advantages to the usage of biometrics over previous and comparable technologies. Although, because of some of the heavy debates that surround the issue of biometrics, it has not come into common use, yet. At this point, the government and other highly secure entities are the main parties to utilize the benefits the biometrics technology. Biometrics has been in the workings for quite a while now, but there still remains much research to be done.

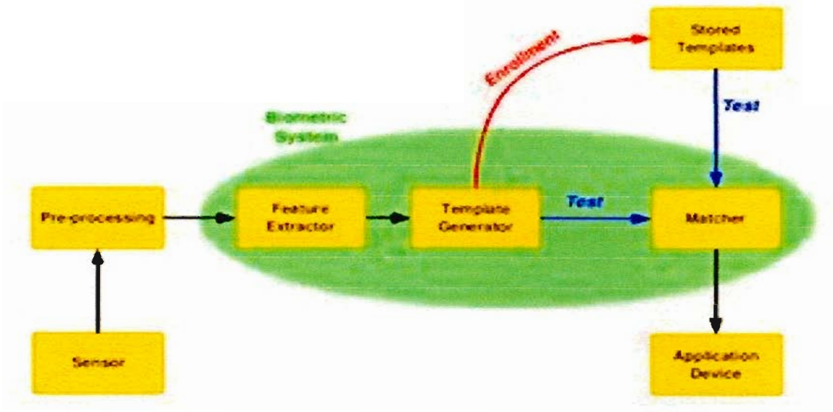

Figure 2.1: General biometrics block diagram. (http://myesbe.blogspot.com/)

2.1 Automated Personal Identification

The information age is quickly revolutionizing the way transactions are completed. Everyday actions are increasingly being handled electronically, instead of using pencil and paper or via face to face interaction. This growth in electronic transactions has resulted in a greater demand for fast and accurate automatic user identification and authentication. (Braghin, 2003)

Traditionally, two major types of automatic personal identification approaches have been used: *knowledge-based* and *token-based.* Knowledge-based approaches use "something you know" to identify you, such as passwords. Token-based approaches use "something you have" to recognize you, such as smart cards, magnetic stripe cards and physical keys. The weakness of these systems is the fact that passwords can be forgotten, shared, or observed and tokens can be lost, stolen, duplicated, or left at home. In addition, these systems are unable to differentiate between an authorized person or an impostor using the token or the knowledge fraudulently acquired from the authorized person. The banking industry reports that false acceptances at Automatic Teller Machines (ATM) are as high as 30 percent, resulting in worldwide financial fraud of $2.98 billion a year. MasterCard alone reports over $1.2 million in fraudulent ATM losses every day. (Braghin, 2003)

Another personal identification approach is biometrics. Biometric technologies are automated methods of recognizing a person based on a physiological or behavioral characteristic. Examples of human traits physical characteristics used for biometric recognition include fingerprints, speech, face, retina, iris, handwritten signature, hand geometry, and wrist veins. Using biometrics for identifying and authenticating human beings ensure much greater security, basing the identification on an intrinsic part of a human being. In a way, you are your own password. (Braghin, 2003)

Biometric techniques have been used a lot in the past for criminal identification and prison security, but since the technology is rapidly evolving, with low cost and high accuracy, it is currently in consideration for adoption in a broad range of civilian applications, like financial transaction and control access to secure areas. While biometrics is not an identification panacea, it is beginning to provide very powerful tools for the problems requiring positive identification. As the technology becomes more economically viable, technically perfected and widely deployed, we can expect biometrics to become the passwords of the twenty-first century. (Braghin, 2003)

2.2 Biometric

Biometrics refers to an automated system that can identify an individual by measuring their physical and behavioral uniqueness or patterns, and comparing it to those on record. In other words, instead of requiring personal identification cards, magnetic cards, keys or passwords, biometrics can identify fingerprints, face, iris, palm prints, signature, DNA, or retinas of an individual for easy and convenient verification.

With the boom in Internet-based business and the increased need for accurate verification when accessing accounts, biometrics is the simplest and most convenient the solution. Its universal, unique, permanent and measurable features ensure security of information in E-commerce, such as on-line banking and shopping malls. Biometrics can also provide you with convenience and security, by enabling a machine to verify the individual by itself and to respond to the individual's requests. Through the use of such physical controls as access control, and punch card maintenance, user restrictions on certain apparatus can be made possible with an automated verification system. (www.exsight.com)

Biometrics is the automated method of recognizing a person based on a physiological or behavioral characteristic. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. Biometric characteristics can be divided in two main classes that are physiological and behavioral. 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. Behavioral are related to the behavior of a person. Examples include, but are not limited to typing rhythm, gait, and voice. (www.wikipedia.org).

Some researchers have coined the term behaviometrics for this class of biometrics. Firmly 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. A biometric system can operate in the following two modes that are verification and identification. Verification is a one to one comparison of a captured biometric with a stored template to verify that the individual is who he claims to be. It can be done in conjunction with a smart card, username or ID number. Identification is a one to a many comparisons of the captured biometric against a biometric database in attempt to identify an unknown individual. The identification