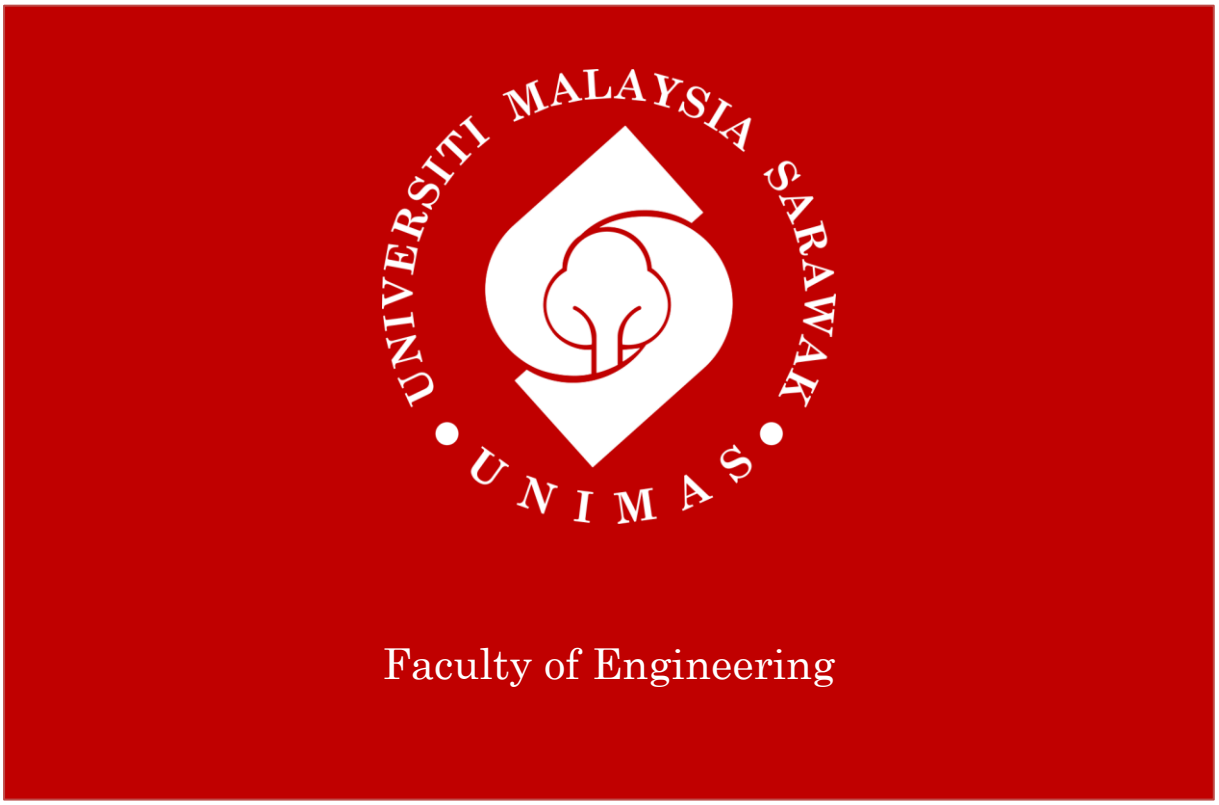


PERSON IDENTIFICATION BASED ON MULTIMODAL BIOMETRIC RECOGNITION

Alex Ng Ho Lian

Bachelor of Engineering with Honours in
Electronics (Telecommunications)
2019/2020

UNIVERSITI MALAYSIA SARAWAK

Grade: _____

Please tick (√)

Final Year Project Report ☑

Masters ☐

PhD ☐

DECLARATION OF ORIGINAL WORK

This declaration is made on the 28 day of August 2020.

Student's Declaration:

I **ALEX NG HO LIAN (55399), FACULTY OF ENGINEERING** hereby declare that the work entitled **PERSON IDENTIFICATION BASED ON MULTIMODAL BIOMETRIC RECOGNITION** is my original work. I have not copied from any other students' work or from any other sources except where due reference or acknowledgement is made explicitly in the text, nor has any part been written for me by another person.

28/08/2020 — Date submitted

ALEX NG HO LIAN(55399) — Name of the student (Matric No.)

Supervisor's Declaration:

I **DR. ANNIE ANAK JOSEPH** hereby certifies that the work entitled **PERSON IDENTIFICATION BASED ON MULTIMODAL BIOMETRIC RECOGNITION** was prepared by the above named student, and was submitted to the "FACULTY" as a * partial/full fulfillment for the conferment of **BACHELOR OF ENGINEERING (HONS) IN ELECTRONICS (TELECOMMUNICATIONS)**, and the aforementioned work, to the best of my knowledge, is the said student's work.

Received for examination by: DR. ANNIE ANAK JOSEPH (Name of the supervisor) Date: 28/08/2020

I declare that Project/Thesis is classified as (Please tick (√)):

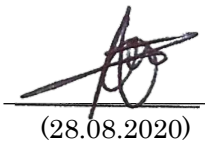
☐ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1972)*
☐ **RESTRICTED** (Contains restricted information as specified by the organisation where research was done)*
☑ **OPEN ACCESS**

Validation of Project/Thesis

I therefore duly affirmed with free consent and willingness declare that this said Project/Thesis shall be placed officially in the Centre for Academic Information Services with the abiding interest and rights as follows:

- This Project/Thesis is the sole legal property of Universiti Malaysia Sarawak (UNIMAS).
- The Centre for Academic Information Services has the lawful right to make copies for the purpose of academic and research only and not for other purpose.
- The Centre for Academic Information Services has the lawful right to digitalise the content for the Local Content Database.
- The Centre for Academic Information Services has the lawful right to make copies of the Project/Thesis for academic exchange between Higher Learning Institute.
- No dispute or any claim shall arise from the student itself neither third party on this Project/Thesis once it becomes the sole property of UNIMAS.
- This Project/Thesis or any material, data and information related to it shall not be distributed, published or disclosed to any party by the student except with UNIMAS permission.

Student signature Alex (28.08.2020)

Supervisor signature:  (28.08.2020)

Current Address: LOT 202, JALAN HILLTOP UATAMA, TAMAN HILLTOP, 98000 MIRI, SARAWAK

Notes: * If the Project/Thesis is **CONFIDENTIAL** or **RESTRICTED**, please attach together as annexure a letter from the organisation with the period and reasons of confidentiality and restriction.

[The instrument is duly prepared by The Centre for Academic Information Services]

PERSON IDENTIFICATION BASED ON MULTIMODAL BIOMETRIC RECOGNITION

ALEX NG HO LIAN

A final year project report submitted in partial fulfilment of
the requirement for the degree of
Bachelor of Engineering (Hons) in Electronics (Telecommunications)

Faculty of Engineering
Universiti Malaysia Sarawak

2020

ACKNOWLEDGMENT

First and foremost, I gratefully thanks to my supervisor, Dr. Annie Anak Joseph her generous support, comments, advice, and guidance throughout the duration of my project. Thanks to the lecturers at the Faculty of Engineering of UNIMAS for their support. Without them, this project would not be the same as presented here.

A lot of thanks also to my friends as well as those who shared their thoughts on this project, for their constant kind help, and moral support despite the hectic semester that I had undergo.

Last but not least, my deepest appreciation to our parents, for their co-operation, support, love, patient, and care throughout this project. Your fully support and encouragement is gratefully appreciated.

ABSTRACT

Unimodal biometric systems have limited effectiveness in identifying people, mainly due to their susceptibility to changes in individual biometric features and presentation attacks. The identification of people using multimodal biometric systems attracts researchers' attention due to their advantages, such as greater recognition efficiency and greater security compared to the unimodal biometric system. A multimodal biometric system can overcome various unimodal biometric systems' limitations, so it is suitable and recommended use for this society. In this project, face and fingerprint recognition are used to develop a multimodal biometric system. In the process of face recognition, Classic Convolutional Neural Network (CNN) is used for training face datasets. After done training face dataset, the testing process is needed to recognize a face with face dataset. In the process of fingerprint recognition, the ORB algorithm is recommended to use in feature matching. ORB (Oriented FAST and Rotated BRIEF) algorithm consists of 3 stages: feature point extraction, defining feature point descriptors, and computing feature point matching. For these three stages, the fingerprint image is matching with the fingerprint database. For the process of fusion of face and fingerprint recognition, two features are fused by match score level fusion based on Weighted Sum-Rule. If the fusion score is higher than the threshold level is given, then the verification process is matched. The result of accuracy is displayed if the user selects the same biometric characteristics for both recognition. If the fusion score is less than the threshold level, then the verification process indicates a mismatch. The result of accuracy will not be displayed if the user selects different biometric characteristics for both recognition.

ABSTRAK

Sistem biometrik unimodal mempunyai keberkesanan terhad dalam mengenal pasti orang, terutamanya kerana kerentanan mereka terhadap perubahan ciri biometrik individu dan serangan persembahan. Pengenalpastian orang yang menggunakan sistem biometrik multimodal menarik perhatian penyelidik kerana kelebihannya, seperti kecekapan pengiktirafan dan keselamatan yang lebih besar berbanding sistem biometrik unimodal. Sistem biometrik multimodal dapat mengatasi pelbagai batasan sistem biometrik unimodal, jadi penggunaannya sesuai dan disarankan untuk masyarakat ini. Dalam projek ini, pengecaman wajah dan cap jari digunakan untuk mengembangkan sistem biometrik multimodal. Dalam proses pengecaman wajah, Rangkaian Neural Konvolusional Klasik (CNN) digunakan untuk melatih set data wajah. Setelah selesai membuat set data wajah, proses ujian diperlukan untuk mengenali set data wajah dengan wajah. Dalam proses pengecaman cap jari, algoritma ORB disarankan untuk digunakan dalam pemadanan ciri. Algoritma ORB (Oriented FAST and Rotated BRIEF) terdiri daripada 3 peringkat: pengekstrakan titik ciri, menentukan deskriptor titik ciri, dan pemadanan titik ciri pengkomputeran. Untuk ketiga tahap ini, gambar cap jari sepadan dengan pangkalan data cap jari. Untuk proses penggabungan wajah dan pengecaman cap jari, dua ciri digabungkan dengan gabungan skor skor pertandingan berdasarkan Jumlah Berat Peraturan. Sekiranya skor gabungan lebih tinggi daripada tahap ambang yang diberikan, maka proses pengesahan sesuai. Hasil ketepatan ditunjukkan jika pengguna memilih ciri biometrik yang sama untuk kedua-dua pengiktirafan. Sekiranya skor peleburan kurang dari tahap ambang, maka proses pengesahan menunjukkan ketidakcocokan. Hasil ketepatan tidak akan ditampilkan jika pengguna memilih ciri biometrik yang berbeza untuk kedua-dua pengiktirafan.

Table of contents

List of Tables

List of Figures

List of Equations

List of Abbreviations

AI	-	Artificial Intelligence
CNN	-	Convolution Neural Network
ORB	-	Oriented FAST and Rotation Briefing
UBS	-	Unimodal Biometric System
MBS	-	Multimodal Biometric System
GUI	-	Graphic User Interface
ERR	-	Equal Error Rate
FAR	-	False Accept Ratio
FRR	-	False Reject Ratio
DCT	-	Discrete Cosine Transform
PCA	-	Principal Component Analysis
ICA	-	Independent Component Analysis
LDA	-	Linear Discriminant Analysis
ILDA	-	Incremental Linear Discriminant Analysis
SVM	-	Support Vector Machine
BGR	-	Blue Green Red
RGB	-	Red Green Blue
FCL	-	Fully Connected Layer
MLP	-	Multi-layer perception

CHAPTER 1

INTRODUCTION

1.1 Research Background

Nowadays, the security system becomes more important than ever because this is an era of industry 4.0. However, some security systems do not use the latest technology, making it easy for unauthorized people to access or invade the system, so it is called traditional security. In the past few years, it has been confirmed that the use of traditional security systems will lead to a rising crime rate of cyber-attacks. These attacks now target industrial espionage, financial crime, and even government and critical infrastructure from time to time. It also has many flaws such as passwords that may be lost, hacked or passed, plastic IDs may be duplicated, and RFID cards can be copied. All these flaws occur because it does not provide strong security in data protection. Therefore, all these problems will be solved in the generation of Industry 4.0. Industry 4.0 generation's focus has shifted to artificial intelligence (AI) applications such as neural networks, machine learning, and deep learning, which define new working cultures in almost all industries. For AI applications, biometric systems can make cybersecurity more effective and respond to growing threats and improve an organization's cybersecurity posture [1]. A biometric system is a technical system used to identify a person with information about him. It provides high accuracy and confident automatic recognition to identify the person based on biometric traits such as hand, finger-vein, iris, face, voice, fingerprint, signature, and keystroke, as shown in Figure 1.1.1. The advantages of using Biometric systems were, it only can be accessed when the user to identify with the recognition devices. It provides a high accessibility system for the user without memorizing the passwords or codes. It makes it difficult for cybercriminals because they really cannot easily access the entry points and devices of the network [2].

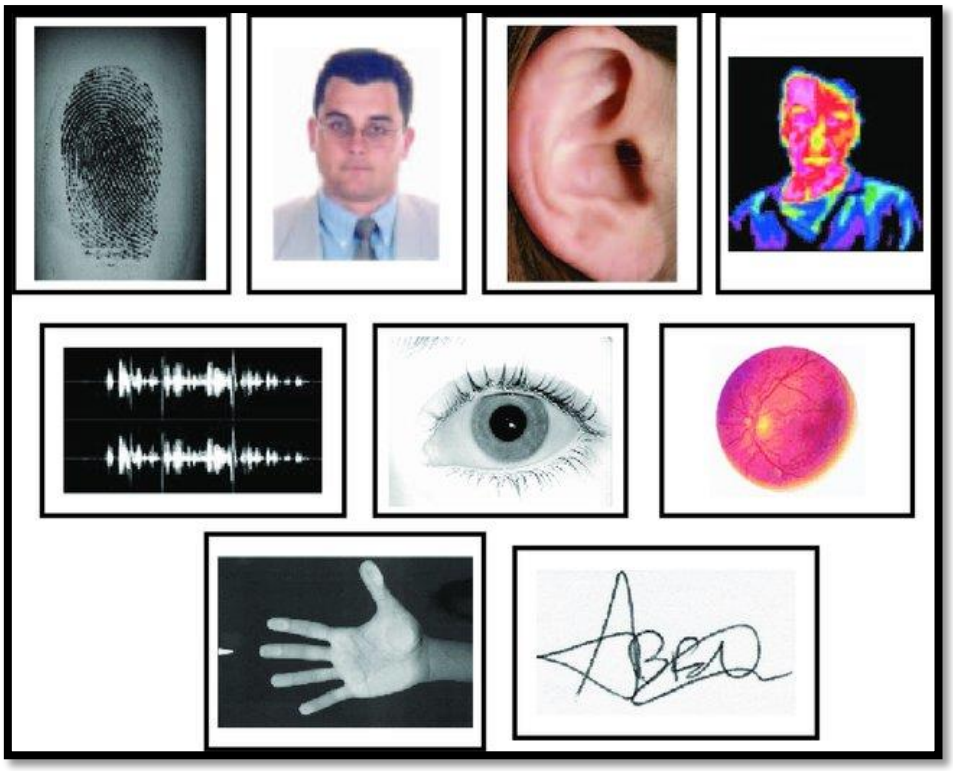


Figure 1.1.1: Biometric System [1]

As shown in Figure 1.1.1, the biometric system has two main characteristics: physiological and behavioral. Physiological characteristics refer to human traits, such as fingerprint, face, hand, iris recognition, etc. For behavior, it refers to keystrokes, signatures, sounds. It relates to human behavior. However, there are many types of biometric systems, namely Unimodal biometric systems and Multimodal biometric systems. For unimodal biometric systems, they use only one identification function. In contrast, multimodal biometric recognition systems use more than one feature for recognition, involving multiple sensors [2].

With the development of the technological world, the use of biometric technology to implement secure personal identification protocols is facing more and more challenges. In almost every market in the world, there is an increasing demand for targeted identification. The biometric management market has discovered that using a single hardware model for identification in many industries may no longer be the wisest choice. The unimodal biometric identification system must deal with various issues, such as noisy data, non-universality, mutations within the class, uniqueness, and

deceptive attacks. By deploying a multimodal biometric system that integrates multiple biometric patterns in a single scan, some of these limitations are solved, thereby solving an unimodal system's challenge [3].

A multimodal biometric system is a system that can use multiple physiological or behavioral characteristics for registration, identification, and verification. Multimodal biometric recognition has become the latest technology in human attention, and one of the most important reasons for combining different modes is to improve recognition accuracy. There are other reasons for combining two or more biometrics, for example, different biometrics are more suitable for various deployment scenarios, or this fact becomes a reality when security is essential to protect sensitive data [4].

The multimodal biometric system obtains input from multiple biometric identification devices to measure different biometrics traits. For example, combining faces and fingerprints for biometric identification is called a multimodal biometric system, even if different facial and fingerprint images are acquired through different devices or the same biometric identification. There is no need to combine various indicators mathematically, because the biological characteristics are always independent of each other, which can improve the accuracy of identifying people [3].

There are some advantages of multimodal biometric system as shows [2]:

- Accuracy: Multi-pattern biometrics uses multiple patterns to identify people who can ensure higher accuracy.
- Security: The multi-mode biometric identification system improves security by eliminating the possibility of spoofing. It is impossible for one to deceive multiple biological characteristics at once.
- Activity detection: The multi-mode biometric identification system requires end users to randomly submit multiple biometrics to ensure reliable activity detection to prevent fraud or hacking.
- Universality: The multimodal biometric system is universal; even if the disabled person cannot provide some form of biometric information, other forms of biometric information can also be used for identity verification.

- Cost-effective: Multi-mode biometric systems reduce the risk of violations or criminal attacks by providing a higher level of security, which is cost-effective.

When the input of the system is destroyed, problems will occur in the unimodal biometric system. The performance of the system will also decrease. Therefore, the multi-mode biometric system can solve the problem and improve the accuracy, and the system will be more difficult to breakthrough. In this project, face and fingerprint recognition will be selected for multi-modal biometric recognition [5].

Face recognition is to identify people related to the face through the scanning process. Because of its use in security systems, video surveillance, access control, business, and even Facebook and other social networks, it has become an essential tool for human-computer interaction. With the development of artificial intelligence, face recognition has attracted people's attention compared with other recognition. It is the primary method of human personal identification. In an uncontrolled environment, face recognition is easily checked, even if the subject cannot understand [5].

Researchers can find that the problem has been solved [5]. Traditional learning methods always faces challenges such as posture changes, facial camouflage, scene lighting, image background complexity, and facial expression changes. Methods based on shallow learning only use some features of the image and rely on artificial experience to extract sample characteristics. Deep learning methods can extract more complex face characteristics. Deep learning has made significant progress in solving the problems that have plagued the AI industry's best attempts for many years. The practice has proved that it is very good at revealing the intricate structure in high-dimensional data, so it is suitable for many fields such as science, business, and government. It uses one or several algorithms to solve the problem of learning hierarchical representation and performs well in natural language processing, semantic segmentation, image recognition, and many other practical scenarios. Deep learning involves some methods, such as deep belief networks (DBN) [6], stacked auto encoders [7], and convolutional neural networks (CNN).

CNN is an algorithm that mostly used in face recognition. CNN is an artificial neural network that uses a convolution technique to extract features from input data.

CNN was first proposed by LeCun and first applied to the recognition of handwriting His network was the origin of many modern constructions and the real inspiration of many scientists. Researchers published their production in the ImageNet contest [8]. It is known as one of the most influential publication figures in the field of computer vision. It also shows that the performance of recognition on CNN is better than that based on manual methods. Besides, with the help of the computing power of the graphics processing unit (GPU), CNN achieved extraordinary cutting-edge results in many fields, including scene recognition, image recognition, edge detection, and semantic segmentation [8].

The overall structure of the face recognition process in this project consists of three steps. For the preprocessing step, it involves color space conversion and image resizing, and then continues to extract facial features, and then classifies the feature set has been extracted. At last, Softmax Classifier is the last stage of classifier the dataset file's name based on the facial features extracted from CNN. Hence, the CNN algorithm will be used in face recognition.

Fingerprints are the most commonly used biometric function in judicial and law worldwide [9]. Today, embedded fingerprint chips used in mobile devices such as smartphones have become common. Fingerprints chips can provide excellent security for various information and memory they save on mobile devices. Nevertheless, the chip size has its limitation, such as cost and space. It can usually only collects a small number of fingerprints at a time.

Therefore, multiple templates are needed combining in the fingerprint enrollment process, so each template includes different parts of the fingerprint. Traditional minutiae fingerprint image requires a large amount of overlapping two fingerprint images in merging technology. However, the fingerprint sensor chip extracts insufficient details at a size of 160 * 160 and dpi 500. Therefore, detail-based technology requires touch sensors to capture many images. At this moment, due to insufficiently detailed features such as endpoints, triangle points, and some detailed comparison algorithms are applied to compare parts of the fingerprint, which significantly reduces the accuracy. Previous researchers have found solutions to combine feature details and texture features for various alignment algorithms [10].

Reseachers	Features	Database	Types
Jea et al.(2005)[2]	Secondary features around minutiae	FVC 2002	Partial to full
Chen et al.(2007)[3]	Level 3 features	NIST sd30	Partial to full
Fang et al.(2007)[4]	Ridge points and minutiae	FVC 2002	Partial to partial
Zanganeh et al.(2014)[5]	pixel-wise correlation	FVC 2002	Partial to partial
Yamazaki et al.(2015)[6]	SIFT	Private Database	Partial to partial
Surbhi et al.(2016)[7]	AKAZE	FVC 2002	Partial to partial

Figure 1.1.2: Partial Fingerprint in Feature Matching[11]

In Figure 1.1.2, most of the fingerprint algorithms in feature matching are mainly based on multiscale texture descriptors. Besides, SIFT [12] and SURF [13] algorithms are the most popular two-dimensional multiscale description and feature detection. However, ORB is the algorithm that is used in fingerprint recognition in this project. ORB (Oriented FAST and Rotation Briefing) is an algorithm that extracting and describing feature points very quickly. ORB algorithm was proposed by Vincent Rabaud et al. [14]. The ORB algorithm improves and optimizes the datasets by combining the detection between FAST feature points and Brief descriptors. Also, the process of the ORB algorithm is faster than SIFT and SURF.

After used CNN algorithm in face recognition and ORB algorithm in fingerprint recognition. Both recognition are fused by using score level fusion based on weighted sum-rule. Graphical User Interface (GUI) will be developed as a system to combine face and fingerprint recognition and calculate the accuracy after both are merged.

1.2 Problem Statement

In recent years, a non-biometric system such as a password or a code system has been used to make a payment or unlock a phone a thing of the past. In the age of information technology, people are already switching to biometric systems such as face

and fingerprint recognition. It was used to maintain the security system resources and to manage the identity of the user.

Semi-automated biometric devices such as face recognition were developed at the 1960s. Then, fingerprint and face recognition were widely used in law enforcement at 1969s. In 1985, the idea was proposed that was unique to everyone, including fingerprints, irises. In 1994, the first iris recognition algorithm was patented. Then, the first real-time recognition was developed in 1991. Hundred recognition algorithms were patented and functional by 2000s [15]. Apple Company also developed fingerprint to unlock the iPhone in 2013. All these biometric histories were helped to overcome the limitation of a non-biometric system. Therefore, the biometric system has been gaining popularity since the last two decades [16]. The efficiency of this system demonstrates the robustness of the security of the system.

The biometric system has two main features: physiological or behavioral, and controls the identity of a person and ensures much higher security than traditional person identification system. Physiological features of the biometrics are easy to use compared to behavioral features such as keystroke, voice or even signature. These features have categorized into Unimodal Biometric System and Multimodal Biometric System. For Unimodal Biometric System, it involve the face or fingerprint. It can store information in the data, but there are limitations. Although Unimodal has been chosen to recognize the face or fingerprints, there are a lot of tasks require to complete this project. In-person identification will not fully match when the system extracts data from the same biometric features because people are constantly changing over time. For example, a facial structure such as hairstyle, facial expression, facial angles and age changes will be a problem in facial recognition. In recognition of fingerprints, the valleys and ridges of the fingerprint will change due to human age. It is also a serious problem if there is a biometric trait disfigured. For example, it only can require one single task, and it has does not provide high accuracy for identification due to noise data, spoof attack, and so on [3].

Therefore, the Multimodal Biometric System (MBS) can perform two or more biometric features that used to overcome this limitation of a unimodal biometric system. The MBS development system has enhanced the recognition rate. The multimodal