FACIAL RECOGNITION DOOR LOCK USING RASPBERRY PI

MUHAMMAD HARIS AZMAN BIN ANUAR

UNIVERSITI SAINS MALAYSIA

2018

FACIAL RECOGNITION DOOR LOCK USING RASPBERRY PI

by

MUHAMMAD HARIS AZMAN BIN ANUAR

Thesis submitted in partial fulfilment of the requirement for the degree of Bachelor of Electric and Electronic Engineering

JUNE 2018

ACKNOWLEDGEMENT

First and foremost, I would like to convey my sincere gratitude to my supervisor, Dr. Mohd Ilyas Sobirin Bin Mohd Sazali for his precious encouragement, guidance and generous support throughout this work in facial recognition door lock using raspberry pi.

Apart from that, I would also like to thank all School of Electrical and Electronic Engineering staffs for their kindness cooperation and helping hands. Indeed their willingness in sharing ideas, knowledge and skills are deeply appreciated. I would like to express my deepest gratitude to my beloved mother, Rohani Binti Ab. Rahman and my beloved father Anuar Bin Ab. Rahman for they continuous love and support.

Once again, I would like to thank all the people, including those whom I might have missed out and my friends who have helped me to the accomplishment of this project. Thank you very much.

Muhammad Haris Azman Anuar

May 2018

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

2D	Two Dimensional
ARMv8	Acorn RISC Machine version 8
CPU	Central Processing Unit
CSI	Camera Serial Interface
DNA	Deoxyribonucleic Acid
FR	Facial Recognition
GPIO	General Purpose Input Output
GUI	Graphical User Interface
LAN	Local Area Network
LBP	Local Binary Patterns
LDA	Linear Discriminant Analysis
OpenCV	Open Source Computer Vision
OS	Operating System
PCA	Principal Component Analysis
PIN	Personal Identification Number

FACIAL RECOGNITION DOOR LOCK USING RASPBERRY PI

ABSTRACT

There are many possible applications, hardware and devices that exist under the Ubiquitous Computing field. Facial recognition security system is one of key areas under this field. Facial recognition security system is widely used for identity verification due to its capability to measure and subsequently identify user for providing security, informal matching, law enforcement applications, user verification, user access control and is mostly used for recognition for various applications. Facial recognition is the ability to detect and identify a person by characteristics on their face. Face is multidimensional that requires a lot of mathematical computations to detect and recognize. There are many methods for facial recognition that are already proposed but have low performance recognition capability, less accuracy rate, etc. Therefore, this task of the research is to develop a facial recognition security system with an improved accuracy rate and provide high performance of a facial recognition security system to access a building. This facial recognition security has been implemented on an embedded platform Raspberry Pi and OpenCV (Open Source Computer Vision Libraries). Raspberry Pi 3 Model B is used to implement open source code including debugging and testing. Focus for this project is implement facial recognition security with high accuracy rate and better performance recognition capability. Accuracy rate and recognition capability is one of important things for this Facial Recognition Door Lock Using Raspberry Pi

PENGUNCI PINTU PENGENALAN WAJAH DENGAN MENGGUNAKAN RASPBERRY PI

ABSTRAK

Terdapat banyak aplikasi, perkakasan dan peranti yang ada di bawah bidang Pengkomputeran Ubiquitous. Sistem keselamatan pengenalan wajah adalah salah satu bidang utama di bawah bidang ini. Sistem keselamatan pengenalan wajah digunakan secara meluas untuk pengesahan identiti kerana keupayaan untuk mengukur dan kemudian mengenal pasti pengguna untuk menyediakan keselamatan, pemadanan tidak formal, aplikasi penguatkuasaan undang-undang, pengesahan pengguna, kawalan akses pengguna dan kebanyakannya digunakan untuk pengiktirafan dalam pelbagai aplikasi. Pengenalan muka adalah keupayaan untuk mengesan dan mengenal pasti seseorang dengan ciri-ciri wajah mereka. Wajah adalah multidimensi yang memerlukan banyak perhitungan matematik untuk mengesan dan mengenal. Terdapat banyak kaedah untuk pengenalan muka yang sudah dicadangkan tetapi mempunyai keupayaan pengenalan, prestasi yang rendah, kadar ketepatan kurang, dan lain-lain. Oleh itu, tugas penyelidikan ini adalah untuk membangunkan sistem keselamatan pengenalan wajah dengan kadar ketepatan yang lebih baik dan memberikan prestasi tinggi. Keselamatan pengenalan wajah ini telah dilaksanakan pada platform Raspberry Pi dan OpenCV (Open Source Computer Vision Libraries). Raspberry Pi 3 Model B digunakan untuk melaksanakan kod sumber terbuka termasuk penyahpijatan dan pengujian. Tumpuan dalam projek ini adalah melaksanakan keselamatan pengenalan wajah dengan kadar ketepatan yang tinggi dan menpunyai prestasi keupayaan pengenalan yang lebih baik. Kadar ketepatan dan keupayaan pengenalan adalah salah satu perkara penting untuk Pengunci pintu pengenalan wajah menggunakan Raspberry Pi.

CHAPTER 1: INTRODUCTION

1.1 Research Background

Nowadays, securities become a very important issue that need to pay attention and with the advancement in information technology, biometric has become an important research area due to high demand in real world, but needs improvement for security application. Traditional or physical security methods nowadays not enough for daily work activities or asset protection. Therefore, it is essential to incorporate an integrated security system. This system consists of different security components such as: Access Control, Video Surveillance and Intrusion systems that protect corporate goods and personnel [2].

In recent years, biometric technology plays a vital role in security systems because biometric characteristics are used to enhance safety. Biometric technology takes part as a useful tool to increase safety since it can effectively authorize or deny access into specific areas. The security systems need changing throughout the time, traditional identification technologies such as PIN (Personal Identification Number) passwords or identity cards are pushed to their limits [2]. Biometric security is the most reliable technology regarding identification because it uses biological characteristics that are unique for each person [3].

The main advantage of a biometric authentication system, is that it can connect directly with user and grant access to the system. Two types of biometric properties are useful for authentication. Firstly, physical biometrics such as DNA (Deoxyribonucleic acid), fingerprints, facial recognition, and iris. Secondly, is behavioural biometrics include voice recognition and handwritten signatures. The biometric authentication process consists of several stages: measurement, signal processing, pattern matching, and decision making [4]. Nowadays, industry has conducted recognition to the physiological features that is peculiar from another person that includes fingerprint recognition, iris recognition, palm recognition, facial recognition (FR), voice recognition, vein recognition and so on.

The advantage of using facial recognition is least intrusive and more secure instead of other recognition methods [5]. For example, fingerprint recognition are reliable biometric methods of identification. But there are some disadvantages associated with fingerprint recognition such as if the user of the system gets his/her fingers injured, the access will be difficult. Facial recognition is more secure as no one can plagiarize or whip a face to gain access to a security system. Based on that, facial recognition is progressively acceptable as it is a deferential and non-intrusion way of verification.

There are several techniques and algorithms that can be implemented but they differ in terms of processing speed of languages. For example, Java, is pretty slow and was not successfully implemented because of complexity issues.

The Raspberry Pi Foundation based in United Kingdom develops the Raspberry Pi series. The Raspberry Pi series of small single-board computer provide low-cost and high performance computer to promote the teaching of basic computer science in school and engineering field [6] . The security system algorithm has been proposed to implement Facial Recognition System on Raspberry Pi 3 model B. Raspberry Pi 3 model B is the third generation for Raspberry Pi series and it is more powerful processor by 10x faster than the first generation of Raspberry Pi [7].

The Raspberry Pi 3 Model B as shown in Figure 1.1 with specification a quad-core ARMv8 CPU is used in this project because it is a powerful single board in range low cost computer board that can be used for many applications and supersedes the original Raspberry Pi Model B+ and Raspberry Pi Model B. It has provision of connecting with Pi Camera via CSI Camera Connector. This model also adds with the wireless LAN and Bluetooth connectivity making it the ideal future solution for security system with less power consumption computer board. The advantages of single computer board are low-cost, low-space, low-power and portability of the entire identification security system of implementation.

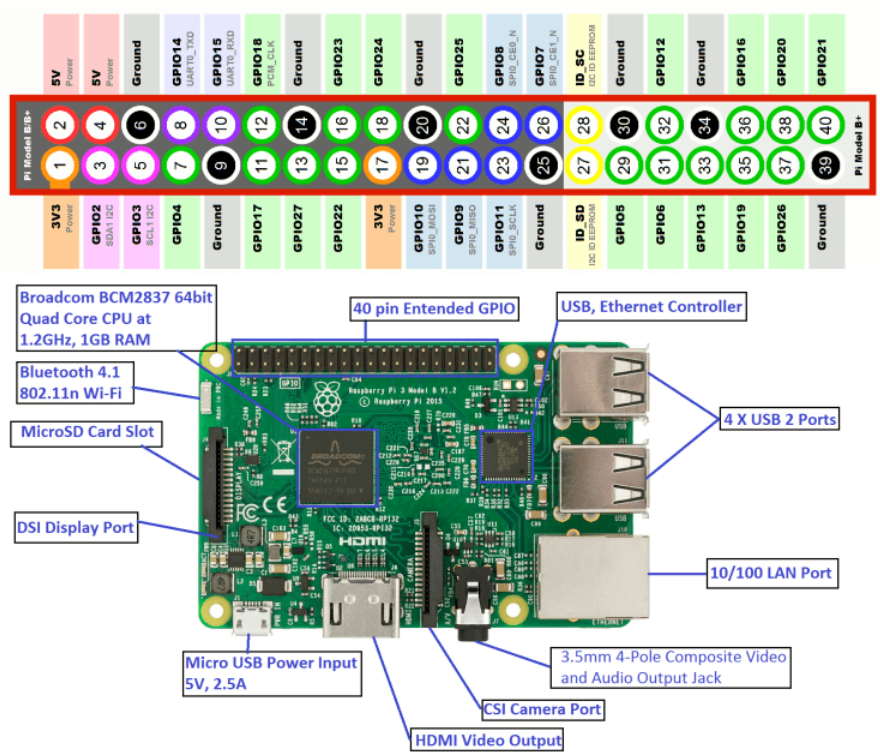

Figure 1.1 Raspberry Pi Diagram [1]

1.2 Problem Statements

The main problem of security system for facial recognition can consider in closer based solutions which are impossible to merge in high accuracy rate and good performances capability. The existing systems available are fingerprint recognition has some complexity in obtaining high quality images of finger patterns because issues of dirty, cuts, tear and wear that effect the ridges and minutiae of fingertip. There are issues that contribute in decreasing the accuracy of iris recognition such as wearing glasses, eye lenses, etc. Another issues are types of recognitions used in related work, most of it used PCA algorithm (Eigenface) that less accurate and it is not compatible with current technology. Low specifications of microcontrollers that will effect processing time. Due to high demand for security systems that can provide high protection the development of

Facial Recognition System needs improvements in terms of algorithm and hardware to increase the rate of accuracy security system.

These limitations provided solution to build a high accuracy rate, high speed processing and good performance facial recognition security system for accessing a building that became easy to control and user not need to look up the command line to run the program or this system.

1.3 Research Project Objectives

To implement a facial recognition security system with a high accuracy rate and good performance for door lock using Raspberry Pi 3 and OpenCV with facial recognition algorithms.

1.4 Research Project Scope

In this project, a facial recognition system will be developed in Raspberry Pi 3 Model B. The code can be run on a certain operating system such as Linux, Windows also Mac. Firstly, Python is used to simulate and run the code. After that, Raspbian OS software is used to install the code. In order to measures the performances of the facial recognition system, many testing are done based on few parameters;

1. Accuracy rate
2. Time consumption of the system
3. Performance on various accessories
4. Performance with various distance

1.5 Report Outline

This thesis consists of five main chapters, which are introduction, literature review, methodology, result and discussion and finally conclusion.

Chapter 1 is the introduction that covers the research background of the project, problem faced by Facial Recognition Door Lock, objectives to achieve, research scope of the project and also project outline.

Chapter 2 covers the Literature Review from different journals on the security system and is also include facial recognition is discussed. In this chapter, an overview of the security system and facial recognition. Moreover, a summary on the advantages of some of the previous work is included. This chapter also touches on the knowledge about coding.

Chapter 3 covers the methodology on which techniques are to be implemented in this project. Raspberry Pi 3 Model B is used as microcontroller for this part after install Raspbian OS on it. Haar cascades and local binary patterns histogram are used as algorithms for facial detection and recognition.

Chapter 4 discusses the results obtained by using Python and OpenCV. Then, the performance and accuracy rate of the Facial Recognition of security system is discussed.

Chapter 5 present the conclusion of the project and provides some recommendations for future improvement.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

By increasing technologies of security system nowadays, all software or hardware also require updates to provide high performance and high accuracy rate. In security purposes, it becomes important to replace the old methods with to new methods which can increase the level of threat detection systems. It should be able to automatically detect and recognize the authorized person and restrict the unauthorized person.

Many different methods have already been done in Facial Recognition area, making it become popular due to various applications in a few decades. Two features that Facial Recognition system should have are high recognition rate and high recognition speed. The correct recognition algorithm will speed up facial recognition process and increase the accuracy.

There is certain hardware that already implemented for Facial Recognition system. Nowadays, new single computer board can process the algorithm faster compared to previous version. By selecting the suitable hardware, it will reduce the cost and speed up the facial recognition process.

2.2 Types of Recognition System

There are many existing papers related to biometric security system. The term biometrics is the combination of two-word Bio and Metric that is an emerging technology for recognizing individuals based on their physical [8]. The main advantage of a biometric authentication system is it can improved security, improved customer experience, cannot be forgotten or lost and reduced operational costs.

Examples types of physiological recognition:

a. Fingerprints

b. Facial Recognition

c. Iris Recognition

Figure 2.1 lists the general classification biometric authentication system and the current deployed biometric techniques in the security market.

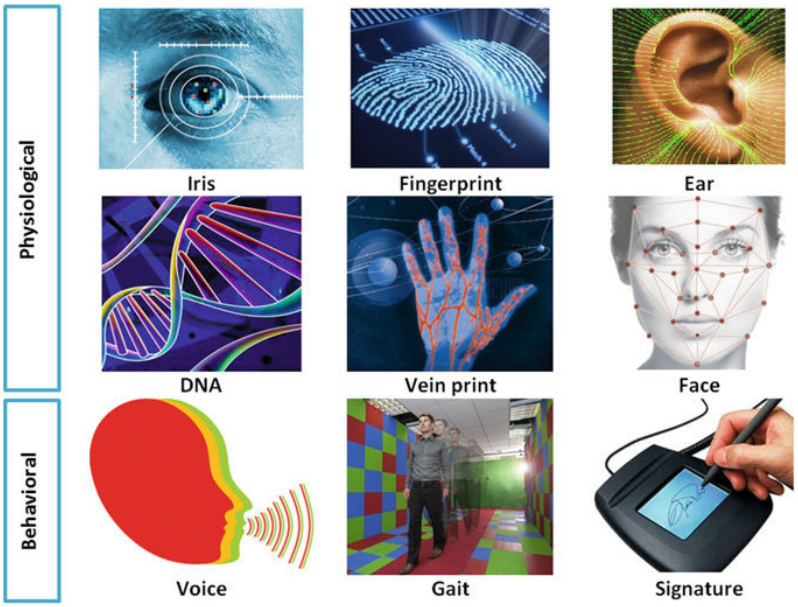

Figure 2.1 Various types of biometric modalities [10]

2.2.1 Fingerprint Recognition

Fingerprints are the most popular biometric features used in security system due to easy to use, install and integrate with other security system. Besides, Fingerprint readers are commonly used in security systems because individuality and persistence. But nowadays fingerprint is not reliable when the user of the security system gets his/her fingers injured, then the user will be unable to get access to the system [9].

Figure 2.2 shows examples of fingerprint patterns, such as loop pattern, double loop pattern, central pocket loop pattern, plain whorl pattern, plain arch pattern, tented arch pattern, etc.

Figure 2.2 Fingerprint patterns. From top left to bottom right: loop, double loop, central pocket loop, plain whorl, plain arch, and tented arch [12]

2.2.2 Iris Recognition

The human iris is considered as highly universal because iris are extremely unlikely to be equal even in the case of genetically identical twins or in the case of single individual [8]. The iris of eye is a stable biometric characteristic because the human iris is developed in humans at baby age and does not change throughout time [2].

There are five major steps for iris recognition system:

1. iris segmentation
2. iris normalization
3. feature encoding
4. template matching
5. human identification

It is a non-invasive technique, in which no physical contact is required for identification [2]. The existence of human iris is in between dark pupil and white sclera of eye as shown in Figure 2.3.

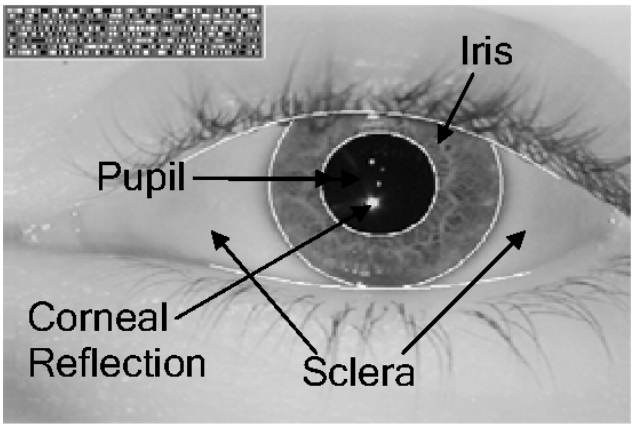

Figure 2.3 The structure of human iris [10]

2.2.3 Facial Recognition

Face recognition is generally used because it does not require physical contact between the user and the device. It uses a digital camera to perform the authentication [2]. The facial recognition becomes the most important user identification method because it is better performance and accurate compared with fingerprint and iris, as Figure 2.4 shows how biometric facial recognition work well as facial recognition based systems easy to install and do not require expensive hardware.

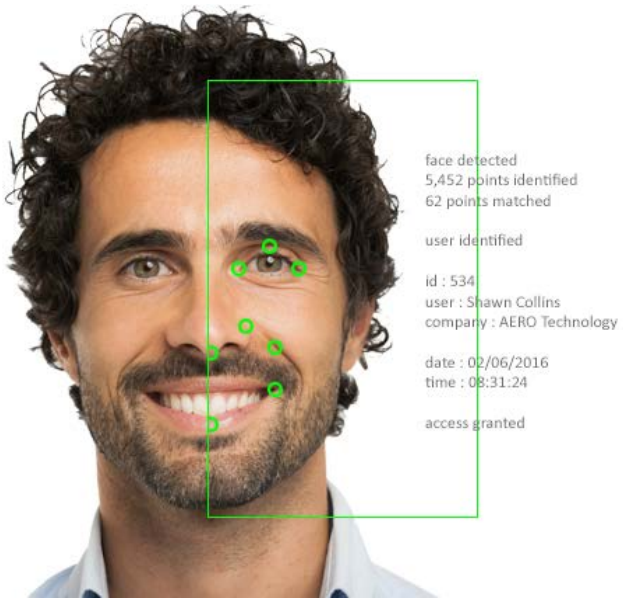

Figure 2.4 Biometric Facial Scanner [11]

Figure 2.5 shows literature survey statistics of research work in face recognition system. Nowadays, facial recognition system is in its booming era. Based on number of publications in facial recognition in forty years, the research in this field has increased exponentially [12].

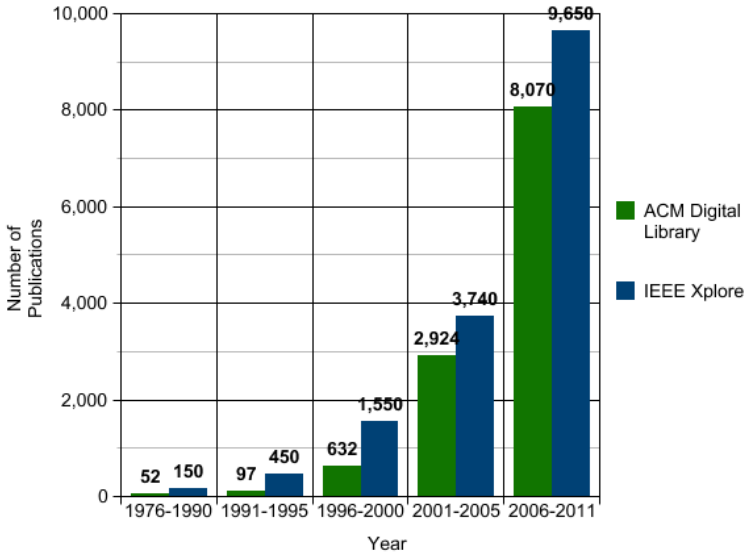

Figure 2.5 Research Statistics of Face Recognition [12].

2.2.4 Summary of Types Recognition System

In general, most of biometrics based authentication systems have a common characteristic for the automatic recognition of individuals. Table 1 shows the advantages and disadvantages of among biometric recognition system.

Table 2.1 Advantages and Disadvantages of Types Recognition System

	Advantages	**Disadvantages**
Fingerprint	• Ease of use this method. • Small storage space required for the biometric template, reducing the size of the database memory required.	• Has some complexity in obtaining high quality images of images of finger patterns because issues of dirty, cuts, tear and wear that easily effect the ridges and minutiae of fingertip. • High cost of implementation for high effective solution • Fingerprint recognition needs extra hardware apart from the software. • For some people it is very intrusive, because is still related to criminal identification.
Iris Recognition	• Ease of use. • Flexible operating of scanning devices.	• There are issues that contribute in decreasing the accuracy of iris recognition such as wearing glasses, eye lenses, etc. • Difficulty of deploying due to the high cost of implementation. • A large storage space required for the data to be stored.

Facial Recognition	• Ease of use. • Fully automate the process. • High accuracy rate. • Low cost of system implementation (does not require high-end cameras). • Unlocking the system quickly while on the go (contactless). • Not require so much power. • Small storage space required for database.	• These factors affect the performance such as quality or resolution of collected photos, light conditions, angles of face, etc.

2.3 Facial Detection Using Haar Cascades

The facial detection is one important module in facial recognition. Facial detection using Haar feature-based cascade classifiers algorithm is an effective method proposed by Paul and Michael Jones [13]. It is a machine learning based approach in which a cascade function is trained from several positive and negative images and it is used to detect facial in other images [12].

The algorithm requires a lot of positive images (images of faces) and negative images (images without faces) to train the classifier and the features are extracted from it. For this, Haar Classifier patterns shown in Figure 2.6. Every feature is a single value obtained by subtracting sum of pixels under the white rectangle from sum of pixels under black rectangle, then all possible sizes and locations of each kernel are used to calculate lots of features [12]. For single feature obtained by subtracting sum of pixels under white with sum of pixels under the black rectangles.

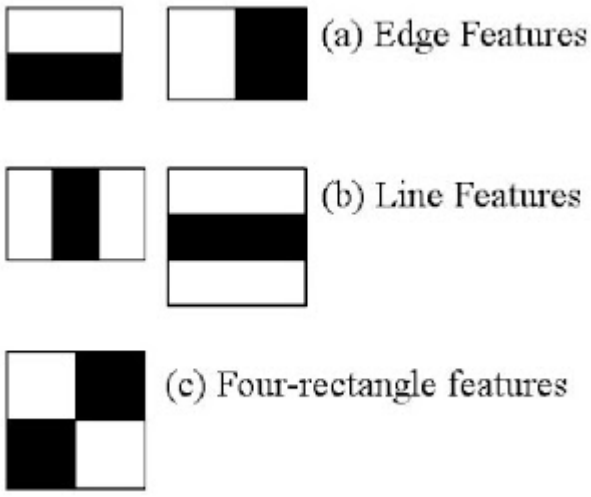

Figure 2.6 Haar Classifier Patterns [14]

The integral image, it reduces the calculations for large pixel to an operation involving just four pixels. It makes the process super-fast. This process has applied on all the training images, and it finds the best threshold which will classify the facial to positive and negative. The minimum error rate is selected, that means the most accurately classify the facial and non-facial images. The concept of cascade classifiers is grouped the features into different stages of classifiers and applied one by one. If the first stage it discards the remaining features are not considered, but if it passes, second stage of features an applied and continue the process. The facial region is obtaining when passes all stages.

2.4 Types of Facial Recognition

The facial recognition has been researched for several years, different type algorithms are used to perform face recognition. There are few algorithms currently available to use:

1. Local Binary Patterns Histograms
2. Eigenfaces
3. Fisherfaces

2.4.1 Local Binary Patterns Histograms

Local Binary Patterns Histograms (LBPH) is a real time face recognition. LBPH is a powerful method to solve facial recognition problem, LBPH methodology has its roots in 2D texture analysis that is simple and efficient scale texture [7]. It can describe the relationship between a pixel and its neighborhood.

After that, take the threshold of its neighbors that against the pixel as the central. If the intensity central pixel is greater than or equal to a the intensity neighbors, then the binary value 1, otherwise it is 0 [7]. Example of LBPH operator shown in Figure 2.7 below.

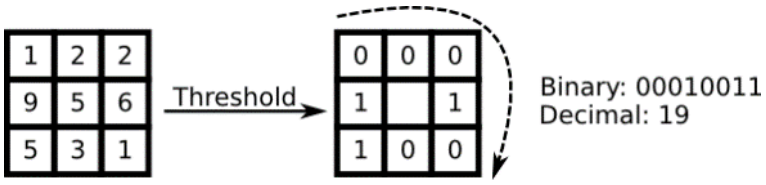

Figure 2.7 LBP operator (a fixed 3 x 3 neighborhood)[15]

The LBP operator with the central pixel can be defined as:

$$LBP_{P,R} = \sum_{P}^{P-1} s(g_P - g_c)2^P$$

where P, R as central pixel with intensity g_P , and g_c is the intensity of the neighbour pixel, and $s(g_P - g_c)$ is the threshold function defined as [7]:

$$s(g_P - g_c) = \begin{cases} 1, g_P \geq g_c \\ 0, g_P < g_c \end{cases}$$

By this, the capture is very fine grained details in images. Point (x_c, y_c) the position of the neighbor $(x_{p,} y_p), p \in P$, can be calculated by:

$$x_p = x_c + R\cos(\frac{2\pi p}{P})$$

$$y_p = y_c - R\sin(\frac{2\pi p}{P})$$

where R is radius of the circle and P is number of sample points.

Intuitively, different facial parts may possess different features. Some facial parts may be dominant in facial recognition.

The detail face features for facial recognition can be gained by dividing a face image into many blocks and calculating the LBPH histogram of each block [7].

In extension LBPH code called extended LBPH or Circular LBPH, if a points coordinate on the circle does not correspond to image, the point gets interpolated.

$$f(x,y) \approx \lceil 1 \quad -x \quad x \rceil \begin{bmatrix} f(0,0) & f(0,1) \\ f(1,0) & f(1,1) \end{bmatrix} \begin{bmatrix} 1-y \\ y \end{bmatrix}$$

LBPH is robust against monotonic gray scale transformations, so that can be easily verified by looking on LBPH image of an artificially modified image. Figure 2.8 shows an example of LBPH modified image.

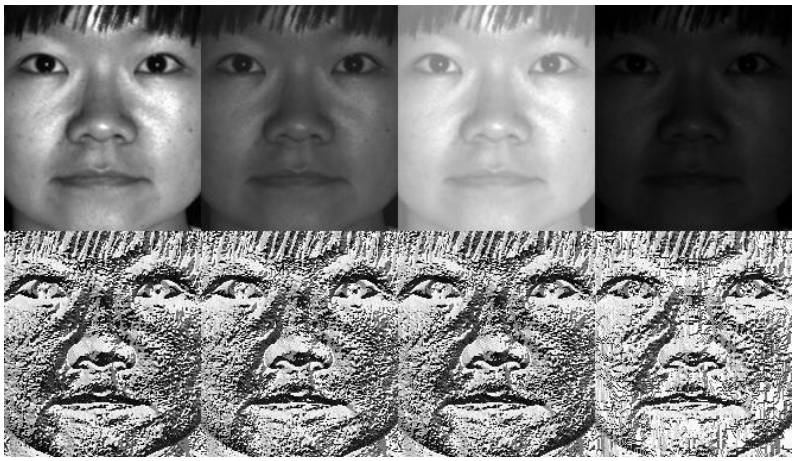

Figure 2.8 Example of LBP modified image [16]

2.4.2 Eigenfaces

In a previous research, the facial recognition algorithm used is Principal Component Analysis (PCA), that involves a mathematical procedure. Principal components or number of uncorrelated variables are transformed from a number of possible correlated variables. The high dimensional dataset is often described by correlated variables. The Eigenfaces reduces the size of the database that is required for recognition [12]. However, it is designed in a way to best preserve data in the embedding space and consequently cannot promise good discriminating capability [17].

The Eigenfaces method performs face recognition by projecting all training samples into PCA subspace or projecting the query image into the PCA subspace, and it can also be performed by finding the nearest neighbour between the projected training images and the projected query image.

When $x = \{x_1, x_2, x_3, \ldots x_n\}$ is random vector with $x_i \in R^d$

Mean μ can be computed as

$$\mu = \frac{1}{n}\sum_{i=1}^{n} x_i$$

Covariance Matrix S is

$$s = \frac{1}{n}\sum_{i=1}^{n} (x_i - \mu)(x_i - \mu)^{T_i}$$

The eigenvalues λ_i , eigenvectors v_i of S

$$Sv_i = \lambda_i v_i, i = 1,2, \dots, n$$

The k principal components is the eigenvectors that correspond to the k biggest eigenvalues. By observing vector x from the equation

$$y = W^T(x - \mu)$$

where $W = (v_1, v_2, \dots, v_k)$

Reconstruct equation from PCA basis

$x = Wy + \mu$, where $W = (v_1, v_2, \dots, v_k)$

The result at eigenvectors are orthogonal, when its normalized to unit length, it can be orthonormal eigenvectors. Figure 2.9 shows example of eigenface reconstruction.

Figure 2.9 Example of eigenface reconstruction [18]

2.4.3 Fisherfaces

Linear discriminant analysis (LDA) is used for dimensionality reduction, and it provide a good discriminating capability [17]. LDA maximizes the ratio of between classes to within classes scatter in order to find the combination of features. The same classes cluster tightly together and different classes are as far away as possible from each in other in the lower dimensional representation using discriminable linear projection model [19]. Therefore, the scatter matrix is divided into the between class scatter matrix which be defined as:

$$S_w = \sum_{i=1}^{c} \sum_{x_j \in X_i} (x_j - \mu_i)(x_j - \mu_i)^T$$

Where μ_i is the mean image of class X_i, and N_i is the number of samples in class X_i, total c classes. The scatter matrices S_B are calculated as:

$$S_B = \sum_{i=1}^{c} (N_i(x_j - \mu_i)(\mu_i - \mu)^T$$

The solution for Fisherfaces is given by solving the General Eigenvalue Problem:

$$\begin{aligned} \mathrm{S_B} v_i &= \lambda_i \mathrm{S}_w v_i \\ \mathrm{S}_W^{-1} \mathrm{S_B} v_i &= \lambda_i v_i \end{aligned}$$

A Linear Discriminant Analysis was then performed on the reduced data, because S_w is not singular anymore, and the optimization problem can then be rewritten as[17]:

$$\begin{aligned} W_{\mathrm{pca}} &= \arg\max_W |W^{\mathrm{T}} \mathrm{S_T} W| \\ W_{\mathrm{fld}} &= \arg\max_W \frac{|W^{\mathrm{T}} W_{\mathrm{pca}}^{\mathrm{T}} \mathrm{S_B} W_{\mathrm{pca}} W|}{|W^{\mathrm{T}} W_{\mathrm{pca}}^{\mathrm{T}} \mathrm{S}_W W_{\mathrm{pca}} W|} \end{aligned}$$

The discriminant analysis method finds the facial features to discriminate between the person, the performance of the Fisherfaces heavily depends on the input data. The Figure 2.10 shows the first, at most 16 Fisherfaces:

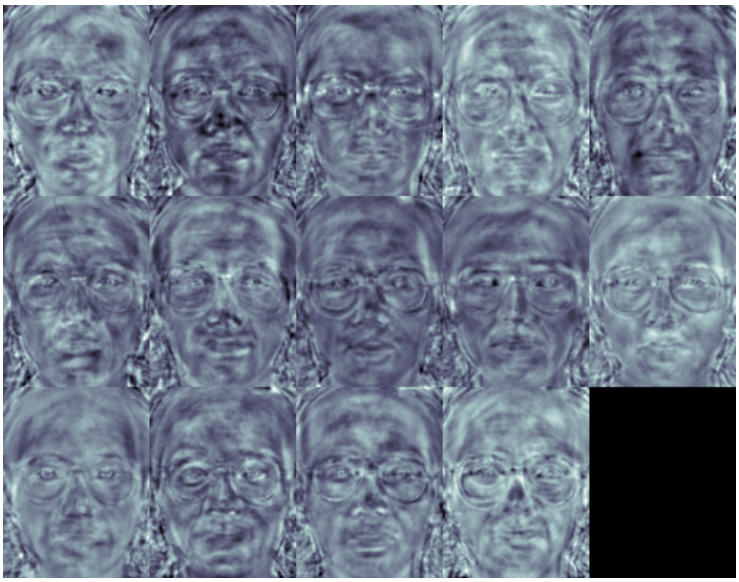

Figure 2.10 16 Fisherfaces [20]

The comparison of different facial recognition algorithms, the accuracy rate for three methods testing without imposter are showed in table 2.2, based on table that shown LBP had high accuracy rate compare PCA and LDA.

Table 2.2 Accuracy of three methods tested without imposter [17]

Methods	Neutral	Illumination	Expression	Pose
PCA	0.8027	0.8108	0.8455	0.7736
LDA	0.9150	0.9189	0.8902	0.8302
LBP	0.9422	0.9730	0.9106	0.9245

2.5 Types of Microcontroller

A microcontroller is a small, low-cost and self-contained computer on a chip that used as an embedded system. Based on related work, it includes single computer board or microcontroller. These are type of microcontroller that used in related work:

1. Raspberry Pi 2, with CPU 700MHZ and 256MB RAM using low power consumption. It consists input/output, RAM, GPU/CPU ,USB hub, Ethernet, HDMI port [12]. Figure 2.11 shows Raspberry Pi 2 Model B.

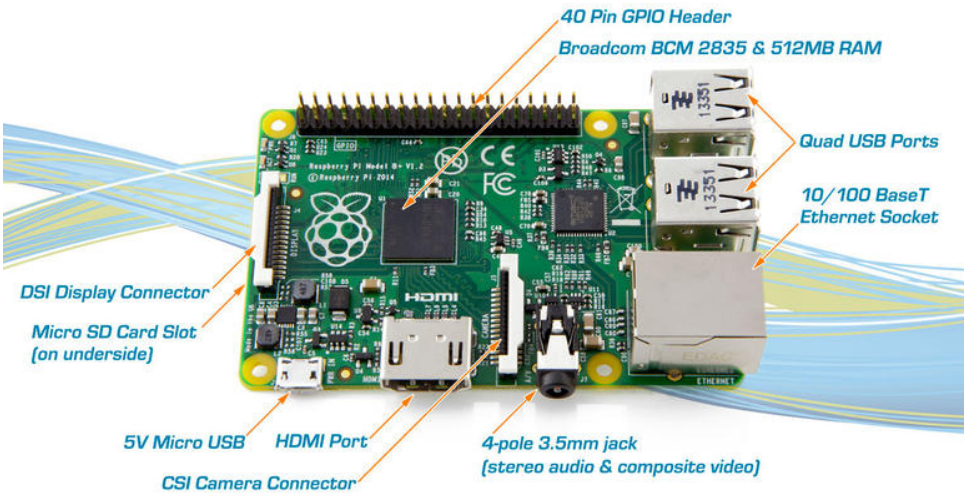

Figure 2.11 Raspberry Pi 2 Model B [21]

2. MyRIO 1900 microcontroller and requires webcam connected by USB cable. MyRIO microcontroller which is programmed using LabVIEW and Personal computer (PC) as user interface, image display and monitoring [22]. Figure 12 shows myRIO-1900 by National Instruments.

Figure 2.12 myRIO-1900 [23]

3. Raspberry Pi 1 model B with specification 512 MB of RAM, with 26 pin connections. Raspberry Pi as microcontroller which is programmed using MATLAB [24].

   Table 2.3 lists the pinouts of the Raspberry Pi 1.

Table 2.3 Raspberry Pi 1 Model B Pin Connections

1	3.3 V	7	GPIO 4	13	GPIO 21	19	GPIO 10
2	5 V	8	GPIO 14	14	GND	20	GND
3	GPIO 0	9	GND	15	GPIO 22	21	GPIO 9
4	5 V	10	GPIO 15	16	GPIO 23	22	GPIO 25
5	GPIO 1	11	GPIO 17	17	3.3 V	23	GPIO 11
6	GND	12	GPIO 18	18	GPIO 24	24	GPIO 8
25		GND		26		GPIO 7	