“Smart Door Lock System with Face Recognition Based on IoT”

Project Report

Submitted to

Sant Gadge Baba Amravati University

In partial fulfillment of the Requirement for the award of

Degree of

Bachelor of Engineering

By

Dnyanesh Sudhakar Kolhe

Under the guidance of

Prof. P. N. Pusdekar

Department of Electronics and Telecommunication Engineering

P. R. Patil College of Engineering & Technology,

Amravati – 444605 (M. S.)

2020-2021.

Department of Electronics and Telecommunication Engineering

P. R. Patil College of Engineering & Technology,

Amravati – 444605 (M. S.)

2020 – 2021.

CERTIFICATE

This is to certify that the project report entitled

"**Smart Door Lock System with Face Recognition Based on IoT"**

Submitted by

Dnyanesh Sudhakar Kolhe

In partial fulfillment of the requirements for the award of Degree of Bachelor of Engineering in Electronics and Telecommunication Engineering by Sant Gadge Baba Amravati University & is a bonafied work carried out during the session 20120-2021.

Prof. P. N. Pusdekar
Guide

Examiner

Prof. U. W. Hore
Head of the Department

Prof. P. R. Wadnerkar
Principal

DECLARATION

We hereby declare that we have completed the project work towards the Bachelor of Engineering Degree of Sant Gadge Baba Amravati University, Amravati, in Electronics and Telecommunication discipline on the topic entitled **"Smart Door Lock with Face Recognition Based on IoT''** under supervision of **Prof. U. W**. **Hore** Head of Department of Electronics and Telecommunication Engineering, P. R. Patil College of Engineering & Technology, Amravati.

This report embodies the original work done by us in fulfilment of the requirement of the Bachelor of Engineering Degree of Sant Gadge Baba Amravati University, Amravati, in Electronics and Telecommunication discipline.

Amravati
Date:

Name of Student
Dnyanesh Sudhakar Kolhe

ACKNOWLEDGEMENT

It is our supreme duty and desire to express acknowledgement to the various torchbearers, who have rendered valuable guidance during the preparation of our project.

First of all, we extend our deepest gratitude to our revered Principal **P. R. Wadnerkar** without whose support; our project could not have been transformed into present form.

We are grateful to **Prof. U. W. Hore** HOD, Electronics and Telecommunication Engineering Department; and guide **Prof. P. N. Pusdekar** for providing immense support and guidance. We are beholden for guiding us at every step in the project. He has most honestly guided us throughout; never leaving us unanswered for any of our doubts. It was his constant persuasion, encouragement, inspiration and able guidance that helped us in completing our project successfully.

Dnyanesh Sudhakar Kolhe

Final Year,
EXTC

Abstract

As we know that today's era of digital world privacy and security of our loved ones is very important, So We have introduced this project. The aim of this project to makes every home secure and build modern, easily used smart door lock system. This smart door lock system is user friendly, convenient that allows user to unlock their home door better secure way. It allows users to open their home door remotely through IoT app, or by using face recognition through camera which is mounted front to the door. The system made of three components onboard logical unit, cloud system and IoT app. However instead of using door model we assume solenoid lock is door lock which is used for lock and unlock mechanism. This prototype system work on images instead of video due to this system cost efficient and also limit the internet traffic. This system captures images by the camera and saves photos in databases it will local system or clous system. Then facial recognition technology start work when any person detected in front of home system matches captures images to the known databases if found in the system database then door unlock if not found then system inform to the owner about unknown person through any type messaging system. This system includes raspberry pi, facial recognition technology, deep learning, IoT, security mechanism.

Keywords: Deep learning, Facial recognition, Home security system, Internet of things (IoT),

Raspberry pi.

TABLE OF CONTENT

LIST OF FIGURE

LIST OF ABBREVIATION

Sr. No.	Title	Full Form
1	IoT	Internet of Things
2	IR	Infrared Sensor
3	OS	Operating System
4	Open CV	Open Computer Vision
5	AI	Artificial Intelligence
6	ML	Machine Learning
7	GSM	Global System for Mobile Communications
8	USB	Universal Serial Bus
9	HD	High Definition
10	API	Application Programming Interface
11	RFID	Radio Frequency Identification Card
12	PCA	Principle Component Analysis
13	CNN	Convolutional Neural Network
14	PC	Personal Computers
15	HDMI	High-Definition Multimedia Interface
16	PIR SENSOR	Passive Infrared Sensor

Chapter 1

INTRODUCTION

1.1 INTRODUCTION

The aim of this project was to design and build a door lock system that allows users to unlock a door via face recognition, through a camera implanted on the door. In this method chapter, we will discuss how we detailed the process of implementing this mechanism. In current digital world of connectivity where smart devices need to be modified this makes life easier. I today's world we can't trust anyone and also compromise with old conventional security system.

The major drawbacks in a common door lock are that anyone can open a conventional door lock by duplicating or stealing the key and its simply impossible if we want our friends and family to enter our house, without being actually present over there. Therefore, why not just remove these problems. So, we have directly converted this normal door lock into a smart lock system. Which can open the door lock whenever we turn up in front of the home door or remotely.

Nowadays, home security system is a crucial issue. Indeed, this system is to ensure properties and loves ones is always safe and protected. For the past few years, it is important to have a solid security system for home, which can secure in the most ideal and safe way. Many countries are step by step deployed home security system. The important part of any home security system is the person identification to enter and exit the house. Previously, people use the traditional method for their home security system. The traditional security system relies on the use of external things such as key, password and ID card to gain access. However, due to some limitation, biometric takes place to deliver such a promising security system. The biometric is a unique and quantifiable parameter for individual recognition. Biometric system required the used of specialized hardware such as fingerprint scanner, palm print scanner, DNA analyzer and etc. Furthermore, this specific machine required the target to touch the hardware to acquire data of human unique features. Biometric technology is viewed as a standout among the most secure verification system accessible, by giving a more elevated amount of security than conventional method.

Face recognition is the most famous method in biometric technology besides fingerprint characteristics. This is due to more stability as face contains more features. Besides, it is considered highly secure as face cannot be stolen, borrowed or forge in order to enter the house. Face recognition is likely the most natural approach to perform biometric verification between individuals. Face detection is the first step of the face recognition system. Face pictures can be caught at a distance with the use of a web camera. The individual can be recognized without physical contact on any special hardware to perceive the person's identity.

Face recognition using deep learning technique is used. Deep learning is a piece of the more extensive group of machine learning methods based on learning data representations, as opposed to task specific algorithms. Learning can be managed, semi-directed or unsupervised. With the deep learning, the system is improved from time to time. Some images of authorizing user are used as the database of system and the system will train the face recognition automatically. Thus, the accuracy is increased. Home security is an example of an Internet of Things (IoT) applications. IoT refers to the network of associated physical objects that can interact and trade information among themselves without the need of any human intervening. IoT is a futuristic technology where devices and internet is interconnected. It is different from the internet due to internet exceed connectivity by allowing any embedded circuit to communicate with each other using the current internet infrastructure. No doubt IoT helps users to control one or more devices and capabilities to automate with many daily chores. By using IoT, it can help in controlling the door access and also sent notification throughout the internet. In this system, Blynk apps are used. Blynk apps is an app that enables us to control the door access by designing the graphical interface in the apps according to the specific function to perform. It also able to send notification to computer, smartphone and other smart devices.

The individual can be recognized without physical contact on any special hardware to perceive the person's identity. Face recognition using deep learning technique is used. Deep learning is a piece of the more extensive group of machine learning methods based on learning data representations, as opposed to task specific algorithms. Learning can be managed, semi-directed or unsupervised. With the deep learning, the system is improved from time to time. Some images of authorizing user are used as the database of system and the system will train the face recognition automatically. Thus, the accuracy is increased.

Nowadays, there is a growing interest in the smart home system using IoT. Face recognition is one of the most used biometric identification system beside fingerprint and iris. A typical face recognition system is shown in figure 1.1.

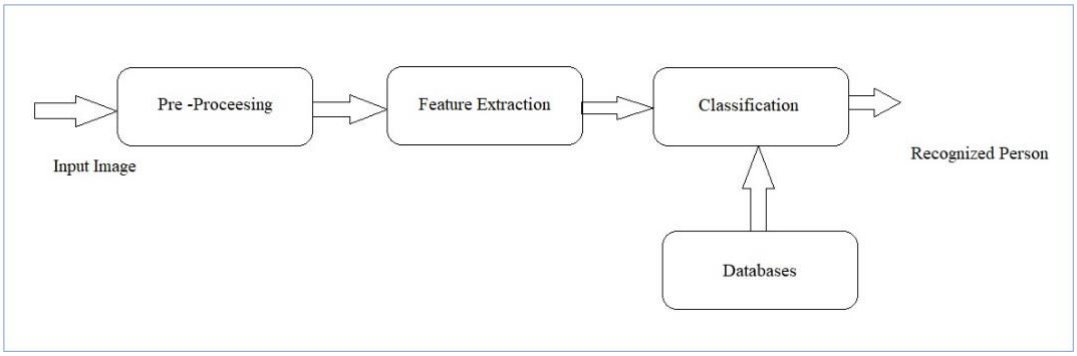

Figure 1.1 Typical Face Recognition System

The individual can be recognized without physical contact on any special hardware to perceive the person's identity. Face recognition using deep learning technique is used. Deep learning is a piece of the more extensive group of machine learning methods based on learning data representations, as opposed to task specific algorithms. Learning can be managed, semi-directed or unsupervised. With the deep learning, the system is improved from time to time. Some images of authorizing user are used as the database of system and the system will train the face recognition automatically. Thus, the accuracy is increased.

1.2 PROBLEM DEFINATION

In the world of emerging technology, security became an essential component in day-to-day life. Information theft, lack of security and violation of privacy etc. are essential component which are needed to be protected. Using smart secure system for lock and unlocking became popular now a days. This system is being adapted by many countries such as USA, Japan etc. already makes use of this system.

This system provides either a facial recognition security feature or a keypad or the both is provided to enter the new and more efficient use of hardware. Human body will be identified

as an input within environment by capturing live video from a web camera or pi camera and the process will be done on captured video frames. Instead of using live video we can used capture still images from camera when human body is detected in front of camera by IR sensor. The used of this we can save processing time and also save from massive data storage in the system.

The images will run through hardware and check with the stored data base. The compilation process will be performed through hardware itself with the help of Raspbian OS and the response will be sent to the cloud and then to the app.

1.3 OBJECTIVES

There are few objectives while design face detection system. The objectives of face detection are to design real time face detection system, to utilize the face detection system based on the selection algorithm, to develop face detection system using open CV, face recognition using Amazon Rekognition could operate on entering the house by the recognizing face. For face detection recognition, an image will be captured by camera and preprocessed and converting, resizing and cropping, then face detection and recognition are performed. This project proposes how such system can be setup emphasizing on the aspects of low cost, installation and easy handling and maintenance.

1.4 ORGANIZATION OF REPORT

Smart door lock system with face recognition is introduce in chapter 1. In, chapter 2, summarizes different papers of smart door lock system with face recognition. In chapter 3, actual implementation of smart door lock system with face recognition system how it's working. In chapter 4 is related hardware and software description. In chapter 5 is given about the experimental results, advantages, disadvantages with application. And finally, in chapter 6 information related to conclusions and future scopes of the smart door lock system with face recognition.

Chapter 2

Literature Survey

2.1 HISTORY

Since 2010 the industry has seen a dawn of work being done in fields of Artificial Intelligence (AI), Machine Learning (ML), Neural Networks, IoT, Big Data Analytics all this thing a common aim to make things better and easier, self-learning and to the connects internally to the all types of devices by making everyday objects internally connected and operable. The need has been identified in the field of digital security tools and hence a greater number of works has been modelled on making daily life locks smart by introducing locks movable using of stepper motor.

A major study of literates implemented Smart Door Locks System is to be been done and literature also implemented Smart Door Locks with the help of GSM phones and the stepper motors has been study. The model introduced by us is the unique one. The features of this system is offers with its one of a kind combination of functionalities and the simplicity. The large difference is in the reduction by the application as it detects the face out of the image store in the databases and sends it to app program which is interfaced with our app system, which is not introduced in any other system which efficient used of solenoid. we have to eliminates the used use of not necessary components such as stepper motors and drivers which is used in the existing system, and also without compromising facial recondition features.

The goal proposed this system work is to be to implemented to convert to the working model of a smart door lock system. Also, to give reliable solution which problem faced by the people in day-to-day life in case loss of key.

Face Recognition Technology

Daily, the lost thefts, identity fraud have been reported in frequent time and also become significant issues. Traditional ways for personal identification require external element, such as key, security password, Radio Frequency Identification card (RFID), and ID card to have access into a private asset or entering public space many processes such as drawing out money from banks requires password. This technique which is required to use of the special type hardware like as fingerprint scanner, palm print scanner, DNA analyzer to gather information for the large majority of the biometric system.. As biometric is a system or technic that

identifies physical highlights of people accordingly it has been a large variety of utilization in security frameworks and one of the best secure methods. Actually, biometrics can be divided in two categories which are physical and behavioral. Recently, the face recognition technology has engaged an overwhelming number of researchers and it is gradually supplanting other biometric security frameworks. Face recognition is also called as image matching. It is a rapidly growing field where it is heading in a direction such that it will replace the traditional method. Face recognition is more stable among others biometric identification method as it is using the human face that results in high accuracy, lowest false recognition rate and it does not change in people's life. Thus, this method is much practical for a lot of usage, including face recognition for the unlocking house door.

Method Used For Face Recognition

In This New Era, Face Recognition Plays An Important Role In Security And Observation. Consequently, There Is A Requirement For A Proficient And Cost-Effective System. Face Recognition Is A Technique That Is Able To Identify And Verify Peoples. Face Recognition, Define As Steps To Identify, Distinguish And Processed Face Is Compared With The Images That Stored In The Database To Verify Who The Person Is. This Face Recognition Is To Become A Significant Technique For User Identification. There Are Many Techniques That Can Be Used For Face Recognition But The Principle Component Analysis (PCA) Is One Of The Famous Techniques Used For Face Recognition. This Method Involves A Mathematical Procedure To Transform A Number Of Possibly Correlated Variables Into A Number Of Uncorrelated Variables Known As Principal Component. Generally, The PCA Technique For Face Recognition Will Utilize The Use Of Eigenfaces. It Is The Effective And Efficient Ways To Represent Pictures Into Eigenfaces Component As It Can Reduce The Size Of The Database Of The Test Image. Numerous Methods Are Developed And Deployed In Order To Improve The Performance Of Face Recognition Technology.

Face Recognition In Raspberry Pi

The first research on face recognition goes way back in 1950 psychology field. The actual work of automatic machine recognition of faces really started in 1970. From all the research done, there two types of face recognition method which are the image-based face recognition and video-based recognition. Video-based face recognition is the process of finding 3D images

from its 2D while the image based recognition method, is the process by which human train the machine using a camera by showing the camera sets of still images. A Face Recognition System is a framework which consequently recognizes and additionally checks the identity of a person from digital images or a video outline from a video source. Many researchers choose to use embedded device called as Raspberry Pi for training and identification purpose. The fundamental reasons why they have picked this particular component because it has high handling limit, low cost and its capacity adjusts in various programming modes. By the used of Raspberry Pi, this helps to resolve the limitation of PC like as its weight, size and high power consumption. Raspberry Pi is a device that can divide the software part into three parts which are recording images, training and face recognition.

IoT In Face Recognition

IoT has been applied in face recognition in many applications such as unmanned arial vehicle, smart classroom, home security system, smart house, smart surveillance and many more applications. The previous implementation of IoT in face recognition are using conventional method such local binary pattern, neural network, support vector machine and k nearest neighbor.

Chapter 3

OVERVIEW OF SMART DOOR LOCK SYSTEM WITH FACE RECOGNITION BASED ON IOT

3.1 SYSTEM DESCRIPTION

This project will design face recognition for real-time use. It is integrated with IoT to perform smart home security system. The deep learning is technique which is used in this project. In order to ensure the expected result are obtained, several major steps need to be conducted such as data collections, implementing, testing, and troubleshooting. These steps are used to analyze the data and output. With these steps, this project is able to be evaluated.

The proposed system architectures generally incorporate a raspberry-pi computer for the purposes of network management and provision of remote access. Raspberry-pi can be configured according to our required system. The user will communicate to raspberry-pi through Wi-Fi network. The system is scalable and flexible, allows additional appliances made by multiple vendors, to be securely and safely added to the home network with the less amount of effort. The Wi-Fi network should be having adequate strength also. We can use a Wi-Fi modem for steeping a Wi-Fi. The system also connects to the blynk app.

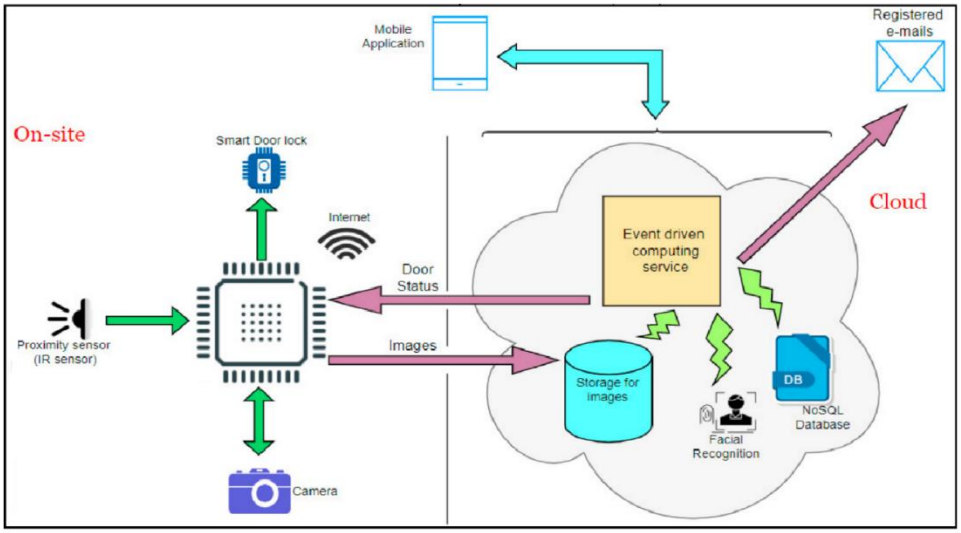

Figure 3.1.1 Architecture of System

The camera for motion detection is also connected in the same network. The raspberry-pi board is configured for each appliance. So, according to user intervention the matched out will make high and the corresponding relay will switch on and device start function. The system is scalable and allows multi-vendor appliances to be added with no major changes to its core.

The system has three main components :

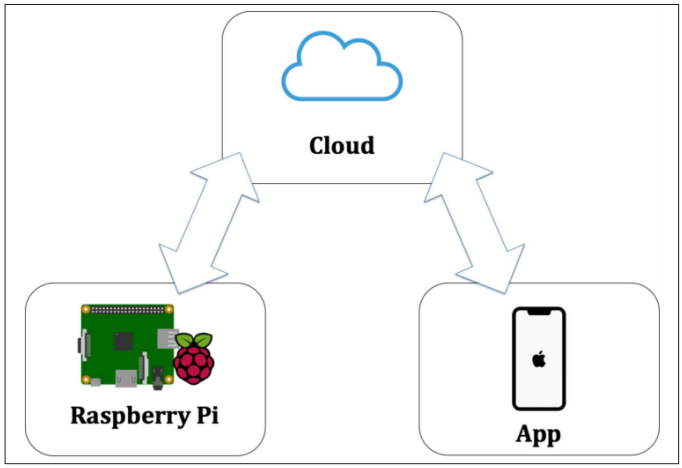

Figure 3.1.2 The three main components smart door lock system

- Raspberry Pi.
- Cloud System.
- Android App/Blynk App for access control.

3.2 WORKING

Face recognition and smart lock access system uses pi camera attached to Raspberry Pi 3 b+ for face detection, face recognition and assume solenoid lock for lock and unlock. The system is designed on the basis of simple Machine Learning. Initially the owner image is captured in different angles and is store in database. These images are trained to produce a single data set so that it helps in fast comparison and recognition. Figure 3.1.1 shows block diagram system prototype.

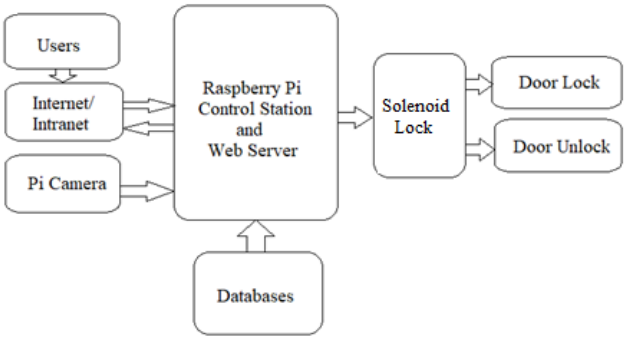

Figure 3.2.1 System Block Diagram

The prototype is built by combining the part of face recognition and IoT together. Face recognition is operated at first place. There are five steps in face recognition, which are collecting images, creating database, pre-processing images, training images and testing images. Firstly, images are collected. These images are obtained by capturing using camera and used the existing images. This image is used for training purpose for the system to be more accurate when dealing with new images. A total of five persons, each with five pictures is taken from different positions. Each picture is approximately 268 x 350 pixels of height and width. Images that are collected are stored in the database as shown in Figure 3.2.2.

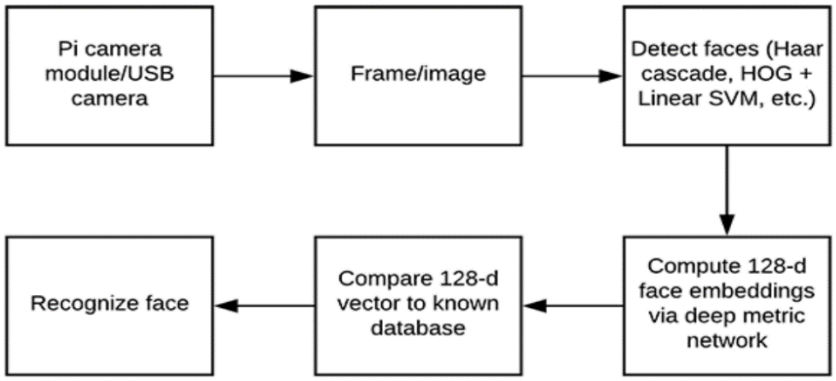

Figure 3.2.2 System Process Flow Diagram

Since face recognition framework a need large number of images, existing images have been augmented. This is done by using an algorithm. Each picture per person will augment into 100 pictures, resulting 2500 images stored in database. The images vary in brightness, color, intensity, and angle. This is to ensure that face recognition system can detect even in different conditions. Figure 3.2.3 shows the transformation from the original image in the database into

the processed photo. The result of each person categorized into each folder. Next, the cropping process takes place. This process will crop the exact face from the images. This process is carried out by using an algorithm. The pixel of each picture is reduced to 48 x 48 pixels of height and width. Following figure shows extract features by separating the face from the background.

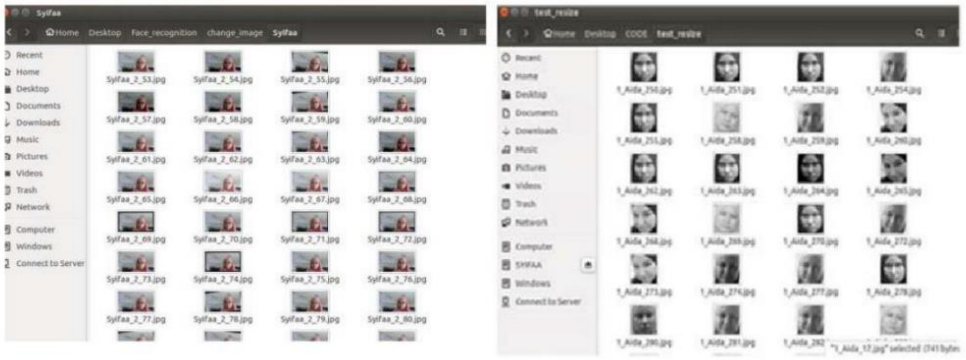

Figure 3.2.3 Face Extraction

Deep learning Existing architecture was used in the training process. Images were train using deep learning method using Convolutional Neural Network (CNN) technique. The current architecture used is Alex Net which consist of eight layers. This architecture builds with several layer and activation function such as Convolution, Max pooling, Flatten, Dense, Activation and Dropout. The entire neural network approach was implemented in Python language and Keras library. The training involves 100 epochs at first and repeated with 20 epochs after the testing phase. Figure 3 will illustrate the training process of the dataset. After training process was done image testing is required to determine the accuracy achieved by the system. In this stage, image that are not in the database are used as test images. There are ten images tested for each labelled which are recognized and unrecognized person. Each image tested will labelled the image with name or as an unknown.

```
4448/5006 [=======================>....] - ETA: 4s - loss: 0.0021 - acc: 0.999
4480/5006 [=======================>....] - ETA: 4s - loss: 0.0021 - acc: 0.999
4512/5006 [========================>...] - ETA: 3s - loss: 0.0020 - acc: 0.999
4544/5006 [========================>...] - ETA: 3s - loss: 0.0020 - acc: 0.999
4576/5006 [========================>...] - ETA: 3s - loss: 0.0020 - acc: 0.999
4608/5006 [========================>...] - ETA: 3s - loss: 0.0020 - acc: 0.999
4640/5006 [========================>...] - ETA: 2s - loss: 0.0020 - acc: 0.999
4672/5006 [========================>...] - ETA: 2s - loss: 0.0020 - acc: 0.999
4704/5006 [========================>..] - ETA: 2s - loss: 0.0020 - acc: 0.999
4736/5006 [=========================>..] - ETA: 2s - loss: 0.0019 - acc: 0.999
4768/5006 [=========================>..] - ETA: 1s - loss: 0.0019 - acc: 0.999
4800/5006 [=========================>..] - ETA: 1s - loss: 0.0019 - acc: 0.999
4832/5006 [=========================>..] - ETA: 1s - loss: 0.0019 - acc: 0.999
4864/5006 [=========================>.] - ETA: 1s - loss: 0.0019 - acc: 0.999
4896/5006 [=========================>.] - ETA: 0s - loss: 0.0019 - acc: 0.999
4928/5006 [=========================>.] - ETA: 0s - loss: 0.0019 - acc: 0.999
4960/5006 [=========================>.] - ETA: 0s - loss: 0.0019 - acc: 0.999
4992/5006 [=========================>.] - ETA: 0s - loss: 0.0019 - acc: 0.999
```

Figure 3.2.4 Training the dataset

Chapter 4

HARDWARE & SOFTWARE DESCRIPTION

4.1 HARDWARE COMPONENTS

- Raspberry Pi Model 3B+
- Raspberry Pi camera module v2
- PIR Sensor
- Solenoid Lock
- Relay
- Jumper Wires

4.2 SOFTWARE & ALGORITHM

- Raspbian Stretch OS (kernel 4.14)
- New Out OF Box Software (NOOBS)
- Python IDLE (for program development)
- Open CV
- Internet of things (IoT) Platform

4.1 HARDWARE COMPONENTS

4.1.1.[A] Raspberry Pi Model 3b+

Raspberry Pi is a series of small single board computers developed in the United Kingdom by the Raspberry Pi Foundation in association with Broadcom. Raspberry Pi board was developed for applications and installations where space is premium and projects are made as permanent setups.

Figure 4.1.1 A (1) Raspberry Pi Model 3B +

- **Overview**

The Raspberry Pi 3 Model B+ is the latest product in the Raspberry Pi 3 range, boasting a 64-bit quad core processor running at 1.4GHz, dual-band 2.4GHz and 5GHz wireless LAN, Bluetooth 4.2/BLE, faster Ethernet, and PoE capability via a separate PoE HAT.

The dual-band wireless LAN comes with modular compliance certification, allowing the board to be designed into end products with significantly reduced wireless LAN compliance testing, improving both cost and time to market.

The Raspberry Pi 3 Model B+ maintains the same mechanical footprint as both the Raspberry Pi 2 Model B and the Raspberry Pi 3 Model B.

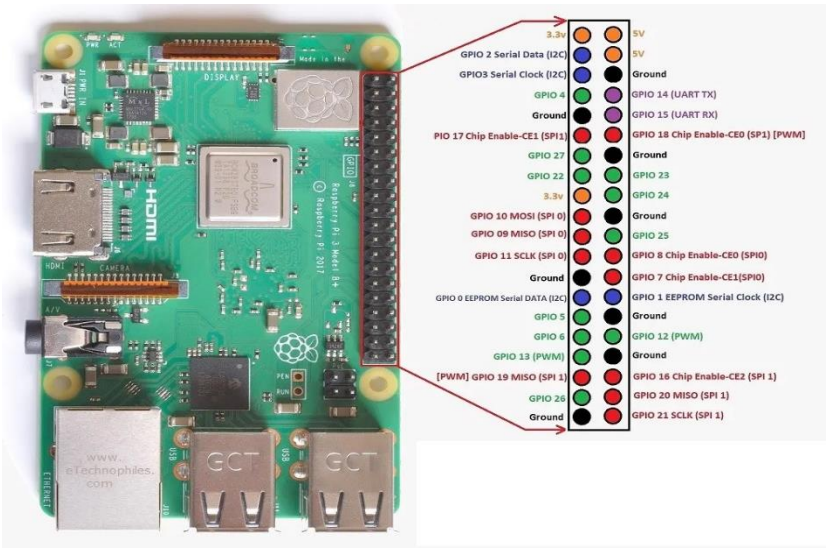

Figure 4.1.1 A (2) Raspberry Pi Pin Out Details

Raspberry Pi 3 B+ Power Pins: The model B+ board consists of two 5V pins, two 3V3 pins, and 9 Ground pins (0V), which are unconfigurable.

5V: The 5v pins are used to directly deliver the 5v supply coming from the mains adaptor. This pin can use to power up the Raspberry Pi, and it can also use to power up other 5v devices.

3.3V: The 3v pin is used to provide a stable 3.3v supply to external components and also to test LEDs.

GND: Ground is commonly referred to as GND. All the voltages are measured with respect to the GND voltage.

Input/Outputs pins:

A GPIO pin set as **Input** reads the signal received by the Raspberry Pi, sent by the device connected to this pin. Any voltage between 1.8V and 3.3V is read as HIGH and voltage lower than 1.8V as LOW by the Raspberry Pi. A GPIO pin set as an **output** pin sends the voltage

signal as high (3.3V) or low (0V). When this pin is set to HIGH, the voltage at the output is 3.3V and when set to LOW, the output voltage is 0V.

Along with the simple function of input and output pins, the GPIO pins can also perform a variety of specific functions. Some specific pins are:

PWM (pulse-width modulation) Pins on Model 3B+ :

Software PWM is available on all pins

Hardware PWM is available on these pins only: GPIO12, GPIO13, GPIO18, GPIO19.

SPI Pins on Model 3B+ :

SPI (Serial Peripheral Interface) is another protocol used for master-slave communication. It is used by the Raspberry pi board to quickly communicate between one or more peripheral devices. Data is synchronized using a clock (**SCLK** at GPIO11) from the master (RPi) and the data is sent from the Pi to our SPI device using the **MOSI** (Master Out Slave In) pin. If the SPI device needs to communicate back to Raspberry Pi, then it will send data back using the **MISO** (Master In Slave Out) pin. 5 pins are needed for the SPI communication:

GND: Connect all GND pins from all the slave components and the Raspberry Pi 3 board together.

SCLK: Clock of the SPI. Connect all SCLK pins.

MOSI: It stands for Master Out Slave In. This pin is used to send data from the master to a slave.

MISO: It stands for Master In Slave Out. This pin is used to receive data from a slave to the master.

CE: It stands for Chip Enable. We need to connect one CE pin per slave (or peripheral devices) in our circuit. By default, we have two CE pins but we can configure more CE pins from the other available GPIO pins.

SPI pins on R-Pi Model 3B+ :

SPI0: GPIO9 (MISO), GPIO10 (MOSI), GPIO11 (SCLK), GPIO8 (CE0), GPIO7 (CE1)

SPI1: GPIO19 (MISO), GPIO20 (MOSI), GPIO21 (SCLK), GPIO18 (CE0), GPIO17 (CE1), GPIO16 (CE2)

I2C Pins on R-Pi 3B+ :

I2C is used by the Raspberry Pi board to communicate with devices that are compatible with Inter-Integrated Circuit (a low-speed two-wire serial communication protocol). This communication standard requires master-slave roles between both the devices. I2C has two connections: **SDA (Serial Data)** and **SCL (Serial Clock).** They work by sending data to and using the SDA connection, and the speed of data transfer is controlled via the SCL pin.

Data: (GPIO2), Clock (GPIO3)

EEPROM Data: (GPIO0), EEPROM Clock (GPIO1)

UART Pins on R-Pi 3B+ :

Serial communication or the UART (Universal Asynchronous Receiver / Transmitter) pins provide a way to communicate between two microcontrollers or the computers. TX pin is used to transmit the serial data and RX pin is used to receive serial data coming from a different serial device.

TX (GPIO14)

RX (GPIO15)

- **Technical Specification**

The Raspberry Pi 3 Model B+ is the final revision in the Raspberry Pi 3 range.

Processor	: Broadcom BCM2837B0, Cortex-A53 64-bit SoC @ 1.4GHz.
Memory	: 1GB LPDDR2 SDRAM
Connectivity	: 2.4GHz and 5GHz IEEE 802.11.b/g/n/ac wireless LAN, Bluetooth 4.2, BLE. Gigabit Ethernet over USB 2.0 (maximum throughput 300Mbps).
Access	: Extended 40-pin GPIO header
Video & Sound	: 1 × full size HDMI MIPI DSI display port MIPI CSI camera port 4 pole stereo output and composite video port
Multimedia	: H.264, MPEG-4 decode (1080p30); H.264 encode (1080p30); OpenGL ES 1.1, 2.0 graphics
SD card support	: Micro SD format for loading operating system and data storage.
Input power	: 5V/2.5A DC via micro USB connector. 5V DC via GPIO header. Power over Ethernet (PoE)–enabled (requires separate PoE HAT.
Environment	: Operating temperature, 0–50°C.

4.1.1 [B] Power Supply

The power supply requirement differs by Raspberry Pi model. All models require a 5.1V supply, but the current supplied generally increases according to model. All models up to the

Raspberry Pi 3 require a micro USB power connector. Exactly how much current (mA) the Raspberry Pi require is dependent on what you connect to it. Raspberry Pi have developed their own power supplies for use with all models. These are reliable, use heavy gauge wires and are reasonably priced. For Raspberry Pi 0-3, recommend 2.5 A micro USB supply.

The power requirement of the Raspberry Pi increase as you make use of various interfaces on the Raspberry Pi. The GPIO pins can draw 50mA safety, distributed across all the pins; an individual GPIO pin can safely only draw 16 mA. The HDMI port uses 50 mA, the camera module requires module requires 250mA, and keyboards and mice can take as little as 100 mA or over 1000 mA. Check the power rating of the devices you plan to connect to the Pi and purchase a power supply accordingly. If required more power above specified valued then must connect it to an externally powered USB hub.

4.1.2 Raspberry Pi Camera Module V2

The Raspberry Pi Camera Module v2 used for to capture images in the system.

Figure 4.1.2 Raspberry Pi Camera Module v2

The Raspberry Pi Camera Module v2 replaced the original Camera Module in April 2016. The v2 Camera Module has a Sony IMX219 8-megapixel sensor (compared to the 5-megapixel Omni Vision OV5647 sensor of the original camera).

The Camera Module can be used to take high-definition video, as well as stills photographs. It's easy to use for beginners, but has plenty to offer advanced users if you're looking to expand your knowledge. There are lots of examples online of people using it for time-lapse, slow-motion, and other video cleverness. You can also use the libraries we bundle with the camera to create effects. It supports 1080p30, 720p60 and VGA90 video modes, as well as still capture. It attaches via a 15cm ribbon cable to the CSI port on the Raspberry Pi.

The camera works with all models of Raspberry Pi 1, 2, 3 and 4. It can be accessed through the MMAL and V4L APIs, and there are numerous third-party libraries built for it, including the Pi Camera Python library. The camera module is very popular in home security applications, and in wildlife camera traps.

4.1.3 PIR Sensor

Passive Infrared Sensors are made of pyroelectric sensors, which can detect levels of infrared radiation. Everything radiates some low level of radiation. However, the hotter the object is, the more radiation is emitted. The sensor in a motion detector is split in two halves in order to detect change between the two. The two halves work with each other by cancelling out normal IR levels in the background. When one half detects more IR radiation than the other, the output will swing high or low, therefore detecting motion. The heat released of the human body is enough to trigger this sensor, making it one of the most commonly used in security and lighting appliances.

Figure 4.1.3 PIR Sensor

- Specification

Range : 5.2 m

Angle : 90 degrees for 1 m/s

Type of Info : Type of Info : HIGH, LOW

4.1.4 Solenoid Lock

In conventional door lock, there is a key to pull or push the latch, and we have to operate it manually, but in solenoid lock, the latch can be operated automatically by applying a voltage. Solenoid lock has a low-voltage solenoid that pulls the latch back into the door when an interrupt (Pushbutton, Relay, etc.) is activated. The latch will retain its position until the interrupt is enabled. The operating voltage for the solenoid lock is 12V. You can also use 9V, but it results in slower operation. Solenoid door locks are mainly used in remote areas to automate operations without involving any human effort.

Figure 4.1.4 Solenoid Lock

4.1.5 Relay

A relay is an electromagnetic switch where a small control signal usually from a microcontroller at the input of the Relay will control a high voltage supply usually AC mains. Since this is a Raspberry Pi based project. The Raspberry Pi computer, although a powerful device, works on a 3.3V Logic.

Solenoid lock works on 9-12 volt, due to this we are using relay circuit. Relay is a simple electromechanical device that consists of a coil and few electrical contacts. When the coil is energized, it acts as an electromagnet and closes a switch. If the coil is de-energized, the coil loses its magnetic nature and releases the switch.

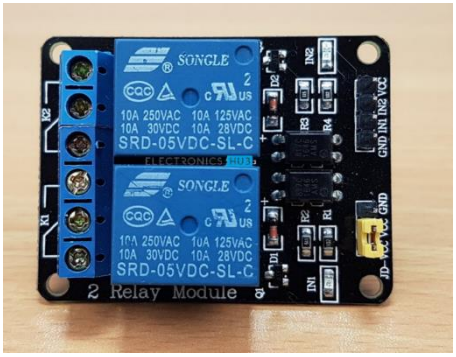

Figure 4.1.5 Relay

So, by controlling the coil, you can control a switch, which in turn will control an electrical load. You can control the coil of the relay with the help of Raspberry Pi although not directly, but with additional circuitry as all you need is a small current to energize the coil.

4.1.6 JUMPER WIRES

Jumper wires are used to make it easier to manage circuits built on the system. They allow the components of the circuit to be spread out more, allowing easier access, and also allows them to be laid out in a more logical fashion.

Figure 4.1.6 Jumper wires

4.2 SOFTWARE & ALGORITHM

4.2.1 Raspbian Stretch OS (Kernel 4.14)

Raspberry Pi OS is also formerly known as Raspbian. It is a Debian based operating system for Raspberry Pi . Since 2015, it has been officially provided by the Raspberry Pi as the primary operating system for the Raspberry Pi family of compact single board computers. The first version of Raspbian was created by Mike Thompson and Peter Green as an independent project. The initial build was completed in June 2012.

Raspberry Pi OS is highly optimized for the Raspberry Pi line of compact single-board computers with ARM CPUs. It runs on every Raspberry Pi except the Pico microcontroller. Raspbian Stretch is the 9th Debian version of OS with Kernel 4.14 version.

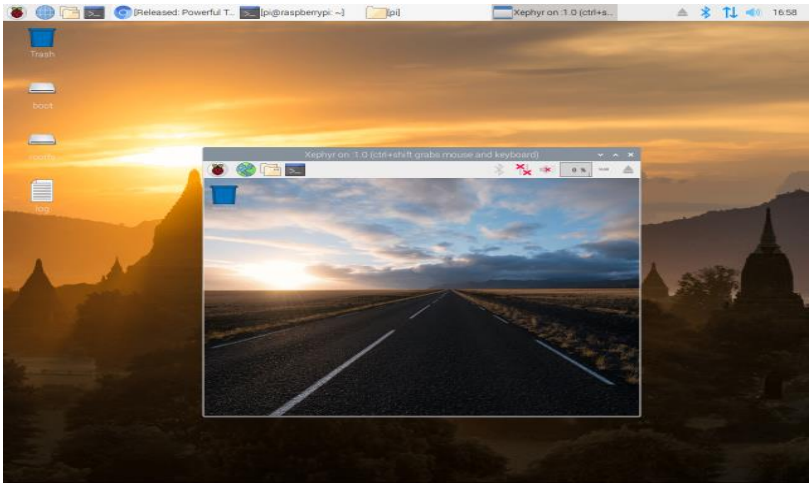

Figure 4.2.1 Interface of Raspberry OS

4.2.2 New Out Of Box Software (Noobs)

The Raspberry Pi itself doesn't come with an operating system. For that, you need NOOBS, In short for New Out of the Box Software. It's an operating system manager that makes it easy to download, install, and set up your Raspberry Pi. When you first boot up NOOBS, you'll get a selection of OS to choose from. Which operating systems are available depends on which model of Raspberry Pi you are using. For this guide,

we'll stick to the most common OS's operating systems available on the newest models of the Raspberry Pi. Right now, that's Raspbian, OSMC, Open ELEC, Windows IoT Core, and RISC OS.

4.2.3 Python Idle

IDLE is Python's Integrated Development and Learning Environment. Python integrated development environment. As the name implies, ide integrate several tools usually include an editor designed to handle code with for example syntax, highlighting and auto completion of code etc.

4.2.4 Open CV

OpenCV is an open source computer vision software library. The library has a lot of optimized algorithms, which can be used in many IOT related sectors including face detection and recognition. As the libraries of our project, we liked to use the Haar classifier, LBPH (Lower Binary Pattern histogram) face recognizer.

OpenCV and its primary interface are written in C++. OpenCV also provides bindings in Python, Java and MATLAB/OCTAVE. OpenCV is available on Windows, Linux, macOS, FreeBSD, NetBSD, and OpenBSD desktop operating systems, and Android, iOS, Maemo, and BlackBerry 10 mobile operating systems.

4.3.5 Internet Of Things (IoT) Platform

Blynk is a famous apps since it has been downloaded more than 100 thousand users. Blynk is a platform for iOS and Android apps that managed to control Raspberry pi and many other microcontrollers. It is a digital dashboard that designed for the user to create their own graphic interface for the project. It is easy and simple to use as the user can simply drag and drop the widgets that they need according to their project type. This app is used in IoT part. Blynk start online as the Raspberry Pi connected to the internet over Wi-Fi. Besides, it is also will get online by link to the internet through the Ethernet or the new ESP8266 chip. For condition where face cannot be recognized, that person can press the doorbell and notification are sent to smartphone of house owner. Hence, live streaming video will appear to identify the person trying to unlock the door.

Chapter 5

RESULTS AND DISCUSSION

5.1 RESULTS

This work was aimed to be complete system for detection and recognition of human faces, which is easy to build and cost effective. Its utility is to be set as an alert for home visitors, industries, air ports or in offices and provide information about the visitors. An automatic smart lock monitoring system using webcam, Python, Open CV, Raspberry Pi, controller is designed for monitoring and security purpose, Since IoT is booming technology, we can also explore the possibilities of IoT in security and automation.

Face recognition is tested on two types which are by testing image and real-time to determine the system accuracy. For testing image, there are ten images that are not in the database are tested for each label which are authorized and unknown person. The tested image will have labelled the image with names for authorized person while unknown for unauthorized person. Figure 5 (a) shows the IoT app interface before login, figure 5 (b) shows IoT app interface after login and figure (c) shows the smart door lock system.

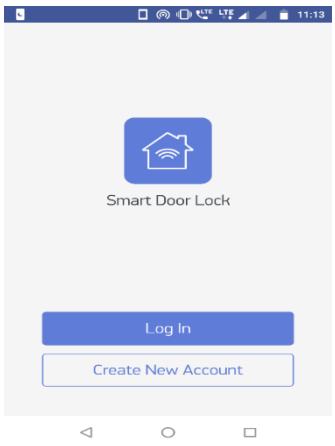

Figure 5.1 (a) Blynk IoT App Login Interface

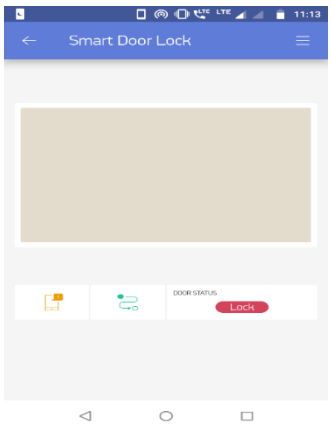

Figure 5.2 (b) Blynk IoT App After Login Interface

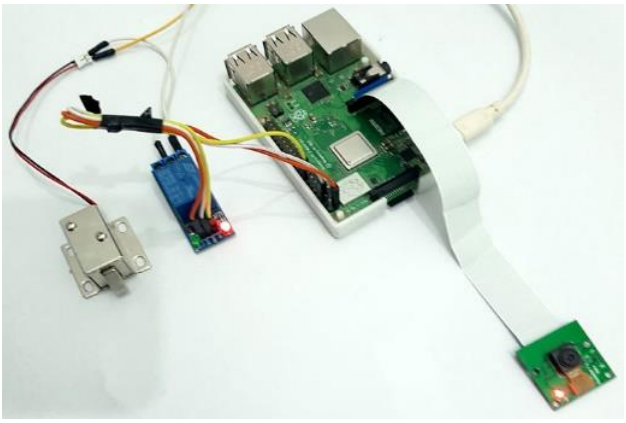

Figure 5.3 (c) Smart Door Lock System

5.2 ADVANTAGES

- Reliability of system is very good.
- It provides enough flexibility to suit the requirement.
- More secure to the face detection and recognition.
- Simple and easy access.
- System is littler, lighter and has required lower power.
- System cost is moderate.

5.3 DISADVANTAGES

- Slightly lower accuracy of system is less as expected as.
- System can be continuously connected to the internet.

5.4 APPLICATIONS

1. Control of doors.

2. The mechanism is based on the security protocols

3. With smart door lock system you can decide who can enter your home.

4. By using smart app, disabled or elderly people can control lock from anywhere inside house.

5. Used at Industries, Home, Office, Shop.

Chapter 6

CONCLUSIONS AND FUTURE SCOPE

6.1 CONCLUSIONS

- As a conclusion, security system by using face recognition combined with IoT is successfully done.

- The face recognition is able to recognize the face and able to send notification to a user when an unknown being has been detected through IoT.

- On the other hand, this project is this project still has a big room of improvement to be done, especially in the efficiency of the image processing part.

- Due to the module used which is Raspberry Pi 3, the processing time of the coding took a long time so process the image taken and take action. By using another better module, this project can be improved greatly.

- It can be used in other settings and for multiple door locks, and can also be extended to other use-cases which involve safeguarding and or surveillance.

6.2 FUTURE SCOPE

In this system can be changed into double number verification mechanism such retina scanner, fingerprint, OTP, Pin Code, etc. This system will first recognize the face and if face is found in the database if face is not recognizable then it will ask for second verification mechanism will may be any one of the above and if person passes both the verification test then only door will open and if face is not found in the database the image will be sent to system. This system will provide excellent security. The face recognition mechanism can be combined with any other. In future the accuracy, reliability can be increased at great extent and also in future more functionality will be added in an app and make it more user friendly.

REFERENCES

[1] Jay Patel, Sundar Anand, Rohan Luthra, "Image-Based Smart Surveillance and Remote Door Lock Switching System for Homes", *International Conference on Recent Trends In Advanced Computing 2019, ICRTAC 2019, Vellore Institute of Technology, Vandalur-Kelambakkam Road, Chennai 600127, India.*

[2] Teddy Surya Gunawan, Muhammad Hamdan Hasan Gani, Farah Diyana Abdul Rahman, Mira Kartiwi, "Development of Face Recognition on Raspberry Pi for Security Enhancement of Smart Home System" *Indonesian Journal of Electrical Engineering and Informatics (IJEEI), Vol. 5, No. 4, December 2017, pp. 317-325.*

[3] Sourav Roy; 2 Md Nasir Uddin; 3 Md Zahirul Haque; 4 Md Jahidul Kabir, "Design and Implementation of the Smart Door Lock System with Face Recognition Method using the Linux Platform Raspberry Pi", *IJCSN - International Journal of Computer Science and Network, Volume 7, Issue 6, December 2018, pp. 382-388.*

[4] Thulluri Krishna Vamsi, Kanchana Charan Sai, Vijaylakshmi M, " Face recognition based door unlocking System using Raspberry Pi", *International Journal of Advance Research, Ideas and Innovation in Technology, Volume 5, Issue 2, 2019, pp. 1320-1324.*

[5] Rajat Bhise, Nikilesh Phadnis, Rahul Bari, Vijay Dhage, "IoT Based Door Lock and Unlock System Using Face Recognition", *International Research Journal of Engineering and Technology (IRJET),* Volume 05, Issue 12, Dec 2018, pp. 1136-1138.

[6] Prof. M. R. Sanghavi, Srujal Sancheti, Bhakti Patel, Sanjana Shinde, Neha Lunkad, "Smart Door Unlock System Using Face Recognition and Voice Commands" *International Research Journal of Engineering and Technology (IRJET), Volume 07, Issue 06 , June 2020, pp. 3304-3307.*

[7] Aleksander Ibro, Augusto Rolando Woong, Mario A. Zyla, "Face Recognition Door Lock" *Digital WPI, April 2019, Worcester Polytechnic Institute.*

Appendix

Programs :

```
# For Face Detection
import cv2
from picamera.array import PiRGBArray
from picamera import PiCamera
import numpy as np
import os
import sys

camera = PiCamera()
camera.resolution = (640, 480)
camera.framerate = 30
rawCapture = PiRGBArray(camera, size=(640, 480))

faceCascade = cv2.CascadeClassifier("haarcascade_frontalface_default.xml")

name = input("What's his/her Name? ")
dirName = "./images/" + name
print(dirName)
if not os.path.exists(dirName):
                    os.makedirs(dirName)
                    print("Directory Created")
else:
                    print("Name already exists")
                    sys.exit()
```

```
count = 1
for frame in camera.capture_continuous(rawCapture, format="bgr", use_video_port=True):
                    if count > 30:
                        break
                    frame = frame.array
                    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
                    faces = faceCascade.detectMultiScale(gray, scaleFactor = 1.5,
minNeighbors = 5)
                    for (x, y, w, h) in faces:
                        roiGray = gray[y:y+h, x:x+w]
                        fileName = dirName + "/" + name + str(count) + ".jpg"
                        cv2.imwrite(fileName, roiGray)
                        cv2.imshow("face", roiGray)
                        cv2.rectangle(frame, (x, y), (x+w, y+h), (0, 255, 0), 2)
                        count += 1

                    cv2.imshow('frame', frame)
                    key = cv2.waitKey(1)
                    rawCapture.truncate(0)

                    if key == 27:
                        break

cv2.destroyAllWindows()
```

```
# Training the Recognizer
import cv2
from picamera.array import PiRGBArray
from picamera import PiCamera
import numpy as np
import pickle
import RPi.GPIO as GPIO
from time import sleep

relay_pin = [26]
GPIO.setmode(GPIO.BCM)
GPIO.setup(relay_pin, GPIO.OUT)
GPIO.output(relay_pin, 0)

with open('labels', 'rb') as f:
                                        dicti = pickle.load(f)
                                        f.close()

camera = PiCamera()
camera.resolution = (640, 480)
camera.framerate = 30
rawCapture = PiRGBArray(camera, size=(640, 480))


faceCascade = cv2.CascadeClassifier("haarcascade_frontalface_default.xml")
recognizer = cv2.face.LBPHFaceRecognizer_create()
recognizer.read("trainer.yml")
```

```
font = cv2.FONT_HERSHEY_SIMPLEX


for frame in camera.capture_continuous(rawCapture, format="bgr", use_video_port=True):
                frame = frame.array
                gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
                faces = faceCascade.detectMultiScale(gray, scaleFactor = 1.5,
minNeighbors = 5)
                for (x, y, w, h) in faces:
                    roiGray = gray[y:y+h, x:x+w]


                    id_, conf = recognizer.predict(roiGray)


                    for name, value in dict.items():
                            if value == id_:
                                    print(name)


                    if conf <= 70:
                            GPIO.output(relay_pin, 1)
                            cv2.rectangle(frame, (x, y), (x+w, y+h), (0, 255, 0), 2)
                            cv2.putText(frame, name + str(conf), (x, y), font, 2, (0, 0
,255), 2,cv2.LINE_AA)


                    else:
                            GPIO.output(relay_pin, 0)


                cv2.imshow('frame', frame)
                key = cv2.waitKey(1)


                rawCapture.truncate(0)
```

```
                    if key == 27:
                        break

cv2.destroyAllWindows()
```

Blynk Python Library

```
import blynklib

# import blynklib_mp as blynklib # micropython import


BLYNK_AUTH = '<YourAuthToken>' #insert your Auth Token here

# base lib init

blynk = blynklib.Blynk(BLYNK_AUTH)


# advanced options of lib init

# from __future__ import print_function

# blynk = blynklib.Blynk(BLYNK_AUTH, server='blynk-cloud.com', port=80,
ssl_cert=None,

#                        heartbeat=10, rcv_buffer=1024, log=print)


# Lib init with SSL socket connection
```

```
# blynk = blynklib.Blynk(BLYNK_AUTH, port=443, ssl_cert='<path to local blynk server certificate>')

# current blynk-cloud.com certificate stored in project as

# https://github.com/blynkkk/lib-python/blob/master/certificate/blynk-cloud.com.crt

# Note! ssl feature supported only by cPython



# register handler for Virtual Pin V22 reading by Blynk App.

# when a widget in Blynk App asks Virtual Pin data from server within given configurable interval (1,2,5,10 sec etc)

# server automatically sends notification about read virtual pin event to hardware

# this notification captured by current handler

@blynk.handle_event('read V22')

def read_virtual_pin_handler(pin):



    # your code goes here

    # ...

    # Example: get sensor value, perform calculations, etc

    sensor_data = '<YourSensorData>'

    critilcal_data_value = '<YourThresholdSensorValue>'



    # send value to Virtual Pin and store it in Blynk Cloud
```

```
    blynk.virtual_write(pin, sensor_data)


    # you can define if needed any other pin

    # example: blynk.virtual_write(24, sensor_data)


    # you can perform actions if value reaches a threshold (e.g. some critical value)

    if sensor_data >= critilcal_data_value


        blynk.set_property(pin, 'color', '#FF0000') # set red color for the widget UI element

        blynk.notify('Warning critical value') # send push notification to Blynk App

        blynk.email(<youremail@email.com>, 'Email Subject', 'Email Body') # send email to
specified address


# main loop that starts program and handles registered events

while True:

    blynk.run()
```


CERTIFICATION
OF PUBLICATION
IJIRSET
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY
Website: www.ijirset.com Email: ijirset@gmail.com
Impact Factor 7.512
This is hereby Awarding this Certificate to
DNYANESH SUDHAKAR KOLHE
U.G. Student, Department of Electronics and Telecommunication, P. R. Patil College of Engineering and Technology, Amravati, Maharashtra, India
Published a paper entitled
Smart Door Lock System with Face Recognition Based on IoT
in IJIRSET, Volume 10, Issue 6, June 2021
e-ISSN: 2319-8753
p-ISSN: 2320-6710
INTERNATIONAL STANDARD SERIAL NUMBER
INNO SPACE
SJIF Scientific Journal Impact Factor
Editor-in-Chief

Plagiarism Checker X Originality Report

Plagiarism Quantity: 30% Duplicate

Date	Tuesday, June 29, 2021
Words	1461 Plagiarized Words / Total 4932 Words
Sources	More than 63 Sources Identified.
Remarks	Medium Plagiarism Detected - Your Document needs Selective Improvement.

Chapter 1 INTRODUCTION INTRODUCTION The aim of this project was to design and build a door lock system that allows users to unlock a door via face recognition, through a camera implanted on the door. In this method chapter, we will discuss how we detailed the process of implementing this mechanism. In current digital world of connectivity where smart devices need to be modified this makes life easier. I today's world we can't trust anyone and also compromise with old conventional security system. Nowadays, home security system is a crucial issue. Indeed, this system is to ensure properties and loves ones is always safe and protected. Face recognition is the most famous method in biometric technology besides fingerprint characteristics. This is due to more stability as face contains more features.

Besides, it is considered highly secure as face cannot be stolen, borrowed or forge in order to enter the house. Face recognition is likely the most natural approach to perform biometric verification between individuals. Face detection is the first step of the face recognition system. Face pictures can be caught at a distance with the use of a web camera. The individual can be recognized without physical contact on any special hardware to perceive the person's identity. Face recognition using deep learning technique is used. Deep learning is a piece of the more extensive group of machine learning methods based on learning data representations, as opposed to task specific algorithms. Learning can be managed, semi-directed or unsupervised. With the deep learning, the system is improved from time to time. Some images of authorizing user are used as the database of system and the system will train the face recognition automatically.

Thus, the accuracy is increased. Home security is an example of an Internet of Things (IoT) applications. IoT refers to the network of associated physical objects that can interact and trade information among themselves without the need of any human intervening. IoT is a futuristic technology where devices and internet is interconnected. It is different from the internet due to internet exceed connectivity by allowing any embedded circuit to communicate with each other using the current internet infrastructure. No doubt IoT helps users to control one or more devices and capabilities to automate with many daily chores. By using IoT, it can help in controlling the door access and also sent notification throughout the internet. In this system, Blynk apps are used. Blynk apps is an app that enables us to control the door access by designing the graphical interface in

Sources found:

Click on the highlighted sentence to see sources.

Internet Pages

<1% https://www.academia.edu/40090962/FINGER
<1% https://www.irjet.net/archives/V8/i5/IRJ
6% https://pdfs.semanticscholar.org/5518/8e
<1% https://www.mdpi.com/2079-9292/9/8/1188/
<1% https://www.quora.com/What-are-some-appl
<1% https://drrajivdesaimd.com/2016/07/19/in
<1% https://www.arubanetworks.com/techdocs/A
<1% https://www.igd.fraunhofer.de/en/institu
<1% https://dokumen.pub/machine-learning-and
1% https://www.academia.edu/39042426/Face_r
1% http://umpir.ump.edu.my/id/eprint/327/3/
<1% https://www.tbmc.edu.vn/07S_face-detecti
1% https://www.irjet.net/archives/V5/i12/IR
<1% https://dokumen.pub/machine-learning-and
<1% https://issuu.com/itsligo/docs/sete21_ev
<1% https://www.coursehelponline.com/
<1% http://iosrjen.org/Papers/vol2_issue12(p
<1% https://www.sciencedirect.com/science/ar
<1% https://open.library.ubc.ca/clRcle/colle
<1% https://jivp-eurasipjournals.springerope
<1% https://randomnerdtutorials.com/cctv-ras
<1% https://www.ijariit.com/manuscripts/v3i2
<1% https://web.wpi.edu/Pubs/E-project/Avail
<1% https://www.academia.edu/43411267/IOT_BA
<1% https://www.intechopen.com/books/face-re