DOOR LOCKING SYSTEM USING FACE RECOGNITION

A Project Report submitted in partial fulfillment of the requirements for the award of the degree

BACHELOR OF ENGINEERING

In

ELECTRONICS & TELECOMMUNICATION

Of

SAVITRIBAI PHULE PUNE UNIVERSITY

By

RISHABH MANTRI	**Exam No. 72022536B**
ROHIT KALVENI	**Exam No. 72022545M**
MAYUR VISHWAKARMA	**Exam No. 72022755M**

Under the Guidance of

PROF. A. B. KALE

Department of Electronics & Telecommunication Engineering
Sinhgad College of Engineering,
Vadgaon (BK), Pune - 411041

2022-2023

Sinhgad Institutes

CERTIFICATE

This is to certify that the project report entitled

"DOOR LOCKING SYSTEM USING FACE RECGONITION"

Submitted by

Rishabh Mantri
Rohit Kalveni
Mayur Vishwakarma

Has successfully completed his Project under the supervision of **Prof. A B Kale** for the partial fulfillment of Bachelor of Engineering **Electronics Telecommunication** of Savitribai Phule Pune University. This work has not been submitted elsewhere for any degree.

Prof. A B Kale
Guide

Dr. M B Mali
Head - Dept. of E & TC

Examiner

Dr. S D Lokhande
Principal SCOE

Contents

List of Figures

Abstract

Computer vision has become an extremely evolving field in recent years, addressing strategies for getting, processing, examining, and understanding digital pictures. Face recognition in PC vision encompasses a very important role to play in security and police work and the mechanisms for increasing the protection levels square measure strengthening day by day. The present face recognition system has been increased by introducing an associate degree anti-spoofing mechanism which can facilitate to prevent of a villainous person from designedly getting around with the system.

The system is predicated on object detection and identity verification code developed in Python programming language. Through a digital camera, it obtains pictures in a period to form a comparison with the faces kept in a database. For paradigm implementation, the associate degree embedded platform (Raspberry Pi) was accustomed offer the bottom package for programming and supplying associate degree analog signals in response to the system.

The aim of this project is to form the precedent of an associate degree easy-to-use home security door lockup system that will simply and safely be put in in any family for tiny value while giving correct details still because of the potential for quantifiability and upgrades. It additionally shows the potential of IoT devices like the Raspberry Pi, which is employed during this project.

Acknowledgements

We are feeling very humble in expressing our gratitude. It will be unfair to bind the precious help and support that we got from many people in a few words. But words are the only media for expressing one's feelings and our feeling of gratitude is absolutely beyond these words. It would be our pride to take this opportunity to say thanks.

Firstly, we would thank our guide Prof A.B. Kale for her valuable guidance, patience, and support; She was always there to force us a bit forward to get the work done properly and on time. She has always given us the freedom to do dissertation work and the chance to work under her supervision.

We would like to express our sincere thanks to Prof. V. B. Baru, Major Project Coordinator, Department of ETC, for his constant encouragement in the fulfillment of the major project work. We would also like to express our sincere thanks to Dr. M.B. Mali, HOD, Department of Electronics and Telecommunication, and all the Staff Members for permitting us to carry on with our project work in the required college laboratories and use the instruments required for it. We would like to extend our sincere thanks to Principal Dr. S.D. LOKHANDE for his valued support and faith in us.

We hope that this project has been a valuable learning experience for all of us. We are confident that the skills and knowledge that we have gained will be of benefit to us in our future endeavors.

Thank you all!

Chapter 1

Introduction

1.1 Introduction :

In today's digital age, the need for robust security systems has become increasingly vital. Traditional methods of door-locking systems, such as keys and passwords, are gradually being replaced by innovative technologies that offer enhanced convenience and security. One such cutting-edge technology is face recognition, which utilizes artificial intelligence (AI) algorithms to authenticate individuals based on their unique facial features.

Face recognition has gained significant attention and has become a prominent research area in computer vision and AI. It has found applications in various fields, including surveillance, law enforcement, and access control systems. This technology has the potential to revolutionize the way we secure our homes, offices, and public spaces, offering an advanced level of security while eliminating the need for physical keys or passwords.

This report aims to explore the concept of a door-locking system using face recognition technology and its benefits over conventional methods. By understanding the fundamentals and mechanics of face recognition, we can gain insights into its applications, limitations, and potential future advancements. Furthermore, we will discuss the impact of face recognition systems on security, convenience, and privacy, addressing concerns that arise with the adoption of this technology.

The primary objective of implementing a door-locking system using face recognition is to provide a secure and seamless access control mechanism. This system typically consists of a camera or a set of cameras, an AI-powered facial recognition algorithm, and a locking mechanism. When an individual approaches the door,

the camera captures their face, and the algorithm analyzes the facial features to determine their identity. If the face matches an authorized user's data, the locking mechanism grants access; otherwise, it remains locked.

The advantages of a face recognition-based door-locking system are numerous. Firstly, it eliminates the need for physical keys or to remember complex passwords, reducing the chances of unauthorized access due to lost or stolen credentials. Secondly, face recognition offers a high level of accuracy in identifying individuals, making it difficult to bypass the system through impersonation. Additionally, the system can be seamlessly integrated with other security measures, such as alarms or surveillance cameras, enhancing overall security.

However, while face recognition technology brings several benefits, it also raises concerns regarding privacy and the potential misuse of personal data. Issues such as data protection, consent, and storage of facial images need to be addressed to ensure the responsible implementation of this technology.

In conclusion, a door-locking system using face recognition offers an advanced and convenient approach to access control, enhancing security while simplifying the authentication process. By delving into the mechanics and implications of this technology, we can better understand its potential and the considerations that need to be taken into account when implementing such systems.

1.2 Aim:

The aim of this report is to explore and evaluate the concept of a door-locking system using face recognition technology, with a focus on understanding its benefits, limitations, and implications. By studying the fundamentals of face recognition and its application in access control systems, we aim to assess the potential of this technology in enhancing security and convenience. Additionally, we aim to address concerns surrounding privacy and data protection, ensuring that the implementation of face recognition systems is done responsibly and ethically. Ultimately, this report aims to provide valuable insights into the effectiveness and viability of a face recognition-based door-locking system as a modern security solution.

1.3 Objectives :

- To study a wise and secure door protection system that works by capturing the face of the traveler and checking it into its information.
- To develop a system within which whenever someone rings the bell, the image of the person is captured and would be sent to the homeowner.
- To analyze that if a person's image is present in information, then consequently perform its practicality.
- And if the image isn't gifted within the information, then the good lock system can send the image to IOT website to the owner

Chapter 2

Literature Review

2.1 Introduction :

We aim to develop a better method to implement a proper image recognition system as well as how to transfer data from the hardware to the user's/owner portal via GSM, to achieve this goal we studied prior research on this subject. The below literature surveys are carefully studied, and measures are taken to reduce drawbacks, using better, more sensitive, less costly components.

2.2 Literature Review :

1. **Yugashini, S. Vidhyasri, K. Gayathri Devi et al in Design and Implementation of Automated Door Accessing System with Face Recognition, a user-friendly face recognition system has been developed for automated door access control application.** [1]

   The secured system is implemented using a technique of Eigenfaces, a cost effective and SMS operated home security system has been designed and the system is also tested with the GSM network. But aiming in improving reliability and robustness in both the recognition system and detection process can be concentrated more.

   The system they developed utilizes face recognition technology to provide secure access control to doors. By using facial biometrics, individuals can gain access to authorized areas without the need for physical keys or access cards. This automated system aims to enhance security and convenience in various settings such as residential complexes, offices, and other controlled environments.

The paper likely discusses the design and implementation details of the system, including the hardware and software components involved. It may also cover the underlying algorithms and techniques used for face detection, feature extraction, and face matching. Additionally, the authors may have evaluated the system's performance in terms of accuracy, speed, and robustness.

Overall, this user-friendly face recognition system for automated door access control could potentially offer an efficient and secure alternative to traditional access control methods.

2. **Paul Viola, Muhammad Waseem, Sundar Ali Khowaja proposed an efficient face detection algorithm.** [2]

   This paper introduces the concepts of integral image, efficient AdaBoost classifier and cascading of classifiers thus reducing the computations and resulting in an efficient and fast detection algorithm. The most used detection algorithms namely Fisher faces, Eigenfaces and Local Binary Pattern (LBP) is compared in Eigenfaces is based on PCA in which the focus is to analyse the dataset and discover the pattern in it, while the Fisher faces algorithm is based on Linear Discriminant Analysis (LDA) which tries to spot out features that can distinguish between two or more classes. LBP is an efficient algorithm which assigns binary values to the pixel by comparing it with the neighbourhood of each pixel. Based on the experimental results, the paper concluded that LBP is the best among the three in terms of recognition accuracy, operating time, and recognition accuracy for different distances from the camera

3. **H. Lwin.et al., Ramesh Kumar Ayyasamy, Farhan Bashir introduced an entryway lock system which comprises of three subsystems: face recognition, face identification and last is door entry.** [3]

   The recognition is done by using PCA algorithm. The entrance gate will open automatically for the authorized person and caution will ring for the unapproved individual. Restriction of this framework was taking pictures using webcam consistently until stop button is pressed.

   The integration of these subsystems provides a comprehensive entryway lock system that combines face recognition for detection and recognition, face identification for matching against a database, and door entry for controlling access to the secured area. This system aims to enhance security and streamline the entry process by eliminating the need for traditional keys or access cards.

4. **Meera Mathew.et al. proposed secure gateway locking system with multi-factor confirmation also used various method for encryption by using RFID, which can authorize the user.** [4]

   His main target was to structure and deploy an advanced security system that can be used in critical place where simply authorized persons can be entered.By combining multi-factor confirmation, RFID technology for user authorization, and encryption methods, the proposed secure gateway locking system aims to provide a robust and secure access control solution. This approach helps prevent unauthorized access and enhances the overall security of the system.

5. **Ibrahim Mohammad Sayem.et al., Amritha Purushothaman, Suja Palaniswamy presented face recognition security system using IOT in which raspberry pi is used with camera module for input taking image and compared to dataset, OpenCV library were used in python for feature extraction.** [5]

   His proposed system was able to recognize person from poor image quality.By combining IoT technology, Raspberry Pi with a camera module, and the OpenCV library for face recognition and feature extraction, this system provides a framework for building a face recognition security system. It offers the capability to capture and process face images, extract features, and compare them with a dataset, enabling reliable identification and security applications.

6. **Mamoon Tahnoon. et al proposed face recognition security system using deep neural network** [6]

   It uses histogram equalization for enhancing image quality, a wavelet transforms for compress image size and multi neural network for extract main features from face and results compared to present database for classification. By leveraging the power of deep neural networks, the proposed face recognition security system aims to achieve robust and accurate face recognition. Deep neural networks can effectively learn and represent complex patterns in face images, leading to improved recognition performance compared to traditional methods.

7. **Jaiswal, Arvind. et al, Mrutyunjaya Sahani, Chiranjiv Nanda, Abhijeet Kumar Sahu and Biswajeet Pattnaik [24] presented real time security surveillance system due to public security concerns** [7]

   In this system IP CCTV Camera is used, for extracting features from every person's face LBPH algorithm is used and Haar Case Cade for face detec-

tion.It's important to note that the specific features and implementation details of a real-time security surveillance system can vary depending on the requirements, budget, and scope of the project. The mentioned authors may have provided further insights and details in their paper, which could provide a more specific understanding of their proposed system.

8. **AamirNizam Ansari and Mohamed Sedky et al in Internet of Things Approach for Motion Detection using Raspberry Pi has come out with an idea where the Subject is captured using an motion detection sensor and capturing the person face, and too take snapshots and videos of the motion when detected and the same will be uploaded to an external server.** [8]

   The reason behind using a 'Motion Detection' is keeping a security aspect in mind, the detection appliance at homes, buildings and also for surveillance, for example of server rooms. But using all these, enhancing the security by integrating them, a 'Motion Detection' system can be introduced which is then contributed to the exiting laid current security system. This system would be an alternative for expensive security systems being used in the present day. Without any extra special changes to the infrastructure for the installation is not required and is implemented.

   The paper presents a novel implementation of a motion detection system using Raspberry Pi and IoT technology. By utilizing a motion detection sensor, capturing face images, and recording videos, the system offers an effective means of monitoring and capturing motion events. The integration of IoT capabilities enables remote access and storage of the captured data, enhancing the system's flexibility and scalability.

9. **Siddhi Kavde, Riddhi Kavde, Sonali Bodare, Gauri Bhagat et al in Smart Digital Door Lock System Using Bluetooth Technology** [9]

   A smart digital door lock system is proposed, and this application is used to control over home from outside at any time. This application improves security level and via Android app user can easily access this application remotely and regulate the home access system. Indian government started a new campaign for disabled person named as "Accessible India Campaign" so this application can be used by disabled person.

   The authors propose a smart digital door lock system that leverages Bluetooth technology for authentication and control. The system consists of two main components: a mobile device with Bluetooth capabilities and a digital lock mechanism installed on the door.By utilizing Bluetooth technology,

the system eliminates the need for physical keys or access cards, offering a more convenient and secure solution for door access control. The integration with mobile devices provides flexibility, allowing users to manage door access remotely and leverage the security features available on their mobile devices.

2.3 Summary :

The existing methods mostly employ shallow learning algorithms which have been proven to not perform as well as deep learning methods. Moreover, the studies employing deep learning strategies mostly focus on a single-tier recognition system. We prove in our ablation study that the single-tier recognition system fails to generalize the recognition performance when fake images or spoofed images from the Internet are used to gain authorization access. In this work, we add another tier of security check in the form of a discriminative learning strategy so that the diversified representation is learned which can distinguish between authorized and unauthorized users while dealing with spoofed images.

Chapter 3

Methodology

3.1 Introduction :

The methodology section of this report aims to outline the approach taken to investigate and evaluate the door locking system using face recognition technology. By understanding the methodology employed, readers can gain insights into the experimental design, data collection process, and analysis techniques used to obtain the results presented in this study.

The primary objective of the research was to explore the effectiveness and feasibility of a door-locking system based on face recognition technology. The study involved a combination of theoretical analysis and practical implementation to assess the security, convenience, and potential limitations of the system.

To begin, an extensive review of existing literature was conducted to understand the underlying principles of face recognition technology, its applications in access control systems, and the current state-of-the-art techniques. This literature review formed the foundation for establishing the theoretical framework and identifying key research questions.

The experimental setup involved the implementation of a prototype door-locking system using face recognition. The system consisted of a camera or a set of cameras, an AI-powered facial recognition algorithm, and a locking mechanism. The hardware and software components were carefully selected and configured to ensure optimal performance.

The collected data underwent pre-processing to enhance the quality and consistency of the images. Techniques such as normalization, noise reduction, and

alignment were applied to ensure accurate facial feature extraction and comparison during the recognition process.

Overall, the methodology employed in this study enables a comprehensive analysis of the face recognition-based door-locking system, contributing to a better understanding of its capabilities, limitations, and practical implications.

3.2 Methodology :

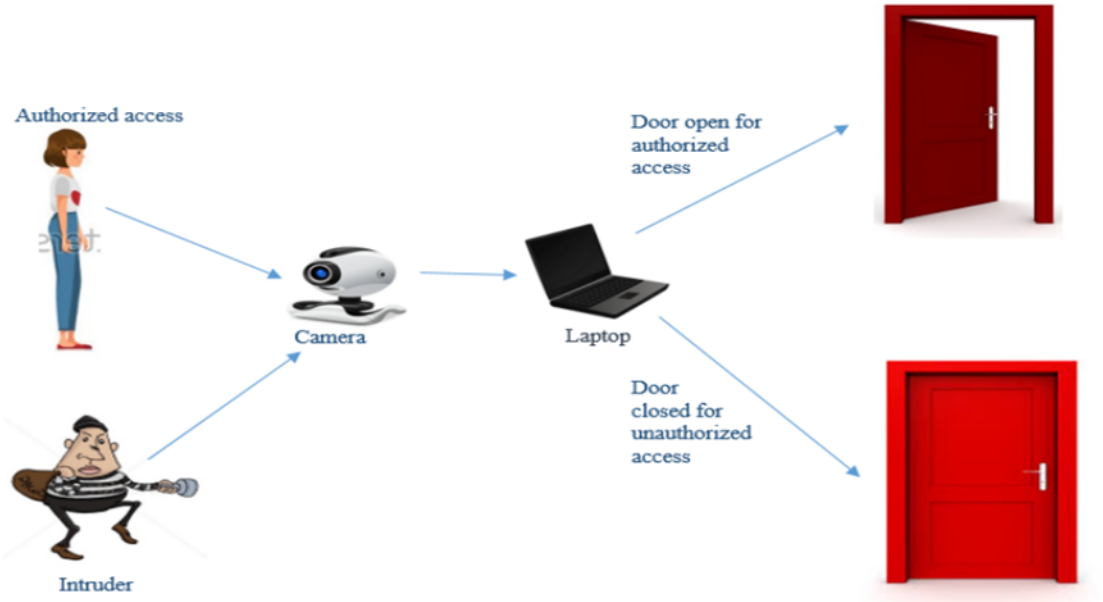

Figure 3.1: Basic Understanding of the working of the project.

The figure above illustrates the system methodology of a face recognition-based door lock system. The image of the person standing in front of the door will be captured by the camera. Then this image will be compared with the images in the database. The door will open automatically only for authorized access i.e., only if the face of the person matches with that in the database. If the face of the person does not match with images in the database, the system will conclude that the person at the doorstep is an intruder or trespasser, and the door will remain

closed. The image is captured using the webcam and all the processing is done on the laptop. As discussed LBPH is used for face recognition.

3.3 System Block Diagram :

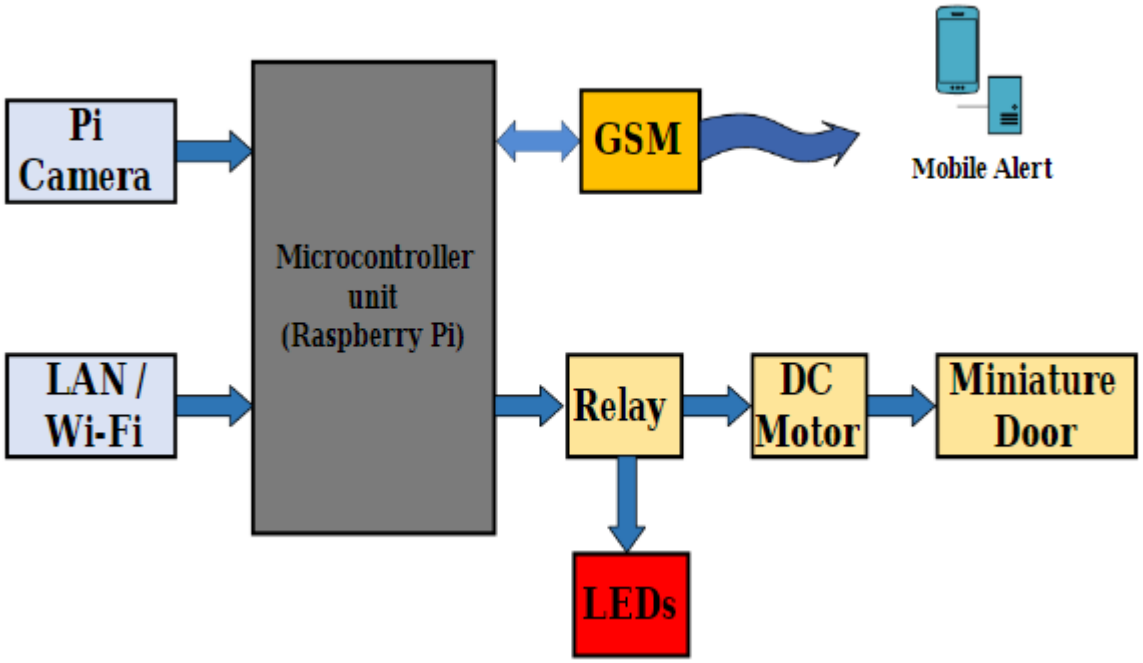

Figure 3.2: Block diagram of Door Locking System using Face Recognition.

3.3.1 Block Diagram Description :

- The Microcontroller Unit during this diagram i.e., RASPBERRY PI is the brain of the whole design. because it connects each part of the project with one another.
- The person who arrives outside the door, his/her image is captured victimization the Pi Camera. Then that image is checked within the info that the owner has already created. This all is completed through the GSM module.
- If the image matches with the pre-stored image within the databases, then through raspberry pi the message is distributed to the relay module to open

the door. And if the image doesn't match them the message can move to the owner through the portal.

- Then the owner can have full authority regarding what to try and do, whether to permit the person or not and consequently, save that person's information within the prestored info.

3.4 Hardware Requirements :

3.4.1 Raspberry Pi 4b :

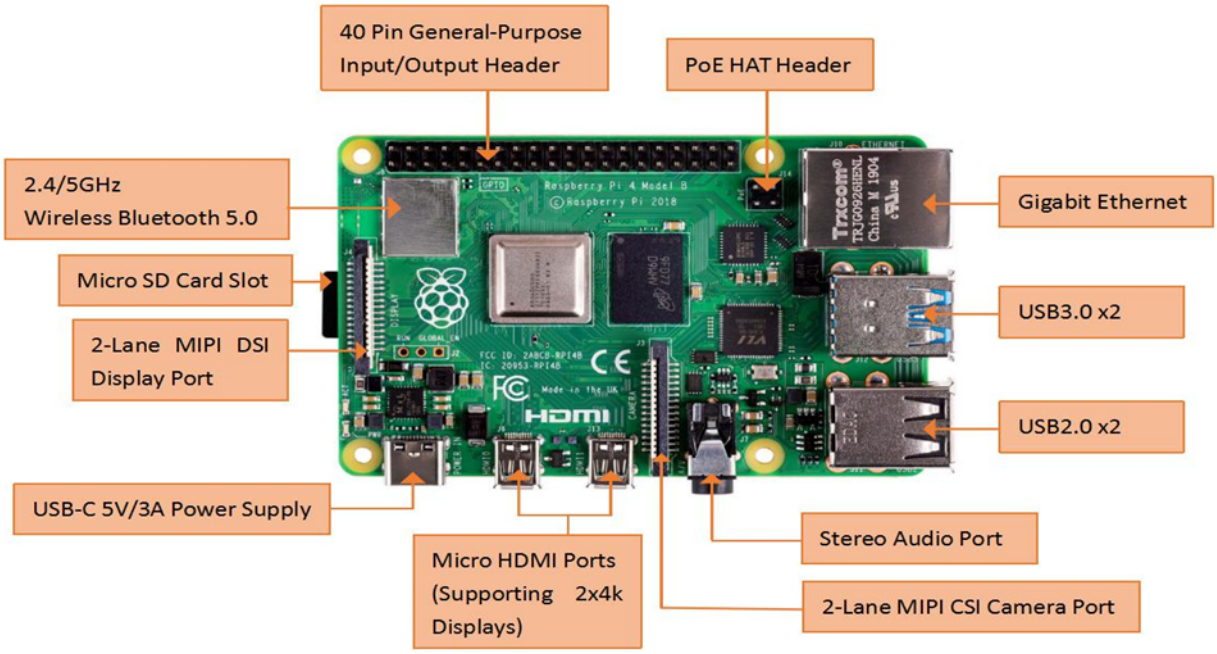

Figure 3.3: System Diagram of Raspberry Pi 4

The Raspberry Pi 4 Model B is a popular single-board computer that offers a significant upgrade in performance and capabilities compared to its predecessors. It is part of the Raspberry Pi family of devices known for their versatility, affordability, and community support. Here is a description of the Raspberry Pi 4 Model B:

- **Processing Power:** The Raspberry Pi 4 Model B is equipped with a quad-core ARM Cortex-A72 processor running at up to 1.5 GHz. This provides a significant boost in processing power, making it suitable for a wide range of applications that require faster computations and multitasking.

- **Memory and Storage:** It is available in different configurations with varying amounts of RAM, including 2GB, 4GB, and 8 GB. The increased RAM capacity allows for smoother multitasking and better performance in resource-intensive applications. It features a Micro-SD card slot for storage, providing flexibility in choosing the storage capacity and type of storage medium.

- **Connectivity:** The Raspberry Pi 4 Model B offers enhanced connectivity options, including dual-band 802.11ac Wi-Fi, Bluetooth 5.0, and Gigabit Ethernet. This enables seamless wireless connectivity, high-speed networking, and the ability to connect to a wide range of devices and peripherals.

- **Video and Display Capabilities:** It features dual micro HDMI ports that support up to 4K resolution, allowing for crisp and high-quality video output. The improved graphics processing capabilities make it suitable for multimedia applications, digital signage, and media center setups.

- **GPIO Pins:** Like previous Raspberry Pi models, the Raspberry Pi 4 Model B provides a 40-pin GPIO (General-Purpose Input/Output) header. These GPIO pins allow for easy interfacing with a variety of external devices and sensors, expanding the possibilities for creating custom projects and prototypes.

- **USB Ports:** It includes two USB 2.0 ports and two USB 3.0 ports, providing ample connectivity options for USB devices such as keyboards, mice, storage drives, and other peripherals. The USB 3.0 ports offer faster data transfer speeds compared to USB 2.0, making them ideal for high-bandwidth devices.

- **Operating System Support:** The Raspberry Pi 4 Model B supports various operating systems, including the official Raspberry Pi OS (previously known as Raspbian), as well as popular Linux distributions such as Ubuntu, Fedora, and others. This flexibility allows users to choose an operating system that best suits their needs and preferences.

3.4.2 Raspberry Pi Camera :

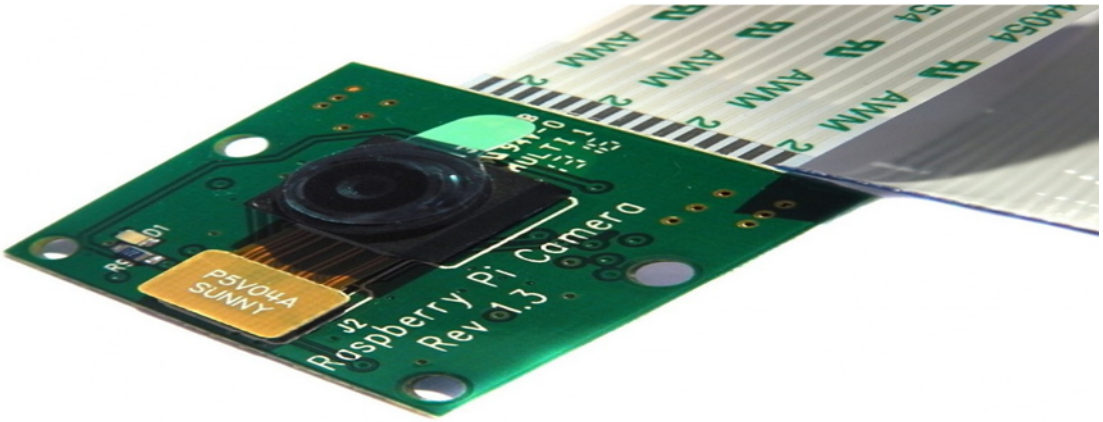

Figure 3.4: Raspberry Pi Camera

The Raspberry Pi Camera, also known as the Raspberry Pi Cam, is a small camera module specifically designed for use with Raspberry Pi single-board computers. It provides a compact and cost-effective solution for capturing images and videos in various projects and applications. Here is a description of the Raspberry Pi Camera:

- **Camera Module Variants:** The Raspberry Pi Camera is available in different module variants, including the Raspberry Pi Camera Module V1, V2, HQ Camera, and the NoIR Camera Module. Each variant offers specific features and capabilities, such as image resolution, sensor type, lens options, and low-light sensitivity.
- **Image and Video Capture:** The camera module is capable of capturing both still images and videos. It supports different image formats, including JPEG and RAW, as well as video formats such as H.264 and MJPEG. The captured media can be saved directly to Raspberry Pi's storage or transmitted over networks.
- **High-Resolution Imaging:** Depending on the camera module variant, the Raspberry Pi Camera can offer different levels of image resolution. The V1 module provides 5MP (megapixels), while the V2 module offers 8MP. The HQ Camera, equipped with a high-quality Sony IMX477 sensor, provides even higher resolution capabilities up to 12.3MP.

- **Compact Size and Connectivity:** The Raspberry Pi Camera module is small and lightweight, making it easy to integrate into various projects. It connects directly to the Raspberry Pi board via a dedicated camera connector, ensuring a reliable and secure connection.
- **Software Support:** The Raspberry Pi Camera is supported by the official Raspberry Pi operating system, Raspbian, as well as other popular operating systems compatible with the Raspberry Pi. Software libraries and APIs are available to access and control the camera module, allowing developers to capture and process images and videos in their projects.

3.4.3 LCD Display :

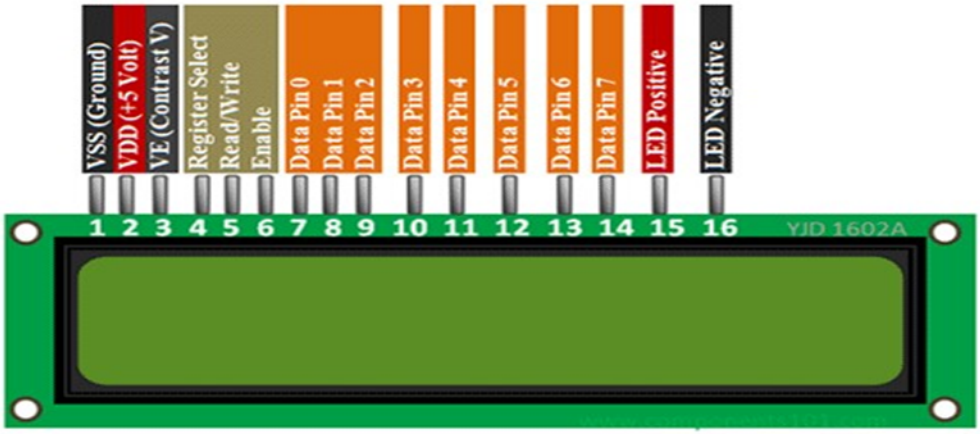

Figure 3.5: LCD Display

LCD display One type of electronic gadget utilized to show the message and data is a 16×2 LCD. Liquid crystal display is the full name for the phrase LCD. It contains 16 columns and 2 rows the display is known as a 16×2 LCD. Each character will be made up of 58 Pixel Dots and can be displayed in a total of 32 characters (16×2=32). Multi-segment light-emitting diodes are the primary technology behind these displays

3.4.4 Node MCU :

Figure 3.6: Node MCU

NodeMCU is an open-source firmware and development board that combines the functionality of a microcontroller with built-in Wi-Fi capabilities. It is based on the popular ESP8266 Wi-Fi module and provides an easy-to-use platform for Internet of Things (IoT) projects. Here is a description of NodeMCU and its features:

- **Wi-Fi Connectivity:** NodeMCU has built-in Wi-Fi capabilities, allowing it to connect to wireless networks and communicate with other devices or web services over the internet. This feature enables the development of IoT applications that require internet connectivity and remote control or monitoring capabilities.
- **Integrated Development Environment (IDE):** NodeMCU is typically programmed using the Arduino IDE or the NodeMCU firmware's own Lua-based IDE. These IDEs provide a user-friendly environment for writing and uploading code to the microcontroller, simplifying the development process.
- **GPIO Pins:** NodeMCU offers multiple General Purpose Input/Output (GPIO) pins that can be used to connect and control external devices such as sensors, actuators, or displays. These pins allow for the expansion and customization of NodeMCU-based projects.
- **Analog-to-Digital Converter (ADC):** The NodeMCU board includes an ADC, which enables the measurement of analog signals from sensors or other devices. This functionality is useful for applications that require analog sensing or control.

- **Small Form Factor:** NodeMCU has a compact size, making it suitable for projects with limited space or where portability is desired. The small form factor of the NodeMCU board allows for easy integration into various IoT applications.
- **Open-Source Community:** NodeMCU is supported by a large and active open-source community. This community provides extensive documentation, tutorials, and code examples, making it easier for developers to learn and leverage the capabilities of the NodeMCU platform.

3.4.5 Single-Channel Relay Module:

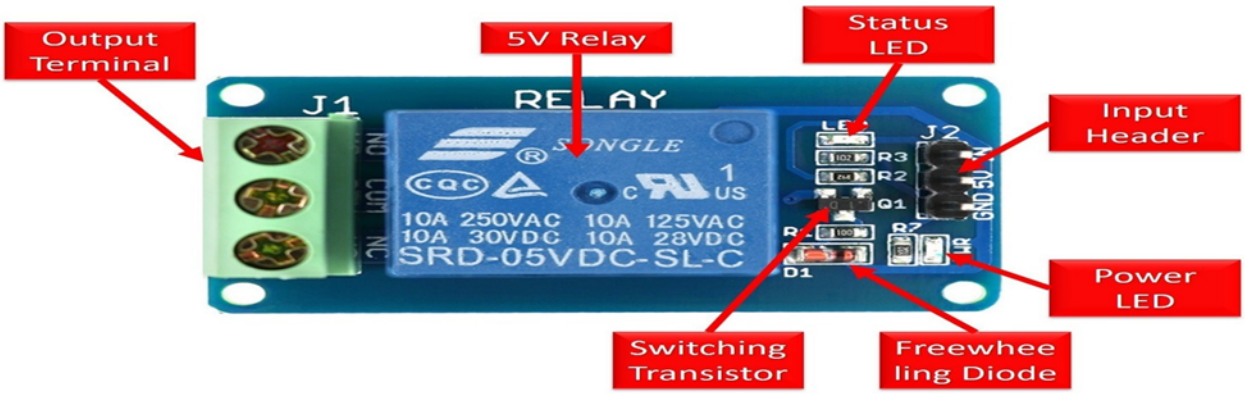

Figure 3.7: Relay Module

A single-channel relay module is a commonly used electronic component in microcontroller-based systems. It provides a convenient way to control high-power electrical devices using low-power signals from the microcontroller. Here is a description of the single-channel relay module and its features:

- **Voltage and Current Rating:** Single-channel relay modules are available in various voltage and current ratings to accommodate different load requirements. Common voltage ratings include 5V and 12V, while current ratings can range from a few amps to several tens of amps.
- **Opto-isolation:** Many single-channel relay modules feature an optoisolator, which provides electrical isolation between the microcontroller and the

relay circuitry. Opto-isolation helps protect the microcontroller from voltage spikes or noise generated by the high-power circuit, ensuring reliable operation and preventing damage to the microcontroller.

- **LED Indicator:** The relay module often includes an LED indicator that provides visual feedback on the status of the relay. The LED may be lit when the relay is energized (contacts closed) or vice versa, depending on the design of the module. This feature helps in easily identifying the relay's current state.
- **Screw Terminals:** To facilitate easy connection to the high-power circuit, single-channel relay modules often include screw terminals. These terminals allow for secure and reliable connections between the relay module and the external devices, minimizing the need for soldering or additional wiring.
- **Low Power Consumption:** When the relay is not actively switching the high-power circuit, the single-channel relay module typically consumes very little power. This low power consumption makes it suitable for battery-powered applications or energy-efficient systems.

3.4.6 Solenoid Lock :

Figure 3.8: Solenoid Lock

A solenoid lock is a type of electric lock that utilizes a solenoid, an electromagnetic coil, to control the locking and unlocking mechanism. When an electric current passes through the solenoid, it generates a magnetic field, causing the lock to either engage or disengage.

In the context of microcontrollers, solenoid locks can be interfaced and controlled using digital output pins. Here are the description and features of solenoid locks in microcontrollers:

- Iron Body Material
- High-quality ultra-compact electric lock.
- Rustproof, durable, safe, and convenient to use.
- Suction tightly sucks the iron, thus locking the door.
- Applicable for being installed in the escape door or fire door electronic controlled system.
- Adopts the principle of electric magnetism, when the current is through the silicon, the electromagnetic lock will achieve a strong

3.5 Software Requirements :

1. **Open CV (Open-Source Computer Vision):** Open CV is an open platform for programmers for real-time laptop vision and computations. It supports. several libraries of programming functions. it's designed in C++ and has bindings with Java, Python and MATLAB. It runs on an enormous kind of platforms like Windows, Linux, Android, iOS, Mac OS, and many others. more. Image and Video processes square measure 2 of the most applications of Open CV.
2. **Python package Development Kit:** Python may be a high-level general-purpose programming language. Its style philosophy emphasizes code. Readability with the employment of serious indentation.
3. **Operational System:** Windows/Linux
4. **Language Used:** Python (In Raspberry Pi), Embedded C (In Node MCU)

3.6 Algorithms :

3.6.1 Face Recognition:

- **Local Binary Pattern Histogram (LBPH)**. The LBPH algorithm assigns the pixels of an image with binary values by comparing each pixel with the neighborhood. Suppose that we are interested in calculating the LBPH value for the pixel. The Local Binary Pattern Histogram (LBPH) algorithm is illumination invariant. If the lighting condition of the scene is changed, all the pixel values will vary but the relative difference between the pixels will remain the same making the algorithm illumination invariant.

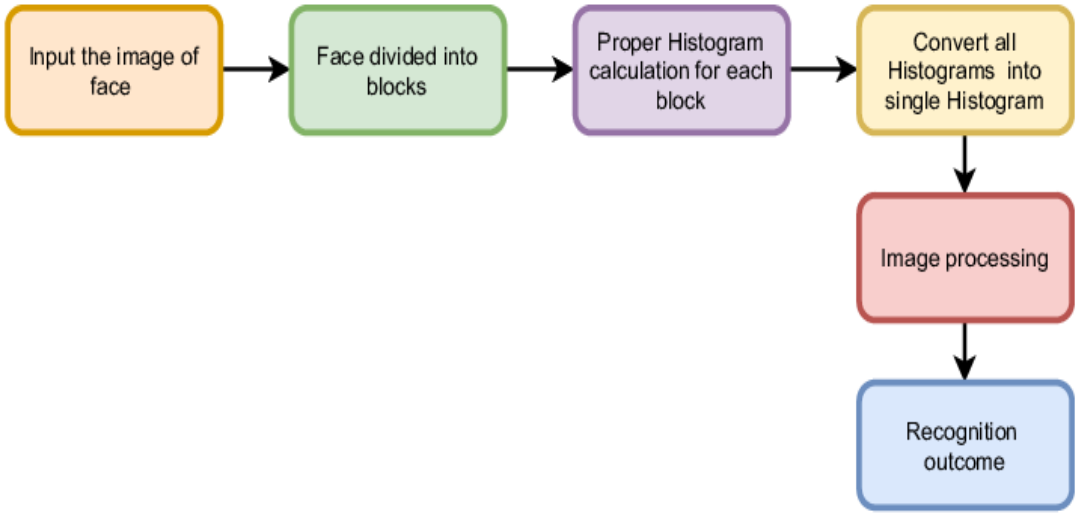

Figure 3.9: LBPH workflow algorithm

3.7 Code Implemented :

3.7.1 Code 1- Main Code :

```
# Main program
def main():
    # LCD initialization
    lcd_init()

    # Load known face images and encode them
    images = []
    names = []
    today = date.today()
    now = datetime.now()
    dtString = now.strftime("%H:%M:%P")
    path = "/home/rpi/Desktop/56/images/*.*"

    for file in glob.glob(path):
        image = cv2.imread(file)
        a = os.path.basename(file)
        b = os.path.splitext(a)[0]
        names.append(b)
        images.append(image)

    encodelist = encoding1(images)

    cap = cv2.VideoCapture(0)
    frame_count = 0
    process_this_frame = True

    while True:
        ret, frame = cap.read()
        frame_count += 1

        if frame_count % 3 == 0:
            process_this_frame = True
        else:
            process_this_frame = False

        if process this frame:
```

```
if process_this_frame:
    frame1 = cv2.resize(frame, (0, 0), None, 0.25, 0.25)
    face_locations = face_recognition.face_locations(frame1)
    curframe_encoding = face_recognition.face_encodings(frame1, face_locations)

    for encodeface, facelocation in zip(curframe_encoding, face_locations):
        results = face_recognition.compare_faces(encodelist, encodeface)
        distance = face_recognition.face_distance(encodelist, encodeface)
        match_index = np.argmin(distance)
        name = names[match_index]
        print('name', name)
        unique_names.add(name)
        if name:
            try:
                with open(current_date + '.csv', 'w+', newline='') as f:
                    lnwriter = csv.writer(f)
                    current_time = now.strftime("%H-%M-%S")
                    print(current_time)
                    for name in unique_names:
                     lnwriter.writerow([name, current_time])
                    relay()
                    lcd_string("Access Granted", LCD_LINE_1)
                    lcd_string(name, LCD_LINE_2)
                    insert_authorization(name, datetime.now().strftime("%Y-%m-%d %H:%M:%S"))
            except KeyboardInterrupt:
                print("Keyboard interrupt")
        else:
            lcd_string("Access Denied", LCD_LINE_1)
            lcd_string("", LCD_LINE_2)

        x1, y1, x2, y2 = facelocation
        x1, y1, x2, y2 = x1 * 4, y1 * 4, x2 * 4, y2 * 4
        cv2.rectangle(frame, (y1, x1), (y2, x2), (0, 0, 255), 3)
        cv2.putText(frame, name, (y2 + 6, x2 - 6), cv2.FONT_HERSHEY_COMPLEX, 1, (255, 0, 255), 2)

cv2.imshow("FRAME", frame)
```

```
                    try:
                        with open(current_date + '.csv', 'w+', newline='') as f:
                            lnwriter = csv.writer(f)
                            current_time = now.strftime("%H-%M-%S")
                            print(current_time)
                            for name in unique_names:
                             lnwriter.writerow([name, current_time])
                            relay()
                            lcd_string("Access Granted", LCD_LINE_1)
                            lcd_string(name, LCD_LINE_2)
                            insert_authorization(name, datetime.now().strftime("%Y-%m-%d %H:%M:%S"))
                    except KeyboardInterrupt:
                        print("Keyboard interrupt")
                else:
                    lcd_string("Access Denied", LCD_LINE_1)
                    lcd_string("", LCD_LINE_2)

                x1, y1, x2, y2 = facelocation
                x1, y1, x2, y2 = x1 * 4, y1 * 4, x2 * 4, y2 * 4
                cv2.rectangle(frame, (y1, x1), (y2, x2), (0, 0, 255), 3)
                cv2.putText(frame, name, (y2 + 6, x2 - 6), cv2.FONT_HERSHEY_COMPLEX, 1, (255, 0, 255), 2)

        cv2.imshow("FRAME", frame)
        if cv2.waitKey(1) & 0xFF == 27:
            break

    print("Clean up")
    GPIO.cleanup()
    cap.release()
    cv2.destroyAllWindows()


if __name__ == '__main__':
    main()
```

3.7.2 Code 2- Face CSV :

```
# Main program
def main():
    # LCD initialization
    lcd_init()

    # Load known face images and encode them
    images = []
    names = []
    today = date.today()
    now = datetime.now()
    dtString = now.strftime("%H:%M:%P")
    path = "/home/rpi/Desktop/56/images/*.*"

    for file in glob.glob(path):
        image = cv2.imread(file)
        a = os.path.basename(file)
        b = os.path.splitext(a)[0]
        names.append(b)
        images.append(image)

    encodelist = encoding1(images)

    cap = cv2.VideoCapture(0)

    while True:
        ret, frame = cap.read()
        frame1 = cv2.resize(frame, (0, 0), None, 0.25, 0.25)
        face_locations = face_recognition.face_locations(frame1)
        curframe_encoding = face_recognition.face_encodings(frame1, face_locations)

        for encodeface, facelocation in zip(curframe_encoding, face_locations):
            results = face_recognition.compare_faces(encodelist, encodeface)
            distance = face_recognition.face_distance(encodelist, encodeface)
            match_index = np.argmin(distance)
            name = names[match_index]
            print('name', name)
```

```
            x1, y1, x2, y2 = facelocation
            x1, y1, x2, y2 = x1 * 4, y1 * 4, x2 * 4, y2 * 4
            cv2.rectangle(frame, (y1, x1), (y2, x2), (0, 0, 255), 3)
            cv2.putText(frame, name, (y2 + 6, x2 - 6), cv2.FONT_HERSHEY_COMPLEX, 1, (255, 0, 255), 2)
            if name:
                try:
                   with open(current_date + '.csv', 'w+', newline='') as f:
                    lnwriter = csv.writer(f)
                    current_time = now.strftime("%H-%M-%S")
                    print(current_time)
                    lnwriter.writerow([name, current_time])
                    relay()
                    lcd_string("Access Granted", LCD_LINE_1)
                    lcd_string(name, LCD_LINE_2)
                    insert_authorization(name, datetime.now().strftime("%Y-%m-%d %H:%M:%S"))
                except KeyboardInterrupt:
                    print("Keyboard interrupt")
            else:
                lcd_string("Access Denied", LCD_LINE_1)
                lcd_string("", LCD_LINE_2)



        cv2.imshow("FRAME", frame)
        if cv2.waitKey(1) & 0xFF == 27:
            break

    print("Clean up")
    GPIO.cleanup()
    cap.release()
    cv2.destroyAllWindows()


if __name__ == '__main__':
    main()
```

3.7.3 Code 3- LCD Relay :

```
# Main program
def main():
    # LCD initialization
    lcd_init()

    # Load known face images and encode them
    images = []
    names = []
    today = date.today()
    now = datetime.now()
    dtString = now.strftime("%H:%M:%P")
    path = "/home/rpi/Desktop/56/images/*.*"

    for file in glob.glob(path):
        image = cv2.imread(file)
        a = os.path.basename(file)
        b = os.path.splitext(a)[0]
        names.append(b)
        images.append(image)

    encodelist = encoding1(images)

    cap = cv2.VideoCapture(0)

    while True:
        ret, frame = cap.read()
        frame1 = cv2.resize(frame, (0, 0), None, 0.25, 0.25)
        face_locations = face_recognition.face_locations(frame1)
        curframe_encoding = face_recognition.face_encodings(frame1, face_locations)

        for encodeface, facelocation in zip(curframe_encoding, face_locations):
            results = face_recognition.compare_faces(encodelist, encodeface)
            distance = face_recognition.face_distance(encodelist, encodeface)
            match_index = np.argmin(distance)
            name = names[match_index]
            print('name', name)
```

```
            results = face_recognition.compare_faces(encodelist, encodeface)
            distance = face_recognition.face_distance(encodelist, encodeface)
            match_index = np.argmin(distance)
            name = names[match_index]
            print('name', name)

            if name:
                try:
                    #relay()
                    lcd_string("Access Granted", LCD_LINE_1)
                    lcd_string(name, LCD_LINE_2)
                except KeyboardInterrupt:
                    print("Keyboard interrupt")
            else:
                lcd_string("Access Denied", LCD_LINE_1)
                lcd_string("", LCD_LINE_2)

            x1, y1, x2, y2 = facelocation
            x1, y1, x2, y2 = x1 * 4, y1 * 4, x2 * 4, y2 * 4
            cv2.rectangle(frame, (y1, x1), (y2, x2), (0, 0, 255), 3)
            cv2.putText(frame, name, (y2 + 6, x2 - 6), cv2.FONT_HERSHEY_COMPLEX, 1, (255, 0, 255), 2)

        cv2.imshow("FRAME", frame)
        if cv2.waitKey(1) & 0xFF == 27:
            break

    print("Clean up")
    GPIO.cleanup()
    cap.release()
    cv2.destroyAllWindows()


if __name__ == '__main__':
    main()
```

3.8 Simulation :

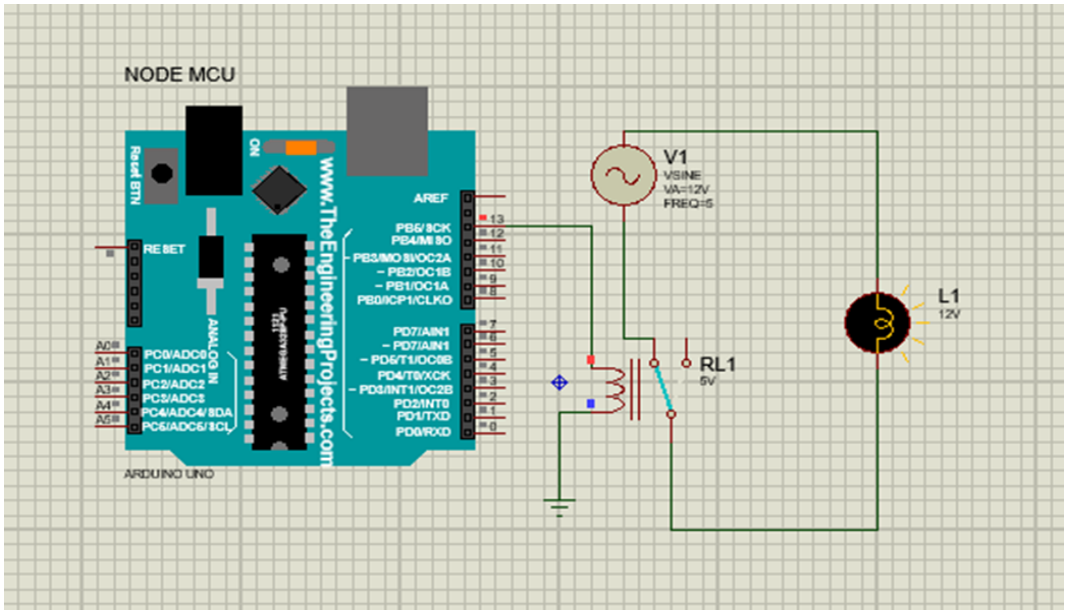

Figure 3.10: Relay is ON as the face does matches and the LCD display anything access granted

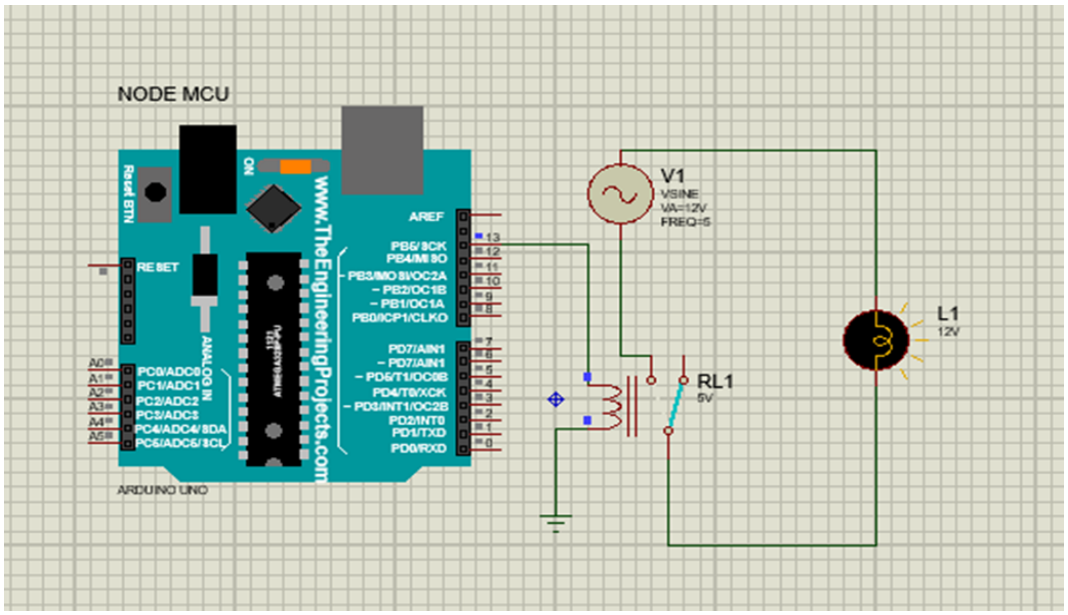

Figure 3.11: Relay is OFF as the face does not matches and the LCD does not display anything

3.9 Flow Charts :

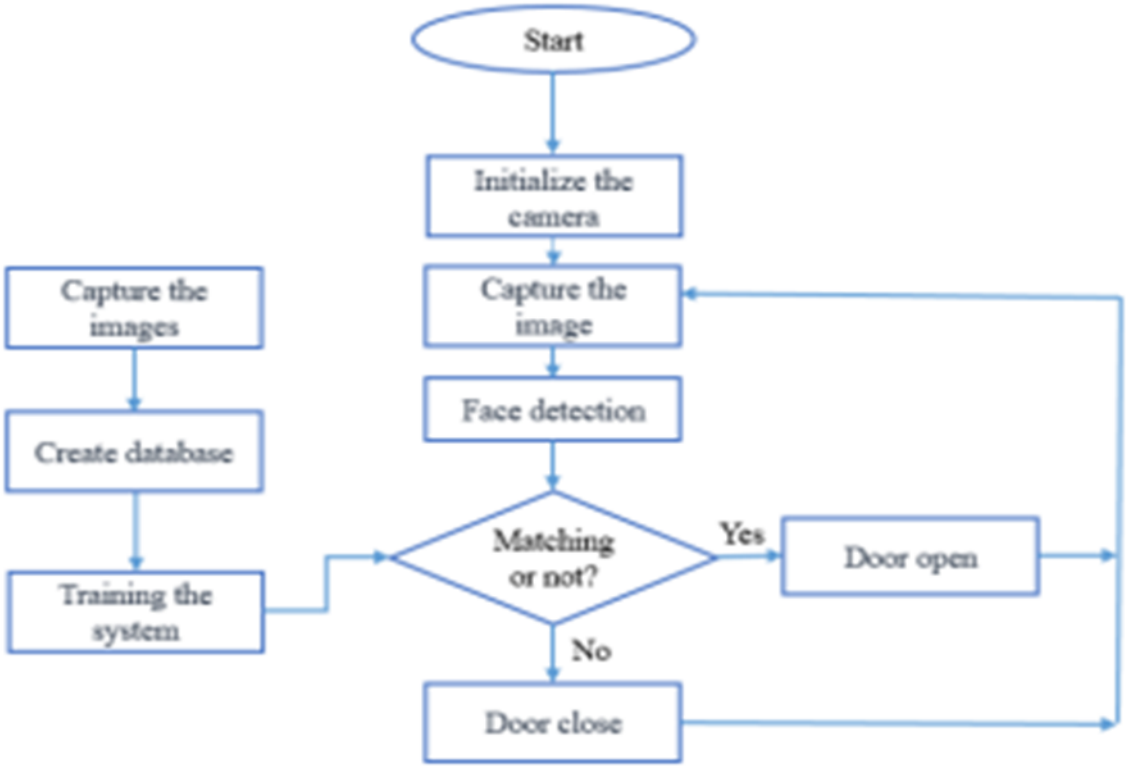

Figure 3.12: Flowchart

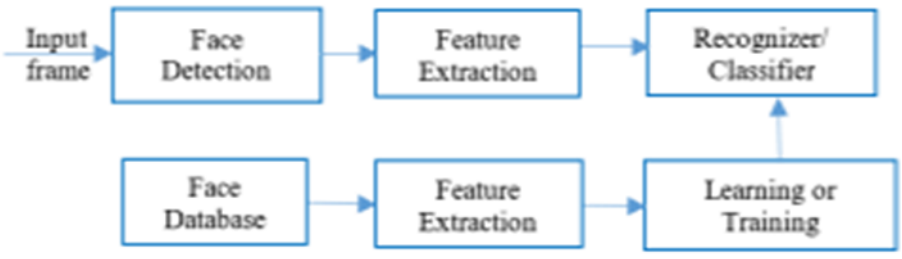

Figure 3.13: Face Recognition Workflow

3.10 Implementation :

Fig 3.12 gives the steps carried out to perform face recognition :

1. The database is created which will contain the images of the persons to be recognized.
2. The features are extracted, and the system is trained using it.
3. When an image is input to the system, first it checks whether the image contains any face with the help of a face detection algorithm.
4. The features of the face are extracted and given to the recognizer/ classifier.
5. The recognizer based on the input from the trainer and the features of the input image will recognize the face.

The flowchart for face recognition is depicted in Fig 3.12. Initially, images of the person to be recognized are captured and a database is created. When the system is switched on, the camera is initialized, and images are captured, and face detection is done. The detected face is compared with the images in the database.

Chapter 4

Results & Discussions

4.1 Results :

The experimental results show that the system detects and recognizes the face for different poses and illumination variations. Using LBPH for face recognition helped in achieving a good result in terms of recognizing faces at varying lighting conditions since LBPH is inherently illumination invariant. The pose invariant system has been achieved by training the algorithm by feeding the database with images of persons with varying poses so that the system is capable of recognizing faces with different head orientations up to $\pm 45^{\circ}$ (along the Z axis).

The result of our project is that with recognition of stored images in the database after recognizing the face the door lock will get open. If any other person comes to the home whose image is not stored in the database that time the image of the person will get captured and sends the image to the user portal. Also, it saves all the entries of the person that is given access in the CSV file or Excel form with the time of their entry.

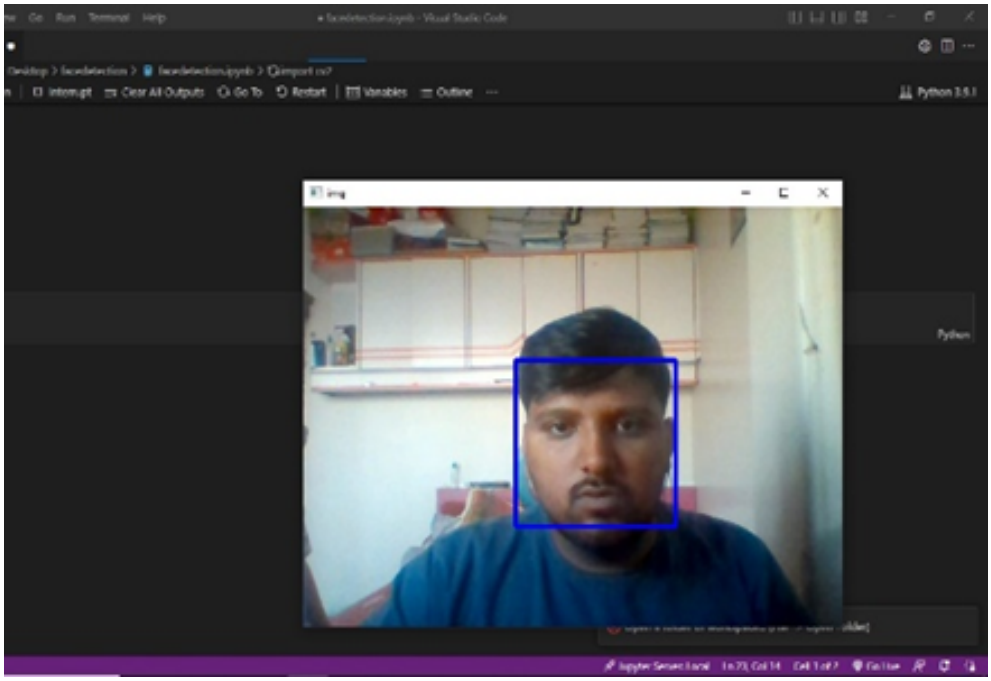

Figure 4.1: Detecting the front face of the person using the raspberry cam

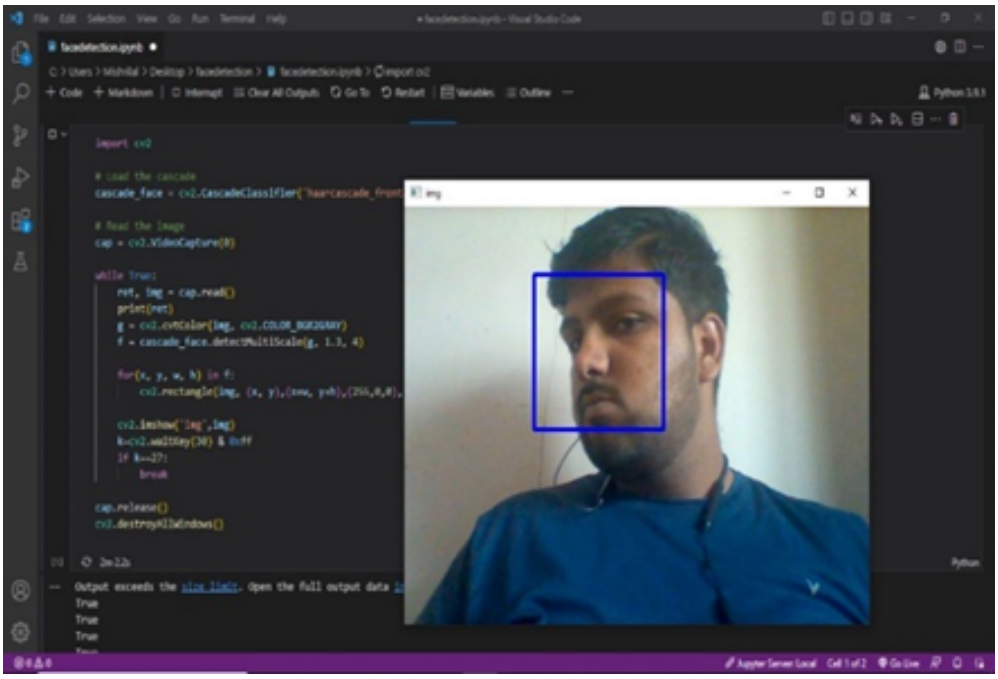

Figure 4.2: Detecting the profile face of the person using the raspberry cam

4.2 Project Prototype :

The project prototype developed for this study was based on the Raspberry Pi 4 Model B single-board computer. The prototype integrated various components, including a high-resolution camera module, an LCD display, and a custom-designed face recognition algorithm. The Raspberry Pi's processing power and connectivity options provided a solid foundation for building the door-locking system using face recognition technology. The camera module captured facial images of individuals approaching the door, which were then processed by the face recognition algorithm running on the Raspberry Pi. The LCD display provided real-time feedback, displaying the recognition results and the status of the locking mechanism. The prototype successfully demonstrated the feasibility and functionality of the system, showcasing the potential of using face recognition for secure access control.

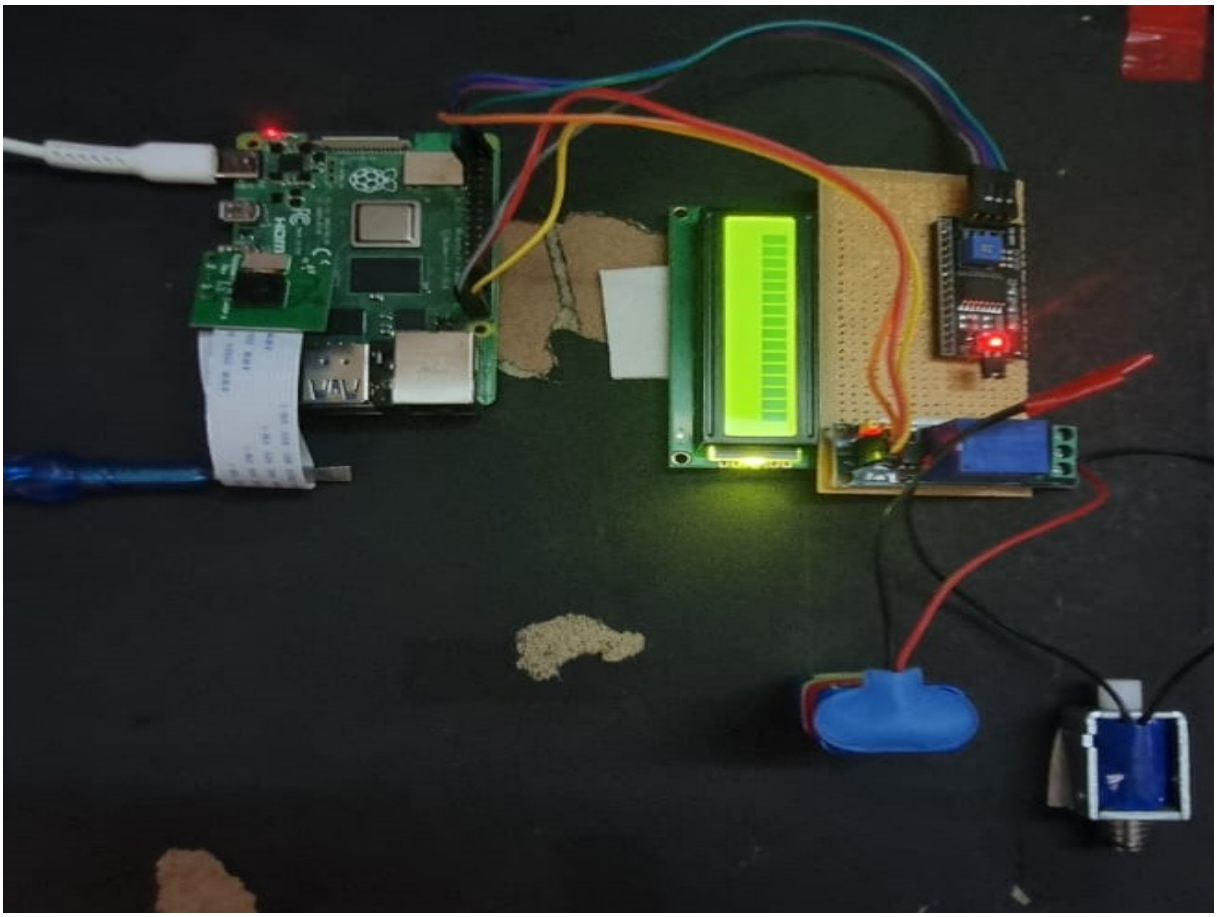

Figure 4.3: Hardware setup of the system

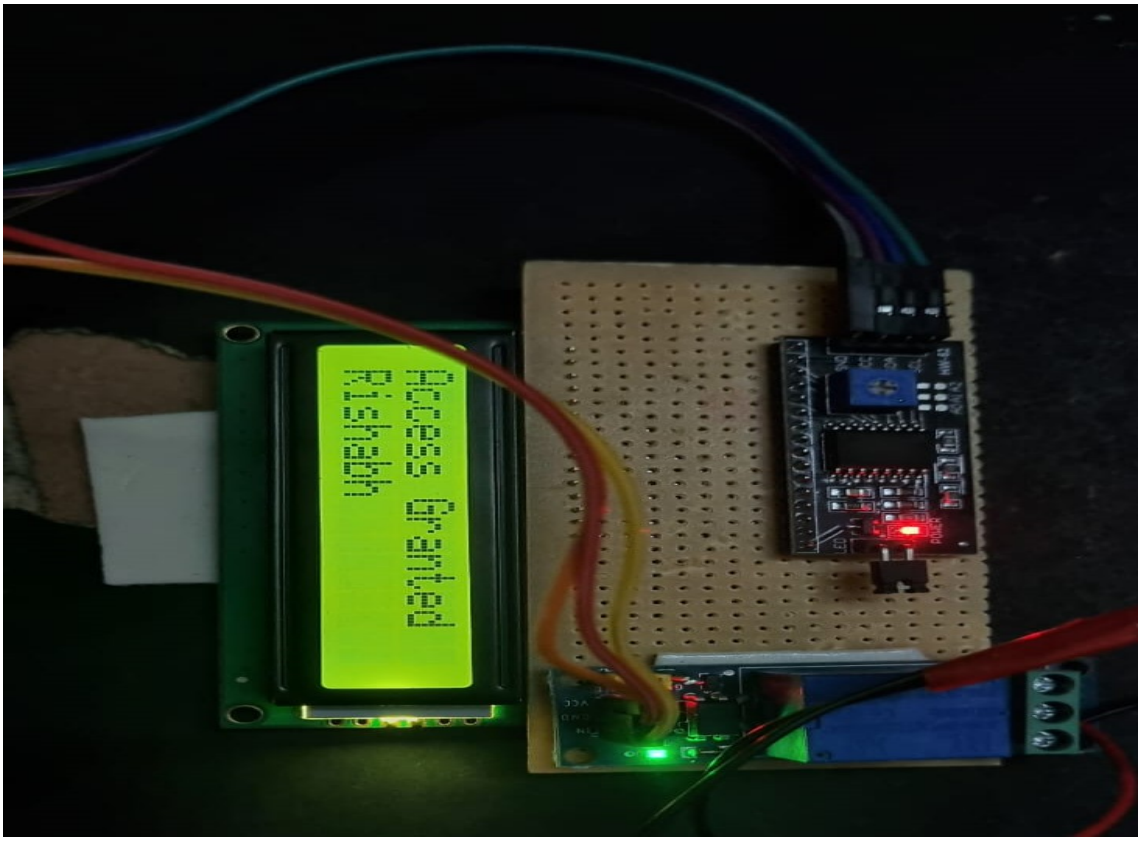

Figure 4.4: Access Granted to the identified person

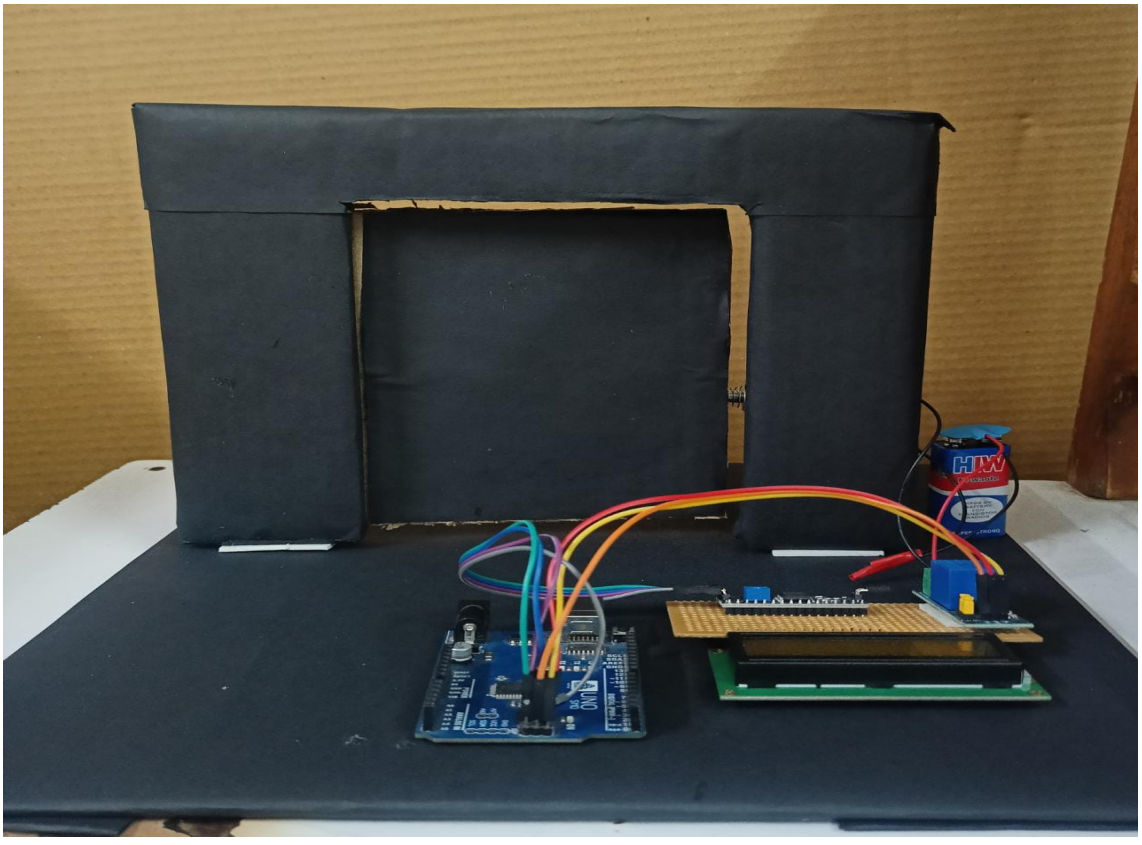

Figure 4.5: Prototype of the project

Figure 4.6: Profile side of the project

Chapter 5

Conclusions

5.1 Conclusions :

The door-locking system using face recognition technology represents a significant advancement in access control systems. By leveraging AI algorithms and analyzing unique facial features, this technology offers enhanced security and convenience over traditional methods such as keys and passwords. The system eliminates the need for physical credentials and reduces the risk of unauthorized access due to lost or stolen items. Moreover, the high accuracy of face recognition ensures that only authorized individuals gain entry, making it difficult to bypass the system through impersonation.

This work has demonstrated the effectiveness of working with Raspberry Pi to implement an initial version of a low-cost embedded facial recognition system for controlling an electromagnetic lock using deep learning techniques. However, the implemented system can be improved not only based on the purpose described on this work, such as an even more reliable facial recognition with a lower error rate, and implementing a more robust face spoofing detection algorithm such as the one presented in. Extra biometrical parameters for access control, such as voice authentication, can also be incorporated to increase security for authorized-only personnel

However, it is essential to address concerns regarding privacy and data protection when implementing face recognition systems. Strict protocols should be in place to ensure responsible handling and storage of facial images, and individuals' consent must be obtained before capturing and using their bio-metric data. By prioritizing privacy and transparency, we can foster trust in the technology and mitigate potential misuse of personal information.

5.2 Future Scope :

The door-locking system using face recognition technology has immense potential for further development and integration. Here are some areas of future scope for this technology:

1. Enhanced Accuracy: Continued research and advancements in AI algorithms can further improve the accuracy of face recognition systems. This includes better handling of variations in lighting conditions, facial expressions, and occlusions, making the system more robust and reliable.

2. Multi-Factor Authentication: Integrating face recognition with other biometric modalities, such as fingerprint or iris scanning, can create a multi-factor authentication system that offers even higher levels of security. Combining multiple biometric factors ensures a more comprehensive and reliable identification process.

3. Real-Time Threat Detection: By integrating the system with advanced surveillance technologies, such as video analytics and machine learning, it becomes possible to detect and respond to potential security threats in real-time. The system can identify suspicious individuals or behavior patterns and trigger appropriate actions or alerts.

4. Integration with Smart Home Technology: The door locking system can be integrated with other smart home devices and automation systems. This allows for seamless control of access, such as remotely granting access to trusted individuals or receiving notifications when unauthorized access attempts occur.

5. Accessibility and Adaptability: Future developments should focus on making face recognition systems more accessible and adaptable to different environments. This includes accommodating individuals with disabilities, addressing diverse facial features, and optimizing performance across various lighting and environmental conditions.

In conclusion, the door locking system using face recognition technology offers a secure and convenient approach to access control. With ongoing research and development, along with responsible implementation practices, this technology has the potential to transform the way we secure our homes, offices, and public spaces, providing an advanced level of security and convenience while respecting privacy and data protection..

References

[1] M. Waseem, S. A. Khowaja, R. K. Ayyasamy, and F. Bashir, "Face recognition for smart door lock system using hierarchical network," *2020 International Conference on Computational Intelligence (ICCI) and IEEE*, 09 November 2020.

[2] A. Purushothaman and S. Palaniswamy, "Pose and illumination invariant face recognition for automation of door lock system," *2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing Communication Engineering (ICATIECE)*, vol. 205-208, 2019.

[3] V. Pandit, P. Majgaonkar, P. Meher, S. Sapaliga, and S. Bojewar, "Intelligent security lock," *2017 International Conference on Trends in Electronics and Informatics (ICEI)*, 2017.

[4] A. Nag, J. N. Nikhilendra, and M. Kalmath, "Iot based door access control using face recognition," *3rd International Conference for Convergence in Technology (I2CT)*, vol. 1-3, 2018.

[5] M. Waseem, S. A. Khowaja, R. K. Ayyasamy, and F. Bashir, "Face recognition for smart door lock system using hierarchical network," *2020 International Conference on Computational Intelligence (ICCI)*, vol. 51-56, 2020.

[6] S. Jahnavi and C. Nandini, "Smart anti-theft door locking system," *," 2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing Communication Engineering (ICATIECE)*, vol. 205-208, 2019.

[7] M. Sahani, C. Nanda, A. K. Sahu, and B. Pattnaik, "Web-based online embedded door access control and home security system based on face recognition," *2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]*, vol. 1-6, 2015.

[8] Yugashini, S. Vidhyasri, and K. G. Dev, "Design and implementation of automated door accessing system with face recognition," *2018 Second Interna-*

tional Conference on Inventive Communication and Computational Technologies (ICICCT), vol. 1105-1108, January 2018.

[9] A. N. Ansari and M. Sedky, "An internet of things approach for motion detection using raspberry pi," *Proceedings of 2015 International Conference on Intelligent Computing and Internet of Things*, May 2015.