ABSTRACT

In response to growing concerns regarding personal security and property protection, there is an increasing demand for advanced and intelligent security systems. Traditional locking mechanisms often lack the necessary adaptability and features needed to ensure comprehensive safety. This project aims to address these shortcomings by developing a robust face recognition system utilizing Haar Cascade classifiers. The proposed system leverages an Arduino to control an automatic locking mechanism, which can lock or unlock doors based on the identification of recognized faces. This innovative approach not only enhances security but also streamlines access for authorized personnel. This system also features an automatic LED lighting module that activates in low-light conditions when motion is detected, improving visibility and safety during the night. Additionally, it implements a dynamic One-Time Password (OTP) generation feature that sends a secure OTP to users' mobile phones through an API, providing an extra layer of verification and safety. To further enhance user interaction, the system includes a pre-recorded voice module (ISD1820), which offers audio guidance to visitors and delivery personnel, ensuring they receive clear instructions upon approach. The results of this project demonstrate a significant improvement in security efficiency and user-friendliness, effectively combining face recognition technology with responsive environmental sensing to create a seamless security solution.

TABLE OF CONTENTS

	Particulars	Page. No
	Abstract	i
	Acknowledgement	ii
	Table of Contents	iii
	List of Figures	v
	List of Tables	vi
	Glossary	vii
1	Introduction	1
	1.1 Introduction to Project	1
	1.2 Problem Definition	1
	1.3 Existing System	2
	1.4 Proposed System	2
	1.5 Objectives of the Project Work	3
	1.6 Scope of the Project Work	3
	1.7 Project Report Outline	4
2	Review of Literature	6
	2.1 System Study	6
	2.2 Review of Literature	6
	2.3 Comparison of Literature	7
3	System Requirement Specification	8

3.1 Functional Requirements 8

3.2 Non Functional Requirements 8

3.3 Hardware Requirements 9

3.4 Software Requirements 13

4 System Design 15

4.1 Design Overview 15

4.2 System Architecture 15

4.3 Class Diagram 16

4.4 Modules 18

4.4.1 Face Recognition Module

4.4.2 Access Control Module

4.4.3 Notification and Monitoring Module

4.4.4 Lighting and Voice Assistance Module

5 Implementation 21

5.1 Steps for Implementation 21

5.2 Implementation Issues 22

5.3 Algorithms 22

5.3.1 Facial Recognition Algorithm

5.3.2 OTP Generation and Verification Algorithm

5.3.3 Automatic Lighting Control

5.3.4 Voice Assistance Using Pre-Recorded Audio

6 Testing 26

6.1 Test Environment 26

6.2 Unit Testing of Modules 26

6.2.1 Module 1

6.2.2 Module 2

6.3 Integration Testing of Modules 27
6.3.1 Module 1
6.3.2 Module 2
6.4 System Testing 27
6.5 Functional Testing 28
7 Results 29
8 Conclusion 30
8.1 Major Contributions
8.2 Future Enhancements
Bibliography 31
Appendix 32

LIST OF FIGURES

Figure	Title	Page No.
Fig. 3.1	Solenoid Lock	9
Fig. 3.2	LDR Resistor	9
Fig. 3.3	LED Light Module	10
Fig. 3.4	Speaker Module	10
Fig. 3.5	4x4 Keypad	10
Fig. 3.6	Buzzer	11
Fig. 3.7	LCD Display	11
Fig. 3.8	Motion Sensor	11
Fig. 3.9	Arduino Uno	12
Fig. 3.10	Relay Module	12
Fig. 3.11	ISD1820 Voice Module	13
Fig. 3.12	PAM8403 Audio Amplifier	13
Fig. 4.1	System Architecture	15
Fig. 4.3	Face Detection Module	18
Fig. 4.4	OTP Module	19
Fig. 4.5	Lighting and Voice Module	20
Fig. 5.3.1	Face Recognition Module Implementation	23
Fig. 5.3.2	OTP Module Implementation	23
Fig. 5.3.3	Light Module Implementation	24
Fig. 5.3.4	Voice Module Implementation	25
Fig. 6.5	Prototype of the Project	28

GLOSSARY

Term	Description
Arduino Uno	A microcontroller board used for hardware control and automation.
Haar Cascade	A machine learning object detection method used in face recognition tasks.
Solenoid Lock	An electromechanical lock controlled via signals from a microcontroller.
OTP (One-Time Password)	A randomly generated numeric password used once for secondary authentication.
ISD1820	A voice recording/playback module used for pre-recorded audio instructions.
OpenCV	An open-source computer vision and machine learning software library.
Relay Module	A device that allows a low-power microcontroller to control high-voltage components.
PIR Sensor	Passive Infrared Sensor used to detect motion.
LDR (Light Dependent Resistor)	A sensor that detects the intensity of ambient light.
Circuit Digest API	An SMS API used to send OTPs to registered users.
LBPH	Local Binary Pattern Histogram — an algorithm for facial recognition.
LCD Display	A screen used to show status messages for the system.
Buzzer	A sound-generating component used for audio alerts.

CHAPTER 1- INTRODUCTION

1.1 Introduction to the Project

With the rapid advancements in technology and the growing emphasis on safety, modern homes and workplaces are increasingly adopting intelligent security solutions. The conventional key-and-lock systems, though still in use, have become outdated due to their inability to adapt to modern threats such as unauthorized duplication, theft, and lack of remote control.

This project aims to develop an advanced smart door locking system that leverages computer vision and automation to enhance security. The core of this system is a **face recognition module** developed using **Haar Cascade classifiers**—a machine learning-based approach that detects and identifies human faces in real-time. Once a face is recognized as an authorized user, the system communicates with an **Arduino microcontroller**, which operates a **physical locking mechanism** (e.g., a servo motor) to grant or deny access.

For enhanced security, the system also integrates an **OTP (One-Time Password)** mechanism. When a face is not confidently recognized or secondary verification is required, the system generates a unique OTP and sends it to the authorized user's mobile number through an API. Only after successful OTP verification is access granted. This integrated approach ensures a secure, automated, and user-friendly experience that surpasses the limitations of traditional locking systems.

1.2 Problem Definition

Modern security systems face a number of challenges, especially in residential areas and small office environments. These include:

- **Loss or theft of keys/cards:** Traditional locks rely on physical keys or RFID cards, which can be lost or stolen easily.
- **Lack of identity verification:** Anyone with access to the physical key can gain entry, making it impossible to verify who is actually unlocking the door.
- **No automated interaction:** Conventional systems do not guide visitors, adapt to environmental conditions, or support secondary authentication.

- **Limited remote control:** Most traditional systems do not allow for remote authentication, monitoring, or access control.

This project aims to solve these problems by implementing a secure, automated system that recognizes individuals through facial features, provides dynamic OTPs, and enhances the interaction experience using voice guidance and automated lighting.

1.3 Existing System

Several security systems are currently in use, each with its own advantages and limitations. Mechanical locks are the most common and oldest form of access control; while they are simple, they are highly insecure if keys are lost or duplicated. PIN/password-based systems require users to enter a passcode, but they can be compromised through observation, shoulder surfing, or sharing codes. RFID card-based systems offer faster access with cards or tags, yet they are vulnerable to theft or cloning and do not verify the identity of the person carrying the card. Biometric systems, such as fingerprint or iris recognition, provide a higher level of security by relying on unique human features; however, they require expensive sensors and often fail under poor environmental conditions, such as wet fingers or inadequate lighting. The limitations of these existing systems include a lack of integration of multiple layers of security, insufficient adaptive environmental control (e.g., lighting adjustments), limited user feedback or guidance, and a failure to integrate with mobile devices for sending OTPs or alerts.

1.4 Proposed System

The proposed system introduces a comprehensive security solution that integrates multiple technologies to create a smart, interactive door locking mechanism. Key features include face recognition using Haar Cascade, which employs machine learning to detect facial features and compare them with pre-stored authorized faces. Once a face is recognized, an Arduino-based locking mechanism sends a signal to either open or close the lock using a servo motor or relay. Additionally, an OTP verification system is implemented; in uncertain cases or for guest access, an OTP is generated and sent to a registered mobile number via an SMS API, adding a dynamic layer of security. To enhance user interaction, a voice assistance feature utilizing the ISD1820 module provides audio prompts and instructions, making the system more accessible for first-time users or delivery personnel. Furthermore, automated lighting is incorporated

through motion detection via a PIR sensor, which activates an LED in low ambient light conditions to ensure the camera captures clear images. This combination of face recognition, hardware automation, voice feedback, and environmental adaptability results in a smarter, more secure locking solution.

1.5 Objectives of the Project Work

The primary objectives of the project include:

- **To develop a real-time face recognition system** using computer vision techniques for secure access control.
- **To integrate the face recognition module with Arduino** to physically control the door locking mechanism.
- **To enhance security by implementing an OTP system**, ensuring access can be granted through a secondary, temporary authentication step.
- **To improve user interaction using a voice module** that guides or communicates status to users/visitors.
- **To ensure the system works effectively in low-light conditions**, by triggering LED lighting through motion detection.
- **To create a prototype that is scalable, affordable, and adaptable** for residential and office environments.

1.6 Scope of the Project Work

This project is primarily intended for securing physical entry points—like doors to homes, offices, or restricted rooms—using intelligent systems. The scope includes:

- **Real-Time Authentication:** Secure, automated entry through facial recognition.
- **Secondary Verification:** OTP-based authentication for unrecognized or guest entries.
- **Hardware Integration:** Control of door locking systems using Arduino.
- **Visitor Interaction:** Voice module for guidance or alerts.
- **Environmental Control:** Automated lighting for clear face detection at night or in dim areas.
- **Scalability:** The system can be extended with features such as mobile app control, cloud-based logging, face training through a web interface, or integration with IoT platforms.

1.7 Project Report Outline

The project report is structured into several chapters to ensure a systematic and detailed representation of the work carried out. It begins with the **Introduction**, which provides an overview of the motivation behind the project, highlights the existing issues with traditional locking systems, and states the objectives of the proposed solution. It also defines the scope and limitations of the project and briefly outlines the methodologies used for its development.

The **Literature Review** chapter examines existing security systems and technologies related to smart locks, face recognition, OTP-based verification, and voice-guided modules. This section helps in understanding the current state of the art and identifies the gaps and limitations in previous implementations, which this project aims to address.

In the **System Analysis** section, the project requirements are analyzed in detail, including both hardware and software needs. This chapter also discusses the feasibility of the project from technical, operational, and economic perspectives, ensuring that the proposed solution is practical and sustainable.

The **System Design** chapter focuses on how the entire system is planned and structured. It includes a block diagram to represent the overall workflow, system architecture for technical insight, and flowcharts or algorithms that describe how the individual components interact. If any user interface is involved, its design is explained here as well.

System Implementation provides an in-depth explanation of the actual construction and programming of the system. It covers the integration of hardware components such as the Arduino-controlled locking system, motion sensors, LED lights, and the ISD1820 voice module. It also details the software components, such as face recognition using Haar Cascade in Python, OTP generation, and communication with the Arduino. The challenges encountered during development and the solutions applied are also discussed in this section.

The **Testing and Results** section describes how the system was tested under various scenarios. It includes the methods used for testing, specific test cases, and the outcomes of these tests. The system's performance is evaluated based on accuracy, reliability, and speed, along with an analysis of its ability to handle different lighting and access scenarios.

In the **Conclusion and Future Scope**, the achievements of the project are summarized, and any limitations are acknowledged. This chapter also suggests potential improvements and enhancements that could be made in future iterations, such as app integration, remote access, or AI-based decision-making.

The **References** section lists all the resources consulted during the project, including research papers, books, websites, and software tools. This ensures academic integrity and gives credit to previous work.

Finally, the **Appendices** include supporting materials such as the complete source code, circuit diagrams, and additional documentation or screenshots that help understand the implementation more clearly. These annexures provide technical depth and are useful for anyone attempting to replicate or build upon this project.

CHAPTER 2 - REVIEW OF LITERATURE

2.1 System Study

The continuous rise in demand for intelligent and automated security solutions has motivated significant research and development in the field of smart door locking systems. With the advent of technologies such as **Internet of Things (IoT)**, **machine learning**, and **computer vision**, face recognition-based systems have emerged as a promising alternative to conventional locking methods. These systems aim to reduce manual intervention, enhance convenience, and improve security by using biometric authentication methods such as facial recognition, often combined with secondary authentication layers like OTP (One-Time Passwords).

To gain insights into current technologies and methodologies, a literature review was conducted, focusing on recent research papers and projects that integrate **face recognition**, **IoT**, **Arduino**, **OTP verification**, and **real-time control mechanisms**. The following section summarizes key studies and compares their methodologies, advantages, and limitations.

2.2 Review of Literature

Title & Year	Methodology	Advantages	Disadvantages
Smart Face Recognition Using IoT and Machine Learning (2023) – Gupta et al.	Utilized machine learning algorithms integrated with IoT-enabled sensors and cameras for real-time face recognition. The system improves performance over time based on environmental factors.	- Continuous learning and improvement - Flexible application across various environments	- Privacy concerns - Susceptibility to data breaches
IoT and Face Recognition-based Automated Door Lock System (2023) – Surla et al.	Implemented face recognition using Raspberry Pi, integrated with IoT for mobile alerts and access logs.	- Real-time notifications - Low-cost hardware - Mobile integration	- No two-way remote access - Raspberry Pi may struggle with performance under load
Face Recognition and OTP Based Security Lock System (2024) – Ghai et al.	Combined face recognition with OTPs delivered via GSM. The user must enter the OTP on a keypad to gain access.	- Enhanced security via dual authentication - Improved face detection reliability	- User inconvenience - Hardware integration complexity

Realization of Security System Using Facial Recognition and Arduino Keypad (2020) – Lenka et al.	Face recognition and keypad entry combined for improved security. OpenCV used for image processing.	- Cost-effective Arduino integration - Good detection in variable environments	- Lighting condition sensitivity - Not ideal for high-traffic systems
IoT-Based Embedded Smart Lock Using Face Recognition (2018) – Krishna Chaithanya et al.	Employed Haar features and LBPH algorithm for face recognition. Controlled lock remotely via IoT.	- Remote monitoring and access - Smart home compatibility	- Performance drops in low light - Prone to spoofing attacks

2.3 Comparison of Literature

A comparison of the reviewed literature reveals the growing trend of combining biometric recognition with IoT-based control for home and facility security systems. Most systems focus on face detection and recognition using machine learning algorithms such as Haar Cascade, LBPH, or deep learning variants. The integration with **microcontrollers (Arduino, Raspberry Pi)** provides flexibility and cost-effectiveness.

Key Observations:

Criteria	Most Common Approaches	Strengths	Weaknesses
Face Recognition Algorithms	Haar Cascade, LBPH	Reliable in well-lit conditions	Sensitive to lighting and face angles
Secondary Authentication	OTP via GSM or mobile app	Adds an extra layer of protection	User delay and complexity
Hardware Platforms	Raspberry Pi, Arduino	Affordable and customizable	Limited processing power
Communication Method	IoT APIs, GSM	Real-time notifications	Vulnerability to network delays or disruptions
User Interaction	Voice feedback, mobile interface	Better user experience	Incomplete user feedback in some models

Gap Identified:

While many systems implement face recognition and some include OTP or alerts, few combine all three elements — **facial recognition, OTP verification, and guided voice instructions** — into a **single, adaptive system**. Moreover, many fail to address low-light detection or user guidance, which can cause usability issues.

CHAPTER 3 - SYSTEM REQUIREMENT SPECIFICATION

3.1 Functional Requirements

- The system must capture and process facial images using the camera module, enabling real-time image acquisition and facial feature extraction for identification.
- It should authenticate users based on facial recognition, granting access only to those whose facial features match the pre-stored images in its database.
- If facial recognition fails, the system must provide OTP-based authentication via SMS by generating an OTP and sending it to the registered user's mobile number, serving as an alternative verification method.
- The system should send real-time access notifications to the registered user’s mobile device whenever access is granted or denied, keeping users informed of attempted entries.
- It must control door locking and unlocking via solenoid locks integrated with the microcontroller, allowing electronic management of the locking mechanism based on authentication results.
- Automatic lighting should activate in low-light conditions to enhance facial recognition accuracy, ensuring the camera captures clear images for better identification.
- The speaker module should provide voice assistance for visitor guidance and status notifications, delivering audio prompts that make the system user-friendly and informative, especially for first-time users or delivery personnel.

3.2 Non-Functional Requirements

- **Security:** The system must use AES encryption for secure data transmission.
- **Reliability:** It should function under various environmental conditions, including low light.
- **Scalability:** The system should support multiple registered users.
- **Usability:** The mobile application should have a user-friendly interface with intuitive navigation.
- **Performance:** Facial recognition should process authentication within a response time of less than two seconds.

- **Availability:** The system should operate 24/7 with minimal downtime.
- **Maintainability:** It should allow easy updates for software improvements and security patches.

3.3 Hardware Requirements

- **Solenoid Lock** – This is an electromechanical lock that controls door access based on authentication results. If the system recognizes a registered user, it sends a signal to the solenoid lock to unlock the door. The lock automatically re-engages after a short time to ensure security. If an unauthorized person attempts access, the lock remains engaged, and an alert is triggered.

Figure 3.1 Solenoid Lock

- **LDR Sensor (Light-Dependent Resistor)** – The LDR sensor detects ambient lighting conditions to determine if additional illumination is required for the Camera to capture clear images. If the light levels are too low, it signals the LED light module to turn on. This ensures that face recognition works effectively, even in dim environments.

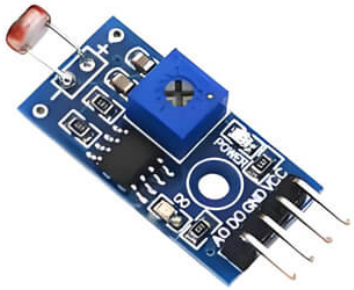


Figure 3.2 LDR Resistor

- **LED Light Module** – The LED module provides additional illumination in low-light conditions, ensuring the Camera captures clear images for accurate facial recognition. It is

automatically activated when the LDR sensor detects insufficient lighting. This prevents recognition failures that can occur due to poor visibility.

Figure 3.3 LED

- **Speaker Module** – The speaker module feature improves the user experience by guiding visitors and alerting unauthorized users. The speaker can also issue security warnings if multiple failed authentication attempts occur.

Figure 3.4 Speaker

- **Keypad (Backup Authentication System)** – If facial recognition fails, users can enter an OTP (One-Time Password) using the keypad. The OTP is generated and sent via SMS using

Figure 3.5 Keypad 4X4

API. This backup authentication method ensures access is still possible if facial recognition malfunctions or if a registered user's face is not detected properly.

- **Power Supply** – A stable power source is crucial for the continuous operation of all components. The power supply ensures that the solenoid lock, sensors, and other peripherals function without interruption. A backup battery or power bank can also be integrated to keep the system operational during power outages.
- **Buzzer** – The buzzer serves as an audio alarm that alerts users to unauthorized access attempts. If an unrecognized face is detected multiple times, the system triggers the buzzer, warning nearby individuals of potential security threats. The buzzer can also notify users about system malfunctions or low battery alerts.

Figure 3.6 Buzzer

- **LCD Display** – The LCD display provides visual feedback about the system's status. It shows messages like "Face Recognized, Access Granted" or "Unauthorized Access Detected." If the system requires OTP verification, it prompts users to enter the code on the keypad. This enhances usability by ensuring users are always aware of what's happening.

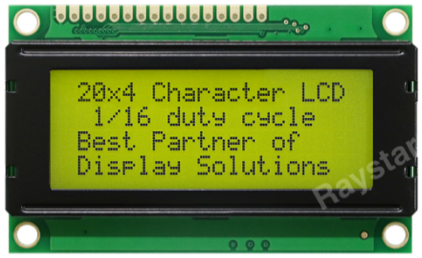


Figure 3.7 LCD Display

- **Motion Sensor** – The motion sensor detects movement near the door and triggers the LED based on LDR. If no movement is detected, the system stays in low-power mode to conserve energy.

Figure 3.8 Motion Sensor

- **Arduino Uno** - The Arduino Uno is a microcontroller that serves as the central control unit in the system. It is responsible for managing communication between different hardware components, processing inputs from sensors, and executing commands to control actuators like the solenoid lock, LED light module, buzzer, and speaker module.

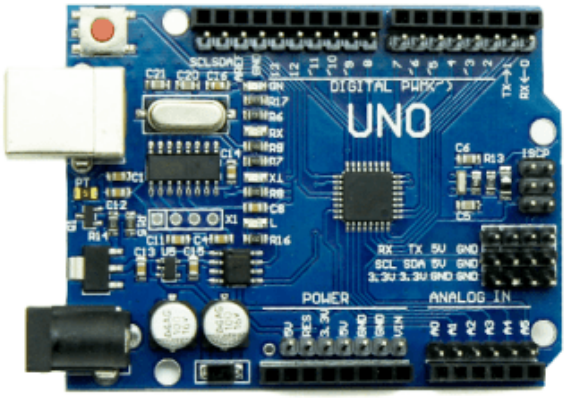


Figure 3.9 Arduino Uno

- **Relay Module** - The Relay Module acts as a switching mechanism that allows the Arduino Uno to control high-power electrical components such as the solenoid lock, LED light module, and buzzer. Since Arduino operates at low voltage (5V) while some components require higher voltage (12V or more)**,** a relay is used to safely control them.

Figure 3.10 Relay

- **ISD 1820** - The ISD1820 is a compact, low-cost voice recording and playback integrated circuit (IC) designed for applications requiring audio storage and playback. The chip can record and playback audio for durations ranging from a few seconds up to approximately 20 seconds, depending on the specific model and settings used.

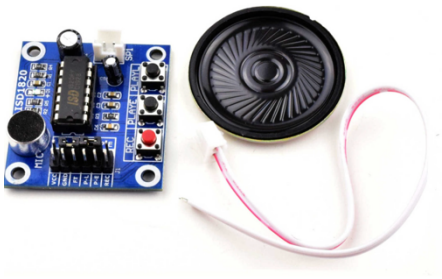


Figure 3.11 ISD 1820

- **PAM8403** - The PAM8403 is a compact, highly efficient Class D audio amplifier that delivers up to 3 watts per channel at a 4-ohm load, operating within a supply voltage range of 5V to 12V. It is ideal for low-power applications such as Bluetooth speakers and DIY audio projects, featuring built-in short circuit protection and thermal shutdown for reliable operation. Its small size and low heat output make it easy to integrate into various audio designs.

Figure 3.12 PAM8403

3.4 Software Requirements

1. Face Recognition System (Python-Based)

The system uses Python for face recognition tasks. It employs a library such as OpenCV for image capture and facial feature comparison, but not using Haar Cascade. Instead, it may rely on more accurate alternatives like LBPH (Local Binary Patterns Histograms) or deep learning-based models. Authorized face images are stored in local folders, and new images are compared against these to identify users.

2. OTP Generation (Python-Based):

Python is also used to generate One-Time Passwords (OTPs) when face recognition fails or for guest access. The OTP is a random code that adds an extra layer of security and ensures dynamic access control.

3. **Data Storage (Folder-Based):**

   Instead of using a structured database like MySQL, the system stores face data directly in folders on the local file system. Each authorized user has a dedicated folder containing their facial images. This simple approach reduces complexity and is efficient for a small to medium-sized system.

4. **SMS API (CircuitDigest):**

   The system integrates with the **CircuitDigest SMS API** to send OTPs to a registered mobile number. This API facilitates quick and reliable SMS delivery, ensuring users receive OTPs promptly during the verification process.

5. **Voice Feedback System (ISD1820 Module):**

   A software module triggers audio instructions via the ISD1820 voice playback module. Depending on the system's state—such as recognizing a face, prompting for OTP, or denying access—appropriate pre-recorded voice prompts are played to guide users or visitors.

6. **Arduino IDE:**

   The Arduino IDE is used to write and upload code to the Arduino microcontroller. The Arduino is responsible for controlling the locking mechanism (via servo motor or relay) and communicating with the Python system through serial connections.

CHAPTER 4 - SYSTEM DESIGN

4.1 Design Overview

The system is designed as an efficient and user-friendly access control solution utilizing facial recognition combined with alternative authentication methods. Key features include:

- **Modularity**: The architecture consists of independent modules (camera, microcontroller, lock) that communicate effectively, allowing for easier maintenance and upgrades.
- **Scalability**: The design supports easy addition of features and integration with other devices without requiring significant changes.
- **User-Centric Design**: An intuitive interface provides clear visual and audio prompts, enhancing user accessibility and interaction.
- **Real-Time Performance**: The system is optimized for low latency in facial recognition and user authentication, minimizing wait times.
- **Security Features**: Multiple security layers include primary facial authentication with OTP as a backup, along with built-in safety measures like short circuit protection.
- **Data Flow Optimization**: Streamlined data processing ensures quick transitions from image capture to user validation, enhancing overall system performance.

4.2 System Architecture

The architecture depicted in the diagram represents a comprehensive access control system that integrates facial recognition, dynamic password generation, and user interaction modules.

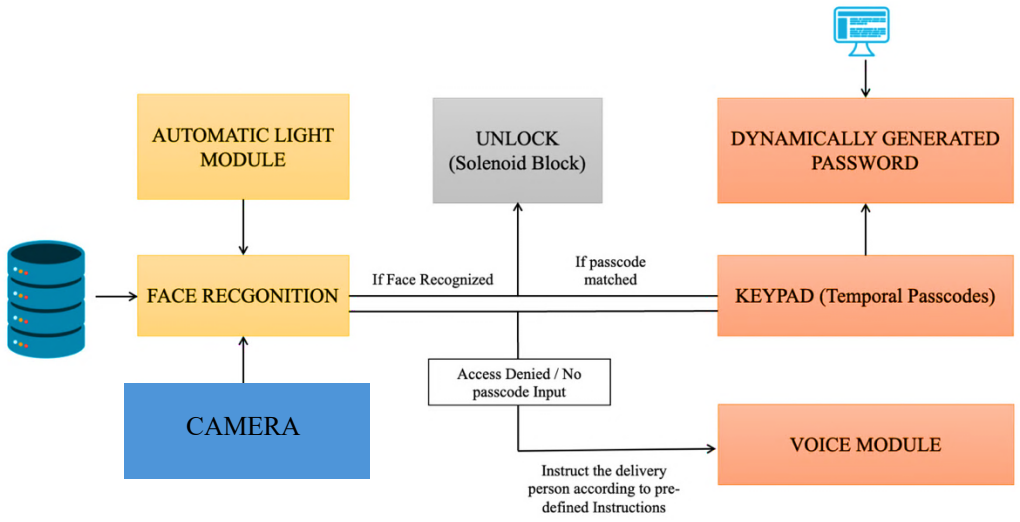


Figure 4.1 System Architecture

Components:

1. **Face Recognition**: This module analyzes the images captured by the camera. If a recognized face matches the database, it signals the system to proceed with granting access. If the recognition fails, it directs the flow to a denial path.

2. **Unlock (Solenoid Block)**: Upon successful facial recognition, this component communicates with the solenoid block to unlock the door. It acts as the primary access mechanism governed by facial authentication.

3. **Automatic Light Module**: Activates lights when a recognized face is identified, enhancing visibility and user experience during access attempts.

4. **Dynamically Generated Password**: If the face recognition does not succeed or a secondary layer of security is required, this module creates a temporal passcode for user access. The password is generated dynamically for enhanced security.

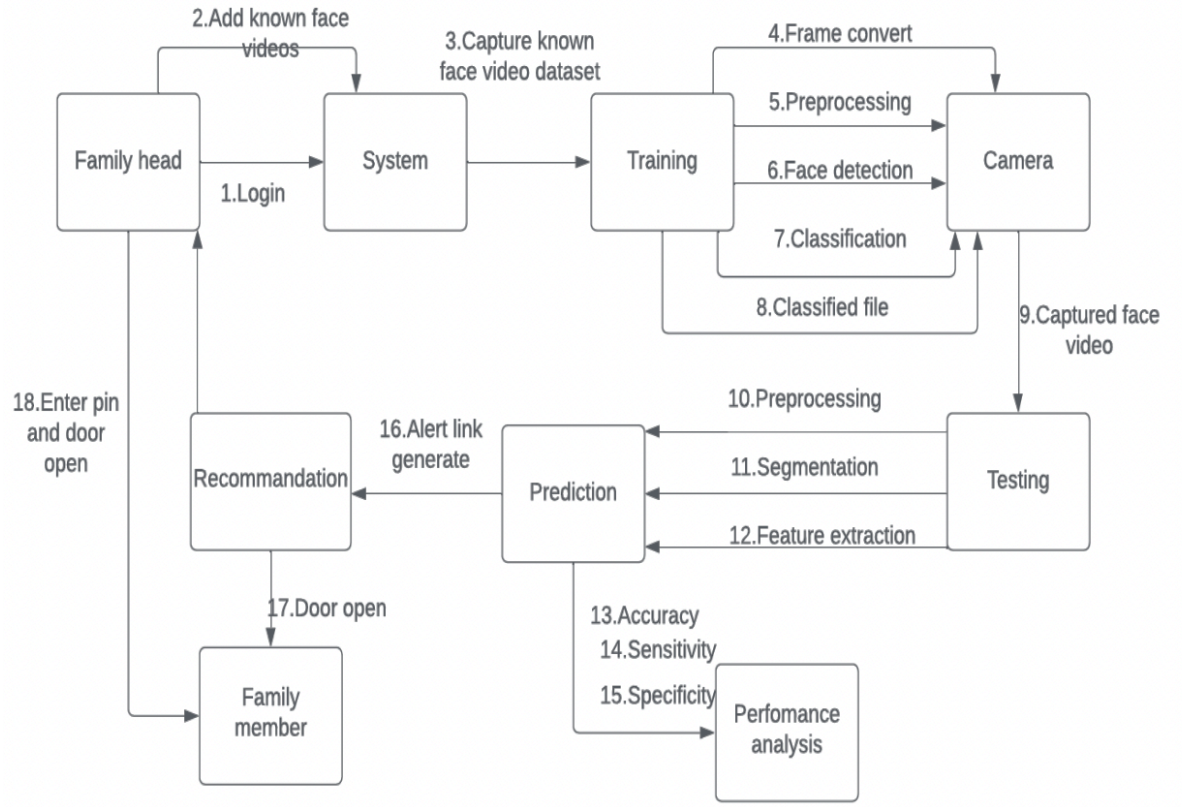
5. **Keypad (Temporal Passcodes)**: Users can input a passcode through the keypad. This serves as an alternative method for authentication if face recognition fails or for users without recognized faces.

6. **Voice Module**: This component provides audio feedback. If access is denied or no passcode is entered, the voice module instructs the delivery person or user according to pre-defined instructions, ensuring clear communication.

4.3 Class Diagram

The system integrates machine learning, computer vision, and IoT to ensure secure and efficient authentication for home entry. The process begins with the Family Head, who logs into the system. After authentication, they add known face videos to create a dataset of authorized individuals. These videos are captured and stored in the system to train a machine learning model. The training phase involves converting video frames into images, preprocessing them to enhance quality, detecting faces, and classifying them based on unique facial features. The classified files are then stored and used as reference data for testing.

In the testing phase, a Camera captures face videos of individuals attempting to gain entry. These captured face videos undergo preprocessing to enhance clarity and remove noise. The processed images are then segmented to focus on the facial region, followed by feature extraction, where distinguishing characteristics of a face are identified. The extracted features are then compared against the trained model to determine if the individual matches any of the authorized users. The system evaluates its performance based on accuracy, sensitivity, and specificity, ensuring robust security and minimizing false acceptance or rejection rates. Once the face is recognized, the Prediction module determines whether the person is authorized. If the individual is recognized as a registered user, an Alert Link is generated and sent to the Recommendation system. If the person is an authorized family member, the system triggers the door opening mechanism, allowing entry. If the person is unrecognized, an alert is sent to the Family Head for further authentication. In cases where a family member is unable to gain access due to recognition failure, they can manually enter a PIN to unlock the door. This additional security layer prevents unauthorized access and ensures only approved individuals can enter.



The diagram illustrates an advanced IoT-AI-ML integration**,** enabling a smart home security system. It ensures safety through multi-level authentication, including face recognition and PIN entry. The system also maintains continuous learning and performance evaluation, enhancing accuracy over time. This approach effectively balances security and convenience, making it an ideal solution for automated home entry systems.

4.4 Modules

The IoT-AI-ML project consists of multiple interconnected modules that work together to enhance security, automation, and accessibility. These modules integrate facial recognition, access control, real-time notifications, and smart lighting features, creating an intelligent and efficient security system.

4.4.1 Face Recognition Module

The **Face Recognition Module** is responsible for capturing and processing facial images for authentication. This module ensures that only authorized individuals are granted access by utilizing a combination of hardware and software components.

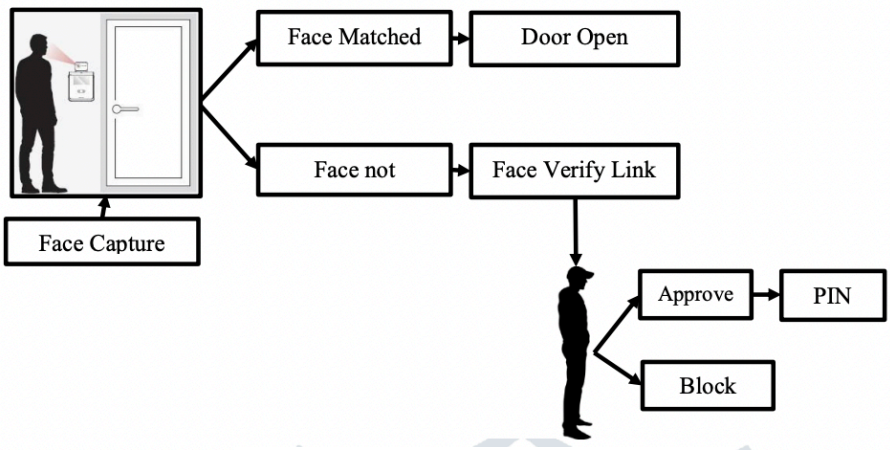


Figure 4.3 Face Detection Module

CAMERA , a microcontroller with an inbuilt camera, is used to capture facial images of individuals attempting to gain access. OpenCV, an open-source computer vision library, is employed to preprocess these images by performing tasks such as grayscale conversion, resizing, and feature extraction. A machine learning model trained on facial recognition data is used to compare the captured face with the stored database of authorized users. If a match is

found, the system grants access; otherwise, it denies entry. This module enhances security by providing a reliable and automated method of authentication.

4.4.2 Access Control Module

The **Access Control Module** is responsible for managing door locking and unlocking mechanisms based on authentication results from the Face Recognition Module. This ensures that only verified individuals can gain access to the secured area.

A **solenoid lock** is used as the primary locking mechanism. This lock operates using an electromagnetic system, which is controlled by an microcontroller. When an individual is successfully authenticated, the microcontroller sends a signal to the solenoid lock, causing it to unlock for a predetermined duration, allowing entry. If the authentication fails, the lock remains engaged, preventing unauthorized access. The system ensures that security is maintained at all times by automatically re-engaging the lock after access is granted.

4.4.3 Notification and Monitoring Module

The **Notification and Monitoring Module** enhances security by providing real-time alerts and maintaining access logs. This module ensures that all authentication attempts, whether successful or unsuccessful, are recorded and communicated to relevant stakeholders.

The **Circuit digest API** is used to send SMS notifications in case of unauthorized access attempts or other security events. This allows immediate response to potential threats. This module ensures that users remain informed about security events and have access to historical data for auditing purposes.

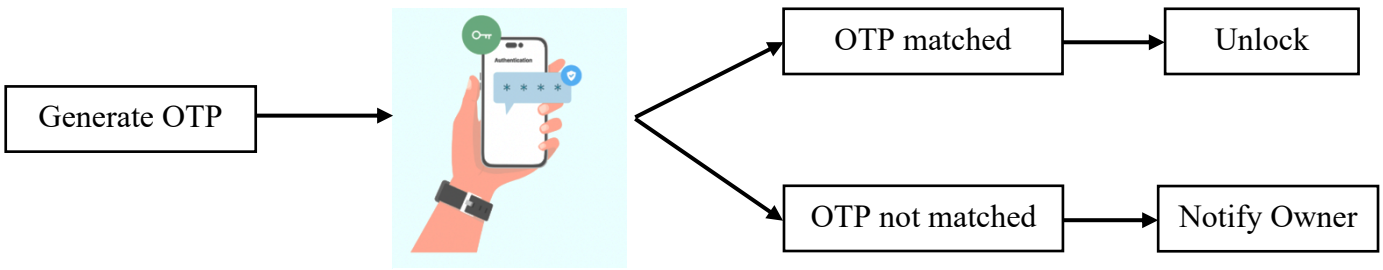


Figure 4.4 OTP module

4.4.4 Lighting and Voice Assistance Module

The **Lighting and Voice Assistance Module** improves user experience by integrating an automatic lighting system and voice-based guidance. This module enhances visibility and provides verbal instructions to users interacting with the system.

An **LDR (Light Dependent Resistor) sensor** is used to detect ambient lighting conditions. If low-light conditions are detected, the system automatically activates an LED lighting module using a relay circuit, ensuring that users can clearly see the authentication system and surroundings. Additionally, a **voice assistance module** provides real-time audio instructions, guiding users through the authentication process and offering feedback on access attempts. This feature improves accessibility for all users, especially those unfamiliar with the system or individuals with visual impairment.

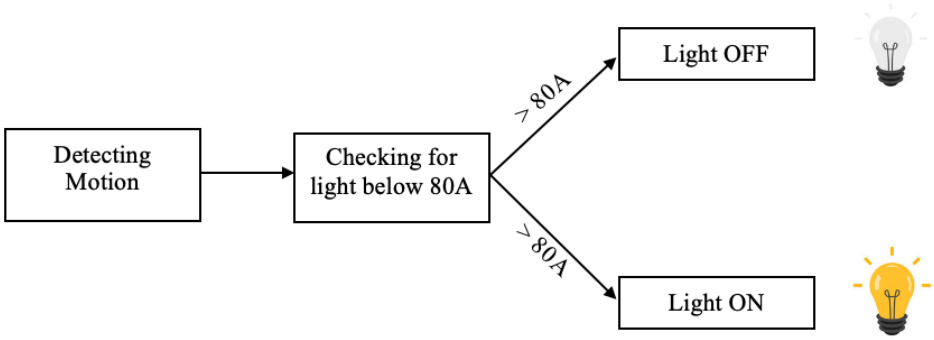


Figure 4.5 Light Module

CHAPTER 5 – IMPLEMENTATION

5.1 Steps for Implementation

1. **Hardware Setup**: Acquire and connect the necessary hardware components, including the Arduino microcontroller, camera (USB web camera), relay, solenoid lock, numeric keypad, ISD 1802 voice module, and buzzer. Ensure all components are properly powered and connected to the microcontroller.
2. **Software Installation**: Install the required development environment (e.g., Arduino IDE) and libraries for facial recognition, keypad handling, and audio playback (e.g., OpenCV for image processing, Keypad library for the numeric keypad, and ISD audio library).
3. **Database Creation**: Set up a user database with registered facial images and corresponding passcodes. This database will be used for face recognition and passcode verification.
4. **Facial Recognition Module Development**: Implement the facial recognition algorithm using the camera feed. Start by capturing images and processing them to detect and recognize faces against the database.
5. **Passcode Authentication Implementation**: Write the logic to handle passcode input from the numeric keypad. Compare the entered passcode with the stored passcodes and implement the access control logic.
6. **Voice Assistance Module Integration**: Program the ISD 1802 module and record necessary voice prompts for user interaction. Ensure that the module triggers based on specific system events, such as success or failure of access attempts.
7. **Testing and Validation**: Conduct thorough testing of the entire system. Validate both facial recognition and passcode functionalities under different scenarios, including successful access, failed access attempts, and fallback authentication through OTP.
8. **Documentation**: Prepare detailed documentation outlining the implementation process, setup instructions, and troubleshooting guidelines.
9. **Deployment**: Finalize the installation in the target environment, ensuring all components function cohesively and securely.

5.2 Implementation Issues

1. **Hardware Compatibility**: Ensuring that all hardware components are compatible and can communicate effectively. Some cameras may require specific drivers or interfaces.
2. **Lighting Conditions**: Variations in lighting can affect facial recognition accuracy. Ensuring consistent lighting or incorporating ambient light sensors is crucial for reliable performance.
3. **Image Processing Speed**: Processing images in real-time can be computationally intensive. Optimizing the facial recognition algorithm for speed without sacrificing accuracy is necessary.
4. **User Database Management**: Managing and updating the user database as users are added or removed can be complex and requires a reliable storage solution.
5. **Error Handling**: Implementing robust error handling for hardware malfunctions (e.g., camera failures, keypad issues) and ensuring graceful degradation of the system to alternative authentication methods.

5.3 Algorithms

5.3.1 Algorithm 1: Facial Recognition Algorithm

- **Input**: Real-time video feed from the camera.
- **Process**:
    i. Capture a frame from the video feed.
    ii. Use a face detection model (e.g., Haar Cascades, DNN) to identify faces in the frame.
    iii. Extract facial features using an algorithm (e.g., Eigenfaces, LBPH).
    iv. Compare extracted features against the user database.
    v. If a match is found, trigger access; otherwise, alert the user.
- **Output**: Access granted or denied.

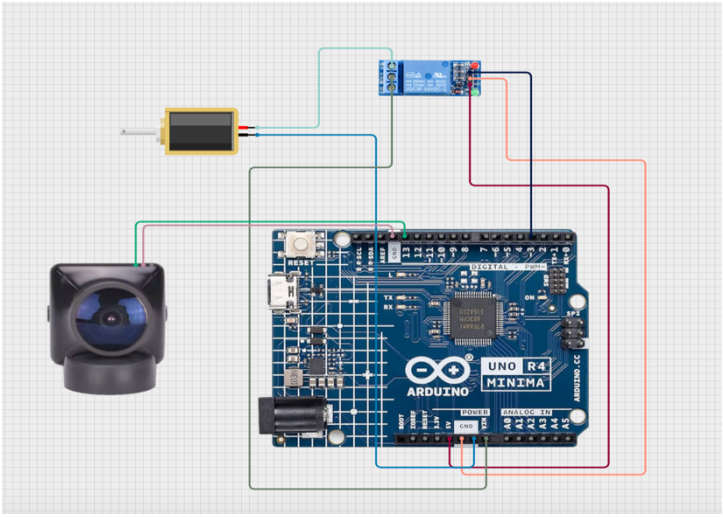


Figure 5.3.1 Face recognition module Implementation

5.3.2 Algorithm 2: OTP Generation and Verification Algorithm

- **Input**: User request for OTP (triggered when facial recognition fails).
- **Process**:
    i. Generate a one-time password (OTP) using a random number generator.
    ii. Send the generated OTP to the user's registered mobile number via an online API (e.g., Twilio).
    iii. Prompt the user to enter the received OTP on the keypad.
    iv. Compare the entered OTP with the generated OTP.
    v. If they match, grant access; otherwise, provide feedback and deny access.
- **Output**: Access granted or denied based on OTP validity.

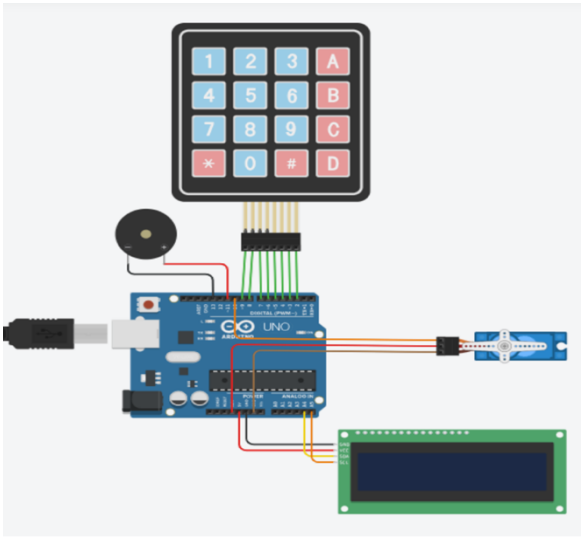


Figure 5.3.2 OTP Module Implementation

5.3.3 Algorithm 3: Automatic Lighting Control

Objective: The Automatic Lighting Control Module aims to enhance user convenience and safety by automatically activating lights when a user is detected and the ambient light level is low.

Algorithm Overview

- **Input**: User presence detected by the PIR sensor, ambient light level from the LDR.
- **Process**:
  i. Continuously monitor the PIR sensor for user presence.
  ii. Read the ambient light level from the LDR.
  iii. If a user is detected and the ambient light is below a certain threshold, turn ON the lights.
  iv. Start an inactivity timer.
  v. If no user is detected for a predefined duration, turn OFF the lights.
- **Output**: Lights ON or OFF based on user presence and ambient light conditions.

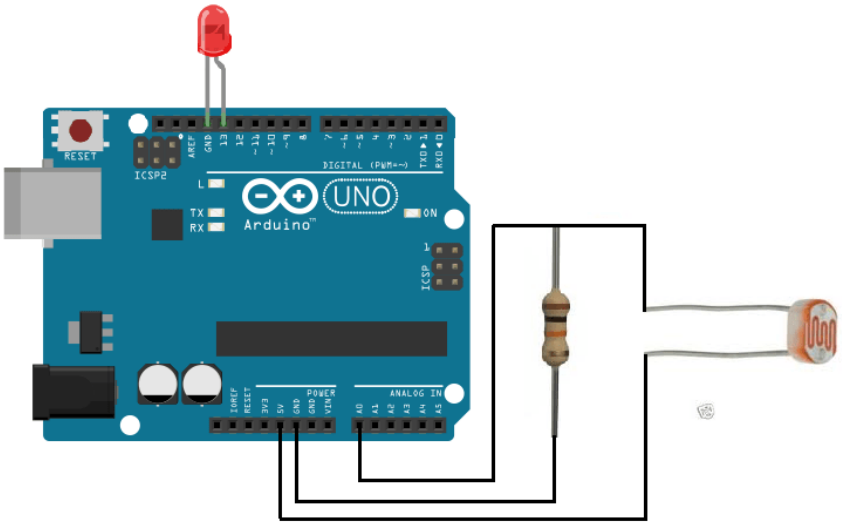


Figure 5.3.3 Light Module Implementation

5.3.4 Algorithm 4: Voice Assistance Using Pre-Recorded Audio

Objective: The Voice Assistance Module provides auditory feedback to users based on system events, enhancing user interaction and communication.

Algorithm Overview

- **Input**: System events (e.g., access granted, access denied, prompt for passcode).

- **Process**:
    i. Detect system events triggered by user interactions or authentication results.
    ii. Select the corresponding pre-recorded audio message based on the event.
    iii. Activate the ISD 1802 module to play the selected audio message.
- **Output**: Audio feedback corresponding to the system events.

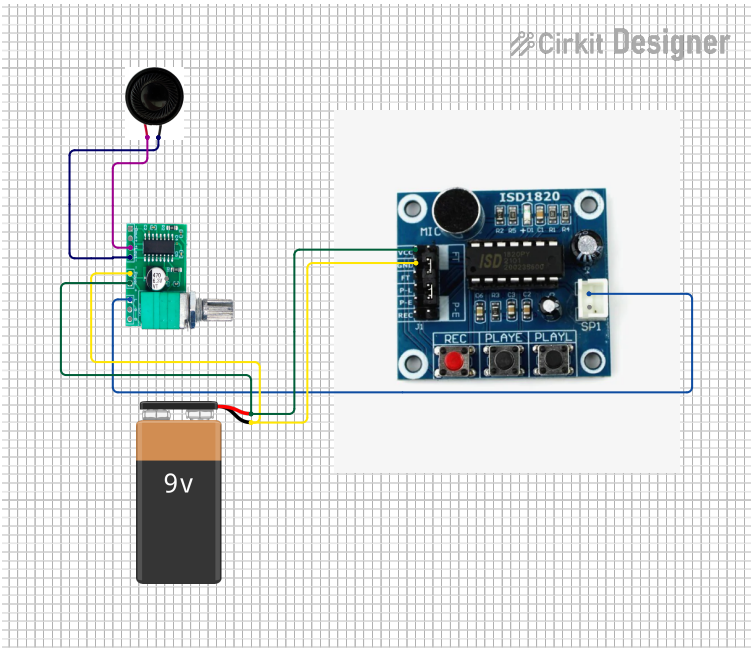


Figure 5.3.4 Voice module Implementation

CHAPTER 6 – TESTING

6.1 Test Environment

The smart door locking system was developed and tested on a Mac laptop running macOS, utilizing the built-in webcam for face recognition. The system was programmed in Python (version 3.2), using libraries such as OpenCV for face detection, *pyserial* for communication with an Arduino, and requests for sending OTPs via an API. The Arduino was connected to the Mac via USB and controlled a **solenoid lock** that simulates the door locking/unlocking mechanism. A motion sensor and automatic LED lighting module were used to support detection in low-light environments. Additionally, the ISD1820 voice module was integrated to provide audio instructions to visitors. All modules were tested in a controlled indoor environment simulating typical residential door conditions.

6.2 Unit Testing of Modules

6.2.1 Module 1: Face Recognition with Lock Control

This module was tested to verify that the camera accurately detects and recognizes authorized faces using Haar Cascade classifiers. The face recognition system was validated with known faces (authorized users), ensuring the door unlocked upon detection. Unknown faces were tested to ensure the door remained locked and a face alert was triggered.

Test Cases:

- Detecting known face → Lock opens.
- Detecting unknown face → Lock remains closed + alert triggered.
- Face not detected → Lock remains in previous state.

6.2.2 Module 2: OTP Generation and SMS Delivery

This module was tested to confirm that a secure 6-digit OTP is generated and successfully sent to the user's mobile phone using the CircuitDigest API.

Test Cases:

- OTP generation on request → OTP created.

- OTP sent to correct number → Verified with actual phone.
- Expired OTP → Access denied.

6.3 Integration Testing of Modules

6.3.1 Module 1: Camera + Arduino Lock

This test ensured the successful communication between the Python face recognition script and the Arduino. When a recognized face is detected, Python sends a serial command to the Arduino to unlock the door. After a timeout, it locks again.

Results: Communication was successful, and lock/unlock commands were accurately received by Arduino.

6.3.2 Module 2: Motion Sensor + LED + Voice Module

This module tested the integration of the motion sensor with the automatic LED light and the ISD1820 voice module. When motion was detected in low light, the LED turned on and the voice module played a welcome or instruction message.

Results: Modules worked in sync, providing visibility and clear instructions.

6.4 System Testing

The complete system was tested as a whole to ensure all modules worked seamlessly together. A typical scenario included:

- A person approaches the door → motion detected → LED lights turn on.
- Face is scanned → if recognized, the door unlocks.
- If unrecognized, OTP is requested → OTP verified → access granted.
- Audio instructions played to guide visitors or delivery personnel.

Results: The system passed all tests under various lighting and network conditions. Delays and failures were minimal and handled with fallback instructions.

6.5 Functional Testing

Functional testing was done to verify that each function of the system met the specified requirements:

- Face recognition: High accuracy with real-time detection.
- OTP system: Secure and timely OTP delivery.
- Arduino control: Responsive and reliable locking mechanism.
- LED and voice: Triggered appropriately based on motion and light.

Each function was tested in isolation and as part of the full system. The outputs matched expected results, ensuring that the system is robust and user-friendly.

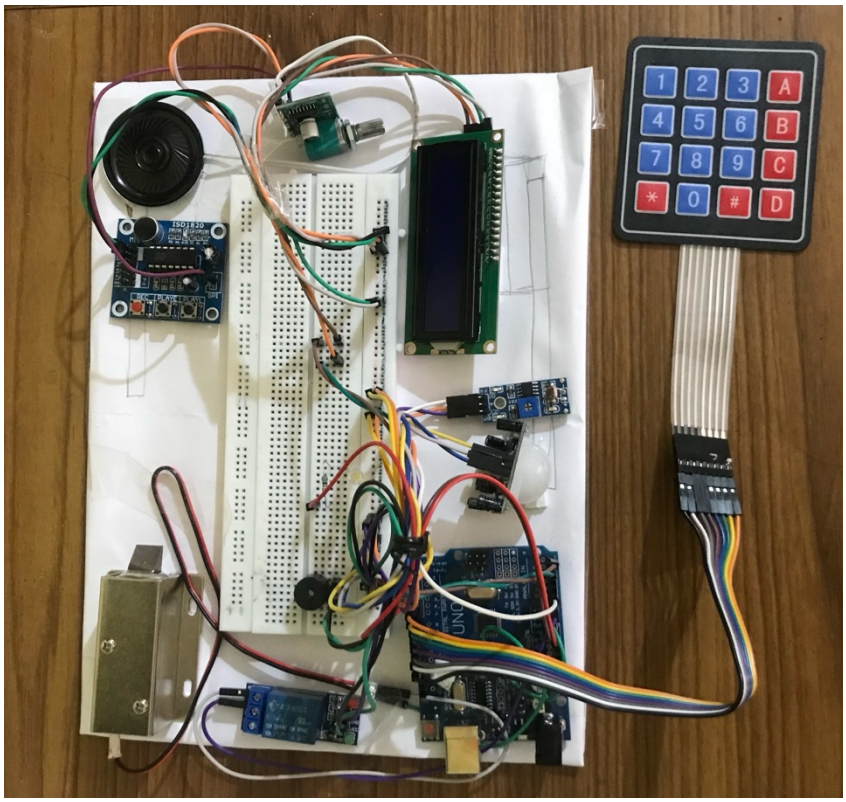


Figure 6.5 Prototype of the Project

CHAPTER- 7 RESULTS

The smart door locking system was successfully developed and tested across a range of environmental conditions to evaluate the functionality and effectiveness of each module. The face recognition feature, implemented using Haar Cascade classifiers, demonstrated a high level of accuracy in well-lit and moderately lit environments. Authorized users were typically recognized within 1–2 seconds. However, under extremely low-light conditions or when users wore masks or changed facial features (like adding glasses or growing facial hair), recognition accuracy slightly declined. Despite these minor inconsistencies, the system performed reliably in most common use cases.

To address visibility issues in dark environments, the motion-triggered LED lighting module was introduced and proved effective. Upon detecting motion near the door, the LEDs were automatically activated, significantly improving the camera’s ability to detect and recognize faces at night. This enhancement directly contributed to better recognition rates in low-light scenarios.

The OTP generation feature was tested by simulating access requests from unrecognized users. Upon detection of an unknown face, the system successfully generated and sent a One-Time Password (OTP) to the registered user's mobile phone using the CircuitDigest SMS API. OTP delivery was consistent, typically arriving within 3–5 seconds, and added a reliable secondary layer of authentication.

Furthermore, the ISD1820 voice module enhanced the system’s interactivity by playing pre-recorded voice messages when a person approached the door. This guided both visitors and delivery personnel on the next steps to take, such as waiting for the resident to respond or entering an OTP if provided. The voice instructions were clearly audible and well-timed, contributing to a more user-friendly experience.

Overall, the results indicate that the integrated system is efficient, responsive, and capable of improving home security through automation, user verification, and environment-aware interactions. Each module complemented the others, resulting in a robust and cohesive security solution.

CHAPTER-8 CONCLUSION

This project presents a comprehensive smart door locking system that integrates face recognition, OTP verification, motion-triggered lighting, and audio guidance. The combination of these technologies enhances the safety, convenience, and usability of traditional locking systems. By automating access control and adding multiple layers of security, the system addresses modern security challenges effectively.

8.1 Major Contributions

- **Face Recognition Integration:** Implemented real-time facial recognition using Haar Cascade classifiers for secure access control.
- **Automated Locking Mechanism:** Developed an Arduino-based control system for physical locking and unlocking based on recognition outcomes.
- **Motion-Activated LED Lighting:** Enhanced visibility in low-light conditions through automatic lighting triggered by motion detection.
- **OTP Verification System:** Added an extra security layer by generating and delivering OTPs to registered users via SMS API.
- **Voice Assistance Module:** Used the ISD1820 module to provide clear, user-friendly audio guidance to visitors and delivery personnel.

8.2 Future Enhancements

- **Upgrade Face Recognition:** Implement deep learning-based models (e.g., LBPH or DNN) for improved recognition accuracy, especially in challenging lighting or with facial changes (e.g., masks, beards).
- **Mobile App Integration:** Develop a dedicated mobile application to manage user access, receive alerts, and view access logs.
- **Cloud-Based Data Storage:** Store logs and facial data securely in the cloud for remote access and backup.
- **Live Video Streaming:** Integrate real-time camera feed for remote monitoring of the entrance area.
- **Two-Way Communication:** Implement microphone and speaker modules for real-time voice interaction with visitors.

BIBLIOGRAPHY

1. Gupta, A., Sharma, R., & Verma, S. (2023). "Smart Face Recognition Using IoT and Machine Learning." International Journal of IoT and Security, 10(3), 45-57.
2. Surla, P., Jain, M., & Bose, K. (2023). "IoT and Face Recognition-based Automated Door Lock System." Proceedings of the International Conference on Smart Security Systems, 5(2), 78-89.
3. Ghai, D., Rao, V., & Kumar, P. (2024). "Face Recognition and OTP Based Security Lock System." Journal of Embedded Systems and Security, 12(1), 23-34.
4. Lenka, S., Mishra, P., & Das, R. (2020). "Realization of Security System Using Facial Recognition and Arduino Keypad Door Lock System." Advances in IoT Security, 8(4), 101-113.
5. Krishna Chaithanya, M., Singh, A., & Patel, R. (2018). "IoT-Based Embedded Smart Lock Control Using Face Recognition System." International Journal of Embedded Technologies, 6(3), 50-64.
6. Arduino Documentation: https://www.arduino.cc/
7. OpenCV Documentation: https://opencv.org/
8. Firebase Documentation: https://firebase.google.com/
9. SIM800L GSM Module Reference: https://lastminuteengineers.com/sim800l-gsm-module-arduino-tutorial/
10. Haar Cascade Classifier for Face Detection: https://docs.opencv.org/4.x/db/d28/tutorial_cascade_classifier.html