ISSN 2277-2685
IJESR/April. 2026/ Vol-16/Issue-2s /86-95
Mohammed Mubasheer Ahmed *et. al.*, / International Journal of Engineering & Science Research
Full Length Article

Multipurpose Locker Security System Using Image Processing and IOT

Mohammed Mubasheer Ahmed [1] , Shaik Azeem Pasha [2] , Shaik Farook [3] , Mrs Nousheen Hashmi[4] , Dr Syeda Gauhar Fatima [5]
[1,2,3]Ug Student, Department Of Electronics And Communication Engineering, Deccan College Of Engineering And Technology Hyderabad, India.
[4]Assisstant Professor, Department Of Electronics And Communication Engineering, Deccan College Of Engineering And Technology Hyderabad, India.
[5]Professor, Department Of Electronics And Communication Engineering, Deccan College Of Engineering And Technology Hyderabad, India.
Accepted 25-04-2026
Author(s) Retains the Copyrights of This Article

ABSTRACT *- Security is becoming an important issue everywhere nowadays. Every person wants his house, factory, bank etc. to be secured.The Implementation of a digital door locker security system using image processing and IOT platform.User face is registered for the accessing the door on all times. If the user face is matched it asks for OTP (One Time Password), which is used as dual step verification.If the locker is accessed by any intruder or an unregistered person, the Pi cam captures the image and stores it in the folder for future reference to the owner.And if the person is wearing mask or doesn't want to go through facial recognition process, they can access the locker remotely through registered mobile. In order to overcome the above problems. Various types of feature sets can be used, such as: Two step verification (Face detection algorithm, and random password generation OTP) to access the locker. IOT based MQTT protocol for saving the data (name, date & time who and when the locker was accessed) for future reference.Owner can give the access of the locker to the people he wanted and can be removed simultaneously.Images are saved from the live feed of the person whose data is not saved in the system. To Study Algorithm used for face recognition, which is Haar Cascade Algorithm, also known as Voila-Jones Algorithm.To design a digital door locker security system using image processing and IOT platform.Implementation of MQTT protocol on the security system and generation of OTP.*

Keywords: *Digital Door Locker, Image Processing, Internet of Things (IoT), Face Recognition, Haar Cascade Algorithm, Viola-Jones Algorithm, One-Time Password (OTP), Two-Step Verification, MQTT Protocol, Raspberry Pi Camera, Smart Security System, Facial Authentication, Remote Access Control, Intruder Detection, Dual Authentication, Smart Locker System, Access Monitoring, Real-Time Surveillance, Secure Authentication, IoT-Based Security System.*

I. Introduction

In today's rapidly evolving digital world, ensuring the safety of personal belongings and sensitive assets has become a major concern across residential, commercial, and industrial domains. Conventional locker security mechanisms such as mechanical locks, PIN-based systems, and biometric authentication methods are commonly used; however, they often lack robustness, flexibility, and real-time monitoring capabilities. Password-based systems are vulnerable to guessing and unauthorized sharing, while biometric systems such as fingerprint recognition can fail due to environmental factors like dirt, moisture, or physical wear. These limitations highlight the need for more reliable, intelligent, and multi-layered security solutions.

Recent advancements in image processing and the Internet of Things (IoT) have opened new possibilities for designing smart security systems that are both efficient and user-friendly. Image processing techniques, particularly facial recognition, provide a non-intrusive and highly effective method for user identification. Unlike traditional biometrics, facial recognition does not require physical contact and can operate seamlessly in real time. On the other hand, IoT enables interconnected devices to communicate over the internet, allowing remote monitoring, data logging, and system control from anywhere. The integration of these technologies makes it possible to develop advanced security systems with enhanced functionality and improved user experience.

This research focuses on the design and implementation of a multipurpose locker security system that leverages image processing and IoT to provide a secure and intelligent access control mechanism. The proposed system employs facial recognition as the primary authentication method, where authorized users are identified using a pre-trained dataset. To strengthen security further, a secondary authentication layer is introduced in the form of a One-Time Password (OTP), ensuring that

access is granted only after successful multi-factor verification. This dual-layer approach significantly reduces the chances of unauthorized entry.

In addition to authentication, the system incorporates real-time monitoring and data management features using IoT protocols. Access details, including user identity, timestamp, and entry status, are recorded and transmitted through a lightweight communication protocol, enabling efficient data handling even in resource-constrained environments. In the event of an unauthorized access attempt, the system captures and stores the image of the individual, providing valuable evidence for security analysis. Furthermore, the integration of a mobile-based interface allows users to remotely manage access permissions, monitor activity, and interact with the system in real time.

Another key aspect of the proposed system is its adaptability and scalability. The design is based on a compact and cost-effective hardware platform, making it suitable for a wide range of applications such as home lockers, office cabinets, bank lockers, and secure storage units. The system can also be extended with additional features such as cloud storage, alert notifications, and advanced recognition algorithms, making it a future-ready solution.

The main objective of this work is to develop a smart locker system that not only enhances security but also ensures convenience, reliability, and efficiency. By combining image processing with IoT-based communication, the proposed system addresses the shortcomings of traditional security mechanisms and provides a modern, intelligent alternative. This research contributes to the growing field of smart security systems by demonstrating how emerging technologies can be effectively integrated to meet real-world security demands.

II. Literature Survey

To understand the advancements in smart security systems, several research works related to image processing, IoT-based authentication, and smart locker systems have been reviewed. Existing systems mainly focus on single-layer authentication such as passwords, biometrics, or IoT-based monitoring. However, many of these systems suffer from limitations such as lack of multi-factor authentication, dependency on environmental conditions, and insufficient real-time monitoring. The following table summarizes key contributions and limitations of relevant research works.

Name of the Paper	Year	Components Used	Contributions	Limitations
Face Recognition Based Smart Locker System	2025	• Camera Module • OpenCV • Face Detection Algorithm	• Real-time face recognition for access control • Contactless authentication	• Performance affected by lighting conditions • Limited accuracy with masks
IoT-Based Smart Security Locker	2024	• Raspberry Pi • Cloud Server • Mobile Application	• Remote monitoring and control • Real-time access logging	• Dependent on internet connectivity • Security risks in cloud storage
OTP-Based Digital Locker System	2023	• GSM Module • Microcontroller • Keypad	• Two-factor authentication using OTP • Improved access security	• Delay in OTP delivery • No biometric verification
Biometric Locker Security System	2022	• Fingerprint Sensor • Microcontroller	• Easy and fast authentication • Widely used security method	• Sensor failure due to moisture or damage • Vulnerable to spoofing
IoT-Based Home Security System	2021	• IoT Sensors • Mobile App • Camera	• Remote surveillance • Real-time alerts and notifications	• High power consumption • Limited authentication mechanisms
Smart Surveillance Using Image Processing	2020	• Camera • Image Processing Algorithms	• Automated intruder detection • Image capture and storage	• High computational cost • False detection possibilities

III. Hardware Specifications

1. Raspberry Pi 3B

The Raspberry Pi 3 Model B serves as the central processing unit of the proposed smart locker system. It is a compact, low-cost single-board computer capable of performing complex tasks such as image processing and IoT communication. The board is powered by a Broadcom BCM2837 chipset with a 1.2 GHz quad-core ARM Cortex-A53 processor and 1GB RAM.

Raspberry Pi supports various interfaces including USB, HDMI, Ethernet, and GPIO pins, allowing easy integration with peripherals such as camera modules, sensors, and actuators. It operates on a

Linux-based operating system and is programmed using Python, making it suitable for real-time applications like face recognition and system automation.

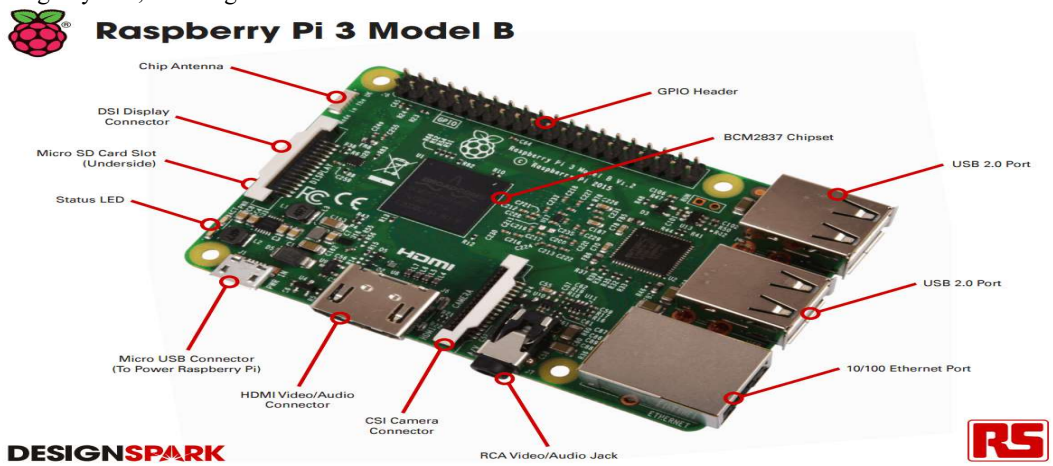


Fig 1: Raspberry Pi 3B

2. Pi Camera Module

The Raspberry Pi Camera Module is used for capturing real-time images of users for face detection and recognition. It connects directly to the Raspberry Pi via the CSI (Camera Serial Interface) port.

The camera supports high-resolution image capture and video recording, which is essential for accurate facial recognition using image processing algorithms.

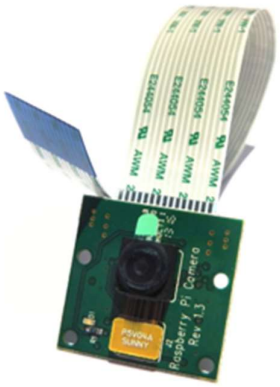


Fig 2: Pi Camera Module

3. 4×3 Matrix Keypad

A 4×3 matrix keypad is used to input the One-Time Password (OTP) for secondary authentication. The keypad consists of rows and columns arranged in a matrix form, allowing efficient detection of key presses.

It enhances system security by adding a second layer of authentication beyond face recognition.

Fig 3: 4×3 Keypad

4. 16×2 LCD Display

The 16x2 LCD Display is used to display system messages such as “Access Granted”, “Enter OTP”, or “Access Denied”. It operates using liquid crystal technology and can display 16 characters per line across two lines.

The LCD reduces user interaction complexity by providing real-time feedback.

Fig 4: LCD Display

5. Solenoid Lock

A solenoid lock is used as the physical locking mechanism. It operates electromagnetically and is controlled by the Raspberry Pi through a driver circuit.
When authentication is successful, the Raspberry Pi sends a signal to activate the solenoid, unlocking the locker.

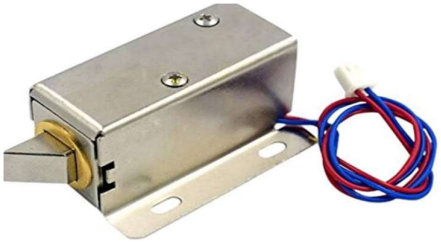


Fig 5: Solenoid Lock Mechanism

6. Buzzer

A buzzer is used as an alert system to indicate unauthorized access attempts or system notifications. It produces sound when triggered and is widely used due to its simplicity and low cost.

Fig 6: Buzzer

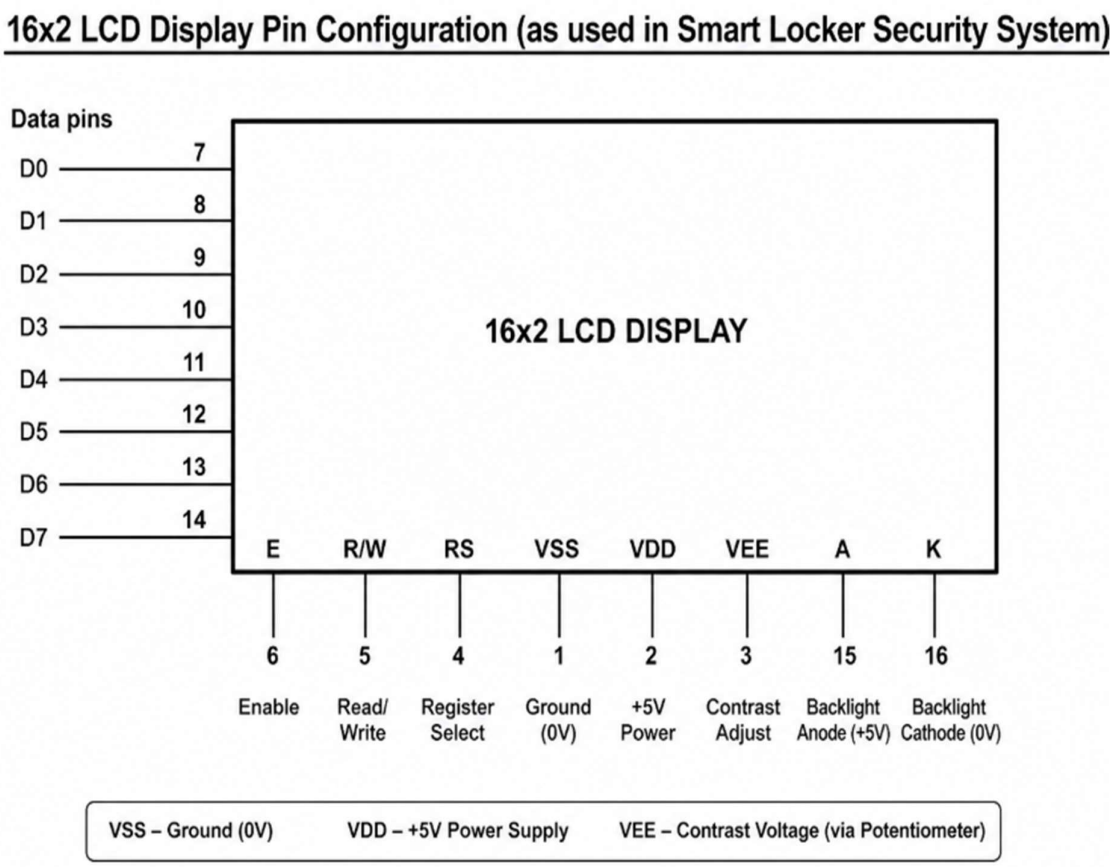
7. Power Supply

A regulated 5V power supply is used to provide stable voltage to the Raspberry Pi and connected components. Proper power management ensures reliable system operation.

Fig 7: Power Supply

Component	Pin No / Symbol	I/O	Description
Raspberry Pi (GPIO)	GPIO2 (SDA)	I/O	I2C data line for LCD communication
	GPIO3 (SCL)	I/O	I2C clock line
	GPIO17	Output	Controls solenoid lock via relay
	GPIO18	Output	Buzzer control signal
	GPIO23	Input	Keypad row input
	GPIO24	Input	Keypad column input
	5V	Power	Power supply for components
	GND	Ground	Common ground connection
16x2 LCD Display	VSS	Input	Ground connection
	VDD	Input	+5V power supply
	V0	Input	Contrast adjustment
	RS	Input	Register select (command/data)
	RW	Input	Read/Write control
	E	Input	Enable signal
	D0–D7	I/O	Data lines
	A (LED+)	Input	Backlight power
	K (LED-)	Input	Backlight ground
Keypad (4x3)	R1–R4	Input	Row connections
	C1–C3	Input	Column connections
Solenoid Lock (Relay)	VCC	Input	Power supply
	GND	Input	Ground
	IN	Input	Control signal from Raspberry Pi
	COM/NO	Output	Switch control for lock mechanism
Buzzer	VCC	Input	Power supply
	GND	Input	Ground
	Signal	Input	Trigger from GPIO
Pi Camera	CSI Port	Input	Connected to Raspberry Pi camera interface

Table: Raspberry Pi System Components and Pin Configuration



IV. Software Implementation

1. Development Environment

The software for the proposed system is implemented using **Python 3.7.5**, which provides a simple and efficient platform for developing real-time applications on the Raspberry Pi 3 Model B. Python is widely used due to its readability, extensive libraries, and ease of integration with hardware components.

The programming is carried out using Thonny IDE, which is a lightweight integrated development environment (IDE) specifically designed for Python and comes pre-installed with the Raspberry Pi operating system.

For image processing, the system utilizes OpenCV, an open-source computer vision library that enables real-time image and video analysis. OpenCV is used to capture live video from the Pi camera and perform face detection and recognition.

2. Face Detection Technique

The system uses the **Haar Cascade algorithm**, a machine learning-based approach for object detection proposed by Paul Viola and Michael Jones. Haar Cascade classifiers are trained using a large number of **positive images** (containing faces) and **negative images** (without faces). In OpenCV, pre-trained models are available as XML files, which are directly used for face detection.

Working Stages of Haar Cascade

1. **Haar Feature Selection** – Identifies relevant features such as edges and lines.
2. **Integral Image Creation** – Converts the image into a representation for fast computation.
3. **AdaBoost Training** – Selects important features and trains the classifier.
4. **Cascade Classification** – Filters out non-face regions quickly and detects faces efficiently.

3. Step-by-Step Software Working

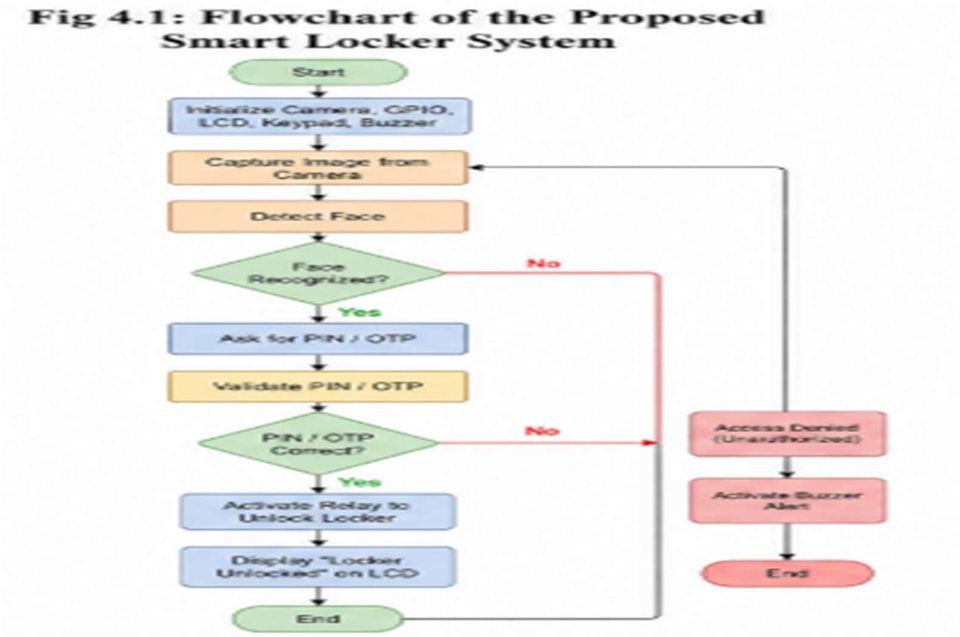
The working of the system follows the sequence shown in the flowchart.

Step 1: Initialization

- Initialize camera, LCD display, and GPIO pins
- Load Haar Cascade XML file
- Start system execution

The system initializes all required hardware components and loads the trained Haar Cascade classifier for face detection.

Fig 4.1: Flowchart of the Proposed Smart Locker System



Step 2: Live Camera View

- Start video stream using Pi camera
- Continuously capture frames

The camera module captures real-time video frames for processing.

Fig 4.2: Live Camera Feed Captured using Raspberry Pi Camera Module

Step 3: Face Detection in Frame

- Convert frame to grayscale
- Apply Haar Cascade detection
- Check for presence of face

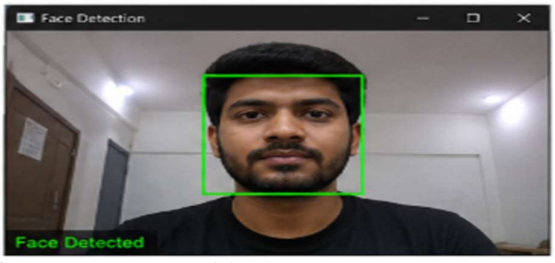
Each frame is processed to detect the presence of a human face within the captured image.

Step 4: Face Highlighting

- If face detected → draw green rectangle

When a face is detected, a bounding box is drawn around the detected region for identification.

Fig 4.3: Face Detection using Haar Cascade Algorithm

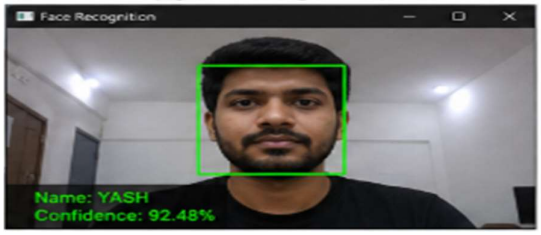


Step 5: Face Recognition

- Compare detected face with stored database
- Check for matching identity

The detected face is compared with stored images in the database to verify the identity of the user.

Fig 4.4: Face Recognition Output (Python + OpenCV)



Step 6: Authentication & PIN Request

- If match found:
  - Prompt user to enter PIN (OTP/password) via keypad

Upon successful face recognition, the system requests a secondary authentication in the form of a PIN.

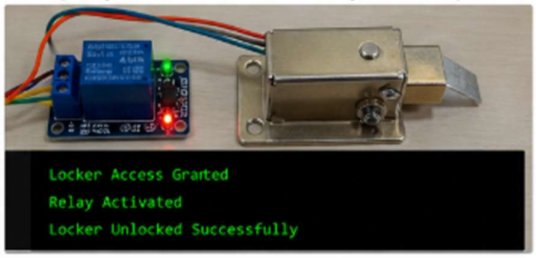
Fig 4.5: PIN/OTP Entry Interface using Keypad and 16x2 LCD Display

Step 7: Access Control

- If PIN correct → unlock solenoid lock
- If incorrect → deny access

The locker is unlocked only when both face recognition and PIN verification are successful.

Fig 4.6: Locker Unlocking Mechanism
(Relay activation controlled via Python GPIO)

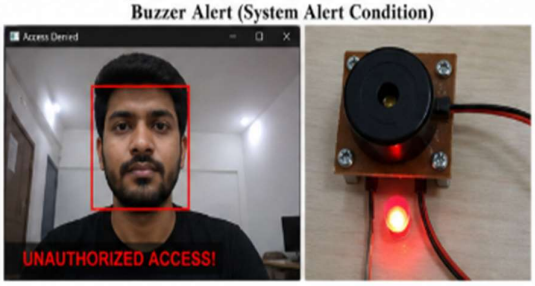


Step 8: Stop / Loop

- After operation:
  - Return to detection mode
  - Continue monitoring

The system continuously monitors for user input and repeats the process.

Fig 4.7: Unauthorized Access Detection and
Buzzer Alert (System Alert Condition)



Circuit Design of the Proposed System

The circuit design of the proposed multipurpose locker security system is centered around the Raspberry Pi 3 Model B, which functions as the main processing unit. All hardware components are interfaced through its GPIO pins to enable real-time monitoring and control.

A Raspberry Pi Camera Module is connected to the CSI interface of the Raspberry Pi to capture live video input. The camera continuously monitors the user and provides frames for face detection and recognition using image processing techniques.

A 4×3 matrix keypad is interfaced with the GPIO pins, where rows and columns are configured as input lines. Once a face is recognized, the system prompts the user to enter a PIN or OTP through the keypad for secondary authentication.

A 16x2 LCD Display is used to display system messages such as “Place Face”, “Face Detected”, “Enter PIN”, “Access Granted”, and “Access Denied”. The LCD is connected using I2C communication through the SDA and SCL pins, reducing wiring complexity.

The locking mechanism is implemented using a solenoid lock controlled via a relay module. The relay input is connected to a GPIO output pin of the Raspberry Pi. Upon successful authentication, the Raspberry Pi activates the relay, which energizes the solenoid lock and opens the locker. If authentication fails, the lock remains in a closed state.

A buzzer is connected to another GPIO output pin and serves as an alert system. It is activated when an unauthorized access attempt is detected, such as an unrecognized face or incorrect PIN entry. Additionally, the system captures and stores the image of the intruder for security monitoring.

The entire system is powered using a regulated power supply to ensure stable and reliable operation. The integration of hardware components with software-based control enables a secure and efficient smart locker system.

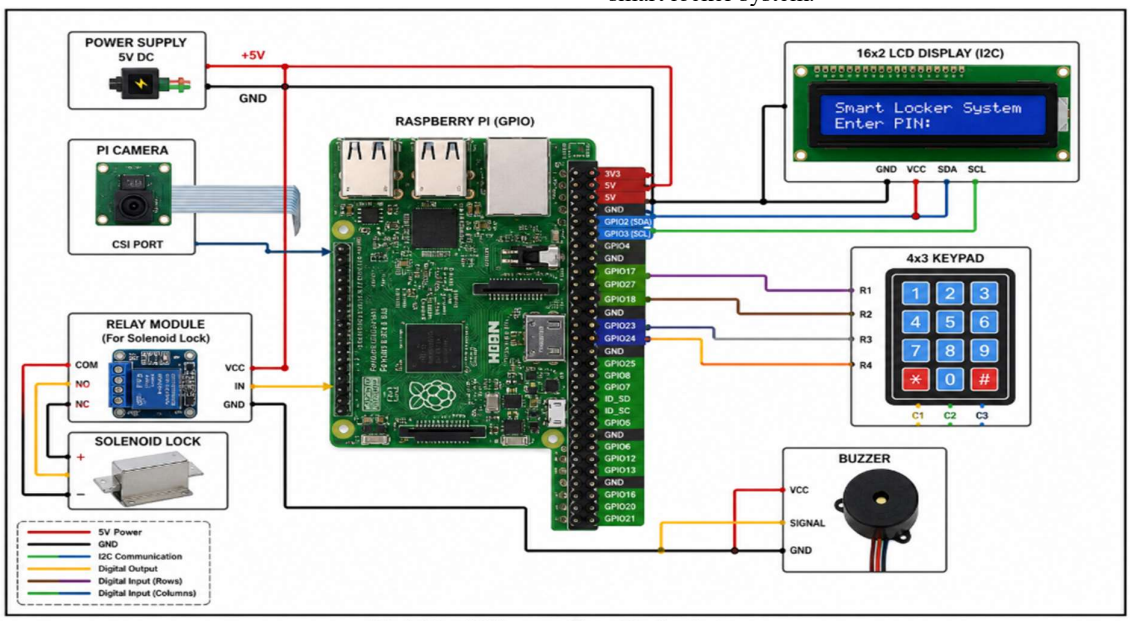


Fig 8: Circuit Diagram of Smart Locker System

The Raspberry Pi acts as the central controller of the system. The Pi Camera is connected through the CSI port for real-time image capture. The keypad is interfaced using GPIO pins to accept OTP input

from the user. The LCD display is connected using I2C or parallel interface to show system status.
The solenoid lock is connected through a relay module or driver circuit, as the Raspberry Pi cannot directly drive high-power devices. When authentication is successful, a signal is sent to the relay, activating the solenoid lock.
The buzzer is connected to a GPIO pin and is triggered during unauthorized access attempts.

V. System Overview

System Breakdown

The proposed system is designed to provide a secure and intelligent locker access mechanism using image processing and IoT-based authentication. Unlike traditional systems that rely only on keys or passwords, this system integrates **face recognition and PIN-based verification** to enhance security.

In this system, the Raspberry Pi 3 Model B acts as the central controller, which processes input from various hardware components and controls the overall operation. The Raspberry Pi Camera Module plays a crucial role by continuously capturing live video frames of the user approaching the locker.
When a user stands in front of the system, the camera captures the image and the system processes it using image processing techniques. The captured face is analyzed and compared with the stored database. If the face is recognized, the system proceeds to the next level of authentication.
Once the face is successfully detected and matched, the system prompts the user to enter a secure PIN or OTP using a keypad. The entered PIN is verified by the controller. If both the face recognition and PIN verification are successful, the system grants access by activating the locking mechanism.

The locking system consists of a solenoid lock controlled via a relay module. Upon successful authentication, the relay is triggered, allowing the locker to open. A 16x2 LCD Display is used to display system messages such as “Place Face”, “Face Detected”, “Enter PIN”, “Access Granted”, and “Access Denied”.
If the system detects an unrecognized face or incorrect PIN entry, access is denied immediately. In such cases, a buzzer is activated to alert unauthorized access attempts, and the system may capture and store the image of the intruder for future reference.

Additionally, the system supports IoT functionality by logging access details such as user identity, time, and access status. These logs can be monitored remotely, improving the overall security and usability of the system.
Figure 1 shows the block diagram of the proposed system. It consists of the Raspberry Pi, camera module, keypad, LCD display, relay module, solenoid lock, and buzzer. The Raspberry Pi processes all inputs and controls the output devices based on authentication results.

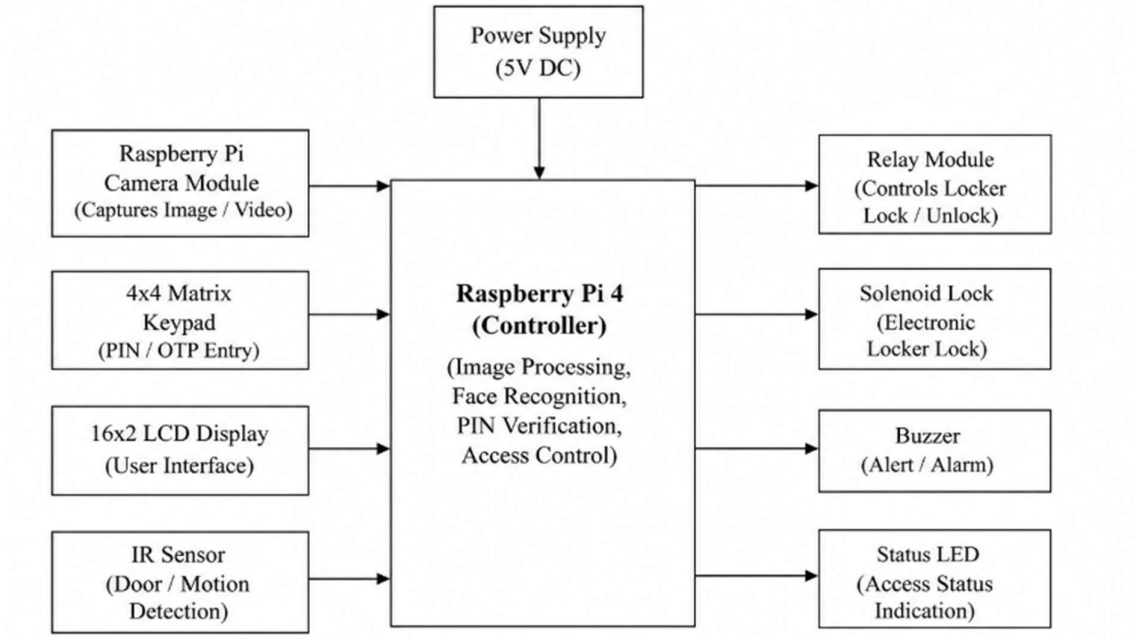


FIG : Block Diagram of Smart Locker Security System

VI. Conclusion

The design and implementation of the proposed **Multipurpose Locker Security System using Image Processing and IoT** has been successfully carried out. The system is developed using the Raspberry Pi 3 Model B as the core controller, integrating both hardware and software components to achieve a secure and efficient locker mechanism.

The proposed system enhances traditional security methods by incorporating **face recognition and PIN-based authentication**, thereby providing a dual-layer security approach. The Raspberry Pi Camera Module enables real-time image capture, and image processing techniques are effectively used to detect and recognize authorized users. The additional PIN verification ensures that even if face recognition passes, unauthorized access is still prevented.

All hardware modules such as the keypad, 16x2 LCD Display, relay-controlled solenoid lock, and buzzer have been carefully integrated and tested. Each component plays a crucial role in ensuring smooth and reliable system operation. The LCD provides real-time feedback to the user, while the buzzer enhances security by alerting in case of unauthorized access attempts.

Furthermore, the integration of IoT capabilities allows the system to log access details such as user identity, time, and authentication status. This feature improves monitoring and provides an additional layer of security through data tracking.

The system has been successfully implemented using modern software tools and image processing libraries, demonstrating reliable performance in real-time conditions. The use of advanced technologies combined with a cost-effective design makes the system suitable for practical applications such as banks, offices, smart homes, and secure storage units.

In conclusion, the project demonstrates an efficient, scalable, and secure locker system that overcomes the limitations of conventional locking mechanisms. With further advancements, the system can be enhanced by incorporating features such as mobile application control, cloud-based monitoring, and improved recognition algorithms for higher accuracy and performance.

References

[1]. Turk, M., & Pentland, A. (1991). Face recognition using eigenfaces. *Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 586–591.

[2]. Viola, P., & Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. *IEEE Conference on Computer Vision and Pattern Recognition*.

[3]. Ahonen, T., Hadid, A., & Pietikäinen, M. (2006). Face description with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28(12), 2037–2041.

[4]. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE*

Transactions on Circuits and Systems for Video Technology, 14(1), 4–20.
[5]. Li, S. Z., & Jain, A. K. (2011). *Handbook of Face Recognition*. Springer.
[6]. Szeliski, R. (2010). *Computer Vision: Algorithms and Applications*. Springer.
[7]. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660.
[8]. Rose, K., Eldridge, S., & Chapin, L. (2015). The Internet of Things: An overview. *Internet Society*.
[9]. Patel, K. K., & Patel, S. M. (2016). Internet of Things-IoT: Definition, characteristics, architecture, enabling technologies. *International Journal of Engineering Science and Computing*.
[10]. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson.
[11]. Bradski, G. (2000). The OpenCV Library. *Dr. Dobb's Journal of Software Tools*.
[12]. Raspberry Pi Foundation. (2020). Raspberry Pi Hardware Documentation.
[13]. Python Software Foundation. (2020). Python Language Reference Manual.
[14]. Banks, A., & Gupta, R. (2014). MQTT Version 3.1.1 Protocol Specification.
[15]. Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks*. Pearson.
[16]. Wachs, J. P., Kölsch, M., Stern, H., & Edan, Y. (2011). Vision-based hand-gesture applications. *Communications of the ACM*, 54(2), 60–71.
[17]. Kumar, D., & Ramesh, S. (2018). IoT based smart security and home automation system. *International Journal of Engineering & Technology*.
[18]. Sharma, P., & Singh, A. (2019). Smart door locking system using face recognition. *International Journal of Scientific Research in Computer Science Engineering*.
[19]. Patel, M., & Shah, R. (2020). Face detection and recognition using OpenCV. *International Journal of Advanced Research in Computer Engineering*.
[20]. Singh, R., & Verma, S. (2021). IoT-based smart surveillance and security system. *International Journal of Computer Applications*.
[21]. Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). Face recognition: A literature survey. *ACM Computing Surveys*, 35(4), 399–458.
[22]. Daugman, J. (2009). How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 21–30.
[23]. Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. *Advances in Neural Information Processing Systems*, 25.
[24]. Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You only look once: Unified, real-time object detection. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*.
[25]. Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University – Computer and Information Sciences*, 30(3), 291–319.
[26]. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164.