IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, June 2026
Impact Factor: 8.2

Development of a Real Time Face Detection and Recognition for Automatic Door Lock System

R. C. Pawar[1], S.A. Harge[2], S. R. Patil[3]
Department of Electronics[1-3]
Smt.Kasturbai Walchand College of Arts and Science, Sangli, Maharashtra
rprutu334@gmail.com[1]

Abstract: *Face recognition systems are revolutionizing everyday access control, from smart homes to secure facilities, yet embedded implementations struggle with real-world variabilities. This study presents a low-cost embedded system for real-time authentication, integrating Python-based computer vision with a PIC18F4550 microcontroller to achieve robust performance under diverse lighting conditions and backgrounds. The core of the recognition process leverages the Python libraries, which are highly effective for facial feature extraction and identity verification, even when challenged by variable lighting and background conditions. The system's methodology involves converting captured facial images into unique numerical templates, which are then rapidly compared against a pre-trained dataset to perform accurate identity verification. The hardware infrastructure, featuring the PIC18F4550 controller, works cohesively to execute the access decision. The experimental results successfully validate the system's effectiveness, demonstrating high recognition consistency with low processing overhead. This work highlights the tangible benefits of integrating high-level vision software (Python) with embedded hardware (PIC microcontroller) to create a practical, scalable, and reliable biometric solution. It provides a strong foundation for future advancements in embedded security systems, including the incorporation of deep-learning models and deployment across diverse applications in security, healthcare, and smart automation.*

Keywords: : Face Recognition, Biometrics, Access Control, Authentication, Embedded Security, Real-Time System

I. INTRODUCTION

Within the rapidly evolving domain of biometric authentication, the human face has undergone a fundamental shift in utility. No longer viewed solely as a passive social identifier, the facial profile is now being leveraged as a sophisticated, high-dimensional digital key. Facial recognition technology has garnered notable attention among various biometric modalities due to its accuracy, reliability, and user-friendly nature [1]. However, what sets facial recognition apart is its sheer versatility. Driven by rapid advancements in machine learning and a global demand for seamless security, it has moved beyond the laboratory to become a fundamental tool in everything from high-stakes cyber investigations to the simple act of unlocking a smartphone. facial recognition emerges as an additional layer of security, ensuring effective authentication and authorization [2].

The system follows a simple three-step process to identify a user. First, the camera takes a live photo. The software then looks at this photo and finds nodal points, which are like fixed landmarks on a person's face. Depending on how the code is written, the system can pick up about 80 of these unique points. Once the system has these measurements, it turns them into a facial signature—essentially a long string of numbers. Instead of comparing a heavy image file, the computer just compares these numbers against its database. This makes the matching process very fast, usually taking less than a second.

Even though this feels like a brand-new smart technology, the basic idea started in the 1960s. A researcher named Woodrow Wilson Bledsoe was the first to try this. He didn't have high-speed cameras, so he used an electronic pen to manually mark coordinates on a person's face.

Even though his tools were basic compared to what we use today, he proved the most important rule of biometrics, you can turn a human face into a math problem. By matching the math from a live face to the math stored in a dataset, we can make sure only authorized people can enter a building or unlock a system. If an abnormal temperature is detected, entry is denied to mitigate health risks and addresses the limitations of traditional access control methods by enhancing both security and safety, offering a comprehensive solution to modern security challenges across various environments [6][7].

Today, facial recognition is used in many different areas, from high-level security to everyday convenience. Because it is fast and does not require physical contact, many industries have adopted it to replace older methods like ID cards or physical keys.

Common Use Cases:

- **Public Safety:** Law enforcement agencies use the technology to help find missing persons, and airports use it at security checkpoints to verify passengers' identities more quickly.
- **Education and Automotive:** Some schools use these systems to ensure the right student is taking an exam, while car manufacturers are starting to replace traditional keys with facial scans to start the engine.
- **Retail:** Some stores use these systems to recognize returning customers and offer a more personalized shopping experience.

II. BLOCK DIAGRAM

In contrast, facial recognition provides a non-invasive, reliable, and efficient method of identity verification, making it particularly well suited for smart door locking systems [3][4][5]. In this system. The fig.1 shows the block diagram of Design of a Cost-Effective Facial Biometrics with Automated Door Actuation System camera sensor capture face image it acts as the primary data source. After processing the image is often converted into the grayscale. Then the mapping phase leads to done feature extraction where the software identifies specific landmarks known as nodal points. which recognizes human face features. The extracted features are converted into a unique mathematical code or a vector.encoding is done by feature extraction which Turns physical traits into data points. then feature matching runs which compares currently available data to the available face database turnout into face identification.

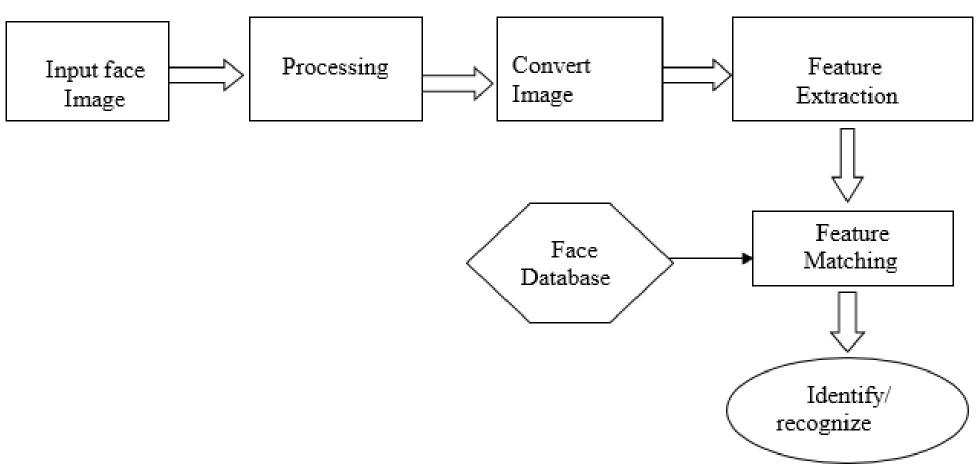


Fig. 1: Block Diagram of Design Facial Biometrics with Automated Door Actuation System.

III. OPERATION OF THE HARDWARE CIRCUIT

Facial recognition is a way of translating human features into language computers actually speak. Since a computer can't see a smile or a jawline the way we do, it breaks a face down into a complex mathematical map. The computer can process that and use the results to compare it with other photos of faces. Then For the matching to be accurate and reap true results, features need to be extracted from an image that makes it unique, so that when compared in the future with other images in the dataset, both images will match only if they share the same features. Formerly, the distances between

key points on a template were taken for such processes; however, that was far from accurate.

Since computers recognize images as matrices where their numbers represent pixel colors, facial recognition focuses are processing such matrices in a way such that faces can be recognized from the way the numbers are organized. Modern approaches have led to passing the digital face image through a series of filters to generate templates that are unique for each face. These filters are used in a form that will produce a distinctive simplified fingerprint for the face being processed.

Facial Recognition Matching Methods: Facial recognition has been approached through various methods over the years. There is two most commonly used methods the first one is holistic matching method and other is hybrid matching method.

The hardware in this setup acts as the eyes and hands of the system, while the computer serves as the brain. Here is how the physical components work together:

1. **Image Acquisition (The Camera)** – The process begins with the USB Webcam. The script initializes the camera and sets a specific resolution (width and height). Once active, the camera continuously captures high-frequency frames. These frames are sent to the computer to be converted into a grayscale format, which makes it easier for the processor to analyze light and shadow patterns on a face.
2. **The Processing Hub (The Computer)** - While not external hardware, the CPU/GPU is doing the heavy lifting here. It uses the LBPH (Local Binary Patterns Histograms) algorithm to take the live feed and compare it against a pre-trained data file stored on the hard drive.
    - The Match: If the computer finds a numerical match with a high enough confidence level, it prepares a command.
    - The Communication: The computer then uses its Serial Port (COM5) to talk to the external controller.
3. **Serial Communication (The Data Bridge)** - The system relies on a serial connection—likely an Arduino or similar microcontroller connected via a USB cable. The script opens a communication line at a speed of 9600 baud.

- When a face is recognized, the computer sends the character 'A' over the wire.
- After a short delay (4 seconds), it sends the character 'B'.

4) Hardware Execution and Actuation Logic: While the core software focuses on data processing, the system is designed to trigger a specific physical response based on the authentication outcome. Although the final hardware—such as an electromagnetic lock or a high-torque motor—can vary depending on the installation, the communication protocol uses simple Serial commands to bridge the gap between the code and the physical world.

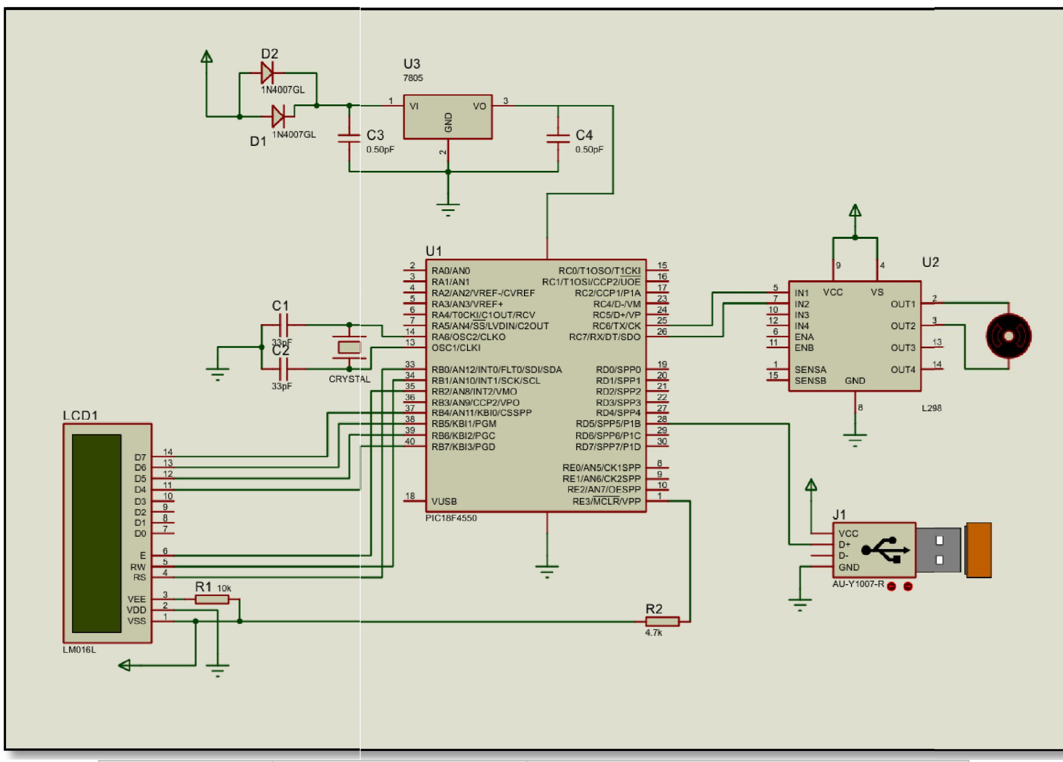
- Activation (Trigger 'A'): Upon successful biometric verification and ID matching, the microcontroller transmits a 'Trigger A' command. In a practical college environment, this would typically activate a relay to unlock a classroom door, illuminate a green status LED, or rotate a servo motor to grant access.
- The Operational Delay: To ensure the student has sufficient time to interact with the hardware (for example, walking through a door), the system is programmed with a 4-second pause. This hold state maintains the physical action without requiring the student to remain at the sensor.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, June 2026
Impact Factor: 8.2

- System Reset (Trigger 'B'): Once the delay concludes, the controller issues a 'Trigger B' command. This serves as a reset signal, returning the hardware to its original secured state—re-locking the door or homing the motor—to prepare the system for the next student in line.

Component	Function
Webcam -	Captures the visual environment and streams raw video data.
Processor -	Runs the LBPH algorithm to identify faces and calculate confidence.
Serial Cable -	Transmits the Unlock (A) and Lock (B) commands to the hardware.
Microcontroller -	Receives the serial characters and toggles GPIO pins to drive a motor or relay.

IV. CIRCUIT DESIGN



Stage	Action	Purpose
Input	Real-time Capture	Gathering raw visual data.
Normalizing	Greyscale/Alignment	Removing noise like color and head tilt.
Encoding	Feature Extraction	Turning physical traits into data points.
Comparison	Database Matching	Finding a numerical twin in the system.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, June 2026
Impact Factor: 8.2

V. DEVELOPMENT OF CODE

```
# Check confidence and display result
        if confidence <= CONFIDENCE_THRESHOLD:</mark>
          name = names.get(str(id), Unknown)
          confidence_text = f{confidence:.1f}%
          print(name)
          ser.write(b'A\r')
          time.sleep(4)
          ser.reset_output_buffer()
          ser.write(b'B\r')
          time.sleep(4)
          ser.reset_output_buffer()
          #x='B'
```

The Python code sends a character (like 'A' or 'B') over USB. On the microcontroller side, specific pins (usually labeled RX for Receive and TX for Transmit) are configured to listen for this data. When the RX pin sees the incoming signal from the face recognition software, the microcontroller's code triggers a pre-programmed response, such as If I receive 'A', unlock the door.

VI. ACTUATOR CONTROL (OUTPUT PORTS):

Once a face is recognized, the microcontroller must move something or switch something on. This is done via Digital Output pins:

1) Relay Triggers:

A pin is set to HIGH (5V) to flip a relay. This relay acts as a high-power switch to engage an Electronic Door Strike or a Magnetic Lock.

2) Servo Motors:

In some systems, a pin uses PWM (Pulse Width Modulation) to precisely rotate a motor that physically moves a latch or pushes a deadbolt.

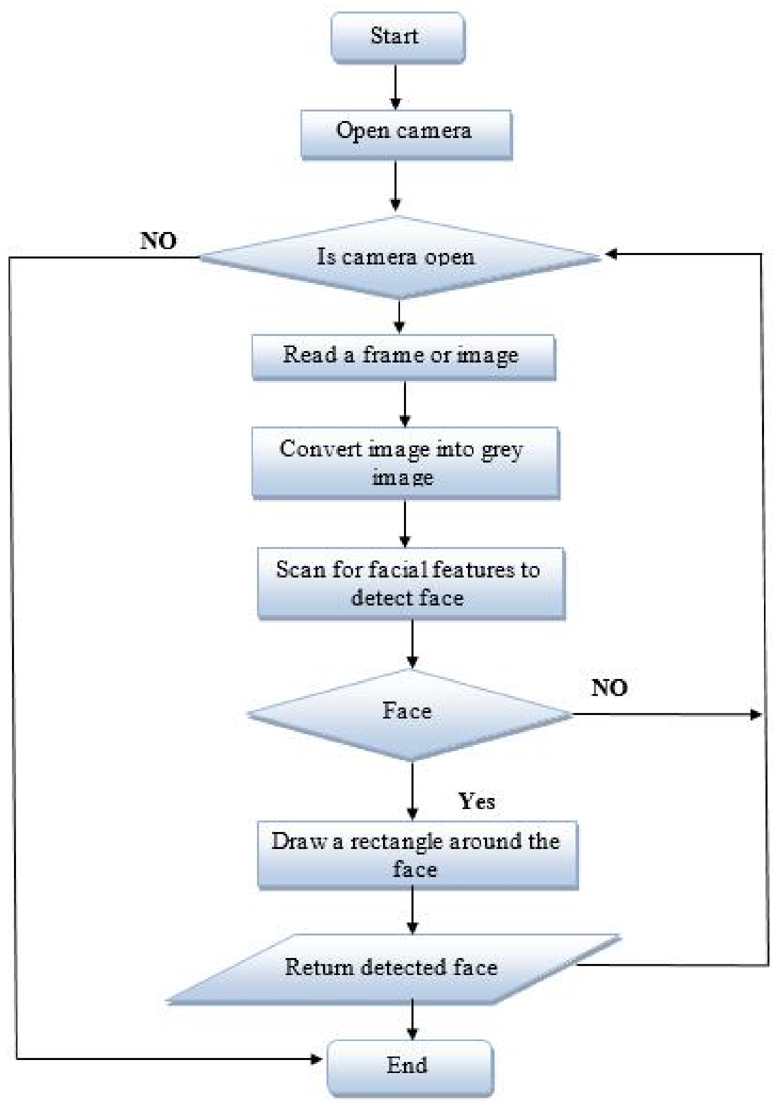
Sensing and Safety (Input Ports)

Component	Pin Type	Direction	Function
Serial/USB	UART (RX/TX)	Input	Receiving Match Found signal from PC
Door Lock	Digital Out	Output	Receiving Match Found signal from PC
Status LEDs	Digital Out	Output	Green/Red light for user feedback
Exit Button	Digital In	Input	Manual override to open door
LCD Screen	I2C/SPI	Output	Manual override to open door

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, June 2026
Impact Factor: 8.2

Microcontroller ports aren't just for sending signals; they also monitor the state of the door or system. An Input Pin can be connected to a sensor on the door frame. This tells the system if the door is actually closed or if it has been propped open too long after a successful face match. A physical Exit button is often connected to an input port so that people can leave the building without needing to scan their faces. Status Displays (I2C/SPI Ports) if the system includes a small screen (like an OLED or LCD) to show Welcome, [Name] or Access Denied, the microcontroller uses specialized communication ports - I2C (SDA/SCL pins): These two pins allow the controller to send complex text and image data to a display using a shared bus, keeping the rest of the pins free for other tasks.

Flowchart



DOI: 10.48175/IJARSCT-36827

VII. CONCLUSION

The evolution of facial recognition from Woodrow Wilson Bledsoe's manual coordinate mapping in the 1960s to today's sophisticated automated systems—underscores its transformative impact on both theoretical research and practical security. While the technology has become a cornerstone of modern law enforcement, airport safety, and human-machine interaction, it remains a field defined by the constant struggle to overcome environmental variables.

This paper has demonstrated that traditional hurdles, such as fluctuating lighting conditions and minor physical alterations like facial hair or makeup, can be mitigated through a more granular analysis of facial structures and edge detection. A significant finding of this study is the effectiveness of zero background extraction. By isolating the facial features entirely from their original environment during the dataset storage phase, the system achieves a level of consistency that is independent of the user's physical location.

Ultimately, while facial recognition remains a polarizing subject due to its broad societal implications, its utility in protecting passengers and locating missing persons is undeniable. Future advancements will likely continue to bridge the gap between holistic and hybrid feature extraction, ensuring that recognition remains accurate even when the real-world environment fails to mirror the controlled conditions of a database. As the technology matures, the focus must remain on refining these algorithms to be as adaptive and resilient as the human eye itself.

REFERENCES

1. Samirul Haque, Biplob Sarker, Atm Rafiqul Mawla, Md Naeem Reza, Aparna Sarker Riya, Development of a Face Recognition Door Lock System with OpenCV Integration for Securing Residential Properties June 2024
2. Rômulo Pedroso Branches, Franciele Pimentel Santarém, Jean Mark Lobo de Oliveira, Pablo Augusto da Paz Elleres Development of a Facial Recognition System Using Python IJAR October 2023, DOI: 10.21474/IJAR01/17735 http://dx.doi.org/10.21474/IJAR01/17735 , 522-526
3. Sayyed Sumaiya Waqar, Shaikh Nofil Nazir, Shaikh Urusa Anwar Husain, Prof. Mohammed Zaid Khan, Smart Home Security: Intelligent Door Locks with Facial Recognition IJPREMS November 2024, Vol. 04, Issue 11,1259-1263 DOI: https://www.doi.org/10.56726/IRJMETS36936
4. Hanaa Mohsin Ahmed, Rana Talib Rasheed, A Raspberry Pi Real-Time Identification System on Facial Recognition, IEEE International Conference on Technology and Electrical Engineering (IT-ELA), 2020.
5. Amritha Nag, Nikhilendra J. N., Mrutyunjay Kalmath, IoT Based Door Access Control Using Face Recognition, IEEE International Conference on Communication and Technology (I2CT), 2018.
6. Puneeth R, Rathna Naik K M, Shashank S Gowda, Shreyas S, Raghavendra Babu T M, Review on Face Authentication for Door Lock System using IOT IJRPR April 2025 , Vol 6, Issue 4, pp 1271-1274, DOI : https://doi.org/10.55248/gengpi.6.0425.1345
7. Sachin Sharma1, Mayank Sharma2, Gopal Sharma3, Akash Bhasney4, IoT-Enabled Smart Door Lock System Using Temperature Sensor (2024).