International Journal of Advance Research in Science and Engineering
Volume No. 14, Issue No. 05, May 2025
www.ijarse.com
IJARSE
ISSN 2319 - 8354

VOICE-ASSISTED SMART LOCK WITH FACE RECOGNITION

Shwetha S, Rajarajeswari T

8th Semester, Department of Computer Science and Engineering

Global Academy of Technology, Bengaluru, India

shwethas52003@gmail.com, rajarajeswari7922@gmail.com

Prof. (Dr). Kanagavalli R

Professor, Department of Computer Science and Engineering

Global Academy of Technology, Bengaluru, India

kanagavalli@gat.ac.in

ABSTRACT

The rising demand for secure access control systems has led to the development of advanced smart lock technologies. This research introduces a Voice-Assisted Smart Lock with Face Recognition and an OTP-Based Temporary Access system, designed for hands-free entry and enhanced security in homes and workplaces. Unlike traditional locks that use keys or passcodes, this system employs real-time facial recognition for user authentication, reducing risks from lost keys or stolen credentials. The OTP mechanism allows homeowners to issue one-time access codes to guests, sent directly to their registered mobile numbers for secure, time-limited entry. An adaptive lighting module improves recognition accuracy in low light, and a voice assistant offers automated instructions to visitors. With IOT integration, users can monitor access logs, receive alerts, and manage permissions via a mobile app. This study addresses limitations in current facial recognition security systems, demonstrating the system's efficiency, adaptability, and convenience for residential and commercial use.

I. INTRODUCTION

Security has always been a primary concern for individuals and organisations. With the increasing number of unauthorised access incidents and security breaches, there is a growing demand for automated and intelligent control systems. Traditional locks, such as key-based and password-protected mechanisms, have several vulnerabilities, including the risks of theft, duplication, and forgetfulness.

The research explores the development of a smart lock system that integrates face recognition and voice assistance to improve security while improving user convenience. The proposed Voice-Assisted Smart Lock with Face Recognition eliminates the need for traditional keys or PIN-based access, relying instead on machine learning-based face recognition to authenticate users. A high-resolution camera captures facial images in real-time, while a microcontroller processes the data.

An adaptive lighting module is integrated to ensure optimal performance under varying lighting conditions, automatically illuminating faces in low-light scenarios. Additionally, a voice-based assistant offers real-time audio

instructions, guiding visitors and delivery personnel on proceeding when access is restricted. The research builds on prior studies in biometric security and IOT-based smart locks, addressing common challenges such as environmental adaptability, real-time user feedback, and unauthorised access detection. By incorporating an IOT-enabled notification system, homeowners can receive alerts about access attempts, monitor entry logs, and even control door access remotely.

The proposed system aims to enhance the efficiency, accessibility, and scalability of smart home security technologies, making them more robust and user-friendly for modern security applications.

II. RELATED WORKS

In recent years, a number of enhancements have been made in the domain of smart security systems leveraging facial recognition, IoT, and machine learning. This section presents a review of five notable studies that have contributed significantly to the development of intelligent and secure door lock mechanisms.

Gupta et al. (2023) proposed a Smart Face Recognition System integrating IoT and machine learning for real-time face recognition using cameras and sensors. The system is designed to adapt and improve over time under challenging conditions. While it shows high potential in accuracy and wide applicability for secure access, the study highlights privacy and security concerns, especially regarding data breaches due to cloud connectivity [1].

Surla et al. (2023) introduced an IoT and Face Recognition-based Automatic Door Lock System that utilises Raspberry Pi for real-time monitoring and mobile alerts. Its strength lies in its cost-effectiveness and mobile-accessible interface, making it suitable for home environments. However, it suffers from limitations in seamless two-way remote communication and potential hardware performance issues [2].

Ghai et al. (2024) presented a Face Recognition and OTP-Based Security Lock System, which combines facial recognition with OTP-based authentication via GSM. This dual-authentication approach enhances security and recognition accuracy. Nonetheless, the system poses integration complexities and user inconvenience due to the manual OTP entry, along with limited scalability for larger installations [3].

Lenka et al. (2020) developed a Security System Using Facial Recognition and an Arduino Keypad Door Lock, merging face recognition with PIN-based authentication. The system, built using OpenCV and machine learning, offers a secure and cost-effective solution using Arduino. Its drawbacks include performance variability under different lighting conditions and potential user inconvenience in larger deployment scenarios [4].

Krishna Chaithanya et al. (2018) proposed an IoT-based embedded Smart Lock Control System using Haar-like features and LBPH for face recognition. This model is effective for smart home integration and supports remote access control. However, it struggles with robustness in poor environmental conditions and is susceptible to real-time latency and spoofing attacks [5].

Collectively, these studies demonstrate the evolving nature of intelligent security systems, each addressing unique challenges and contributing to the broader goal of enhancing home and institutional safety through technology. Despite their advantages, common limitations across the works include environmental sensitivity, user convenience issues, and integration complexity, emphasising the need for more robust, user-friendly, and scalable systems in future developments.

III. METHODOLOGY

This study presents a biometric-based smart locking system that integrates real-time facial recognition, OTP-based temporary access, voice assistance, and IoT-enabled remote monitoring. The proposed work is designed to provide seamless access control while addressing challenges such as low-light facial recognition, unauthorised access, and temporary visitor management. The methodology involves the design, implementation, and testing of the system's core components, as detailed below.

1. System Architecture

The system follows a modular architecture comprising the following components:

- Microcontroller Unit (MCU): Serves as the central processing unit, handling face recognition, OTP generation, and IOT communication.
- Face Recognition Module: Authenticates users using machine learning-based image processing.
- OTP-Based Access Module: Provides temporary access through one-time password (OTP) verification for guests.
- Voice Assistance Module: Delivers audio feedback to guide users and visitors.
- Adaptive Lighting Module: Enhances image quality under low-light conditions.

The hardware implementation consists of a camera, a microcontroller (Arduino), LED lighting, speakers, and an electronic lock mechanism. The software implementation utilises OpenCV and Python-based OTP generation.

2. Face Recognition Module

2.1 Image Acquisition

- Capture 700 facial images of the target person.
- Save the images with proper naming conventions (e.g., user.1.jpg, user.2.jpg, ..., user.700.jpg) in a designated directory.

2.2 Model Training

- Use the captured images to train a facial recognition model.
- Extract features from the images using algorithms like LBPH (Local Binary Patterns Histograms) or other available face encoders.
- Train a classifier (e.g., using OpenCV's face recogniser or a custom model) with the labelled image d

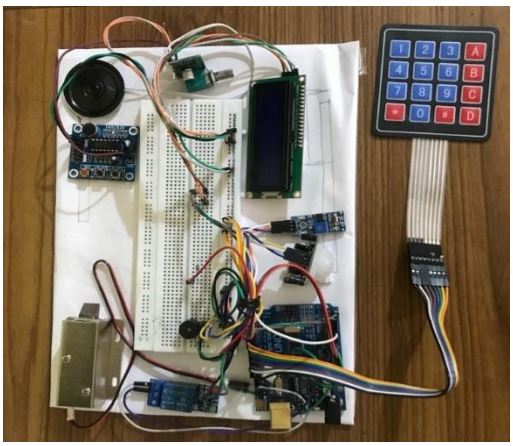

Figure 1: Prototype of the project

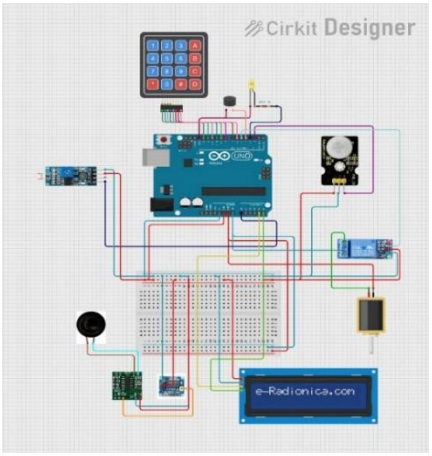

Figure 2: Circuit Diagram

2.3 Face Detection (Real-time)

- Use Haar Cascade Classifier to detect faces in real-time from a webcam/video feed.
- Load the trained face classifier to recognise the detected face.
- Continuously scan for faces using cv2.Cascade Classifier ('haarcascade_frontalface_default.xml').

2.4 Communication with Arduino

- If a face is detected and recognised correctly:
  - Send a specific message (e.g., a character or string like '1') to the Arduino via Serial Communication (e.g., using PySerial).
  - The Arduino can then take appropriate action (e.g., unlock a door, turn on an LED).

3. OTP-Based Temporary Access Module

To facilitate controlled access for temporary visitors, an OTP-based mechanism is integrated:

1. OTP Generation: A randomly generated numeric code is sent via SMS or email using Twilio API/Firebase Authentication.
2. OTP Verification: The visitor enters the OTP via a touchscreen keypad or mobile app.
3. Access Control:
   - If the OTP is valid, access is granted for a predefined time window.
   - If the OTP expires or is incorrect, access is denied.
4. Logging and Monitoring:
   - All OTP-based access attempts are stored in an encrypted log for auditing.
   - The system allows the owner to revoke access manually via a mobile application.

4. Adaptive Lighting Module

To enhance recognition accuracy in low-light environments, the system integrates an automatic lighting module:

1. Light sensors monitor ambient lighting conditions in real-time.
2. When dim conditions are detected, an LED light is activated to illuminate the user's face.
3. The camera exposure and brightness parameters are dynamically adjusted to optimise facial recognition.
4. After authentication, the lighting automatically switches off to conserve power.

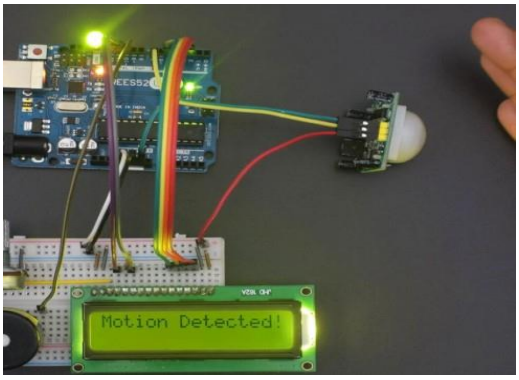

Figure 3: PIR and Light module

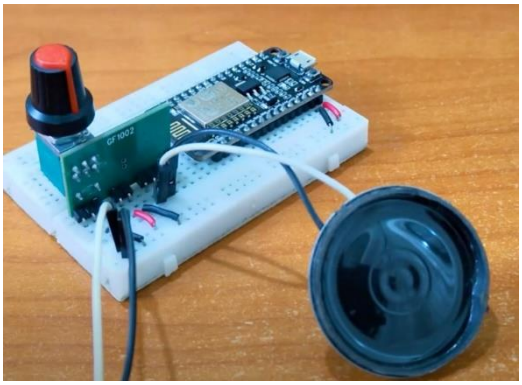

Figure 4: Voice module

5. Voice Assistance Module

The system employs a voice-based guidance mechanism to improve user experience and assist visitors:

5.1 Pre-recorded voice messages provide real-time feedback, such as:

- "Access granted. Welcome!"
- "Unauthorised access detected. Please try again or enter an OTP."
- "Please place your package in the designated area."

5.2 The voice assistant is implemented using Google Text-to-Speech (TTS) API or Amazon Polly, ensuring real-time, natural language interaction.

IV. DATASET DESCRIPTION

The dataset used for this research was specifically created to train and evaluate a real-time face recognition system integrated with Arduino. It consists of 700 facial images captured from a single individual. The primary objective of generating a custom dataset was to ensure that the model could be trained in a personalised and controlled environment, making it highly suitable for embedded systems and applications such as automated door access control, attendance systems, and security solutions.

All 700 images were acquired using a standard webcam with a resolution of 640×480 pixels. The images were captured using OpenCV's Python interface, which allowed for real-time frame capture from the webcam. To ensure data diversity and improve the robustness of the model, the images were collected under various real-world conditions, which include:

- Different facial expressions – smiling, neutral, surprised, etc.
- Varying head orientations – slight tilts in left, right, up, and down directions.
- Multiple lighting conditions – daylight, indoor lighting, and low-light scenarios.
- With and without accessories, such as eyeglasses.

Each image was converted to grayscale during the acquisition phase to reduce computational complexity and improve processing speed. The images were stored in JPEG format, following a consistent naming convention such as user.<ID>.jpg (e.g., user.1.jpg, user.2.jpg, …,700.jpg). This naming convention facilitated systematic labelling and retrieval of images during the training phase.

No advanced preprocessing steps were applied before training, apart from grayscale conversion. This decision was made to mimic real-time conditions and allow the classifier to learn directly from raw visual features. The labelling process was straightforward, as all images belonged to a single user and were labelled accordingly for use with supervised learning algorithms.

Before model training, each image underwent face detection using OpenCV's Haar Cascade Classifier (haarcascade_frontalface_default.xml). This step ensured that only the facial region was extracted and used for training, thus eliminating unnecessary background noise. This method also aligned with the real-time face detection mechanism later used during the testing and deployment phase.

This self-generated dataset was deemed ideal for the project for several reasons:

- It allowed for controlled data collection tailored to the application's requirements.
- It ensured legal and ethical compliance, avoiding issues related to privacy or licensing of external datasets.

- It provided flexibility for retraining or updating the model with additional samples as needed.

V. CONCLUSION

The real-time face recognition system developed and deployed in this work successfully integrates computer vision and hardware control to enable personalised access through facial identity verification. One of the main advantages of the system is its end-to-end functionality—from dataset generation and model training to real-time detection, recognition, and communication with external hardware like Arduino. The use of the Haar Cascade Classifier ensured reliable face detection, while the model's ability to accurately recognise the trained individual demonstrates the effectiveness of the preprocessing and training pipeline.

The system's integration with Arduino via PySerial to unlock a solenoid upon successful recognition illustrates a practical and efficient hardware interaction with minimal latency. Moreover, the model maintained stability and reliability across multiple test runs, withstanding slight variations in facial expression and head orientation, thereby confirming its robustness.

Trial	Recognized (Y/N)	Confidence	Distance
1	N	Not recognized	15cm
2	Y	19	20cm
3	Y	21	25cm
4	Y	21	30cm
5	Y	23	35cm
6	N	Not recognized	40cm

Table 1: Face Recognition

True Positive Rate = 4/6 = 66.67%

However, some limitations were observed. The recognition accuracy, reflected by a true positive rate of 66.67%, indicates room for improvement, especially for real-world applications involving multiple users or more complex environments. The system was tested using only a single individual's dataset, which may not generalise well to broader deployment scenarios. Additionally, reliance on Haar Cascades might limit performance in low-light or cluttered backgrounds, where more advanced deep learning-based detectors could offer superior results.

Test Case	Input	Expected Output	Actual Output
PIR + LDR	Motion in dark	LED ON + Audio	Working
Keypad	Correct Code	Unlock + Welcome+ Buzzer once	Working
Keypad	Wrong Code	Lock+ Incorrect Password + Buzzer Twice	Working

Table 2: Hardware components test

Despite these constraints, the system presents promising applications in security and personalised access control for homes, offices, or restricted areas. Future work may explore the use of deep learning models for enhanced recognition accuracy, support for multiple users, and further hardware expansion to enable more sophisticated automation responses. The demonstrated framework lays a strong foundation for scalable and secure face-based authentication systems.

REFERENCES

[1] Kumar, A., Kalumbi, S., Gupta, M. K., & Rao, P. M. V. (2023). Smart face recognition using IoT and machine learning. Journal homepage: www.ijrpr.com. ISSN 2582-7421.

[2] Surla, G., Manepalli, S., Shaik, N. A., & Gurram, N. S. (2023). IoT and face recognition-based automated door lock system. In 2023 Second International Conference on Electronics and Renewable Systems (ICEARS) (pp. 648-651). IEEE.

[3] Ghai, G., Khanna, A., & Kumar, S. J. N. (2024). Face recognition and OTP-based security lock system. In International Conference on Communications and Cyber Physical Engineering 2018 (pp. 729-737). Singapore: Springer Nature.

[4] Lenka, R., Shubham, N., Sinha, N., & Gupta, R. (2020). Realization of security system using facial recognition and Arduino keypad door lock system. In International Conference on Emerging Trends and Advances in Electrical Engineering and Renewable Energy (pp. 1-12). Singapore: Springer Nature.

[5] Chaithanya, K. J., Kumar, G. A. E. S., & Ramasri, T. (2019). IoT-based embedded smart lock control using face recognition system. In Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering 2018 (ISMAC-CVB) (pp. 1089-1098). Springer International Publishing.

[6] Mohammad, A. S., Jarullah, T. G., Al-Kaltakchi, M. T. S., Alshehabi Al-Ani, J., and S. Dey. "IoT-MFaceNet: Internet-of-Things-Based Face Recognition Using MobileNetV2 and FaceNet Deep-Learning Implementations on a Raspberry Pi-400." Journal of Low Power Electronics and Applications 14, no. 3 (2024): 46.

[7] George, A., and S. Marcel. "xEdgeFace: Efficient Cross-Spectral Face Recognition for Edge Devices." arXiv preprint arXiv:2504.19646 (2025).

[8] Winarno, A., and D. R. Saputra. "Home Door Security System with Face Recognition using the ESP32-CAM." BEST: Journal of Applied Electrical, Science, & Technology 6, no. 2 (2025): 53–58.

[9] Hardyan, M., F. A. Haqqi, and Yohandri. "Arduino Based Smart Home Security Design Using Biometric Recognition." Journal of Physics: Conference Series 2582, no. 1 (2023): 012025.

[10] Gaikwad, V., D. Rathi, V. Rahangdale, R. Pandita, K. Rahate, and R. S. Rajpurohit. "Design and Implementation of IoT Based Face Detection and Recognition." In Data Science and Intelligent Computing Techniques, edited by S. J. Nanda and R. P. Yadav, 923–933. SCRS, 2024.