SPECTRUM OF ENGINEERING SCIENCES
ISSN (E) 3007-3138 (P) 3007-312X VOLUME 4, ISSUE 6, 2026

AN IOT-BASED FACE RECOGNITION SMART DOOR ACCESS CONTROL SYSTEM WITH REAL-TIME SECURITY ANALYSIS AND PERFORMANCE OPTIMIZATION

Shairbaz Ali[*1], Muhammad Naeem Nazeer[2], Sajid Rehman[3], Mustafa Ali Hakeemi[4], Syed Ali Raza Naqvi[5], Sami Ullah[6], Muhammad Jawad Ahmad[7]

[*1,2,3,4,5,6,7]*Department of Information and Communication Engineering (Intelligent Systems and Robotics), The Islamia University of Bahawalpur, Pakistan*

[*1]shairbazali8@gmail.com, [2]nomikhanbaloch05@gmail.com, [3]sajidafghan637@gmail.com, [4]mustafahakeemi799@gmail.com, [5]syedalirazanaqvi443@gmail.com, [6]sammiullah6111@gmail.com, [7]hafizjawad3311@gmail.com

DOI: https://doi.org/10.5281/zenodo.20807621

Keywords
Face Recognition, Smart Door System, Internet of Things (IoT), Arduino, Firebase, Liveness Detection, Access Control, Computer Vision.

Article History
Received: 24 April 2026
Accepted: 03 June 2026
Published: 23 June 2026

Corresponding Author: *
Shairbaz Ali

Abstract
Smart door access control systems are becoming more significant in modern homes and enterprises as the need for better security, automation, and remote monitoring increases. Older locks have issues with lost keys, keys that have been copied, and unlawful entry. This study provides an IoT-based facial recognition smart door access control system that mixes computer vision, integrated hardware, and cloud technologies for safe and automatic authentication. The suggested system is composed of a vision pipeline that includes face detection, face alignment, feature encoding, face matching, and decision making to identify authorized users in real time. Upon successful authentication, an Arduino-controlled servo motor opens the door, a welcome message is shown on an I2C LCD, and the event is logged in a Firebase cloud database. To enhance security, a liveness detection technique based on eye-blink verification is integrated to limit the danger of spoofing attacks utilizing static facial photos. We performed an experimental assessment, and the results indicate that the system is capable of dependable real-time authentication with minimal processing latency and excellent cloud-based monitoring. The suggested system is a low-cost, safe, and scalable strategy for smart access control applications in home and corporate contexts.

INTRODUCTION

In recent years, smart home technologies have received much attention due to the increasing demand for security, automation, and remote monitoring. Traditional lock and key systems provide minimal security and are susceptible to unauthorized access, key duplication, and physical tampering. The increasing prevalence of Internet of Things (IoT), computer vision, and embedded systems makes intelligent access control solutions more realistic and reliable. Smart door systems can automatically identify visitors, control door access, and digitally log entry events. This paper proposes an IoT-based smart door access control system that incorporates face recognition, Arduino-based door control, and cloud-based event logging. This would provide a secure and convenient solution for modern homes and offices [1].

Face detection is a basic problem in computer vision. Finding and identifying human faces in an image or video stream. This is the first step in many biometric and surveillance applications. The technology of face detection is widely applied in security monitoring systems, attendance management, authentication of mobile devices, human-computer interaction, surveillance cameras, and smart home automation. A real-time face detection system can make use of its processing resources to focus on the relevant regions of interest, thus increasing efficiency and performance. The proposed smart door system uses face detection to monitor the entrance area continuously to detect if a visitor is present before proceeding to further recognition processes [2].

Face recognition, a biometric identification method, is used to identify. The identity of a person is determined by unique facial features. Unlike face detection, which only determines whether a face exists or not, face recognition compares the extracted facial features with the stored face templates for the decision whether a person is authorized or not. Modern face recognition systems obtain high recognition accuracy by employing feature encoding and distance-based matching methods [3]. Face recognition has become more popular for applications such as access control, airport security, banking systems, smartphone authentication, and law enforcement. In this research, facial embeddings are extracted from detected faces and compared with stored embeddings by using a Euclidean distance metric. When it finds a match within a certain threshold, the system opens the door and displays user information on an LCD screen, and logs the event in a Firebase cloud database.

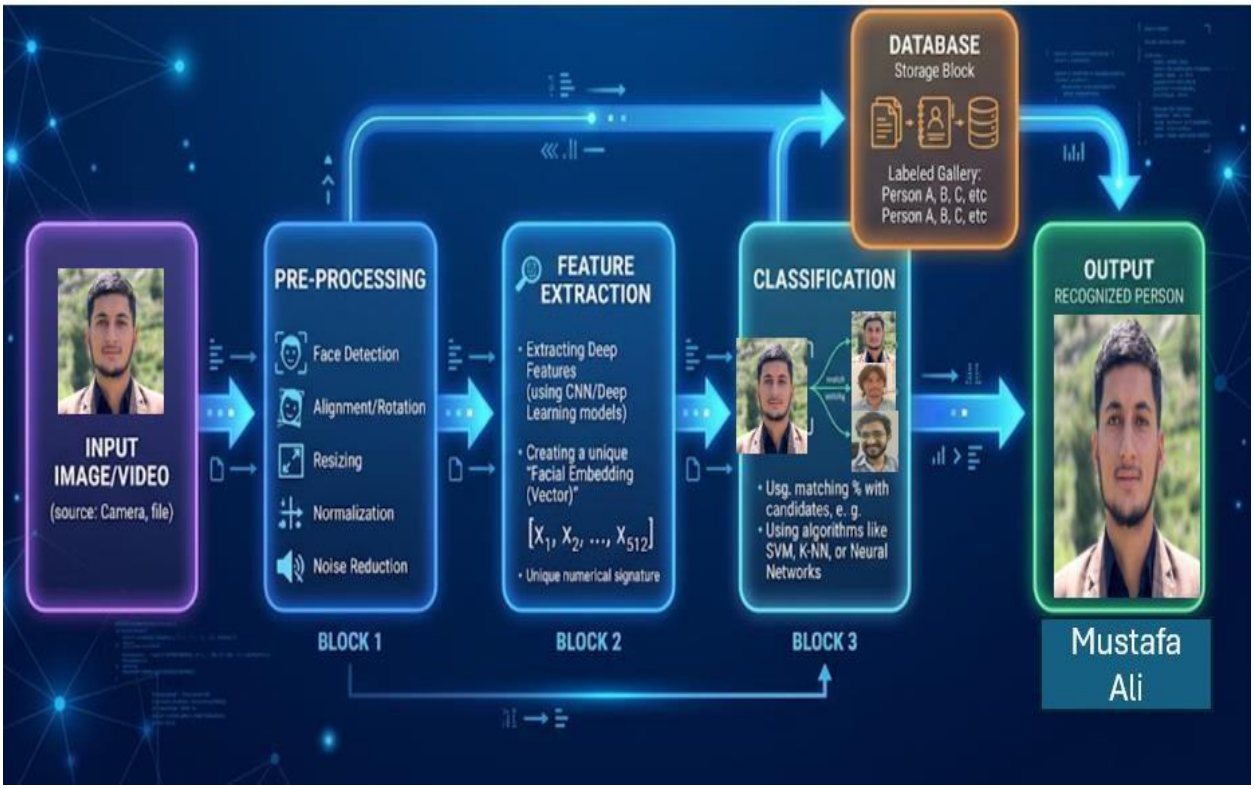

Fig 1. Conventional face recognition Process

The first step includes Pre-processing (Block 1), which detects, aligns, and normalizes a raw input face for standard comparison. Then, in Feature Extraction (Block 2), deep learning algorithms create a unique numerical signature or "facial embedding" of the person. In the Classification

process (Block 3), this signature is compared against a labeled gallery in a database to a human match. Finally, the system provides an Output. It shows the name of the matching individual (Mustafa Ali) and a photo.

RELATED WORK

Several previous studies have built IoT-enabled smart door systems based on RFID, Bluetooth, and cloud-based monitoring for better home security. But those systems depend on physical tokens or passwords that may be lost or hacked [4] [5]. The non-contact nature and high recognition accuracy of face recognition have made it a reliable biometric authentication technique. Some researchers have used facial embeddings and distance-based matching techniques for secure access control applications [6]. While face recognition systems provide a convenient method of authentication, they are still susceptible to presentation attacks such as printed photographs and mobile screen replays. Researchers proposed techniques for blink detection and motion verification to improve the robustness of the system [7] [8]. For real-time deployments of face recognition systems, the optimization of latency with frame reduction, region-of-interest processing, and efficient feature extraction techniques is required [9].

METHODOLOGY

A: System Architecture

The proposed system is an IoT-based smart door access control system that integrates face recognition, embedded hardware, and cloud-based logging to provide secure and automated access control. The system includes a camera for image acquisition, a face recognition module built in Python and OpenCV, an Arduino microcontroller to control the hardware, a servo motor to operate the door, an I2C LCD to display the user information, LED indicators to indicate access status, and a Firebase cloud database for event logging. If a user comes in front of the camera, the system will take the picture, detect the face, do the recognition, and check if the user is authorized. If the user is recognized, then an access granted command is sent to the Arduino. This command rotates the servo motor to unlock the door, activates the green LED, and displays a welcome message on the LCD.

Else access is denied, and a red LED is illuminated. All access events are logged into Firebase for record-keeping and remote monitoring.

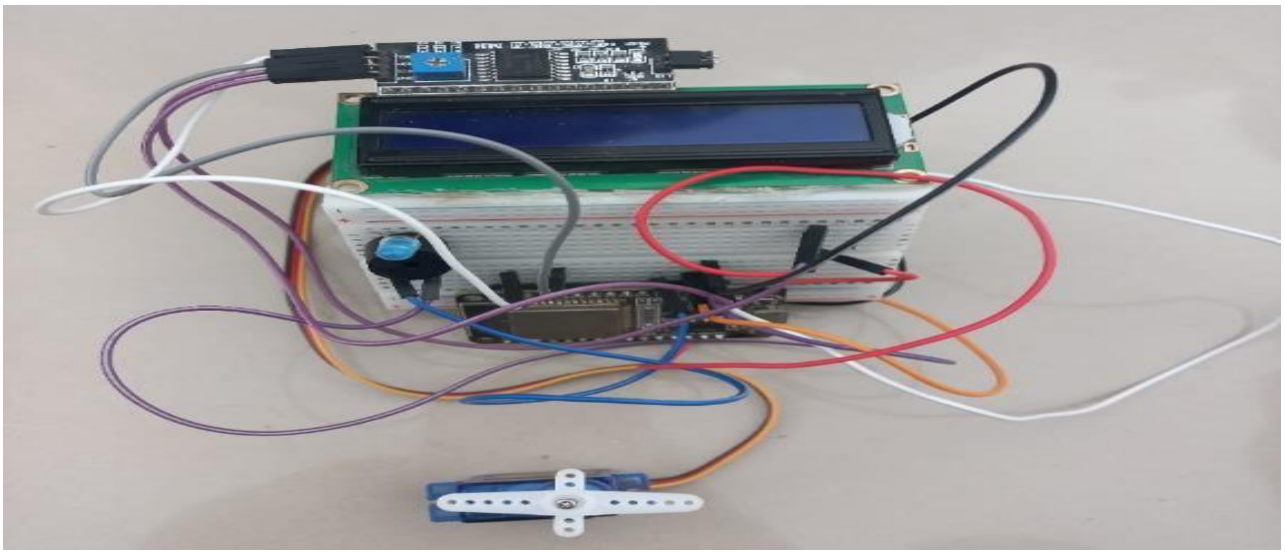

Fig 2. Overall architecture of the proposed IoT-based face recognition smart door access control system

B. Dataset Collection

For the training and evaluation of the proposed system, a custom facial image dataset was created. The dataset consists of facial images of three authorized individuals. In the data collection, to improve the recognition performance in real-world scenarios, we considered multiple variations of facial images by capturing images under different lighting conditions, facial expressions, and head orientations. Each participant supplied approximately 12-17 images, yielding a dataset with enough variability for dependable recognition.

Fig 3. Face images collected from authorized users

C. Vision Pipeline

The face recognition process is done in a series of stages, called the vision pipeline. This pipeline converts the raw camera image to an access control decision.

Face Detection

Face detection is the first step of the pipeline. The camera takes frames continuously, and those frames are processed to find human faces. The detection module detects the coordinates of facial areas and extracts the corresponding face from the image. This step is used to reduce the unnecessary processing by focusing only on the detected face regions.

Face Alignment

Face detection is followed by face alignment to standardize the location and orientation of the recognized face. The alignment reduces the variances caused by head rotation and slight changes of position, and so improves the identification performance. Then the aligned face picture is fed to the feature extraction step.

Feature Encoding

Feature encoding transforms the aligned facial image into a numerical feature vector (facial embedding). Each face is represented by a high-dimensional feature vector that captures its unique facial characteristics. The generated embedding is a compact representation of the person's identity and is used for comparison to stored embeddings [10].

Face Matching

The face matching is done by matching the embedding of the detected face with the embedding in the database of authorized users. For similarity calculation, we use the Euclidean distance metric between two embeddings.

Distance calculated as:

$$d = || f\_input - f\_stored ||$$

where f_input is the embedding of the detected face and f_stored is the embedding of an authorized user stored. The smaller the gap, the more similar the two faces are.

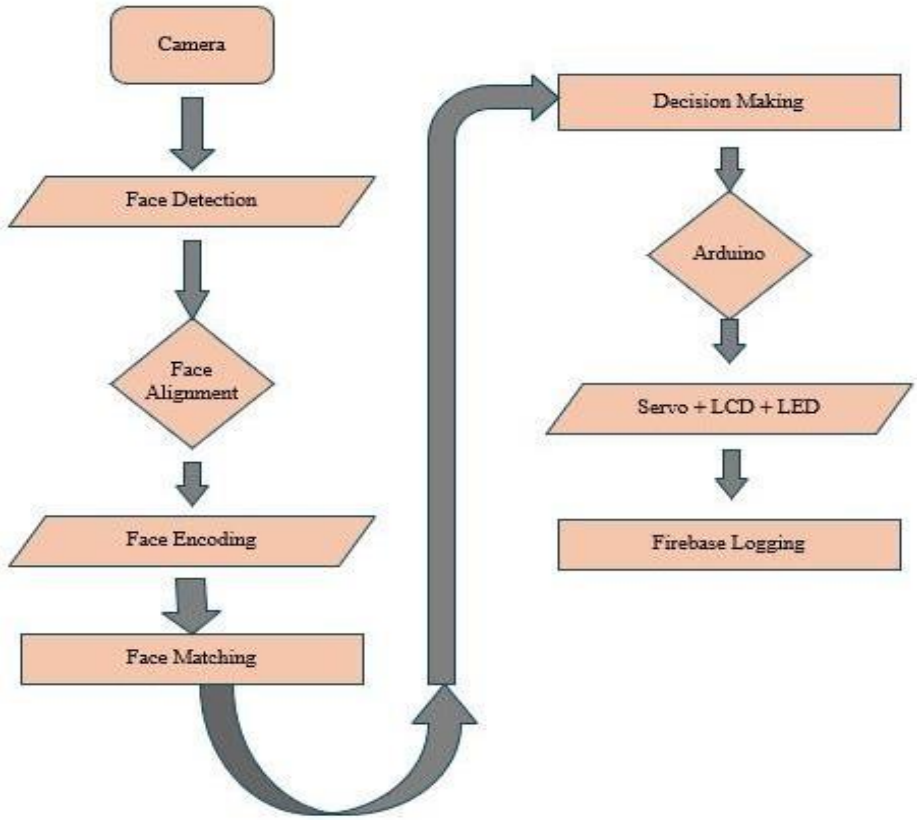

Fig 4. Flow diagram of Vision-based face recognition and access control pipeline

D. Hardware Integration

The hardware subsystem is responsible for conducting physical access control actions after the decision on recognition has been taken.

ESP32 Microcontroller

An ESP32 microcontroller connects the facial recognition software to the door entry hardware. The computer delivers the information to the Arduino via serial connection. The recognition program, based on the recognition result, delivers command strings such as OPEN and DENY.

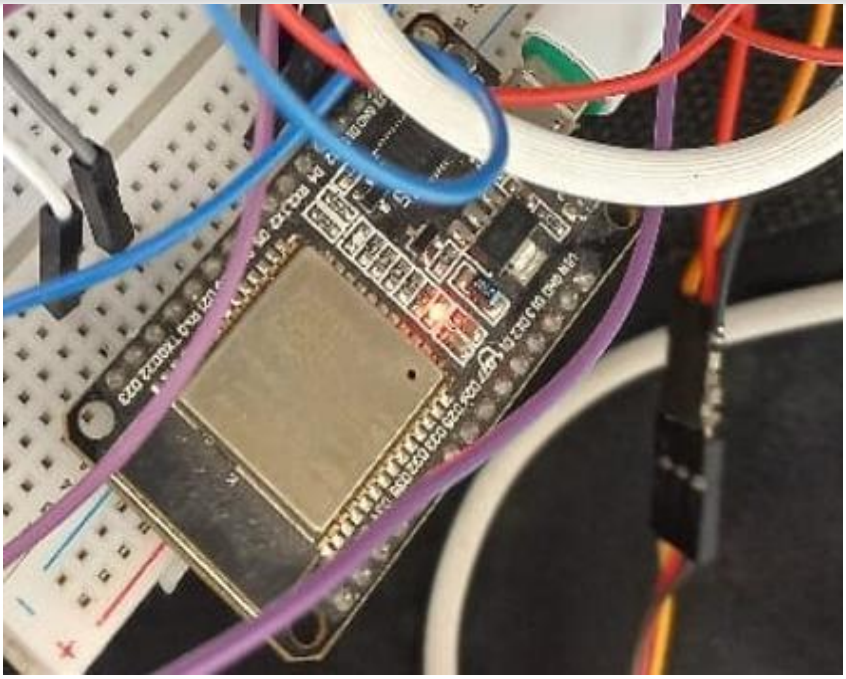

Fig 5. ESP32 Microcontroller used for system control and communication

Servo Motor Control

The servo motor is used to simulate the door locking mechanism. If recognition is successful, the ESP32 receives the signal "OPEN" and the servo motor is rotated 90 degrees to open the door. Then, after some amount of time, the servo goes back to where it started, unlocking it.

Fig 6. Servo Motor used for locking and unlocking mechanism

LCD User Interface

An I2C LCD module provides visual feedback to the user. When access is granted, the LCDs the recognized person's name along with a welcome message. If access is denied, a proper warning message is displayed.

Fig 7. I2C LCD showing access status and user identification messages.

Firebase Cloud Logging

All access records are stored on a Firebase cloud database for remote monitoring and event management [11]. Each record includes the user name, access status, date, and time. A typical Firebase entry contains information like:

username
Access Status (Approved or Denied)
Time and date

This logging mechanism is cloud-based, so administrators can monitor access events remotely and keep a permanent record of system activity.

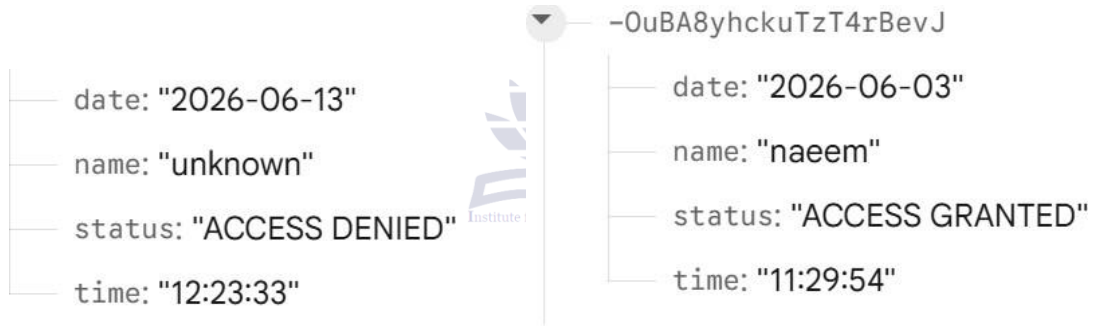

Fig 8. Firebase-based cloud logging of user access records.

E. Performance Evaluation Methodology

The effectiveness of the proposed system has been evaluated by measuring several performance metrics. The recognition accuracy was computed using the test images from authorized users. We measured the latency of each stage in the vision pipeline, face detection, alignment, encoding, matching, and decision. System throughput was measured in frames per second (FPS). Optimization techniques like reducing image resolution, frame skipping, and region of interest processing were applied to improve real-time performance. In addition, the robustness test was also performed in various lighting conditions, background clutter, and multi-user scenarios to evaluate the reliability of the system in real deployment environment.

Table 1. Latency Analysis of the Face Recognition Pipeline

Processing stage	Latency (ms)	Percentage of Total (%)
Face detection	120	50.0
Face Alignment	25	10.4

Features Encoding	80	33.3
Matching	10	4.2
Decision Logic	5	2.1
Total	240	100

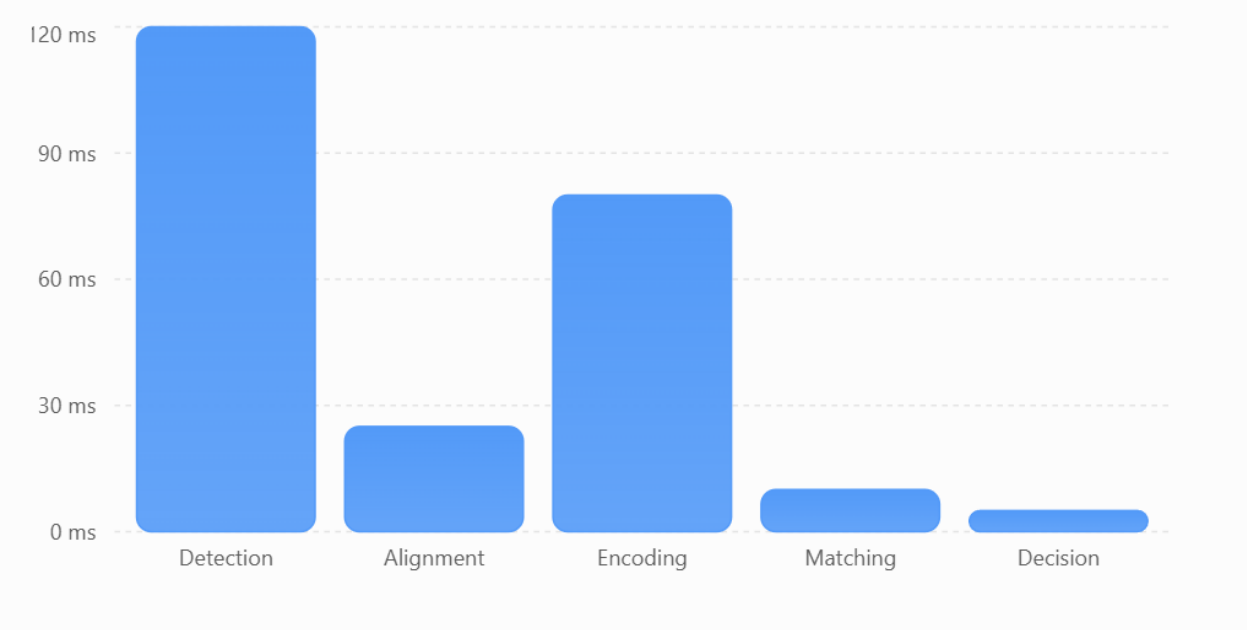

Fig 9. Processing time consumed by each step of face recognition

Latency The latency analysis indicates that face detection requires the largest amount of computational resources, requiring 50% of total execution time (120 ms). The second most time-consuming operation is feature encoding, which takes up 33.3% (80 ms). By contrast, matching and decision logic only need 10 ms and 5 ms, respectively, and therefore have negligible computational overhead. The total processing time of 240 ms (0.24 s) suggests that the proposed system can achieve near real-time face recognition performance, with approximately 4.17 recognition cycles per second.

EXPERIMENTAL RESULTS AND ANALYSIS

Experimental Setup

The proposed smart door access control system was implemented using personal computer, a USB camera, an ESP32, servo motor, I2C LCD module, LEDs and Firebase cloud database. We worked on face detection and recognition algorithms using Python and OpenCV. The experimental data set was composed of the facial images of three authorized users under different lighting conditions, facial expressions and head poses. The experiments were conducted to assess the recognition accuracy, response time, security performance and overall reliability of the system.

Recognition Accuracy

The face recognition system was tested with a testing data set that did not contain images used for training. The recognition accuracy is calculated as the percentage of correctly recognized faces from the total number of testing samples.

Under normal environmental conditions, the system could successfully identify authorized users with good recognition accuracy. Small recognition errors were observed at low light conditions and extreme head orientations.

Table 2. Accuracy of detection under different conditions

Condition	Accuracy (%)
Normal lighting	98
Low lighting	85
Side Pose	80
Multiples faces	70
Background Clutter	87

E. Security Analysis

To increase the security of the proposed smart door access control system, a liveness detection mechanism was included with the facial recognition module. The facial recognition systems used in practice can be subject to a spoofing attack by an intruder who presents a printed photo or a digitized image of an authorized person. To eliminate this danger, the suggested system ensures the identified face is a real person before it can proceed with the recognition process [12].

The liveness identification method utilized is based on eye-blink detection. The device constantly analyzes the facial landmarks surrounding the eyes and recognizes normal blinking activity. Access is allowed only upon recognition of a genuine face and detection of a blink within a specific time frame. If no blink is detected, the system concludes that the given face is not a live one and denies access [8].

The addition of liveness detection to the proposed system greatly increases its security, adding one more step of verification before authentication. This method ensures the efficiency of the system in real time and also prevents illegal access by employing static face photos.

Table 3. Liveness Detection Results

Test Scenario	Result
Live User with Blink	Access Granted
Printed Photo	Access Denied
Mobile Image Display	Access Denied

CONCLUSION AND FUTURE WORK

In this study, an IoT-based facial recognition smart door access control system for security and automation at residential and office places is proposed. The suggested system is a single access control solution that combines face detection, face recognition, liveness detection, ESP32-based door control, I2C LCD, LED status indicators, and Firebase cloud recording. The system uses face recognition to identify authorized people and automatically opens the door, displays a welcome message, and logs the access event in a cloud database for remote monitoring.

Experimental assessment indicated that the suggested system can provide real-time authentication with dependable recognition performance in varied operating settings. The incorporation of liveness detection adds an extra layer of protection, decreasing the potential for unwanted access using static face photos. Moreover, Firebase-based cloud logging enables continuous monitoring and keeping track of access logs, which makes the system suited for smart home and smart office applications.

The suggested system may be improved in various ways, although its performance was adequate. Furthermore, advanced deep learning-based facial recognition models may be utilized to further increase the recognition accuracy under difficult lighting and posture changes. More advanced anti-spoofing techniques, such as head movement analysis and multi-factor biometric authentication, can be implemented to increase security. A specific mobile application may also be built to provide remote access control, real-time notifications, and management of the system. These improvements

will significantly improve the dependability, usability, and security of the proposed smart door access control system.

REFERENCE

Gota, D.-I., et al. Smart home automation system using Arduino microcontrollers. in 2020 IEEE International conference on automation, quality and testing, robotics (AQTR). 2020. IEEE.

Brownlee, J., Deep learning for computer vision: image classification, object detection, and face recognition in python. 2019: Machine Learning Mastery.

Kaur, P., et al., Facial-recognition algorithms: A literature review. Medicine, Science and the Law, 2020. 60(2): p. 131-139.

Prabhakar, A., et al., Password based door lock system. International Research Journal of Engineering and Technology (IRJET), 2019. 6(2): p. 1154-1157.

Aswini, D., et al. Smart door locking system. in 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and
Automation (ICAECA). 2021. IEEE.

Wang, M. and W. Deng, Deep face recognition: A survey. Neurocomputing, 2021.
42G: p. 215-244.

Schuckers, S.A., Spoofing and anti-spoofing measures. Information Security technical report, 2002. 7(4): p. 56-62.

Hadiprakoso, R.B. and H. Setiawan. Face anti-spoofing using CNN classifier & face liveness detection. in 2020 3rd International Conference on Information and Communications Technology (ICOIACT). 2020. IEEE.

Li, H.-C., Z.-Y. Deng, and H.-H. Chiang, Lightweight and resource-constrained learning network for face recognition with performance optimization. Sensors, 2020. 20(21): p. 6114.

Schroff, F., D. Kalenichenko, and J. Philbin. Facenet: A unified embedding for face recognition and clustering. in Proceedings of the IEEE conference on computer vision and pattern recognition. 2015.

Chougale, P., et al., Firebase-overview and usage. International Research Journal of Modernization in Engineering Technology and Science, 2021. 3(12): p. 1178-1183.

Cech, J. and T. Soukupova, Real-time eye blink detection using facial landmarks. Cent. Mach. Perception, Dep. Cybern. Fac. Electr. Eng. Czech Tech. Univ. Prague, 2016: p. 1-8.