Entry Exit Face Identification Door Lock System

DA526 - Image Processing with Machine Learning

Project Report

Team Name: Game Changers

Team Members:

Saireddy Shreyas	Roll Number: 244101046
Vishnu Vardhan G	Roll Number: 244101066
Rohan Jainarayan Dobarkar	Roll Number: 244101040
Parvigari Sai Kiran Chary	Roll Number: 244101031
Rahul	Roll Number: 244101035

Instructor:

Dr. Debanga Raj Neog

Department of Computer Science and Engineering

Indian Institute of Technology Guwahati

Amingaon, North Guwahati, Guwahati, Assam 781039

May 6, 2025

Contents

List of Tables

Abstract

In academic institutions, especially at the postgraduate and doctoral levels, certain laboratories are restricted to a small group of authorized users due to the presence of sensitive equipment, valuable research data, or ongoing experiments. Currently, access to these labs is managed manually, often relying on security personnel or trust-based systems where students present their ID cards. However, these methods are inherently vulnerable to misuse, such as individuals gaining entry using someone else's ID, and they typically lack proper mechanisms for logging who accessed the lab and when. This poses a significant risk to both research integrity and equipment security.

To address these challenges, our project proposes an automated, real-time identity verification system tailored for lab access control. The system utilizes a scanner to read ID cards and a camera to capture a live image of the user at the point of entry. By applying facial recognition and image processing techniques, the live image is compared with the ID card photograph to ensure the person presenting the card is its rightful owner. This adds a robust verification layer that manual systems cannot guarantee.

Upon successful identity matching and verification of authorization, the system automatically grants access by unlocking the door and simultaneously logs the entry. This approach not only enhances security by preventing unauthorized access but also establishes an auditable trail of lab usage, promoting accountability among users. By minimizing human intervention and improving reliability, this solution is well-suited for modern academic environments where both security and efficiency are paramount.

Chapter 1

Introduction

In academic and research institutions, access to specialized laboratories is typically limited to a small group of authorized individuals, such as postgraduate (M.Tech) and doctoral (Ph.D.) students. These labs often contain sophisticated equipment, sensitive experiments, or confidential research data that require a high level of security and controlled access. Despite the critical nature of these environments, many institutions continue to rely on traditional access methods such as manual ID checks or physical keys. These methods are not only inefficient but also susceptible to misuse, such as unauthorized access through borrowed or forged ID cards.

In recent years, advancements in image processing and biometric authentication have opened new possibilities for automating access control systems. Leveraging these technologies can significantly enhance the security, accuracy, and accountability of laboratory access. By integrating hardware components such as ID card scanners and cameras with facial recognition algorithms, it is now possible to verify the identity of individuals in real-time and log their access automatically.

The primary objective of this research is to develop an automated identity verification system for restricted lab access. The system aims to scan a user's ID card, capture a live photograph, and use image processing techniques to match the live image with the ID card photograph. Access will only be granted if the identity is successfully verified and the individual is authorized. This project not only strengthens lab security but also introduces a reliable logging mechanism, ensuring that every entry is recorded. The proposed system is a step toward modernizing access control infrastructure in academic institutions, enhancing both security and operational efficiency.

Chapter 2

Related Work

Various access control methods are currently used in institutional settings, each with its own limitations. Manual ID verification, where users show their ID cards to a guard or lab assistant, is still common in many colleges. However, this method is prone to human error and ID misuse, as there is no reliable way to verify that the person holding the ID is the rightful owner.

RFID-based systems offer automation and convenience by allowing users to tap their ID card for entry. While this speeds up access, it still fails to confirm the identity of the cardholder, making it possible for unauthorized individuals to gain access with someone else's card. Additionally, many RFID systems lack integrated logging mechanisms, making it difficult to track who actually entered the lab.

Biometric systems, such as fingerprint or iris scanners, provide more robust authentication but come with practical challenges. They are costly, require regular maintenance, and can be unreliable in lab environments where users may wear gloves or encounter poor lighting conditions.

To address these shortcomings, our system combines ID card scanning with real-time facial recognition. By comparing the live image captured by a camera with the photo on the ID card, the system ensures the cardholder's identity. Access is granted only if there is a successful match, and each entry is automatically logged with a timestamp, providing both security and accountability. This contactless, efficient solution is particularly well-suited for labs where only a limited number of authorized students are allowed.

Chapter 3

Datasets

To create a good dataset for ID card detection, we captured 240 images of 24 different ID cards, with each card photographed in 10 different orientations. The photos were taken using a smartphone camera at a high resolution of 3000×4000 pixels, in a well-lit indoor environment. To ensure clarity and consistency, we placed the ID cards on a black background and used a tripod to keep the camera steady. Additionally, we used 30 FPS video clips recorded at a resolution of 2160×3840 pixels (height × width) for the final testing of the model, selecting frames from different angles of the cards.

Out of the 240 images, 200 were used for training, and 40 were used for validation. The images are organized in a format expected by YOLOv5: training images are stored in `train_data/images/train`, and validation images in `train_data/images/val`. Labels were created using `makesense.ai`, a simple annotation tool that exports in YOLO format. These annotation files are saved in `train_data/labels/train` and `train_data/labels/val`.

Each label file contains lines in the following format:

```
<class_id> <x_center> <y_center> <width> <height>
```

All values are normalized between 0 and 1 based on the image's size. This format helps the model accurately learn where the ID card is in each image. With high-quality, well-annotated images, this dataset is ready to be used for training an ID card detection model.

Chapter 4

Methodology

4.1 Object Detection

The first and foundational step in our system is the detection of ID cards using a state-of-the-art object detection model—**YOLO (You Only Look Once)**. We specifically fine-tuned the **YOLOv5** model to recognize ID cards with high precision. To achieve this, we created a custom dataset comprising **240 images** of **24 unique ID cards**, each captured in **10 different orientations**. These images included variations in angles, lighting conditions, and backgrounds to simulate real-world scenarios.

To enhance the generalization capability of the model, we applied data augmentation techniques such as *rotation*, *scaling*, *contrast adjustment*, and *flipping*. These augmentations allowed the model to learn invariant features of ID cards despite changes in visual appearance. The model was trained using a supervised learning approach, and performance was validated using a hold-out validation set.

Once the model was trained, we integrated it with a real-time video stream. The YOLOv5 model processed each frame of the incoming video feed, scanning for the presence of ID cards. A **confidence threshold** parameter was established, and only detections above this threshold were considered valid. This ensured that the system only responded to high-confidence ID card detections, minimizing false positives and reducing the likelihood of erroneous captures.

4.2 Crop and Align

Once an ID card is detected using the YOLOv5 model, the next essential step is to isolate and standardize it through cropping and alignment. This step ensures that variations in angle, scale, or orientation do not affect downstream processes like face or text extraction. The procedure involves both geometric transformations

and image processing to normalize the ID card's appearance.

The steps followed are:

- **Grayscale conversion and thresholding:** The input frame containing the ID card is first converted to grayscale. A binary threshold is applied to segment the foreground (ID card) from the background.
- **Contour detection and cropping:** The largest contour is identified, assuming it corresponds to the ID card. A minimum-area rectangle is computed around it, and the bounding box is used to crop the card from the original image.
- **Tilt correction using rotation:** The rotation angle from the bounding box is analyzed. If the angle is less than 45°, it is increased by 90°, and if it is more than 45°, it is decreased by 90°. The image is then rotated using an affine transformation matrix centered on the card's midpoint to correct any tilt.
- **Horizontal alignment:** If the resulting card is taller than it is wide (i.e., in portrait orientation), it is rotated 90° counterclockwise to standardize it to a landscape layout.
- **Final cleanup crop:** After rotation, the image may have unwanted black borders or extra space. A second round of thresholding and contour detection is performed, followed by additional cropping to tightly bound the ID card.

4.3 Image and Text Extraction

Once the ID card is aligned and cropped, the next step is to extract relevant information, such as the roll number and the face image, for authentication purposes.

1. **OCR Processing**: The `pytesseract` library is used to extract text from the preprocessed ID card image. Custom configurations are applied to optimize the OCR process for detecting text in a single block.
2. **Roll Number Extraction**: The extracted text is analyzed to locate lines containing keywords such as "Roll" or "Roll No." The roll number is then isolated by filtering out only the digits from the relevant line.
3. **Face Image Extraction**: A predefined mask is applied to extract the face image region from the aligned ID card. This face image is later used for face recognition during authentication.

This approach enables the efficient extraction of both textual and biometric information, crucial for the authentication process without relying on complex database lookups.

4.4 Face Recognition

To authenticate the identity of the individual presenting the ID card, we employed **face recognition techniques**. A live photograph of the user was captured using a high-definition camera positioned at the point of entry. This photograph served as a real-time representation of the person requesting access.

We then compared the facial features from the live image with those extracted from the ID card using **feature embedding** and **similarity measurement**. Both images were passed through a facial recognition model (e.g., FaceNet or dlib-based system) to extract feature vectors. These vectors were compared using **cosine similarity** or **Euclidean distance** metrics. If the similarity score exceeded a predetermined threshold, the match was considered valid.

This step was critical in determining whether the person holding the ID card was indeed its rightful owner. By relying on biometric matching instead of just visual inspection or barcode scanning, we significantly reduced the potential for impersonation or misuse of ID cards.

4.5 Authentication

In the final stage of our system, **authentication** is performed by verifying the identity of the person presenting the ID card. This is achieved through two checks:

1. **Face matching**, and
2. **Roll number verification**.

After successfully extracting the face image from the ID card and capturing a live face image, the system compares the two using face recognition techniques. If the match confidence exceeds a preset threshold, the identity is considered valid.

Simultaneously, the roll number is extracted from the ID card using OCR. Instead of querying a database, the system uses a **predefined list of student records hardcoded within the program**. This list includes roll numbers along with associated information such as names, valid ID status, and lab eligibility.

The system verifies:

- If the extracted roll number exists in the predefined list.

- If the face match is successful.

If both checks pass, access is granted; otherwise, it is denied. This approach keeps the system **lightweight, fast**, and suitable for **small-scale lab environments** where full database integration is unnecessary.

4.6 Signal to Arduino

The PC sends an HTTP GET request over Wi-Fi to a microcontroller such as an Arduino with Wi-Fi or an ESP32.

The microcontroller is connected to the same local Wi-Fi network and runs a basic web server. It constantly listens for incoming HTTP requests. When a request is received, it checks the URL or parameters to determine the type of access attempt.

The buzzer is connected to a digital output pin of the microcontroller, based on the command received, the microcontroller activates a buzzer with a specific beep pattern: one beep for door open (access granted), two beeps for unauthorized person, and three beeps for face and ID mismatch.

4.7 Buzzer

Once the Arduino or ESP32 receives the HTTP signal from the PC, it responds by activating a connected buzzer. The buzzer is connected to a digital output pin of the microcontroller, which is programmed to generate a high signal for a fixed duration to produce the beep.

Based on the type of signal received, the MCU triggers the buzzer to emit different beep patterns:

1. **Beep:** Indicates the door has been successfully opened and access is granted.
2. **Double Beep:** Warns that the person is not authorized to enter the restricted space.
3. **Triple Beep:** Alerts that both face recognition and ID validation have failed, denying access due to identity mismatch.

These audible signals ensure quick, clear feedback for access events, enhancing security and user awareness in real time.

Chapter 5

Experiments and Results

To evaluate the performance of our face identification door lock system, we conducted a series of test cases simulating real-world lab entry scenarios. Each test involved presenting an ID card to the scanner and capturing a live image of the user. The system then performed face matching and roll number verification before making an access decision.

5.1 Test Environment

The experiments were conducted using a high-resolution camera and ID images captured under controlled indoor lighting. The system was deployed on a workstation with an Intel i5 13th Gen CPU, 16GB RAM for real-time ID card detection.

5.2 Evaluation Metrics

To assess the performance and reliability of the proposed system, we used the following evaluation criteria:

- **Roll Number Verification:** Checks whether the roll number extracted via OCR from the ID card exists in the predefined list of authorized users.
- **Facial Verification Outcome:** Determines whether the live image of the user matches the face extracted from the ID card.
- **Final Access Decision:** Indicates whether access was granted, based on the combined outcome of roll number validation and facial verification.

5.3 Test Case Results

Table 5.1: Access Control Test Case Results

Test ID	Roll Number	Valid Roll Number	Face Match	Access Granted
1	244101046	Yes	Yes	Yes
2	244101066	Yes	No	No
3	244101999	No	Yes	No
4	244101035	Yes	Yes	Yes
5	123456789	No	No	No

The results demonstrate that the system correctly grants access only when both the identity and roll number match. False matches or unauthorized IDs were effectively rejected.

Chapter 6

Conclusions

Our project successfully demonstrates an entry exit face identification door lock system. By combining object detection, image preprocessing, OCR, and face matching, we achieve high accuracy in identifying authorized personnel.

Key Takeaways

- The system eliminates manual checking and impersonation risks.
- It performs well in consistent lighting and fixed camera setups.
- All components operate in real-time with minimal latency.

Limitations

- Performance may degrade in poor lighting or with low-quality cameras.
- The current implementation relies on a hardcoded list of valid roll numbers, making it unsuitable for large-scale deployment.

Future Work

- Integrate dynamic database support for user records.
- Improve robustness under varying lighting conditions.
- Deploy on embedded platforms for portability and cost efficiency.