Grenze International Journal of Engineering and Technology, June Issue

Double Verification System using HOG Algorithm

Srilekha Medichelimi[1], Kiran Babu[2], Poorvi Kotamraju[3], Sneha Ravirala[4] and Manideep Chowdary[5]
[1-2]Assistant Professor, Vignana Bharathi Institute of Technology, ECE Department Hyderabad, Telangana, India
Email: medichelimi.srilekha@vbithyd.ac.in, sangeetha.kiranbabu@vbithyd.ac.in
[3-5]Students, Vignana Bharathi Institute of Technology, ECE Department, Hyderabad, India
Email: poorvik1903@gmail.com, sneharavirala@gmail.com, manideepchowdary111@gmail.com

***Abstract*— The Entry System represents a significant advancement in bolstering security and refining access control measures within educational institutes. By ingeniously integrating cutting-edge technologies like face recognition, RFID authentication, Arduino Uno, and harnessing the computational power of Raspberry Pi, the system ensures a comprehensive approach to security while prioritizing user convenience. As students and staff approach entry points, the system initiates identity checks through RFID technology, followed by an additional layer of authentication via facial recognition. This dual authentication mechanism establishes a robust, multi-layered security framework. The seamless integration of these sophisticated technologies not only fortifies security but also optimizes access procedures, fostering a technologically advanced and secure environment within educational institutions. This approach to security shows our commitment to create a safe and user-friendly educational ecosystem.**

***Index Terms*— access Control, RFID, arduino UNO, raspberry pi, face recognition, Hog Algorithm (Histogram of Oriented Gradients).**

I. INTRODUCTION

An entry system, commonly known as an access control system, serves as an essential technology-driven solution aimed at managing and regulating the entry and exit of individuals within a designated campus or facility. These systems are engineered to oversee and govern the flow of personnel, ensuring authorized entry while preventing unauthorized access. By leveraging a combination of advanced technologies, such as RFID (Radio-Frequency Identification) and face recognition, these entry systems are developed to operate with minimal manual intervention. RFID technology facilitates seamless identification through the use of electronically stored data on tags or cards, enabling easy and efficient access control. Complementing this, face recognition technology provides an additional layer of security by verifying individuals based on their unique facial features, further enhancing the system's reliability and accuracy. Through the integration of these cutting-edge technologies, the entry system not only streamlines access procedures but also fortifies security measures, safeguarding the premises against potential breaches and ensuring smooth operations.

II. LITERARY SURVEY

Wang Xiang [1] conducted a comparative analysis of various face recognition algorithms, including CNN, PCA, SVM, MTCNN, and Facenet, noting CNN's suitability for face recognition due to its effectiveness amidst evolving technologies.
Danmei Li et al. [3] devised a staff access control system utilizing UHF RFID readers, industrial PCs, and a

Grenze ID: 01.GIJET.10.2.77

database server. Deployed at organization entrances, the system matches tag IDs with database records to permit access, recording entries and displaying identification information.
Shreyak Sawhney et al. [4] proposed an automated attendance management system employing face recognition for student classes. Faces are matched with a database for attendance tracking.
Shireesha Chintalapati et al. [5] suggested an automated attendance system based on face detection and recognition, marking attendance upon student entry to classrooms.
Wen Jialong [6] delineated the history and operation of RFID technology, particularly focusing on RFID tags utilizing thin-film transistors (TFTs). Notably, RFID tags employing metal oxide TFTs offer advantages like superior electrical properties, affordability, flexibility, transparency, catering to specific application needs. Various applications of these tags were also discussed.

III. PROPOSED MODEL

This proposed method aims to implement a robust two-step verification method using an Arduino Uno and a Raspberry Pi 3B+. It combines RFID technology and facial recognition to enhance security measures. The Arduino Uno is connected with an RFID module, red and green LEDs, a buzzer, an OLED display, and a servo motor acting as a gate. The Raspberry Pi performs face recognition using OpenCV and HOG algorithms, and stores the user information in a SQLite3 database. This approach ensures a multi-layered authentication process for access control.
This integrated approach to access control optimally balances efficiency and security, using both RFID and facial recognition technologies to minimize false positives while providing a contingency for potential errors in face recognition under challenging environmental conditions.

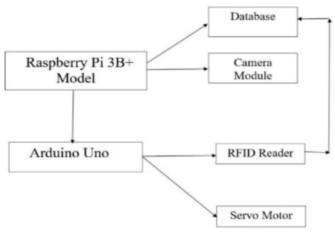

FIGURE 1. BLOCK DIAGRAM

The Arduino Uno acts as the central controller, coordinating the actions of various hardware components for an efficient two-step verification system. The RFID module is the crucial element that enables card-based authentication by reading unique RFID tags. Red and green LEDs acts as indicators, with the red LED signalling access denied and the green LED illuminating for access granted, providing immediate and clear feedback to users. For enhanced user interaction, an OLED display connected to the Arduino Uno displays the message such as "Access Granted" or "Access Denied." A buzzer produces distinctive sounds to indicate the access status, aiding users in understanding result. The servo motor, acting as a gate, physically controls access. Upon successful authentication, the servo motor activates, allowing the gate to open, and in the case of denial, it remains closed. And to use the Arduino system as a backup in case of failure of Raspberry Pi module, we can store the user's information in the EEPROM memory of Atmega328 microcontroller of Arduino Uno.

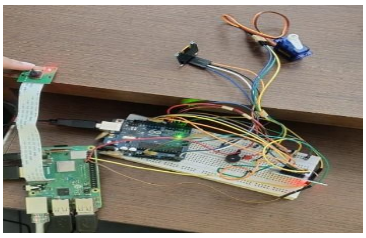

FIGURE. 2. COMPLETE CIRCUIT

The Raspberry Pi plays a major role in this system by adding facial recognition as a crucial authentication factor. A high-resolution Pi camera is utilized to capture detailed images of individuals seeking access. This camera ensures that the facial recognition system receives clear and precise data for accurate identification. FIG 2 shows us the complete above mentioned connections.

Facial recognition, utilizing HOG algorithms, extracts unique patterns from captured images. Open CV compares these with stored data in a SQLite3 database for matching. Successful recognition triggers Arduino Uno for physical access control. Unsuccessful attempts prompt RFID card scan and buzzer activation. If the RFID card is unregistered, access is denied. This integration bolsters security, creating a robust two-step verification system suitable for high-security applications. Arduino Uno and Raspberry Pi communicate via serial protocol for synchronized operation, ensuring efficient data exchange and coordinated functionality, as depicted in FIG. 1 block diagram.

IV. Face Recognition Using Hog Algorithm

The Histogram of Oriented Gradients (HOG) algorithm, developed by Navneet Dalal and Bill Triggs in 2005, excels in facial recognition within computer vision. It effectively captures gradient orientations in images, enabling robust detection of object shapes while remaining resilient to lighting, pose, and facial expression variations. HOG operates through several key steps:

- *Image Acquisition*: Using a Raspberry Pi Camera, the algorithm begins with capturing a facial image under favourable lighting conditions for optimal results.
- *Preprocessing:* The acquired image undergoes preprocessing, including resizing, normalization, and grayscale conversion, to standardize inputs for efficient feature extraction.
- *Gradient Computation*: Gradients, crucial for characterizing image structures, are computed using operators like Sobel or Prewitt in both x and y directions, highlighting edges and intensity changes.
- *Magnitude and Orientation Calculation*: Each pixel's gradient magnitude and orientation are computed, providing essential information about the image's local structure.
- *Cell Formation*: The image is divided into 8x8 pixel cells, enabling localized gradient analysis and accommodating variations in expressions and poses.
- *Histograms for Each Cell*: Histograms of gradient orientations are constructed for each cell, compactly representing local facial features.
- *Block Normalization*: Cells are grouped into blocks (e.g., 2x2 or 3x3), which are then normalized to reduce lighting variations and improve robustness.
- *Feature Vector Concatenation*: Normalized block histograms are concatenated to form a feature vector representing the entire face, capturing its distinguishing characteristics.
- Training: The algorithm may undergo training using a dataset of faces to optimize recognition performance and adaptability to different appearances.
- *SVM Classification*: A Support Vector Machine (SVM) or similar classifier is employed to classify the feature vector, distinguishing between different faces based on learned patterns.
- Recognition and Decision: In the recognition phase, the algorithm compares extracted features with learned patterns to make decisions regarding the individual's identity, successfully recognizing them if the match is positive.

The flowchart for working of Hog Algorithm is given in FIG. 3. and FIG. 4. shows how the cells are divided and formation of histograms.

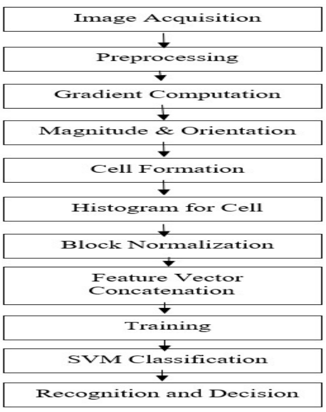

Figure. 3. Hog algorithm working

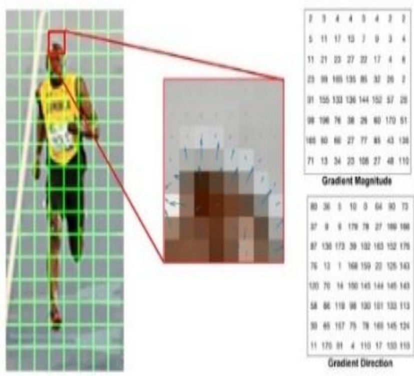

Figure. 4. Representation of hog algorithm

The RFID reader module communicates wirelessly with RFID tags via radio-frequency signals, comprising an antenna, RFID chip, and interface components. The Pi Camera, developed by the Raspberry Pi Foundation, offers an affordable imaging solution for Raspberry Pi boards. It features a 5-megapixel fixed-focus sensor. A servo motor controls the gate's angular position precisely, comprising a motor, control circuit, and feedback mechanism. A buzzer produces sound when an electric signal is applied. Red and green LEDs signify access status. Understanding Arduino Uno and Raspberry Pi functionalities is crucial for implementation. The table gives their roles and features.

V. NEED TO USE BOTH ARDUINO UNO AND RASPBERRY PI

TABLE I. NEED TO USE BOTH ARDUINO UNO AND RASPBERRY PI

Features	Arduino UNO	Raspberry Pi
Processing Power	Suitable for low level tasks, real-time, and interfacing with sensors and actuators.	High processing power, capable of running complex applications, and handling more intensive computations.
I/O and Real-Time Capabilities	Well-suited for interfacing with hardware devices.	I/O capabilities are not as real-time and precise as Arduino.
Cost Effectiveness	Cost-effective and power-efficient for dedicated tasks.	Cost-effective solution for computational power.

VI. ADVANTAGES OF COMBINATION OF FACE RECOGNITION AND RFID OVER EACH TECHNOLOGY INDIVIDUALLY

- *Enhanced security*: Multi-factor authentication with RFID and face recognition reduces unauthorized entry risk.
- *Reduced false positives*: Integration mitigates errors, enhancing identity verification accuracy.
- *Flexibility*: Users choose between RFID or facial recognition for adaptable authentication.
- *Spoofing mitigation*: Dual authentication complicates unauthorized access attempts.
- *Adaptation to lighting*: Combining technologies ensures reliable access regardless of light levels.
- *Comprehensive control*: Users granted access via RFID, facial recognition, or both.
- *User privacy*: RFID-only option respects privacy while maintaining security.
- *Reduced dependency*: Dual technology lessens reliance on single methods, enhancing robustness.
- *Enhanced user experience*: Seamless, user-friendly authentication choice improves satisfaction.
- *Deterrent to unauthorized entry*: Combining methods discourages intruders, bolstering security.

VII. IMPROVEMENTS OF INTEGRATED SYSTEM OVER INDIVIDUAL SYSTEM

TABLE II. IMPROVEMENTS IN INTEGRATED SYSTEM

Features	Face Recognition	RFID System	Integrated System
Security	Vulnerable to spoofing.	Depends on possession of card which could be lost or stolen.	Creates a multi-factor authentication. Access is granted only when RFID card and face matches. Hence reduces the risk due to individual methods.
False Positives	Can have false positives in varying conditions like low lighting or different facial expressions.	Has risk of false positives if the card is lost or stolen.	Reduces the false positives. When one method faces challenges, the other one can provide the required verification.
Flexibility	Provides a contactless method but may fail in certain conditions.	Offers ease of use but does not have uniqueness of biometric system.	Is flexible. Users can choose between RFID card authentication and face recognition.

VIII. PROCESS

The verification begins as the user approaches the gate. He first needs to scan his RFID tag. If the tag id matches with database, he can continue with face recognition. If this process is perfect without any errors, the gate will open and a green led turns on to show that access is granted.
If any mismatch occurs with face recognition, the buzzers activate to alert the security present there. If the RFID tag does not match, the system activates a comprehensive response. The buzzer blares, the red LED turns on and access denied message is displayed on the OLED display. The algorithm is shown in the fig below.

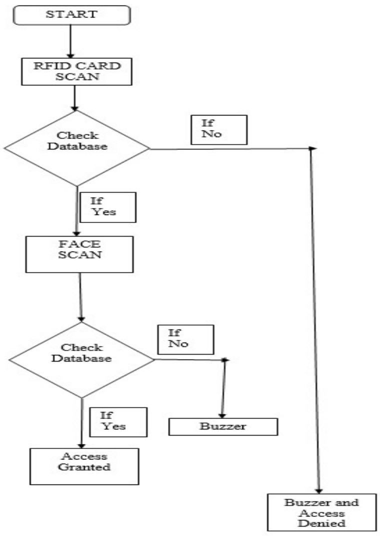

FIGURE. 5. FLOWCHART FOR THE SYSTEM

The entire process can be divided into four steps. They are given as:
Step 1: Python code to capture and store user data in a SQLite3 database for registration, including name, roll number, RFID, and facial data.
Step 2: Geany-assisted Python code which trains the facial recognition model using captured images stored in SQLite3, utilizing OpenCV with HOG algorithms for feature extraction.
Step 3: Arduino IDE compiles and executes C++ code to connect and control components linked to Arduino UNO.
Step 4: Geany integrates Raspberry Pi and Arduino Uno functionalities using Python and C++, coordinating via serial communication.

IX. RESULTS

As soon as the user goes near the gate, he places his RFID tag or card near the scanner as shown in the figures 6 and 7. In figure 6, the green LED is turned on which indicates that the verification process as mentioned in the algorithm is complete and the user is given access. In figure 7, the red LED is turned on which indicates the authentication process has an error and needs to take some security measures. Along with red LED, a buzzer turns on.

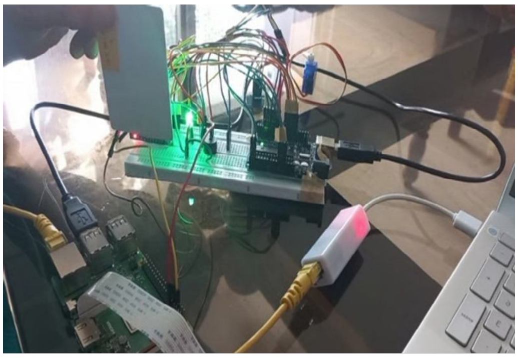

FIGURE. 6. ACCESS GRANTED CONDITION

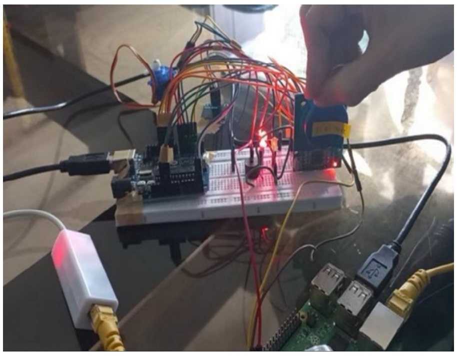

FIGURE. 7. ACCESS DENIED CONDITION

The figure 8 shows the OLED display which gives an access denied message. In the same way when the access is granted to the user, access granted message will be displayed in the OLED display.
A dialogue box showing the user id, whether it is found in the database or is it extracted from Arduino UNO and the captured image frame will be displayed on the monitor screen. This is shown in Fig 9.

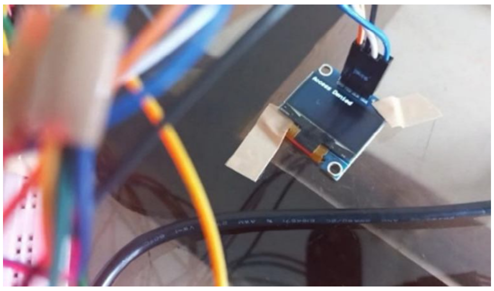

FIGURE. 8. ACCESS DENIED CONDITION IN OLED

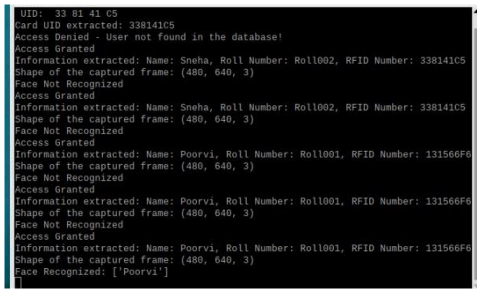

FIGURE. 9. DIALOGUE BOX

Fig. 10. gives the comparison for time taken for the execution of individual process with minimum time required and maximum time required for the execution. The time in milliseconds is taken on the y-axis and the process is taken on x-axis. RFID authentication time includes the time for reading and processing of RFID tag, checking with the database. Face Recognition time includes the time taken to capture image from Pi camera, facial detection and recognition. Overall System Response includes both processing time for RFID authentication and face recognition. In case of this proposed model, the overall system response time is 1800 milliseconds.

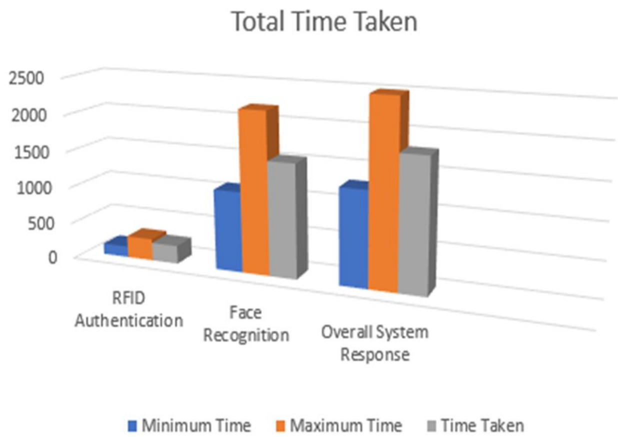

FIGURE. 10. COMPARISON FOR TIME CONSUMPTION

X. Conclusion

In this paper, we saw the two-step verification system, by interfacing Arduino Uno and Raspberry Pi through Geany which captures user information, trains a facial recognition model, and seamlessly integrates physical access control with facial recognition. Its user-friendly interface facilitates efficient coding, resulting in a secure and user-centric access control solution. The real-time console feedback, live frame display, and captured image verification enhance the system's transparency and user experience.

XI. Future Scope

The future scope of this project includes exploring advanced facial recognition algorithms and integrating additional biometric authentication techniques. We can implement a cloud-based storage for storing user profiles to improve scalability, while incorporating machine learning for adaptive access policies which will strengthen the system's security and adaptability. Additionally, exploring edge computing and optimizing the system for IoT integration may make it more useful in a variety of security and access control scenarios.

REFERENCES

[1] Wang Xiang, “The Research and Analysis of Different Face Recognition Algorithms”, J. Phys. : Conf. Ser. 2386 012036, 2022.

[2] Hossein Sahoolizadeh, Youness Aliyari Ghassabeh, “Face Recognition using Eigen-Faces, Fisher-face and Neural Networks”, Cybernetic Intelligent Systems, 2008. CIS 2008. 7th IEEE Conference.

[3] Danmei Li, Huanle Yang, Kayijire Fred, Yuxing Chen, “A Staff Access Control System Based on RFID Technology”, 2015 4th International Conference on Sensors, Measurement and Intelligent Materials 10.2991/icsmim-15.2016.16.

[4] Shreyak Sawhney, Karan Kacker, Samyak Jain, Shailendra Narayan Singh, Rakesh Garg, "Real-Time Smart Attendance System using Face Recognition Techniques", 9th International Conference on Cloud Computing, Data Science & Engineering, 2019.

[5] Shireesha Chintalapati, M. V. Raghunadh, "Automated Attendance Management System Based on Face Recognition Algorithms", IEEE International Conference on Computational Intelligence and Computing Research, 2013.

[6] Wen Jialong, "A Review of RFID Tag Based on TFT", Proceedings of the 2023 International Conference on Functional Materials and Civil Engineering, November, 2023.

[7] Mohammed Abdulhakim Al-Absi, Gabit Tolendiyev, Hoonjae Lee, Ahmed Adbulhakim Al-Absi, "Real-Time Access Control System Method Using Face Recognition", Proceedings of International Conference on Smart Computing and Cyber Security, January, 2021.

[8] R. Rameswari, S. Naveen Kumar, M. Abishek Aananth, C. Deepak, "Automated Access Control System Using Face Recognition", Materials Today Proceedings, May, 2020.

[9] Zhandos Yernazarov, "Development of a Contemporary Access Control System Using Face Recognition", Journal of Problem in Computer Science, September, 2023.

[10] Ajayi Ore-Ofe, S. M. Yahaya, Abubakar Umar, "Design and Construction of Secure Gate Access Control and Monitoring System Using RFID and Fingerprint Technologies", Journal of Science Technology and Education, June, 2022, ISSN: 2277-0011