JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SMART ACCESS CONTROL SYSTEM WITH FACE RECOGNITION AND INTRUSION ALERT

Duvvi Nitesh, K.S.S Soujanya Kumari

Student, Assistant Professor

Andhra University

Abstract

The Smart Access Control System with Face Recognition integrates ESP32-CAM, YOLO for face detection, and a Multi-CNN algorithm for face recognition to provide a secure, real-time access control solution. The system detects and recognizes authorized individuals, granting access via a relay-controlled door lock and triggering an alert system if unauthorized access is attempted. The system achieves high accuracy in face detection and recognition, with a response time of 1.7 seconds, making it suitable for environments requiring fast, contactless access control.

Tested under various lighting and environmental conditions, the system performed reliably, demonstrating robustness across different scenarios. Its modular design allows for scalability and easy integration with cloud services and other security systems. Potential future enhancements include multi-factor authentication and improved adaptability for low-light environments. The system offers a modern, secure, and user-friendly alternative to traditional access control methods.

Introduction

The evolution of access control systems reflects significant technological advancements. Mechanical systems have been largely replaced by electronic solutions that offer more complex security protocols and integration capabilities. These electronic systems utilize magnetic cards, keypads, and more recently, biometric identifiers such as fingerprints, iris scans, and facial recognition to manage access. Each technological leap has aimed to enhance security by making systems harder to bypass and easier to manage.

In recent years, the integration of digital technologies has ushered in the era of smart access control systems. These systems leverage state-of-the-art technology such as artificial intelligence, machine learning, and the Internet of

Things to not only prevent unauthorized access but also to streamline operations. They are capable of performing tasks such as monitoring access patterns to detect anomalies, automating entry procedures during peak hours, and maintaining detailed logs of all access events. This digital transformation is driven by the dual needs of enhanced security and operational efficiency.

The importance of these systems cannot be overstated in today's security landscape, where both physical and digital threats loom large. The impact of security breaches can range from minor inconveniences to catastrophic events, including significant financial losses, damage to reputation, and even threats to personal safety. In sectors such as banking, healthcare, and government, where sensitive information and assets are routinely handled, the need for robust access control systems is critical to prevent data theft and ensure compliance with stringent regulatory requirements.

As the world becomes increasingly interconnected and reliant on digital infrastructure, the potential impact of security vulnerabilities has escalated. This has prompted organizations and entities to invest heavily in advanced security solutions that not only thwart unauthorized access but also provide insights into security management through data analytics. This proactive approach to security underscores the shift from traditional reactive measures to a more strategic, integrated security posture.

The ongoing advancements in access control technology highlight the importance of staying ahead of potential security threats through innovation and adaptation. The move towards smarter, more integrated access control solutions is a reflection of the broader trends in security management, aiming to protect assets with greater precision and intelligence than ever before.

Smart access control systems represent a significant leap forward from traditional mechanical locks and keys, offering enhanced security through the integration of digital technologies and automated systems. These systems utilize a combination of software and hardware to manage and monitor the ingress and egress of individuals, ensuring that only authorized personnel can access specific areas within a facility.

The core components of these systems include electronic locks, biometric scanners, surveillance cameras, access control panels, and networked databases. Electronic locks can be activated remotely and programmed to allow access during specific times. Biometric scanners provide a high level of security by using unique physical characteristics, such as fingerprints, iris patterns, or facial features, to verify an individual's identity. Surveillance cameras offer real-time monitoring and recording capabilities, enhancing security and providing valuable data for forensic analysis. Access control panels serve as the interface for managing and configuring the settings of the entire system, often equipped with user-friendly digital displays and connectivity options for system administrators. Lastly, the networked databases maintain detailed logs of entry and exit, user permissions, and historical access data, essential for audits and security assessments.

The methodologies employed in smart access control systems vary based on the security requirements and organizational policies. Discretionary Access Control is characterized by the owner or administrator of the protected system being responsible for deciding who can access specific resources. It is flexible but considered less secure than other types as it relies heavily on the discretion of the individual managing the access controls. Mandatory Access

Control is often used in high-security environments and enforces access policies based on fixed security attributes assigned to both users and resources. Access decisions are made by comparing these attributes according to a set of rules defined by the system's policy, ensuring a higher level of security by limiting flexibility. Role-Based Access Control assigns access permissions based on roles within an organization, and users are assigned roles based on their responsibilities and qualification criteria. This method simplifies management and ensures that individuals only have access to the information necessary for their roles, thereby minimizing potential security risks.

Smart access control systems are widely used in various sectors, including commercial, industrial, residential, and governmental facilities. They offer numerous benefits such as enhanced security, better compliance with regulatory requirements, and improved efficiency in managing large numbers of users across complex environments. However, they also come with challenges such as higher initial setup and maintenance costs, the need for continuous updates to security protocols, and potential privacy issues related to the use of biometric data.

Face recognition technology has emerged as a sophisticated and highly secure method of ensuring that only authorized personnel gain access to controlled environments. This technology leverages advancements in artificial intelligence, particularly in the fields of machine learning and computer vision, to identify individuals by analyzing facial features from images or video streams.

Face recognition systems work by capturing a digital image of an individual's face, typically using a high-definition camera. Once the image is captured, the system uses algorithms to detect the presence of a face within the image. This is often accomplished through the detection of key facial landmarks, such as the eyes, nose, mouth, and jawline. After detecting a face, the system converts the facial features into a digital data representation—a process known as feature extraction. This data is then compared to the pre-existing database of authorized individuals' faceprints to find a match.

The integration of face recognition technology into access control systems involves several components working seamlessly together, including image capture, real-time image processing, face detection, feature extraction, and matching and verification. The extracted features are compared against a database of known faces. If the system finds a match, it verifies the identity of the individual, allowing access. If no match is found, access is denied.

The drive to incorporate face recognition technology into access control systems is fueled by a combination of emerging security needs and the evolving capabilities of technological advancements. Traditional security systems such as magnetic cards, PINs, or mechanical keys carry inherent risks, including loss, theft, or duplication. Face recognition technology offers a more secure alternative because it is based on biometric data that is unique to each individual and extremely difficult to forge or replicate.

Face recognition technology enhances operational efficiency by streamlining the process of identity verification, reducing entry processing time, and minimizing the need for human intervention. In environments where quick access is essential, such as corporate offices, hospitals, or data centers, the technology facilitates smooth and rapid entry flow while maintaining high security standards. This seamless integration not only improves user satisfaction by reducing wait times but also allows security personnel to focus on more critical tasks, enhancing overall security.

The integration of face recognition technology into access control systems is motivated by a combination of enhanced security needs, technological advancements, regulatory requirements, operational efficiency, societal acceptance, and health considerations. These factors collectively drive the adoption of face recognition as a sophisticated, secure, and socially responsible choice for modern access control solutions.

Literature Survey

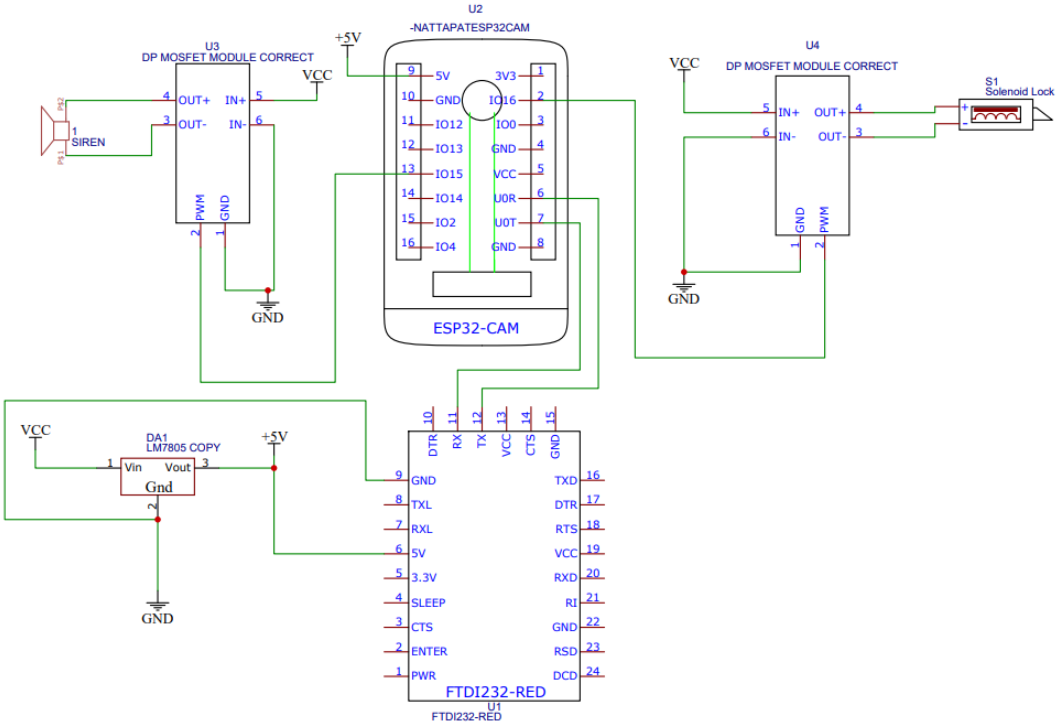
Face detection and recognition have been widely researched and implemented in various security applications. Traditional methods relied on hand-crafted features, while recent advancements in deep learning have significantly improved accuracy and efficiency. Earlier approaches for face detection included Haar cascades and Histogram of Oriented Gradients (HOG), which provided acceptable results but struggled with complex backgrounds, lighting variations, and occlusions.The YOLO (You Only Look Once) algorithm is a real-time object detection model that segments an image into grids and predicts bounding boxes along with confidence scores. Compared to traditional methods, YOLO offers high-speed processing, making it suitable for real-time applications. It provides better accuracy in detecting multiple faces in a single frame and improved robustness against variations in pose and lighting conditions.Face recognition is a biometric method that identifies or verifies individuals based on their facial features. Deep learning techniques, particularly Multi-Convolutional Neural Networks (Multi-CNNs), have improved recognition accuracy by utilizing multiple convolutional layers to extract hierarchical features. Unlike standard CNNs, Multi-CNN architectures process facial images at different levels, enhancing robustness against variations in pose, lighting, and occlusions. Pretrained models like FaceNet and VGG-Face utilize Multi-CNN architectures to generate

embeddings that represent facial features, which are then compared using similarity measures such as Euclidean distance or cosine similarity for identity verification.The combination of YOLO-based face detection and Multi-CNN-based recognition enhances security in authentication systems. Previous studies have demonstrated that YOLO achieves real-time performance with high-speed face detection, while Multi-CNN models provide accurate recognition with minimal false positives. Such systems have been applied in access control, surveillance, and automated security solutions, replacing traditional key-based and RFID access methods. Desite these advancements, challenges such as occlusions, variations in lighting, and adversarial attacks remain areas of active research to improve the robustness of face recognition-based security systems.

Methodology

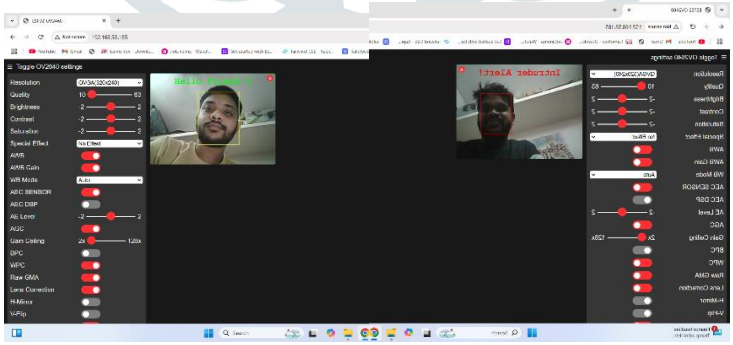
The proposed system utilizes an ESP32-CAM module for face detection and recognition, integrated with a multi-CNN model for enhanced accuracy. The methodology involves image cquisition, preprocessing, face detection, face recognition, and access control mechanisms, ensuring a secure and efficient authentication process.The ESP32-CAM is initialized and configured to capture images in real time. Once an image is acquired, it is processed to enhance quality and remove noise. The YOLO algorithm is employed for face detection, identifying and localizing faces within the captured frame. The detected faces are then passed to a Multi-Convolutional Neural Network (Multi-CNN) model, which extracts hierarchical features and compares them against a stored database of authorized individuals.If the detected face matches an authorized entry, the system triggers the door unlock mechanism using a MOSFET module connected to a solenoid lock. Additionally, an access log is recorded for monitoring purposes. If the face is unrecognized, the system activates a buzzer alert through another MOSFET module, signaling unauthorized access. Simultaneously, an alert notification is sent to the concerned authority, enabling remote monitoring.The hardware setup includes the ESP32-CAM for image processing, an FTDI232 module for serial communication and programming, a 7805 voltage regulator for power stabilization, and MOSFET modules for controlling external components. The system operates in a continuous loop, ensuring real-time access control and security monitoring. After each authentication attempt, the system enters a wait-and-reset state, preparing for the next image capture cycle.

Circuit Diagram:



Result:

The system was tested for accuracy, response time, and environmental adaptability. YOLO-based face detection achieved up to 100% accuracy, while CNN-based face recognition reached 97% accuracy. The total response time was 1.7 seconds, ensuring real-time performance. The system functioned well in various lighting and outdoor conditions with minor adjustments.



Authorized Access: If the system recognizes an authorized user, the output message displayed is **"Hello Friend 0"**, and the solenoid lock is disengaged, allowing access. The buzzer remains silent. **Unauthorized Access:** If the system fails to recognize the user or detects an intruder, the output message displayed is **"Intruder Alert"**, and the buzzer is activated to provide an audible warning. The solenoid lock remains engaged, denying access.

Conclusion & Future work

The ESP32-CAM-based face recognition system using the YOLO algorithm for face detection and a Multi-CNN model for recognition provides an efficient and low-cost solution for access control and security applications. The system effectively detects and recognizes faces in real time, allowing authorized individuals to access secure areas while restricting unauthorized entries. The integration of hardware components such as MOSFET modules, solenoid locks, and buzzers ensures seamless automation, reducing the need for manual intervention. The proposed system enhances security by providing accurate recognition, minimizing false positives, and offering real-time alert mechanisms for unauthorized access attempts.In the future, this project can be extended by integrating liveness detection techniques to prevent

spoofing attacks using printed images or videos. The system can be enhanced with cloud connectivity for remote access monitoring, allowing administrators to track access logs and control entry permissions from anywhere. Additionally, multi-factor authentication, such as combining face recognition with fingerprint or RFID authentication, can be implemented for enhanced security. Further optimization of the Multi-CNN model can improve processing speed and accuracy, making it more suitable for large-scale deployment in smart homes, office buildings, and industrial facilities. The project can also be expanded for use in ATM security, automated attendance systems, and public transportation access control.

References

1. Lulla, G., Kumar, A., Pole, G., & Deshmukh, G. (2021, March). IoT based smart security and surveillance system. In 2021 international conference on emerging smart computing and informatics (ESCI) (pp. 385-390). IEEE.

2. Rakhra, M., Singh, D., Singh, A., Garg, K. D., & Gupta, D. (2022, October). Face recognition with smart security system. In 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 1-6). IEEE.

3. Nadafa, R. A., Hatturea, S. M., Bonala, V. M., & Naikb, S. P. (2020). Home security against human intrusion using Raspberry Pi. Procedia Computer Science, 167, 1811-1820.

4. Lee, H., Park, S. H., Yoo, J. H., Jung, S. H., & Huh, J. H. (2020). Face recognition at a distance for a stand-alone access control system. Sensors, 20(3), 785.

5. Bagchi, T., Mahapatra, A., Yadav, D., Mishra, D., Pandey, A., Chandrasekhar, P., & Kumar, A. (2022). Intelligent security system based on face recognition and IoT. Materials Today: Proceedings, 62, 2133-2137.

6. Majumder, A. J., & Izaguirre, J. A. (2020, July). A smart IoT security system for smart-home using motion detection and facial recognition. In 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 1065-1071). IEEE.

7. Venkata, N. Y. L., Rupa, C., Dharmika, B., Nithin, T. G., & Vineela, N. (2021, August). Intelligent secure smart locking system using face biometrics. In 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT) (pp. 268-273). IEEE.

8. Waseem, M., Khowaja, S. A., Ayyasamy, R. K., & Bashir, F. (2020, October). Face recognition for smart door lock system using hierarchical network. In 2020 International Conference on Computational Intelligence (ICCI) (pp. 51-56). IEEE.

9. Suhaimi, A. F., Yaakob, N., Saad, S. A., Sidek, K. A., Elshaikh, M. E., Dafhalla, A. K., ... & Almashor, M. (2021,

July). IoT based smart agriculture monitoring, automation and intrusion detection system. In Journal of Physics: Conference Series (Vol. 1962, No. 1, p. 012016). IOP Publishing.

10. Mrabet, H., Alhomoud, A., Jemai, A., & Trentesaux, D. (2022). A secured industrial Internet-of-things architecture based on blockchain technology and machine learning for sensor access control systems in smart manufacturing. Applied sciences, 12(9), 4641.