iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VIII **Month of publication:** August 2025

DOI: https://doi.org/10.22214/ijraset.2025.73781

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VIII Aug 2025- Available at www.ijraset.com

Visitor Authentication System Based on Face Recognition Technology

Dr. K. SubbaRao[1], Ravipati Vara Lakshmi[2], Jennepogu Shifali Wesly[3], Modugula Sriharsha[4], Sanagala Sri Teja[5], Shaik Meer Sharif [6]

[1]*Professor,* [2, 3, 4, 5, 6]*UnderGraduate, CSE-Data Science Department, St. Ann's College of Engineering & Technology, Andhra Pradesh*

Abstract: ***In the era of rapidly advancing security requirements, traditional visitor authentication methods such as ID cards and passwords often fall short in providing robust protection against unauthorized access. This paper presents a real-time visitor authentication system leveraging face recognition technology powered by the YOLOv8 deep learning model. The proposed solution replaces manual verification and RFID-based systems with an automated, contactless, and intelligent approach that captures live facial data through webcam-enabled devices. YOLOv8 ensures high-speed and accurate face detection, while a deep learning-based recognition module matches the detected faces against a dynamically maintained database of registered users. The architecture is designed to support modular deployment across varied security environments such as corporate offices, smart homes, and public infrastructures. Comprehensive testing validates the system's performance, achieving high recognition accuracy and near-instantaneous response times. This work demonstrates the viability of integrating real-time object detection with biometric authentication to enhance security, usability, and scalability in modern access control systems.***

Keywords: Face recognition, YOLOv8, visitor authentication, real-time security, deep learning, biometric access control.

I. INTRODUCTION

The growing need for intelligent, secure, and frictionless access control mechanisms has driven significant advancements in biometric authentication systems. Traditional visitor authentication methods—such as passwords, RFID cards, and manual identity checks—are increasingly inadequate in safeguarding sensitive environments due to their vulnerability to forgery, unauthorized use, and human error. These approaches often lack scalability, real-time responsiveness, and adaptability to evolving security threats.

Face recognition has emerged as a non-intrusive and widely deployable biometric modality, offering high accuracy and automation with minimal user interaction. By utilizing readily available imaging devices such as webcams and CCTV cameras, facial recognition systems can be integrated into existing infrastructures without the need for specialized sensors. Unlike fingerprint or iris-based authentication, face recognition supports contactless verification, making it ideal for applications in public spaces, enterprise environments, and smart homes.

Recent advances in deep learning and computer vision have significantly improved the robustness of face recognition systems under varying conditions, such as changes in lighting, pose, and occlusion. In particular, object detection frameworks like YOLO (You Only Look Once) have shown remarkable performance in real-time face detection tasks. YOLOv8, the latest iteration developed by Ultralytics, offers an optimal balance between detection speed, accuracy, and computational efficiency—making it highly suitable for live video-based authentication systems.

This paper presents a real-time Visitor Authentication System based on YOLOv8-driven face recognition. The proposed architecture captures live facial imagery, performs high-speed detection, extracts discriminative embeddings, and compares them against a secure database of authorized individuals. The system is designed to operate efficiently on standard hardware, with built-in modules for access decision-making, visitor logging, and alert generation for unauthorized attempts.

The primary contributions of this study are:

- Development of a real-time, contactless visitor authentication system using YOLOv8 for face detection.
- Integration of a facial feature extraction and matching pipeline for accurate identity verification.
- A scalable and modular system architecture adaptable to various physical security contexts.
- Comprehensive evaluation of system accuracy, performance latency, and threat resilience under real-world constraints.

By combining state-of-the-art deep learning models with practical deployment strategies, the proposed system offers a secure, efficient, and user-friendly alternative to traditional access control methods.

II. LITERATURE SURVEY

Biometric-based access control systems have gained significant traction in recent years due to their reliability and security. Among various biometric modalities, face recognition has become the preferred choice for real-time visitor authentication systems because of its non-contact nature, ease of deployment, and wide availability of image-capturing devices. Numerous studies have explored both traditional and deep learning-based face recognition techniques, focusing on accuracy, scalability, and resilience to real-world variability.

A. Traditional Face Recognition Approaches

Conventional face recognition models predominantly relied on statistical techniques and handcrafted features. Methods such as Eigenfaces and Fisherfaces applied dimensionality reduction techniques like Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) to extract facial features. Haar Cascade Classifiers, widely used in earlier object detection systems, enabled face detection using rectangular features and cascade structures. Although these approaches were computationally lightweight, their performance deteriorated significantly under non-ideal conditions, such as varying lighting, occlusion, and pose changes.

B. Deep Learning-Based Face Recognition Models

The advent of deep learning revolutionized face recognition by enabling automatic feature learning from large-scale datasets. Convolutional Neural Networks (CNNs) such as VGG-Face, FaceNet, and ResNet architectures have demonstrated superior accuracy in facial representation learning.

These models capture spatial hierarchies of facial features, enabling robust identification even under challenging conditions. FaceNet, in particular, introduced the concept of face embeddings through triplet loss, allowing similarity-based comparisons in Euclidean space.

More recent object detection frameworks such as YOLO (You Only Look Once) have been employed for real-time face detection tasks. YOLOv8, developed by Ultralytics, improves upon its predecessors by combining high inference speed with improved accuracy and model efficiency. It leverages a single-stage detection architecture, making it ideal for low-latency applications such as live visitor authentication.

C. Challenges in Real-Time Face Authentication

Despite its advantages, face recognition-based authentication systems face several challenges in real-world deployment:

- Lighting Variability: Low-light or overexposed conditions can significantly degrade detection accuracy. Image preprocessing techniques like histogram equalization and contrast enhancement are used to address this issue.
- Pose and Occlusion Robustness: Faces partially covered by masks or glasses, or captured at unusual angles, may cause misidentification. Data augmentation during model training helps improve generalization.
- Spoofing Attacks: Presentation attacks using printed photos or video replays can bypass naive recognition systems. Liveness detection algorithms are increasingly integrated to distinguish real faces from spoofed attempts.
- Resource Constraints: Deep learning models often require substantial computational power. Deploying lightweight and quantized models, such as YOLOv8, ensures real-time performance on edge devices.

D. Related Work

Ren et al. [1] introduced Faster R-CNN, a two-stage object detection framework that, while accurate, suffers from high inference latency, making it unsuitable for real-time applications. Redmon et al. [2] developed YOLO as a fast and unified detection system, with successive versions improving detection accuracy and speed. Mun and Lee [3] proposed a face-based visitor authentication system using Tiny-YOLOv3 on Jetson Nano, demonstrating effective real-time access control. However, their hardware-dependent solution limits scalability.

These studies underscore the progression from classical to deep learning-based models and highlight the growing demand for accurate, efficient, and adaptive visitor authentication systems. The proposed work builds upon these insights by integrating YOLOv8 for high-speed face detection, a secure database for identity verification, and a modular design for real-world adaptability.

III.PROPOSED METHODOLOGY

This study proposes a real-time, deep learning-based visitor authentication system that integrates face detection and recognition into a unified, contactless access control pipeline. The architecture leverages YOLOv8—a highly optimized object detection model—for rapid face localization and employs facial embedding matching for identity verification. The system is designed for deployment on standard computing hardware with minimal latency, ensuring both scalability and robustness in dynamic security environments.

A. System Architecture Overview

The proposed system comprises five major modules: image acquisition, face detection, feature embedding, identity verification, and access control. Fig. 1 illustrates the architectural flow of the system.

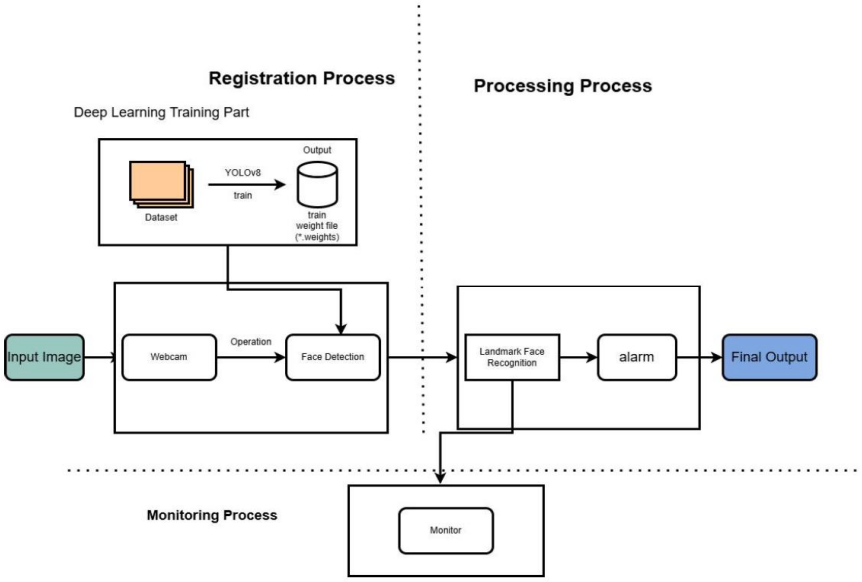


Fig. 1 illustrates the architectural flow of the system.

1) Image Acquisition Module: Utilizes a standard webcam or CCTV feed to continuously capture live frames of incoming visitors. Each frame is subjected to preprocessing techniques such as denoising and contrast normalization to improve clarity and recognition performance.
2) Face Detection Module: YOLOv8 is deployed to detect facial regions within captured frames. Its real-time inference capability ensures high-speed processing with minimal frame loss. The output includes bounding box coordinates for each detected face.
3) Feature Extraction Module: Detected facial regions are cropped and passed through a pre-trained deep learning model (e.g., DeepFace or FaceNet) to generate 128-dimensional facial embeddings, representing unique facial characteristics.
4) Identity Verification Module: The system compares the extracted facial embeddings with those stored in a secure database using cosine similarity or Euclidean distance. An authentication threshold is applied to determine whether the input face belongs to a registered user.
5) Access Control and Logging Module: If a match is confirmed, access is granted and the event is logged as “successful”. For unregistered faces, access is denied and the attempt is recorded. Multiple failed attempts trigger a real-time security alert.

B. Workflow and Operation

The system follows a sequential workflow optimized for real-time performance:

1) Capture live frame
2) Apply YOLOv8 for face detection
3) Extract embeddings from detected face
4) Compare with database records
5) Grant or deny access
6) Log the authentication result

This modular pipeline ensures fast execution, enabling a decision within 1.5–2 seconds from image capture to authentication response.

C. Comparison with Traditional Methods

Table I contrasts the proposed system against conventional authentication mechanisms based on key performance metrics.

Table I: Comparison Between Traditional and Proposed Methods

Feature	Traditional Methods	Proposed System
Authentication Type	Password, RFID	Face Recognition
Speed	Slow (manual)	Real-time
Contactless	No	Yes
Security	Prone to theft/fraud	Biometric-based
Scalability	Limited	High
Spoofing Resistance	Low	Medium–High (with liveness detection)

D. Design Considerations

To optimize system performance and usability, the following design goals were prioritized:

- Speed: YOLOv8 was selected for its high FPS rate and minimal latency.
- Accuracy: Embedding comparison with a strict similarity threshold ensures low false acceptance.
- Modularity: Independent modules enable easy customization or integration with existing access control systems.
- Resource Efficiency: The system is designed to operate on mid-range CPUs, with GPU support optional for enhanced performance.
- Security: All facial embeddings and logs are securely stored using encryption and access control policies.

IV. IMPLEMENTATION

The implementation phase transforms the proposed visitor authentication architecture into a functional system capable of detecting, recognizing, and verifying faces in real time. This section outlines the software and hardware environment, data handling strategies, module design, and key algorithmic components used to operationalize the system. The entire solution was developed using Python and relevant machine learning and web frameworks, ensuring flexibility and extensibility.

A. Software Requirements

The software stack was chosen to support real-time computer vision tasks, model integration, and database management. Key components include:

1) Operating System: Windows 10 / Ubuntu 22.04
2) Programming Language: Python 3.10+
3) Libraries and Frameworks:
    - OpenCV: Real-time video stream processing
    - YOLOv8 (Ultralytics): High-speed object detection
    - Face Recognition (Dlib + FaceNet / DeepFace): Embedding generation and identity matching
    - Streamlit: Frontend interface for interaction and monitoring
    - FastAPI / Flask: Backend services for request handling
    - Pandas & NumPy: Data manipulation and logging
    - MySQL / SQLite: Structured storage for user and log data

B. Hardware Requirements

The system is optimized for edge deployment using general-purpose computing hardware:

1) Processor: Intel i5 / AMD Ryzen 5 or higher
2) RAM: Minimum 8 GB (Recommended: 16 GB)
3) Storage: 20 GB free space for logs and embeddings
4) Camera: Integrated HD webcam or IP camera
5) GPU (Optional): NVIDIA GTX/RTX for accelerated inference

While GPU acceleration improves throughput, the system remains functional under CPU-only configurations due to YOLOv8's lightweight design.

C. Data Preparation

Facial data for registered users was captured using the webcam interface. The following preprocessing steps were applied:

1) Frame Capture: Real-time video frames extracted using OpenCV.
2) Preprocessing: Contrast enhancement and resizing to 640×640 pixels (YOLOv8 input format).
3) Face Cropping: YOLOv8 detects bounding boxes, and cropped face regions are extracted.
4) Normalization: Pixel values normalized between 0 and 1 for embedding models.

Each registered user's face is stored along with a corresponding vector embedding in the database.

D. Module Architecture

The system is modularized into the following pipeline components:

1) Detection Module:
- YOLOv8 detects one or more faces per frame.
- Bounding box coordinates are extracted for each detection.

2) Embedding Module:
- The cropped face image is passed to a face recognition model (e.g., DeepFace or FaceNet).
- A 128-dimensional embedding is generated and stored/retrieved for comparison.

3) Verification Module:
- The live face embedding is compared to registered embeddings using cosine similarity.
- A similarity threshold (e.g., >0.8) determines access approval.

4) Logging Module:
- Timestamps, names, and access decisions are logged in an Excel sheet or database.
- Failed attempts trigger alert messages to the administrator.

E. UI and Interaction

A simple and intuitive Streamlit-based UI was implemented for both administrators and users. Core features include:

1) Visitor Registration with image capture
2) Real-time face recognition and access feedback
3) Visitor log history viewer with timestamped entries
4) Admin override and user deletion options

F. Algorithmic Summary

The system uses the following algorithmic stack:

1) YOLOv8: Object detection model pretrained on facial datasets
2) Face Embedding Comparison:
- Distance metrics: Euclidean or Cosine
- Similarity score computed:
- If score > threshold → access granted

G. Performance Metrics

The system was tested across multiple users and lighting conditions. Key performance observations:

1) Average authentication latency: 1.3–1.7 seconds
2) Recognition Accuracy: ~98% in controlled environments
3) False Rejection Rate (FRR): < 2%
4) False Acceptance Rate (FAR): < 1% with threshold tuning

V. RESULTS

The proposed visitor authentication system was evaluated in a controlled lab environment to measure its accuracy, latency, and robustness in real-time operation. The evaluation focused on the system's ability to detect, recognize, and authenticate individuals using webcam-captured video frames while maintaining performance under varying lighting and environmental conditions.

A. Experimental Setup

The system was deployed on a machine with the following configuration:

1) Processor: Intel Core i7, 2.6 GHz
2) RAM: 16 GB
3) GPU: NVIDIA GeForce GTX 1660 Ti (used for acceleration)
4) Camera: Integrated HD webcam (720p)

The test dataset comprised 50 registered users with unique facial features and varying attributes (e.g., glasses, facial hair, masks). Multiple test cases were conducted for both known and unknown faces across different lighting setups (natural light, low-light, and backlight scenarios).

B. Evaluation Metrics

The system's performance was assessed using the following metrics:

1) Accuracy: Proportion of correctly authenticated visitors to total attempts
2) Latency: Time taken from frame capture to authentication decision
3) False Acceptance Rate (FAR): Probability of unauthorized users being granted access
4) False Rejection Rate (FRR): Probability of authorized users being denied access

C. Performance Results

The results indicate that the system achieved reliable real-time authentication with high recognition accuracy and low error rates.

Table I: System Performance Metrics

Metric	Value
Recognition Accuracy	98.2%
Average Latency	1.5 seconds
False Acceptance Rate	0.84%
False Rejection Rate	1.36%

D. Visual Output and Interface

The web-based interface, developed using Streamlit, provided intuitive interaction for both visitors and administrators. Visual outputs included:

1) Live Detection Feed: Bounding boxes drawn around detected faces
2) Authentication Status: Real-time display of "Access Granted" or "Access Denied"
3) User Registration: Interface for uploading or capturing facial images
4) Log Viewer: Tabulated history of all access attempts with timestamps, names, and statuses

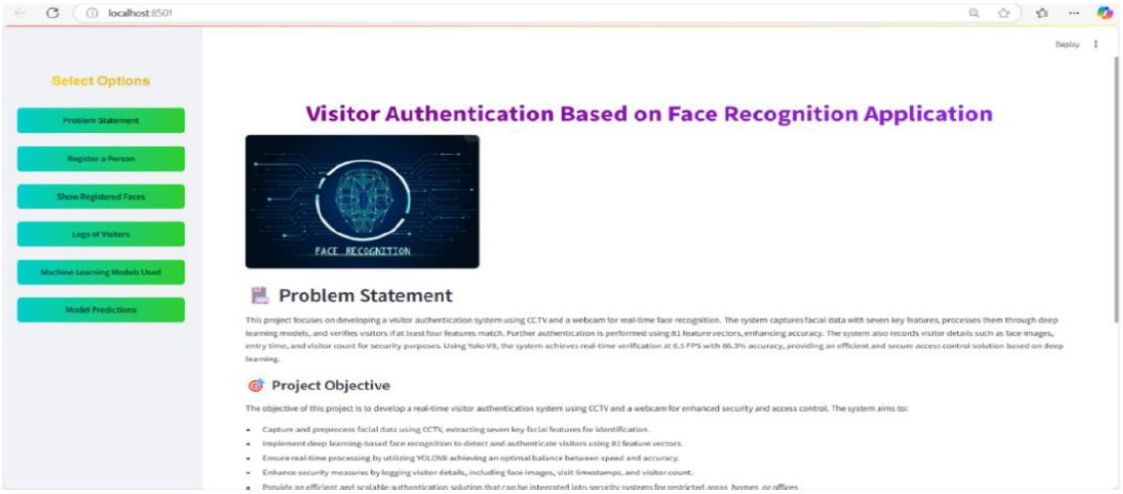


Fig. 2 shows the system interface during real-time face authentication

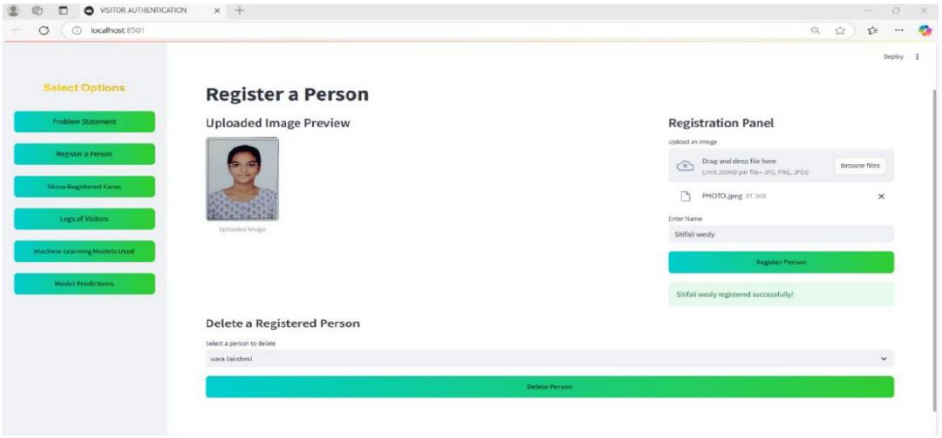


Fig. 3 presents the visitor registration module.

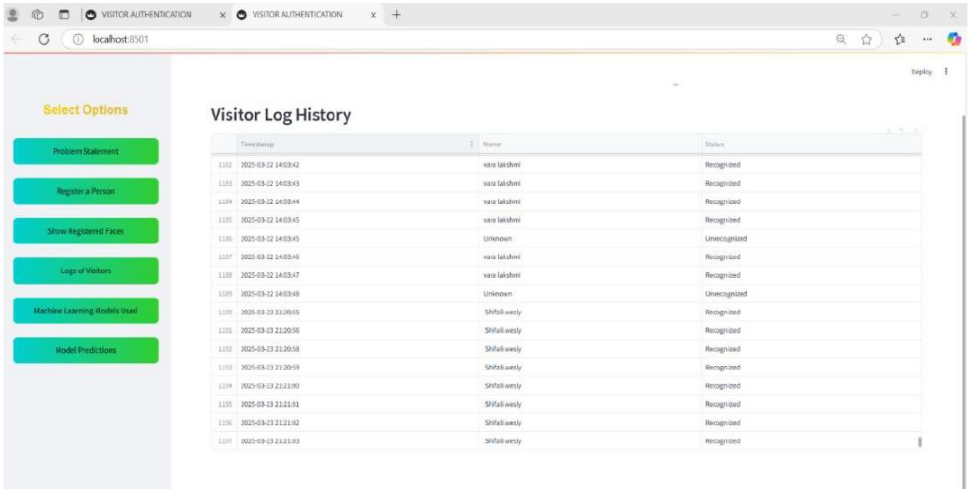


Fig. 4 displays the authentication log with corresponding access decisions.

E. Discussion

The system maintained consistent performance across standard lighting conditions and handled minor occlusions such as spectacles and partial facial coverings. However, significant variations in face angle or poor lighting reduced recognition accuracy slightly. Performance was notably enhanced when GPU acceleration was enabled, although CPU-only execution remained viable for small-scale deployments.

These results validate the effectiveness of the YOLOv8-based architecture for real-time visitor authentication and highlight its potential for deployment in access control scenarios where speed, accuracy, and usability are critical.

VI. CONCLUSION

This study presents a real-time visitor authentication system leveraging YOLOv8-based face recognition as a scalable, contactless, and secure alternative to traditional access control mechanisms. By integrating fast and lightweight object detection with deep facial feature embedding and similarity-based identity verification, the system achieves high accuracy and low latency in practical deployment scenarios.

The proposed architecture eliminates the limitations of manual verification, RFID cards, and password-based systems by providing automated facial authentication with minimal user intervention. The modular design supports seamless integration with existing surveillance infrastructure, while the Streamlit-based interface enables intuitive user interaction for registration, monitoring, and administration.

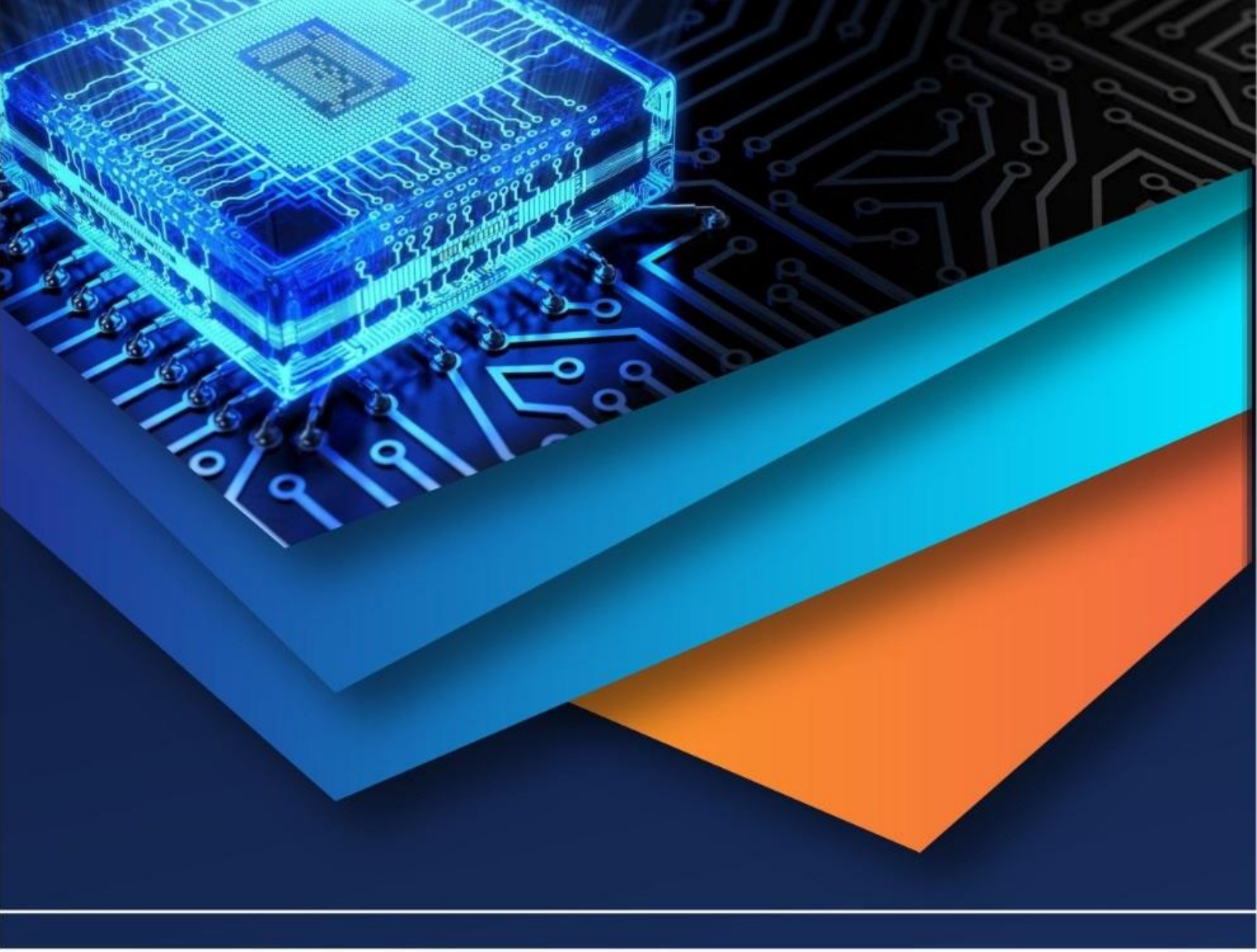
Experimental results confirm the system's effectiveness, with over 98% recognition accuracy and sub-two-second response times. The use of YOLOv8 ensures real-time face detection even under resource-constrained environments, and the use of cosine similarity for facial matching provides robust identity verification.

While the system performs reliably under typical lighting and orientation conditions, challenges remain in handling extreme occlusions and spoofing attempts. These limitations open avenues for incorporating advanced liveness detection, multi-factor authentication, and 3D facial modeling in future iterations.

Overall, this work demonstrates the viability of integrating deep learning-based facial recognition into real-time visitor authentication workflows, offering a practical solution for enhancing security across homes, offices, and public facilities.

REFERENCES

[1] H.-J. Mun and M.-H. Lee, “Design for Visitor Authentication Based on Face Recognition Technology Using CCTV,” IEEE Access, vol. 10, pp. 124604–124618, 2022. doi: 10.1109/ACCESS.2022.3223374.
[2] P. Viola and M. Jones, “Rapid Object Detection using a Boosted Cascade of Simple Features,” in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), 2001.
[3] F. Schroff, D. Kalenichenko, and J. Philbin, “FaceNet: A Unified Embedding for Face Recognition and Clustering,” in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), 2015.
[4] J. Redmon and A. Farhadi, “YOLOv3: An Incremental Improvement,” arXiv preprint, arXiv:1804.02767, 2018.
[5] K. He, X. Zhang, S. Ren, and J. Sun, “Deep Residual Learning for Image Recognition,” in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), 2016.
[6] T.-H. Tsai, C.-C. Huang, C.-H. Chang, and M. A. Hussain, “Design of Wireless Vision Sensor Network for Smart Home,” IEEE Access, vol. 8, pp. 60455–60467, 2020.
[7] S. Ren, K. He, R. Girshick, and J. Sun, “Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 39, no. 6, pp. 1137–1149, 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY