SMART COLLEGE SECURITY:AI-POWERED ID CARD VIOLATION AND FACE RECOGNITION SYSTEM

Adinath Manoj, Alka Tomy Karayil, Athira Thomas, Vismaya Subash

Adinath Manoj Student, Computer Science and Engineering, Holy Grace Academy of Engineering, Kerala, India

Alka Tomy Karayil Student, Computer Science and Engineering, Holy Grace Academy of Engineering, Kerala, India

Athira Thomas Student, Computer Science and Engineering, Holy Grace Academy of Engineering, Kerala, India

Vismaya Subash Student, Computer Science and Engineering, Holy Grace Academy of Engineering, Kerala, India

Vishnupriya E V *Assistant Professor, Computer Science and Engineering, Holy Grace Academy of Engineering, Kerala, India*

Sanam E Anto Head of Department, Computer Science and Engineering, Holy Grace Academy of Engineering, Kerala, India

ABSTRACT

Ensuring effective security within educational institutions remains a critical challenge due to the increasing risks of unauthorized access and identity misuse. Conventional security mechanisms, primarily based on manual verification of identification cards, are often inefficient, time-consuming, and susceptible to human error. This paper presents a Smart College Security System that integrates Artificial Intelligence (AI)-based face recognition with ID card verification to enhance campus security and access control.

The proposed system employs computer vision techniques to capture and analyze facial images of individuals at entry points. Extracted facial features are processed using machine learning algorithms and compared against a pre-existing database for identification. In parallel, the system verifies the associated identification card to ensure authenticity and ownership. Access is granted only when both facial recognition and ID verification are successfully validated; otherwise, the system flags the instance as a violation and triggers appropriate alerts.

The integration of AI enables real-time processing, improved accuracy, and adaptability to varying environmental conditions such as illumination and facial variations. The system significantly reduces dependency on manual supervision while minimizing the risks associated with identity fraud and unauthorized access. Furthermore, it provides a scalable and efficient solution applicable to various domains, including educational institutions, corporate environments, and secure facilities.

Experimental considerations indicate that the proposed system enhances operational efficiency and security reliability; however, challenges such as data privacy, system robustness under diverse conditions, and database management must be addressed for effective deployment. Overall, the system demonstrates the potential of combining biometric identification with intelligent verification mechanisms to establish a secure and automated access control framework

Keywords : *Artificial Intelligence, Face Recognition, Biometric Authentication, ID Card Verification, Computer Vision, Machine Learning, Smart Security System, Access Control, Campus Surveillance.*

1. INTRODUCTION

In the modern era, ensuring safety and maintaining controlled access within educational institutions has become a critical concern. Colleges and universities accommodate a large number of students, faculty members, and visitors on a daily basis, making security management a complex and demanding task. Traditional security methods, such as manual verification of identity cards by security personnel, are still widely practiced. However, these methods are often slow, inefficient, and highly dependent on human judgment. As a result, they are prone to errors, which can lead to unauthorized entry, misuse of identity cards, and difficulty in maintaining accurate records of individuals moving in and out of the campus.

With the continuous advancement of technology, modern solutions based on Artificial Intelligence (AI) and computer vision have gained significant importance in addressing these challenges. AI enables systems to analyze data, learn patterns, and make decisions with minimal human intervention. In this context, face recognition technology has emerged as a powerful biometric approach for identifying individuals based on their unique facial characteristics. Unlike traditional identification methods, face recognition is contactless, faster, and more reliable, making it suitable for real-time security applications. It eliminates the need for manual verification and reduces the chances of impersonation or identity fraud.

The proposed system in this project focuses on developing a Smart College Security System that combines AIbased face recognition with ID card verification. The system operates by capturing the facial image of a person through a camera placed at entry or exit points. The captured image is processed using machine learning algorithms and compared with a pre-existing database containing authorized user information. At the same time, the system verifies the identity card associated with the individual to ensure that it belongs to the same person. This dual verification mechanism enhances security by ensuring that both biometric and physical identification match before granting access.

One of the key advantages of this system is its ability to perform real-time monitoring and automatic decisionmaking. It significantly reduces the workload on security personnel while improving the accuracy and speed of the verification process. In case of any mismatch or unauthorized attempt, the system can instantly generate alerts, allowing authorities to take immediate action. Additionally, the system maintains digital records of entry and exit activities, which can be useful for tracking and analysis.

Furthermore, the proposed system is flexible and can be extended to various applications beyond basic access control. It can be used for automated attendance management, restricted area monitoring, and visitor tracking within the campus. The integration of AI with biometric identification not only strengthens security but also enhances overall operational efficiency.

In conclusion, the adoption of intelligent technologies such as face recognition and AI-based verification systems represents a significant step toward modernizing campus security. By replacing traditional manual methods with automated and accurate systems, institutions can ensure a safer and more controlled environment. This project demonstrates the potential of advanced technologies in improving security infrastructure and highlights the importance of adopting innovative solutions in educational institutions.

2. INFORMATION

End-to-End Object Detection with Transformers (DETR) [1]: proposes a transformer-based detection framework that captures global relationships within images. While it simplifies the overall detection process, it requires extensive training time and shows weaker performance on smaller objects.

SSD: Single Shot MultiBox Detector [2]: applies a convolutional neural network with multi-scale feature extraction for object detection. It offers faster detection speed, although its accuracy is lower when identifying small objects.

Real-Time Flying Object Detection with YOLOv8 (2023) utilizes transfer learning to enhance detection of small and dynamically moving objects. It delivers high accuracy and real-time results but depends on high-performance GPU resources.

Focal Loss for Dense Object Detection (2017) introduces a mechanism that reduces the influence of easily classified samples during training. This improves detection precision but increases computational requirements.

Swin Transformer (2021) employs shifted window-based attention to capture both local and global image features efficiently. Although it reduces computational complexity, it involves a sophisticated design and demands more resources.

Real-time Information Retrieval from Identity Cards (2020) combines image processing techniques with deep learning to extract data from identity cards. It improves recognition performance but may face delays in real-time scenarios. OpenFace 3.0 (2025) presents a lightweight framework for analyzing facial expressions and behavior using multiple integrated models. It performs efficiently in real-time applications but may not achieve the accuracy of larger systems. DeepFace (2017) uses deep learning approaches to analyze and generate facial representations. It provides strong performance but is sensitive to imbalanced datasets.

A Survey of Face Recognition (2022) reviews deep learning-based face recognition techniques, particularly focusing on embedding methods. It highlights improved accuracy while also discussing challenges in training using triplet loss functions.

Automated ID Card Detection using YOLOv5 (2025) implements real-time video analysis to detect ID cards and verify identities automatically. It enhances automation but may experience reduced accuracy in poor lighting conditions.

Presentation Attack Detection on ID Cards (2024) analyzes different techniques for identifying fraudulent ID cards. It provides a structured evaluation approach but is limited by insufficient training data.

Open-Set ID Card Attack Detection (2023) applies GAN-based methods to generate and identify fake ID cards. While it enhances detection capabilities, the generated data may not always be realistic.

Synthetic ID Card Generation (2022) uses generative models to create artificial ID datasets for training purposes. This reduces reliance on real data but can introduce inaccuracies due to unrealistic samples.

Feature Pyramid Networks (2017) combine features from different layers of a neural network to improve object detection. This enhances accuracy but may still struggle with very small objects.

ByteTrack (2022) improves object tracking by associating detection boxes across frames effectively. It increases tracking consistency but requires proper tuning of parameters.

Second Competition on ID Card Detection (2025) evaluates various models for detecting fake identity cards using benchmark datasets. It supports research advancement but requires extensive data and computational resources.

YOLOv9 (2024) introduces programmable gradient learning to improve the training process of object detection models. It enhances performance and efficiency but relies on powerful hardware.

Fake Face Detection using Stegoface (2022) applies steganography techniques to detect manipulated facial data. It strengthens identity verification but increases system complexity.

ArcFace (2018) introduces an angular margin loss function to improve facial recognition accuracy. It enhances feature separation but depends heavily on large-scale datasets.

EdgeFace (2024) focuses on efficient face recognition for edge devices with limited resources. It reduces computational load but may compromise accuracy under certain conditions.

TrackFormer (2021) integrates object detection and tracking using transformer-based architecture. It simplifies tracking pipelines but requires high computational power.

Facial Recognition in Low-Light (2018) uses image enhancement methods to improve recognition under poor lighting conditions. It increases reliability but still faces challenges in extreme lighting environments.

FaceNet (2015) maps facial images into a compact embedding space for accurate recognition and clustering. It achieves high accuracy but demands large datasets and long training durations.

Forged ID Detection using MobileNetV2 (2023) employs deep learning models to identify fake ID cards in real time. It performs effectively but depends on the availability of large datasets.

Pixel-wise Supervision for ID Detection (2022) uses fine-grained feature extraction techniques for detecting fake identity cards. It improves detection accuracy but has limited ability to generalize across datasets.

3. CONCLUSION

The development of a Smart College Security System using Artificial Intelligence-based face recognition and ID card verification provides an effective and modern solution to the growing security challenges faced by educational institutions. Traditional methods of security management, which rely heavily on manual verification processes, are often inefficient, time-consuming, and susceptible to human error. These limitations can lead to unauthorized access, identity misuse, and difficulty in maintaining proper records. The proposed system addresses these issues by introducing an automated and intelligent approach to identity verification and access control.

By integrating face recognition technology with ID card validation, the system ensures a higher level of accuracy and reliability in identifying individuals. The use of biometric features, which are unique to each person, significantly reduces the possibility of identity fraud. The dual verification mechanism strengthens the overall security framework by confirming both the physical identity and the associated credentials of an individual before granting access. This approach not only enhances security but also minimizes the dependency on human intervention.

Another important advantage of the system is its ability to operate in real time. The system can quickly capture and process facial data, compare it with stored records, and make instant decisions regarding access permission. In cases where mismatches or suspicious activities are detected, alerts can be generated immediately, allowing authorities to take prompt action. This real-time monitoring capability improves the responsiveness and effectiveness of the security system.

In addition to improving security, the proposed system contributes to better management and operational efficiency within the campus. It maintains accurate digital records of entry and exit activities, which can be used for monitoring, analysis, and future reference. The system can also be extended to support additional functionalities such as automated attendance tracking, restricted area control, and visitor management, making it a versatile solution for institutional needs.

Despite its advantages, certain challenges must be considered for successful implementation. Factors such as variations in lighting conditions, changes in facial appearance, and data privacy concerns can affect system performance. Proper measures, including secure data storage, regular system updates, and the use of advanced algorithms, are necessary to overcome these challenges and ensure reliable operation.

In conclusion, the Smart College Security System demonstrates how the integration of Artificial Intelligence and biometric technologies can significantly improve campus safety and management. It offers a fast, accurate, and efficient alternative to traditional security methods, while also providing scalability for future enhancements. The adoption of such intelligent systems can play a crucial role in creating a secure and well-organized environment for students, staff, and visitors

4.References

[1] Liu, W., Anguelov, D., Erhan, D., Szegedy,C.,Reed,S.,Fu,C.Y.,andBerg,A.C.,"SSD: Single Shot MultiBox Detector,"European Conference on Computer Vision (ECCV), 2016.

[2] Carion, N., Massa, F., Synnaeve, G., Usunier, N., Kirillov, A., and Zagoruyko, S., "End-to-End Object Detection with Transformers (DETR)," European Conference on Computer Vision (ECCV), 2020.

[3] Lin, T. Y., Goyal, P., Girshick, R., He, K., and Dollár, P., "Focal Loss for Dense Object Detection," IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), 2017

[4] Wang, C. Y., Bochkovskiy, A., and Liao, H. Y. M., "Real-Time Flying Object Detection with YOLOv8," arXiv preprint arXiv:2304.14564, 2023.

[5] Chingovska, I., Anjos, A., and Marcel, S., "Pixel-wise Supervision for Presentation Attack Detection on Identity Document Cards," IEEE Access, 2022.

[6] Deng, J., Guo, J., Niannan, X., and Zafeiriou, S., "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018.

[7] Liu, Z., Lin, Y., Cao, Y., Hu, H., Wei, Y., Zhang, Z., Lin, S., and Guo, B., "Swin Transformer: Hierarchical Vision Transformer using Shifted Windows," IEEE International Conference on Computer Vision (ICCV), 2021.

[8] Shafique, K., and Anwar, S., "Real-time Information Retrieval from Identity Cards," IEEE International Conference on Image Processing (ICIP), 2020.

[9] Baltrušaitis, T., Robinson, P., and Morency, L. P., "OpenFace 3.0: A Lightweight Multitask System for Comprehensive Facial Behavior Analysis," IEEE Conference on Automatic Face and Gesture Recognition (FG), 2025.

[10] Cole, F., and Genova, K., "DeepFace: Face Generation using Deep Learning," IEEE International Conference on Computer Vision Workshops (ICCVW), 2017.

[11] Schroff, F., Kalenichenko, D., and Philbin, J., "FaceNet: A Unified Embedding for Face Recognition and Clustering," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015.

[12] Xu, L., Yang, Y., and Zhao, S., "EdgeFace: Efficient Face Recognition Model for Edge Devices," IEEE Internet of Things Journal, 2024.

[13] Li, Y., and Zhao, R., "A Survey of Face Recognition," Journal of Visual Communication and Image Representation, 2022.

[14] Thomas, A., and Priya, V., "Automated ID Card Detection and Penalty System Using YOLOv5 and Face Recognition," International Journal of Computer Applications, 2025.

[15] Santos, D., and Patel, S., "First Competition on Presentation Attack Detection on ID Card," Proceedings of the International Conference on Biometrics (ICB), 2024.

[16] Wang, X., and Chen, H., "Open-Set: ID Card Presentation Attack Detection Using Neural Transfer Style," Pattern Recognition Letters, 2024.

[17] Meinhardt, T., Kirillov, A., Leal-Taixé, L., and Feichtenhofer, C., "TrackFormer: Multi-Object Tracking with Transformers," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2022.

[18] Li, C., Zhang, Y., and Yang, J., "YOLOv9: Learning What You Want to Learn Using Programmable Gradient Information," arXiv preprint arXiv:2402.13616, 2024.

[19] Raj, R., and Singh, P., "Synthetic ID Card Image Generation for Improving Presentation Attack Detection," IEEE Access, 2023.

[20] Lin, T. Y., Dollár, P., Girshick, R., He, K., Hariharan, B., and Belongie, S., "Feature Pyramid Networks for Object Detection," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2017.

[21] Zhang, Y., Sun, P., Jiang, Y., Yu, D., Yuan, Z., Luo, P., Liu, W., and Wang, X., "ByteTrack: Multi-Object Tracking by Associating Every Detection Box," European Conference on Computer Vision (ECCV), 2022.

[22] Sharma, R., and Gupta, M., "Second Competition on Presentation Attack Detection on ID Card," International Conference on Biometrics (ICB), 2024.

[23] Elgamal, A., and Park, J., "Forged Presentation Attack Detection for ID Cards on Remote Verification Systems," IEEE Access, 2024.

[24] Li, K., Zhang, H., and Yu, X., "Enhancing Facial Recognition Accuracy in Low-Light Conditions Using Convolutional Neural Networks," Journal of Ambient Intelligence and Humanized Computing, 2024.

[25] George, S., and Mathew, J., "Fake Face Detection in Identity Cards Using Stegoface," International Journal of Advanced Computer Science and Applications (IJACSA), 2025