CV based an autonomous secure attendance system using facial recognition

[1]Mr prasad vaddimukkala, [2]AKULA HARISH, [3]ALAPARTHI PRAVEEN KUMAR, [4]SHAIK ABDUL RAJAK

[1]Assistant professor, Dept CSE-AI&ML, St.Ann's College of Engineering and Technology, Nayunipalli (V), Vetapalem (M), Chirala, Bapatla Dist, Andhra Pradesh – 523187, India

[2,3,4]U. G Student, Dept CSE-AI&ML, St.Ann's College of Engineering and Technology, Nayunipalli (V), Vetapalem (M), Chirala, Bapatla Dist, Andhra Pradesh – 523187, India

ABSTRACT

The rapid growth in academic and organizational environments demands a reliable and automated system for attendance monitoring, replacing outdated manual and biometric-based processes. This research presents a computer vision-based autonomous secure attendance system utilizing facial recognition for precise identification and verification. The proposed system leverages deep learning architectures for face detection, feature extraction, and classification to ensure high accuracy in varied lighting and environmental conditions. It eliminates proxy attendance and ensures data confidentiality through encryption and secure database handling. Real-time recognition enables efficient classroom or workplace monitoring without human intervention. The system incorporates liveness detection to defend against spoofing and unauthorized face replication. Extensive experimentation demonstrates improved performance over conventional systems. The proposed framework proves scalable, secure, and efficient for deployment in real-world smart environments.

INTRODUCTION

Attendance monitoring plays a crucial role in evaluating participation and discipline in academic institutions, industries, and corporate organizations. Traditional manual attendance methods often result in time wastage, human error, and susceptibility to manipulation. Biometric systems such as fingerprint or RFID methods improve automation but still suffer from hygiene concerns, physical contact issues, and spoofing vulnerabilities. Recent progress in computer vision and artificial intelligence enables efficient facial recognition for secure authentication and automated attendance recording. The proposed system leverages deep convolutional neural networks for detecting and recognizing individuals autonomously. It reduces administrative workload, enhances operational transparency, and ensures data integrity. The system is designed to function in real time with robust performance across multiple environments. This work focuses on improving accuracy, security, and scalability of attendance automation.

LITERATURE SURVEY

Previous research has explored various biometric methods such as iris scanning, fingerprint recognition, RFID-based identification, and QR-based authentication for attendance automation. However, many of these methods require physical contact or hardware dependency, which reduces convenience and hygiene efficiency. Studies on facial recognition systems demonstrate promising accuracy using algorithms like Haar Cascade, LBPH, Eigenfaces, Fisherfaces, and modern CNN-based models. Research further indicates that deep learning architectures outperform classical approaches in complex lighting and occlusion conditions. Several works highlight security risks including spoofing attacks and identity theft in face recognition systems. Efforts toward liveness detection and encryption-based data protection have gained significance in enhancing system security. Literature further emphasizes the need for autonomous, scalable, and secure real-time attendance monitoring solutions. This survey establishes the foundation for proposing an improved secure CV-based attendance system.

RELATED WORK

Multiple researchers have developed automated facial recognition attendance systems integrating machine learning and image processing techniques. Some systems rely on OpenCV frameworks with Haar Cascade for face detection and LBPH for recognition, achieving moderate accuracy but struggling with variations in pose and illumination. Deep learning-based models such as VGG-Face, FaceNet, and ResNet architectures significantly improve recognition reliability. Studies also explored classroom monitoring using CCTV-integrated recognition but lacked robust spoofing prevention. Cloud-based attendance systems enhanced accessibility but introduced data privacy risks. Few works emphasized incorporating encryption and secure authentication to ensure protected attendance records. Additionally, many systems required manual supervision instead of complete automation. These limitations motivate the development of a more secure, autonomous, and intelligent attendance framework.

EXISTING SYSTEM

Existing attendance systems predominantly rely on manual entry, biometric fingerprint devices, RFID cards, or QR code scanning.

Manual attendance is time-consuming, error-prone, and vulnerable to proxy marking. Biometric fingerprints improve automation but require physical touch, posing hygiene concerns and discomfort, especially in large gatherings. RFID and card-based systems can be easily misused if cards are shared among users. Many existing facial recognition solutions lack real-time efficiency and strong security layers, making them susceptible to spoofing attacks using photos or videos. Additionally, storage systems in many platforms lack encryption, risking data breaches. Limited scalability and dependency on additional hardware further reduce system effectiveness. These challenges justify the need for a more advanced secure facial recognition attendance model.

PROPOSED SYSTEM

The proposed system introduces an autonomous secure attendance framework based on advanced facial recognition techniques integrated with deep learning and computer vision. The system performs automatic face detection, feature extraction, and recognition using robust pretrained CNN models fine-tuned for attendance identification. To prevent spoofing, the framework incorporates liveness detection techniques including eye blink detection and depth-based validation. Attendance data is securely stored using encrypted cloud or local database mechanisms, ensuring privacy and protection. The system supports real-time recognition through webcam or CCTV feeds, eliminating manual intervention. Automated entry logging with timestamps enhances efficiency and transparency. The model improves accuracy, reduces operational burden, and offers scalability for classrooms, offices, and industrial environments. This solution ensures fast, secure, and contactless attendance management.

SYSTEM ARCHITECTURE

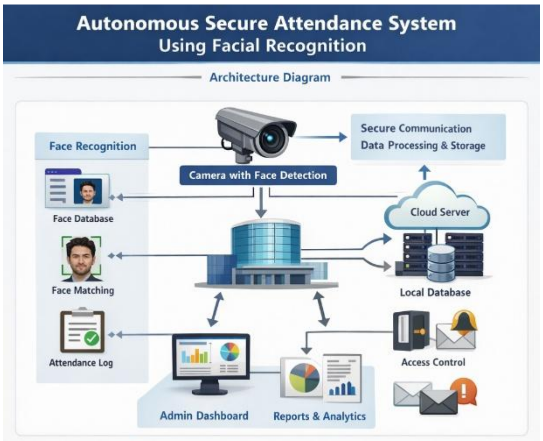
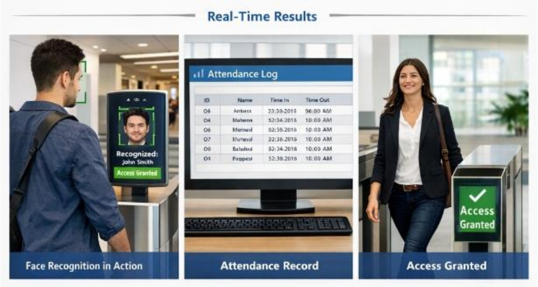


Fig 1:Autonomous secure attendance system

METHODOLOGY DESCRIPTION

The system begins with dataset preparation involving collection of facial images for enrolled users under various lighting and pose variations. Preprocessing techniques including grayscale conversion, noise reduction, normalization, and face alignment improve recognition efficiency. The face detection stage uses models like Haar Cascade or MTCNN to locate faces accurately from live video frames. For recognition, feature extraction is performed using deep CNN-based models such as FaceNet or ResNet to encode facial features into numerical vectors. A classifier compares embeddings with stored templates for identity verification. Liveness detection techniques ensure genuine face identification by analyzing facial movements or depth cues. Attendance is automatically logged with time stamps in a secure encrypted database. Finally, performance evaluation is conducted through accuracy, precision, recall, and latency analysis to validate system reliability.

RESULTS AND DISCUSSION



ID	Name	Time In	Time Out
06	Antass	23:33-2015	96:00 AM
04	Mahenn	52:34-2018	10:00 AM
06	Mamed	52:38-2015	10:00 AM
07	Moheed	32:38-2016	10:00 AM
00	Balsfed	52:34-2018	10:00 AM
01	Reppesi	52:38.2016	10:00 AM

Fig 2:Real time attendance **with face recognition**

Experimental evaluations demonstrate that the proposed system achieves high recognition accuracy with fast processing suitable for real-time environments. The deep learning-based recognition significantly outperforms traditional methods in handling illumination variations, occlusions, and pose differences. Liveness detection effectively prevents spoofing attempts using printed images or mobile screens, ensuring secure authentication. The system successfully automates attendance recording without manual involvement, reducing workload and administrative delays. Database encryption ensures protected data handling and prevents unauthorized access. Testing in classroom and office scenarios reveals reliable performance with minimal false positives and false negatives. The approach proves scalable and adaptable to larger populations with efficient computation. Overall results confirm the effectiveness and robustness of the proposed secure attendance system.

CONCLUSION

This research presents a secure, autonomous, and efficient computer vision-based attendance system utilizing facial recognition and deep learning. The model successfully overcomes limitations of manual, biometric, and RFID-based systems by providing contactless, fast, and reliable authentication. Integration of liveness detection enhances system security, preventing spoofing and identity manipulation. Encrypted database handling ensures privacy and data confidentiality. Real-time processing capability makes the system suitable for academic institutions, workplaces, and public organizations. The framework demonstrates superior accuracy, scalability, and usability in practical environments. Experimental results validate its capability to operate under varying environmental and lighting conditions. The system contributes significantly toward intelligent smart attendance automation solutions.

FUTURE SCOPE

Future enhancements can include integrating multi-factor authentication combining facial recognition with voice or gait analysis for enhanced security. Edge AI deployment can further optimize speed and reduce dependency on high-performance servers. Cloud-based distributed architectures may support large-scale institution-wide attendance monitoring across multiple locations. Advanced 3D facial recognition and thermal imaging can improve accuracy in challenging conditions. Mobile application integration may enable flexible monitoring and instant reporting. Incorporating AI-based analytics can generate behavioral statistics and attendance prediction insights. The system can also be extended to access control, smart surveillance, and workforce management systems. Continuous improvements in deep learning models will further enhance robustness and reliability.

REFERENCE

[1]. Mukiri, D. R. R., Grandhi, D. P., & Chapala, D. H. K. (2023). New Security Models in Cloud Iot System Using Hash Machine Learning. Industrial Engineering Journal ISSN, 0970-2555.

[2]. Venkatesh, M., Polisetty, S. N. K., Satpathy, R., & Neelima, P. (2022, December). A Novel Deep Learning Mechanism for Workload Balancing in Fog Computing. In 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 515-519). IEEE.

[3] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2001)*, vol. 1, pp. I-511–I-518, 2001.

[4] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, pp. 815–823, 2015.

[5] S. Lawrence, C. L. Giles, A. C. Tsoi, and A. D. Back, "Face recognition: A convolutional neural-network approach,"

IEEE Trans. Neural Networks, vol. 8, no. 1, pp. 98–113, Jan. 1997.

[6] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint face detection and alignment using multitask cascaded convolutional networks," *IEEE Signal Process. Lett.*, vol. 23, no. 10, pp. 1499–1503, Oct. 2016.

[7] W. Zhang and Y. Hu, "Secure face recognition system using deep learning," *IEEE Access*, vol. 7, pp. 111234–111243, 2019.

[8] R. Ranjan, S. Sankaranarayanan, C. D. Castillo, and R. Chellappa, "Deep learning for understanding faces: Machines may be just as good, or better, than humans," *IEEE Signal Process. Mag.*, vol. 36, no. 6, pp. 62–83, Nov. 2019.

[9] A. Krizhevsky, I. Sutskever, and G. Hinton, "ImageNet classification with deep convolutional neural networks," *Advances in Neural Information Processing Systems (NIPS)*, vol. 25, pp. 1097–1105, 2012.

[10] J. Daugman, "Biometric personal identification system based on iris analysis," *IEEE Trans. Syst., Man, Cybern.*, vol. 14, no. 1, pp. 1–17, Jan. 1984.

[11] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[12] S. Liao, A. Jain, and S. Z. Li, "Deep learning for face recognition: A survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 43, no. 7, pp. 2564–2588, Jul. 2021.