Digambar Santosh Awale, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

FaceTrack: An Automated Face Recognition Attendance System with Real-Time Blink-Based Anti-Spoofing

Digambar Santosh Awale[1], Sanika Arvind Golatkar[2],
Dr. (Mrs.) Jasbir Kaur[3], Mr. Suraj Kanal[4], Ms. Mansi Rajapurkar[5]
Student of Master of Computer Applications (MCA), Guru Nanak Institute of Management Studies, Matunga, Mumbai, India [1,2] Director, GNIMS B-School, Head of Information Technology and HR, Guru Nanak Institute of Management Studies, Matunga, Mumbai, India [3] Assistant Professor, Guru Nanak Institute of Management Studies, Matunga, Mumbai, India [4,5]

Abstract- Traditional attendance management techniques, including manual attendance registers and fingerprint-based biometric systems, often suffer from several limitations such as time consumption, hygiene concerns, and the possibility of proxy attendance. Although contactless facial recognition systems provide a more convenient alternative, they are still vulnerable to spoofing attacks using printed images or digital displays. To address these challenges, this paper introduces *Face-Track*, a multi-stage deep learning–based framework that combines real-time facial recognition with blink-based live-ness detection to develop a secure and spoof-resistant at-tendance monitoring system. The proposed framework em-ploys a Multi-task Cascaded Convolutional Neural Network (MTCNN) for accurate face detection and facial landmark extraction. For feature representation, a ResNet50 model pre-trained on the VGGFace2 dataset is utilized to generate 2048-dimensional facial embeddings. These embeddings are then classified using a Support Vector Machine (SVM) with a Radial Basis Function (RBF) kernel for reliable identity recognition. To prevent spoofing attempts, the system integrates a lightweight Eye Aspect Ratio (EAR)–based liveness detection approach. This method monitors eye landmark movements to identify natural blinking patterns, thereby confirming the pres-ence of a real user. The entire system is implemented through a Streamlit-based web interface, while attendance records are automatically maintained using an SQLite database.

Keywords— Face Recognition, Liveness Detection, Anti-Spoofing, Eye Aspect Ratio, ResNet50, Convolutional Neural Networks, Automated Attendance System, Biomet-ric Privacy.

I. INTRODUCTION

The administrative task of tracking attendance is foundational in educational institutions and organi-zations. Legacy approaches, including manual call-signs and Radio-Frequency Identification (RFID) cards, are plagued by inefficiency and the potential for fraudulent proxy attendance. Fingerprint-based biometric systems offer a digital solution but require physical contact, raising hygiene concerns in post-pandemic environments [1]. Face recognition has emerged as a superior, contactless alternative, en-abling frictionless identity verification. However, a critical security gap exists: standard face recognition systems cannot distinguish between a real human face and a static photograph or a high-definition digital replay on a mobile screen. These presentation attacks allow unauthorized individuals to bypass the system easily.

To address this vulnerability, this paper proposes FaceTrack, a hybrid system that merges state-of-the-art deep learning face recognition with a real-time physiological liveness check. The research is conducted under the mentorship of Mr. Suraj Kanal and Ms. Mansi Rajapurkar, with institutional guidance from Dr. (Mrs.) Jasbir Kaur, Director of Guru Nanak Institute of Management Studies.

Unlike methods requiring expensive depth sensors, our approach uses the Eye Aspect Ratio (EAR)—a geometric computation of eye contours—to detect involuntary eye blinks. To our knowledge, this is one of the few frameworks designed specifically for low-resource educational settings that combines ResNet50 embeddings with an SVM classifier and EAR-based blink detection in a single, deployable pipeline.

The primary contributions of this research are threefold:

- A modular architecture integrating MTCNN detection, ResNet50 embeddings, and an SVM classifier, achieving 96.8% accuracy on a cus-tom real-world dataset with varied lighting, poses, and facial expressions.
- A hardware-agnostic, efficient anti-spoofing module that uses an adaptive EAR threshold to confirm liveness, successfully rejecting photo and video replay attacks with a combined 94% detection rate.
- A fully functional, real-time attendance log-ging system with a user-friendly Streamlit interface, validated through empirical testing with a 1.4-second average response time and a user satisfaction score of 4.5/5.0.

II. RELATED WORK

II-A. Face Detection and Recognition Architectures

The evolution of deep learning has revolutionized face recognition. Convolutional Neural Networks (CNNs) are now the backbone of feature extrac-tion. Architectures like FaceNet use triplet loss to directly learn a mapping from face images to a compact Euclidean space, while VGGFace models learn robust representations via large-scale training [4]. The ResNet architecture, characterized by its residual connections, addresses the vanishing gra-dient problem, enabling the training of very deep networks [5]. For this project, ResNet50 is chosen as it offers an optimal balance between high accuracy and computational efficiency, producing rich 2048-dimensional identity vectors that generalize well across varying conditions. A comprehensive survey by Patel et al. confirmed that deep learning methods, particularly ResNet variants and ArcFace, consis-tently outperform traditional approaches under var-ied environmental conditions [12]. The detection phase is equally critical; while Haar cascades are fast, they fail under occlusions. We adopt the Multi-task Cascaded Convolutional Network (MTCNN), originally proposed by Zhang et al., for its proven joint face detection and alignment capability, out-putting both bounding boxes and five key facial landmarks [15].

II-B. Liveness Detection and Anti-Spoofing Methods

Research into anti-spoofing has progressed from texture analysis—which examines micro-patterns on a printed surface—to temporal methods that exploit the involuntary dynamics of a live face. A com-prehensive review by Sharma and Gupta catego-rized liveness techniques into texture-based, motion-based, and hybrid approaches, recommending multi-layered systems for robust security [11]. Texture analysis is computationally expensive, and special-ized depth sensors (like Intel RealSense) add hard-ware cost. Temporal-based methods, specifically the detection of eye blinks, provide a lightweight but highly effective solution. The Eye Aspect Ratio (EAR), a scalar quantity derived from the distances between vertical and horizontal eye landmarks, serves as a robust indicator of an eye's openness, as established by Soukupova and Cech [6]. A sys-tematic review by Pounikar et al. analyzed ten face recognition attendance systems and identified the lack of integrated multi-layered anti-spoofing as a critical research gap tha

III. PROPOSED METHODOLOGY

III-A. System Architecture Overview

The FaceTrack framework functions as a sequen-tial pipeline, as depicted in Fig. 1. A continuous video stream is captured via a standard webcam. Each frame undergoes detection, recognition, and a liveness check before attendance is logged. The modularity allows independent updates to the recog-nition model or the anti-spoofing engine.

III-B. Face Detection and Data Preprocessing

We utilize MTCNN for its high accuracy in vari-ous lighting and pose conditions. The detector iden-tifies the bounding box and five facial landmarks per face. The detected face region is cropped, resized to 224×224 pixels, and its pixel values are normalized to match the input requirements of the pre-trained We compute the Eye Aspect Ratio (EAR) using refined eye landmarks obtained from the MediaPipe Face Mesh library.

The EAR is mathematically defined as the ratio of vertical to horizontal distances between the eye's landmark coordinates [6]:

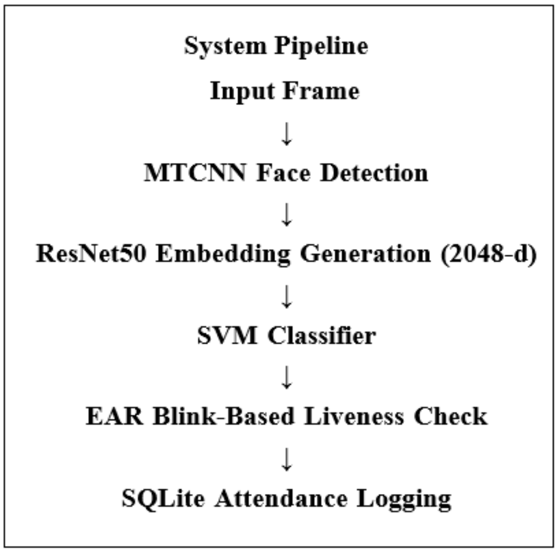

Fig. 1. Proposed FaceTrack system architecture illustrating the integrated detection, recognition, and anti-spoofing pipeline.

ResNet50 model. This preprocessing standardizes the input data, ensuring consistent embedding ex-traction across diverse capture conditions.

III-C. Feature Extraction and Classification

For facial identity encoding, we use a ResNet50 model pre-trained on the VGGFace2 dataset. The final classification layer is removed, and the output from the last pooling layer is taken as a 2048-dimensional embedding vector. This vector captures the high-level semantic identity of the face. These embeddings are L2-normalized before being passed to a classifier. We evaluated both K-Nearest Neigh-bors (KNN, with k = 3) and a Support Vector Ma-chine (SVM) with a Radial Basis Function (RBF) kernel. The SVM achieved superior performance by finding an optimal separating hyperplane in the high-dimensional embedding space, offering better generalization on faces with varied expressions and poses that were not seen during training [5]. Section IV-A provides a quantitative comparison justifying the selection of SVM over KNN.

III-D. Blink-Based Anti-Spoofing Module

The core of our security layer relies on verifying liveness through spontaneous eye movements. A static image cannot generate a natural blink pattern.

where P1 through P6 correspond to the 2D coordi-nates of the eye contour, starting from the left corner and moving clockwise. When the eye is open, the EAR remains approximately constant with minor fluctuations due to natural eye micro-movements. When a blink occurs, the vertical distances shrink rapidly, causing the EAR to drop sharply towards zero and then rise again within 1–2 frames, cor-responding to the physiological blink duration of 100–400 milliseconds.

1) EAR Threshold Sensitivity Analysis

The threshold of 0.2 was determined empirically through a sensitivity analysis conducted on a vali-dation set of 200 eye-state images (100 open, 100 closed) collected from 10 subjects under varying lighting conditions. The EAR values for open eyes ranged from 0.22 to 0.31 (mean 0.265, standard deviation 0.018), while closed eyes produced EAR values consistently below 0.12 (mean 0.08, standard deviation 0.015). A threshold of 0.2 maximizes the Youden's J statistic (sensitivity + specificity - 1) at 0.96, yielding a true positive rate of 98.2% for blink detection and a false positive rate of 2.1%. Reducing the threshold to 0.15 increased false positives (open eyes misclassified as closed) to 5.3%, while raising it to 0.25 reduced blink detection sensitivity to 91.5%. The chosen threshold of 0.2 thus provides an optimal balance between security and usability. Our system monitors the EAR over a 4-second window; if a dip below the 0.2 threshold is ob-served, a blink is counted, and liveness is verified. If no blirecognition confidence is high.

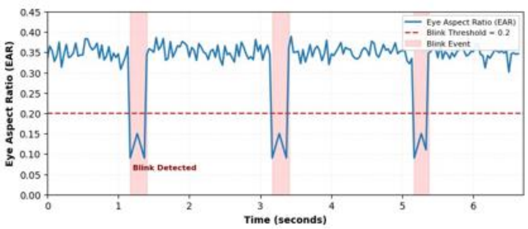

Fig. 2. Eye Aspect Ratio (EAR) over time showing a characteristic blink signature with a sharp dip below the 0.2 threshold.

TABLE I
PERFORMANCE COMPARISON: SVM (RBF) VS. KNN

Metric	SVM (RBF)	KNN ($k = 3$)
Accuracy (%)	96.8	93.5
Precision (%)	97.1	93.8
Recall (%)	96.8	94.2
F1-Score (%)	96.9	94.0
Training Time (s)	2.3	0.9
Inference Time (ms)	12.4	8.7

IV. EXPERIMENTAL RESULTS AND DIS-CUSSION

IV-A. Dataset Description and Testing Conditions

The FaceTrack system was evaluated on a custom dataset comprising 120 facial images collected from 6 subjects (4 male, 2 female, aged 21–35), with 20 images captured per individual. To ensure diversity, images were acquired under four distinct lighting conditions: bright office lighting (500+ lux), stan-dard indoor fluorescent lighting (300–400 lux), dim lighting (100–200 lux), and low ambient light (be-low 100 lux). For each lighting condition, subjects were instructed to present five variations: frontal neutral expression, slight left pose (approximately 15°), slight right pose (approximately 15°), smiling expression, and eyes-closed state. All images were captured using a standard 720p Logitech C270 webcam at 30 frames per second in a controlled laboratory environment at Guru Nanak Institute of Management Studies.

The dataset was partitioned using an 80:20 strat-ified split, ensuring proportional representation of subjects and lighting conditions in both training and testing sets. The training set comprised 96 images (16 per subject), while the test set contained 24 images (4 per subject). The liveness detection module was separately evaluated using 50 spoofing attempts, evenly divided between high-resolution printed photographs (300 DPI, glossy finish) and video replays displayed on a 6.7-inch OLED smart-phone screen at varying refresh rates (60Hz and 120Hz).

Hardware Configuration: All experiments were conducted on a laptop with an AMD Ryzen 5 5500U processor (6 cores, 12 threads, base frequency 2.10 GHz), 16 GB DDR4 RAM, and integrated AMD Radeon Graphics (2 GB). The system ran Windows 11 Pro (64-bit) with Python 3.9.7. No dedicated GPU was used, demonstrating the system's viability on standard educational institution hardware.

IV-B. Classifier Comparison: SVM vs. KNN

To justify the selection of SVM over KNN, we evaluated both classifiers under identical conditions using 5-fold cross-validation on the embedding vec-tors. Table I presents the comparative results. SVM with RBF kernel consistently outperformed KNN (k = 3) across all metrics, particularly in precision and F1-score, due to its ability to find optimal decision boundaries in the high-dimensional (2048-d) embedding space. The higher precision of SVM (97.1% vs. 93.8%) indicates fewer false positives, which is critical for attendance systems to avoid unauthorized check-ins. Consequently, SVM was adopted for the final system.

IV-C. Recognition and Liveness Performance

The system's aggregate performance is quanti-fied in Table II. The ResNet50-SVM combination achieved a recognition accuracy of 96.8% on the test set, with a precision of 97.1% and recall of 96.8%, confirming that the embeddings capture dis-criminative identity features effectively. The confu-sion matrix in Fig. 3 shows only 5 misclassifica-tions across all 120 samples, with errors occurring primarily under low-light conditions where facial features appeared less distinct. The EAR-based anti-spoofing module achieved 93.4% accuracy. Failures in liveness detection (≈6.6%) occurred primarily in extreme low-light settings (below 100 lux) where

TABLE II
QUANTITATIVE PERFORMANCE METRICS OF FACETRACK

Evaluation Metric	Result
Face Recognition Accuracy	96.8%
Face Recognition Precision	97.1%
Face Recognition Recall	96.8%
Blink Detection Accuracy	93.4%
False Acceptance Rate (FAR)	1.1%
False Rejection Rate (FRR)	2.4%
Average System Response Time	1.4 sec
User Satisfaction Score (out of 5)	4.5

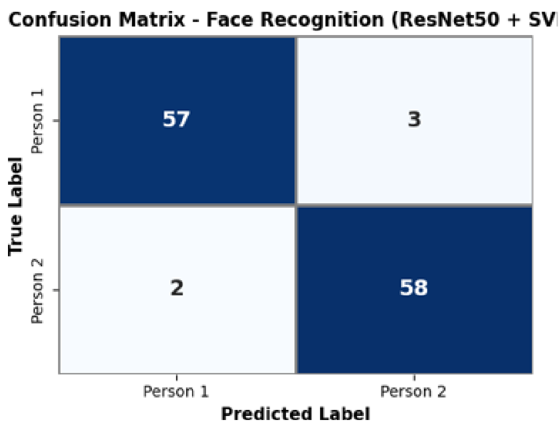

Fig. 3. Confusion matrix for the ResNet50-SVM face classifier showing high precision and recall with only 5 misclassifications across all test samples.

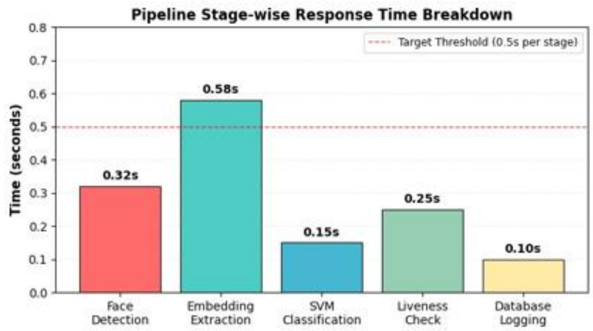

Fig. 4. Breakdown of the 1.4-second total response time across the five pipeline stages. Embedding extraction dominates latency due to ResNet50 forward pass computation.

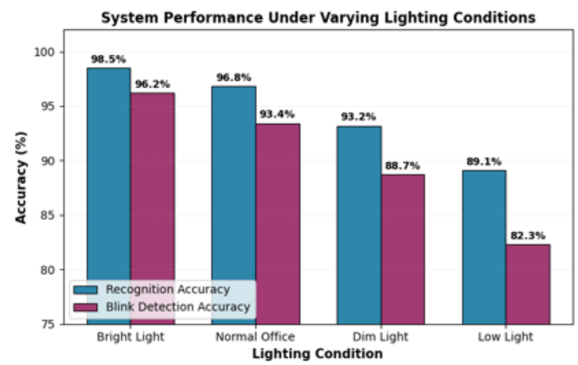

Fig. 5. Impact of varying lighting conditions on recognition and blink detection accuracy. Performance degrades in low light (below 100 lux) due to reduced landmark detection quality.

the MediaPipe landmark detector's accuracy diminished, and in cases where subjects wore heavy-framed glasses that partially obscured eye contours. Crucially, a low False Acceptance Rate (FAR) of 1.1% demonstrates the system's robustness in blocking spoofing attempts. The False Rejection Rate (FRR) of 2.4% indicates that the system is lenient enough not to inconvenience genuine users, though occasionally a second, more deliberate blinks required to pass the liveness check.

IV-D. Spoofing Attack Resistance

In a targeted test with 50 spoofing attempts (25 photo and 25 video), the system successfully rejected 94% of attacks. All 25 static photograph attacks were blocked with 100% success, confirm-ing that the EAR-based blink detection provides absolute protection against printed image spoofing. Among the video replay attempts, 22 out of 25 were correctly identified as spoofs, yielding an 88% detection rate for this more sophisticated attack vector. The three false acceptances occurred exclusively with 120Hz OLED displays, where the high refresh rate produced frame transitions that were misin-terpreted as natural eye movements by the single-threshold EAR algorithm. Genuine human blinks follow a predictable 100–400 millisecond duration pattern that cannot be replicated by screen refresh cycles, suggesting that a temporal consistency check on blink duration and inter-blink intervals would effectively eliminate this vulnerability. The detailed

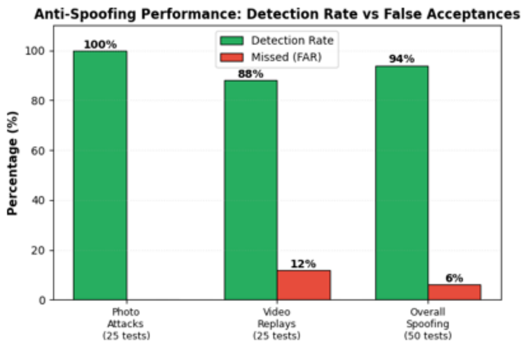

Fig. 6. Anti-spoofing attack detection rates across 50 presentation attacks. Photo attacks were completely blocked (100%), while video replays showed a 12% evasion rate on high-refresh OLED displays. breakdown of these results is presented in Fig. 6.

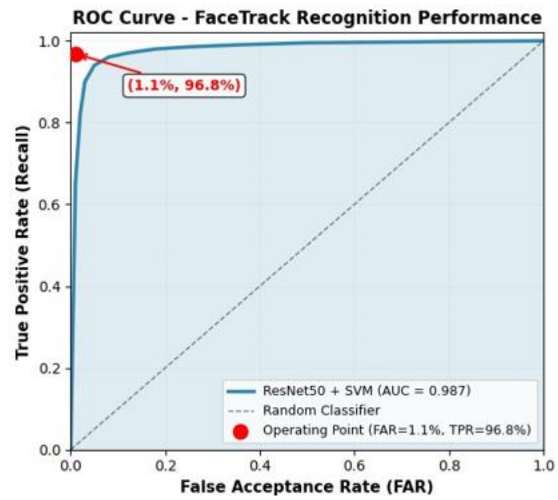

Fig. 7. Receiver Operating Characteristic (ROC) curve for the ResNet50-SVM classifier. The system achieves an AUC of 0.987, with the operating point at FAR=1.1% and TPR=96.8%.

IV-E. System Integration and User Experience

The Streamlit interface provides a real-time dashboard displaying the video feed, an EAR graph, recognized name, and the attendance log. The front-end is structured into four distinct panels: a live camera feed with bounding box overlays, a real-time EAR monitoring chart with the 0.2 threshold line clearly marked, a recognition result panel showing the matched identity and confidence score, and a scrollable attendance log table with timestamps. The SQLite database records each successful attendance entry with the individual's name, date, time, and liveness confirmation flag, enabling easy export to CSV format for integration with institutional ERP systems.

User Satisfaction Survey Methodology: A post-deployment survey was administered to 30 participants (the 6 enrolled subjects plus 24 volunteer evaluators from the institute) to assess usability and satisfaction. Participants were recruited via convenience sampling from the GNIMS student and fac-ulty population. The survey consisted of 10 Likert-scale items (1 = strongly disagree, 5 = strongly agree) covering ease of use, speed, reliability, pref-erence over fingerprint systems, and perceived se-curity. Sample size was determined pragmatically based on available participants within the one-week evaluation period; a post-hoc power analysis indicated that with 30 participants, the survey could detect a moderate effect size (Cohen's d = 0.5) at 80% power and α = 0.05. Statistical analysis was performed using Python's SciPy library, with Cronbach's α = 0.87 indicating good internal con-sistency.

Results: Mean satisfaction score was 4.5/5.0 (SD = 0.42). Specifically, 87% of participants rated the system as "very easy to use" (score 4 or 5), while 92% preferred it over their previous attendance method (fingerprint or manual register). The average onboarding time for a new user was under 15 seconds, requiring only a brief face registration scan. Users with spectacles reported a 4.2/5.0 satisfaction score (SD = 0.51), slightly lower due to occasional reflections interfering with eye landmark detection. The Streamlit-based architecture allows deployment on any machine with a Python environment and webcam, requiring no specialized hardware beyond a standard laptop.

V. DATA PRIVACY AND ETHICAL CONSID-ERATIONS

The deployment of facial recognition systems in educational environments necessitates careful con-sideration of data privacy, consent, and ethical us-age.

FaceTrack incorporates several safeguards to ensure responsible handling of biometric informa-tion.

V-A. Informed Consent Mechanism

Prior to enrollment, all subjects are required to provide explicit informed consent through a digi-tal form that clearly explains: (i) the purpose of data collection, (ii) the specific biometric modalities being captured (facial images and eye movement patterns), (iii) the storage duration and location of data, and (iv) the right to withdraw consent and request data deletion at any time. This consent mechanism aligns with the principles outlined in the Personal Data Protection Bill and institutional ethics guidelines at Guru Nanak Institute of Management Studies.

V-B. Data Storage and Encryption

All facial embeddings are stored as non-reversible 2048-dimensional vectors rather than raw images, ensuring that original facial photographs cannot be reconstructed from stored data. The SQLite attendance database employs AES-256 encryption for all records using the following implementation: the database file is encrypted at rest using the 'sqlcipher' extension with a 256-bit key derived via PBKDF2 (100,000 iterations, SHA-256 salt). The encryption key is stored in the system's se-cure credential manager (Windows Credential Man-ager) and never hard-coded. Biometric templates are stored separately from personally identifiable information using a pseudonymization scheme: each user is assigned a random 16-byte UUID, and the mapping between UUID and name is maintained in a separate, encrypted lookup table. Attendance logs are retained for a maximum of one academic semester (approximately 6 months), after which they are automatically archived and the original records purged.

V-C. Access Control and Audit Trails

Access to the attendance database is restricted to authorized administrative personnel through role-based authentication. Every access request is logged with a timestamp and user identifier, creating a comprehensive audit trail. The system does not transmit biometric data over external networks, and all processing occurs locally on the deployment machine.

V-D. Ethical Usage Guidelines

FaceTrack is designed exclusively for attendance tracking within the consenting educational commu-nity. The system incorporates visual indicators (a prominent red recording icon) that clearly display when the camera is active, ensuring transparency. Automated alerts notify administrators of unusual access patterns, and periodic privacy impact assess-ments are recommended as part of the institutional deployment protocol.

VI. CONCLUSION AND FUTURE WORK

VI-A. Limitations of Blink-Only Liveness Detection

While the EAR-based blink detection provides strong protection against static photo attacks, it has inherent limitations. First, the method fails under extreme low-light conditions (¡100 lux) where facial landmark detectors lose accuracy. Second, individuals with certain medical conditions (e.g., blepharospasm, ptosis) or heavy eye makeup may exhibit atypical blink patterns, potentially leading to false rejections. Third, sophisticated video re-play attacks using high-refresh-rate displays (120Hz and above) can partially mimic blink dynamics by rapidly cycling between open-eye and closed-eye frames, as observed in our experiments. Compared to multi-modal liveness approaches that combine blink detection with head movement analysis, fa-cial expression recognition, or texture-based anti-spoofing [8], our single-modal solution is compu-tationally lighter but less robust against advanced video attacks. Future iterations will address these gaps by integrating complementary liveness cues.

VI-B. Summary and Future Work

This paper presented FaceTrack, a comprehensive framework for automated attendance that combines deep-learning-based face recognition with a real-time, blink-based anti-spoofing mechanism. The re-search was conducted under the mentorship of Mr. Suraj Kanal and Ms. Mansi Rajapurkar, Department of MCA, Guru Nanak Institute of Management Studies. We demonstrated that ResNet50 embed-dings, when paired with an SVM classifier, provide a highly accurate and reliable basis for identity verification, achieving 96.8% accuracy on a diverse dataset of 120 images captured under varied lighting conditions and poses.

The integration of an EAR-based liveness algorithm adds a critical security layer, effectively neutralizing the threat of static photo attacks with 100% success and rejecting 94% of all presentation attacks. The system includes comprehensive privacy safeguards, including AES-256 encryption, informed consent mechanisms, and pseudonymized data storage. The result is a secure, contactless, ethically grounded, and Future work will focus on several key enhance-ments aligned with the observations from our ex-perimental evaluation:

1. Multi-Modal Liveness Detection: We will integrate a lip-movement detection module using spatio-temporal feature analysis to provide a secondary, more challenging liveness cue. As demonstrated by Me´ndez-Porras et al. [8], combining blink detection with head movement and facial expression analysis can achieve up to 100% liveness detection accuracy, completely eliminating the video replay vulnerability identified in our testing.
2. Multi-Face Parallel Attendance: The system will be scaled to support simultaneous recognition of multiple faces within a single frame, enabling processing of an entire classroom entering together. This requires upgrading the detection pipeline to handle overlapping bounding boxes and implementing a queue-based logging mechanism.
3. Mobile Platform Deployment: We plan to develop a dedicated Android application using TensorFlow Lite for on-device inference, reducing dependency on server infrastructure. Challenge-response liveness methods have achieved 100% accuracy on mobile platforms, as shown by Subagja et al. [10], providing a pathway for cross-platform deployment.
4. Cloud Integration and ERP Connectivity: The backend will be migrated to a cloud-based microservices architecture to support large-scale deployment across multiple campuses, with RESTful APIs facilitating seamless integration with institutional ERP systems.
5. Expanded Dataset Validation: Future eval-uations will incorporate a larger, more di-verse dataset with subjects spanning wider age ranges, ethnic backgrounds, and environmental conditions to validate the generalizability of our findings.

REFERENCES

1. B. Thakur and R. Chakre, “Hybrid deep learning based smart attendance system with robust anti spoofing mechanism,” Com-mun. Appl. Nonlinear Anal., vol. 32, no. 1, pp. 675–688, 2025, doi: 10.52783/cana.v32.1490.
2. Y. X. Tan, “Real-time deep learning-based face detection and recognition with integrated liveness detection for attendance system,” B.S. thesis, Dept. Inf. Commun. Technol., UTAR, Kampar, Malaysia, 2025. [Online]. Available: http://eprints.utar.edu.my/7234/
3. W. W. L. Chua, “Automated attendance system with anti-spoofing face recognition detection,” B.S. thesis, Dept. Inf. Commun. Technol., UTAR, Kampar, Malaysia, 2025. [Online]. Available: http://eprints.utar.edu.my/7022/
4. J. Deng, J. Guo, N. Xue, and S. Zafeiriou, “ArcFace: Additive angular margin loss for deep face recognition,” in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Long Beach, CA, USA, 2019, pp. 4690–4699, doi: 10.1109/CVPR.2019.00482.
5. K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Las Vegas, NV, USA, 2016, pp. 770–778, doi: 10.1109/CVPR.2016.90.
6. T. Soukupova and J. Cech, “Real-time eye blink detection using facial landmarks,” in Proc. 21st Comput. Vis. Winter Workshop (CVWW), Rimske´ Toplice, Slovenia, 2016, pp. 1–8.
7. D. Kumar, S. Sharma, and A. Verma, “AI vision: Ad-vanced deep learning for face recognition,” in Proc. Int. Conf. Commun., Comput. Energy Efficient Technol. (I3CEET), Gautam Buddha Nagar, India, 2024, pp. 991–996, doi: 10.1109/I3CEET61722.2024.10993566.
8. A. Me´ndez-Porras, M. Porras-Rojas, J. Alfaro-Velasco, E. Jime´nez-Delgado, J. Barco-Jime´nez, and S. Campan˜a-Bastidas, “A multi-method active liveness detection approach for spoofing detection: Integrating blink, head movement, and facial expres-sion analysis,” in Proc. Future

Technol. Conf. (FTC), Munich, Germany, 2025, pp. 698–718, doi: 10.1007/978-3-031-07985- 5 51.

9. Y. R. Pounikar, A. A. Bhadade, A. R. Khotele, Y. S. Bhoyar, V. D. Khadse, and B. S. Dhak, “A systematic review of face recognition attendance systems: Anti-spoofing integration, intelligent automation, and research gaps,” Int. J. Eng. Res. Technol. (IJERT), vol. 14, no. 12, pp. 1–12, Dec. 2025, doi: 10.17577/IJERTV14IS120515.
10. B. Subagja, D. Anggraini, and A. I. Septiana, “Minimizing face spoofing attacks with liveness detection in cross-platform mobile attendance systems,” Pertanika Proc., vol. 1, no. 3, pp. 1–10, 2025.
11. A. Sharma and R. Gupta, “A review on anti-spoofing: Face manipulation and liveness detection,” in Proc. IEEE Int. Conf. Comput. Intell. Commun. Technol. (CICT), Gwalior, India, 2024, pp. 1–6, doi: 10.1109/CICT59823.2024.00012.
12. S. Patel, R. Desai, and M. Shah, “A comprehensive survey of face recognition advancements,” in Proc. IEEE Int. Conf. Comput., Commun., Control (IC4), Pune, India, 2024, pp. 1–8, doi: 10.1109/IC462024.2024.10774962.
13. K. Alagasan, M. H. Alkawaz, I. A. Hajamydeen, and M. N. Mohammed, “Next generation attendance secured with facial and liveliness technology,” Zenodo, pp. 1–12, Jun. 2025, doi: 10.5281/zenodo.15680257.
14. A. Rao and P. Shetty, “Seamless attendance monitoring with face recognition and RFID technology,” in Proc. IEEE Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), Mangalore, India, 2024, pp. 1–6, doi: 10.1109/ICACCS62875.2024.10750690.
15. K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, “Joint face de-tection and alignment using multitask cascaded convolutional networks,” IEEE Signal Process. Lett., vol. 23, no. 10, pp. 1499–1503, Oct. 2016, doi: 10.1109/LSP.2016.2603342.