International Journal of IoT, Embedded Systems and Industrial Automation (IJIESIA)

July-September-Issue, Vol. 1, No. 2 (2026) | DOI: 10.66261/h211wr12

Article - e004

A COMPREHENSIVE REVIEW ON FACE RECOGNITION, ANTI-SPOOFING LIVENESS VERIFICATION AND AUTOMATED DRESS CODE ENFORCEMENT TECHNIQUES FOR SMART ATTENDANCE FRAMEWORK

Anurag Shandilya[1], Dr. Hare Ram Shah[2]

[1]Institute of Advance Computing, SAGE University, Indore, Madhya Pradesh
[2]Professor, Institute of Advance Computing, SAGE University, Indore, Madhya Pradesh

Received: 16/05/2026 **Revision Received**: 10/06/2026 **Accepted**: 27/06/2026

ABSTRACT

Smart attendance systems have emerged as an effective alternative to traditional attendance management approaches by leveraging advancements in artificial intelligence, computer vision, and deep learning. Face recognition technology enables contactless and automated identification of individuals, reducing manual effort and minimizing proxy attendance. However, the increasing deployment of facial recognition systems has exposed vulnerabilities to presentation attacks such as printed photographs, replay videos, and three-dimensional masks. To address these challenges, anti-spoofing liveness verification techniques have been integrated into attendance systems to ensure that only genuine users are authenticated. Simultaneously, educational institutions and organizations increasingly seek automated dress code monitoring solutions to enforce uniform policies and maintain discipline. Recent developments in object detection and image classification models have enabled real-time dress code compliance verification using surveillance cameras. This review paper presents a comprehensive analysis of face recognition, anti-spoofing liveness verification, and automated dress code enforcement techniques published between 2020 and 2026. The study examines major algorithms, datasets, performance metrics, implementation challenges, and deployment considerations. Furthermore, research gaps are identified, and a unified smart attendance framework is proposed that integrates identity verification, liveness detection, and dress code compliance monitoring into a secure and scalable solution. Existing literature indicates that while significant progress has been achieved in individual domains, fully integrated systems remain limited, creating opportunities for future research and development.

KEYWORDS: Smart Attendance System, Face Recognition, Face Anti-Spoofing, Liveness Detection, Dress Code Enforcement, Computer Vision, Deep Learning, YOLO, ArcFace, Attendance Automation

I. INTRODUCTION

Attendance management plays a crucial role in educational institutions, corporate organizations, and government agencies. Conventional attendance methods such as manual registers, RFID cards, and fingerprint-based systems often suffer from inefficiencies, proxy

July-September-Issue, Vol. 1, No. 2 (2026) | DOI: 10.66261/h211wr12

attendance, maintenance requirements, and hygiene concerns. Recent advances in artificial intelligence and computer vision have led to the development of face recognition-based attendance systems capable of identifying individuals automatically and recording attendance in real time.

Despite their advantages, face recognition systems remain susceptible to spoofing attacks, where unauthorized users attempt to bypass authentication using printed photographs, video replays, masks, or deepfake-generated images. Face Presentation Attack Detection (PAD), commonly known as face anti-spoofing, has therefore become a critical component of secure biometric systems. Modern anti-spoofing solutions employ texture analysis, motion detection, blink detection, depth estimation, and deep learning-based classification models to verify user authenticity.

Another challenge in educational institutions involves monitoring student compliance with prescribed dress codes and uniform regulations. Manual inspection consumes administrative resources and may introduce inconsistencies. Recent computer vision approaches based on YOLO, CNNs, and transfer learning have enabled automated dress code verification systems capable of detecting uniform violations in real time.

This review focuses on three interconnected technologies:

1. Face Recognition
2. Anti-Spoofing Liveness Verification
3. Automated Dress Code Enforcement

and explores their integration into a unified smart attendance framework.

II. RESEARCH WORK

Researchers have proposed various smart attendance solutions based on face recognition, liveness detection, and computer vision-based compliance monitoring. Some systems focus exclusively on facial identification, while others incorporate anti-spoofing mechanisms to prevent proxy attendance. Recent studies have also explored automated dress code verification using deep learning object detection frameworks.

A. Face Recognition Based Attendance Systems

Early attendance systems relied on traditional biometric methods such as fingerprints and RFID cards. With advances in deep learning, facial recognition became the preferred solution because of its contactless operation and scalability.

FaceNet introduced deep facial embeddings that enabled accurate identity matching. ArcFace further improved recognition accuracy through additive angular margin loss. DeepFace, VGGFace, and MobileFaceNet have also been widely adopted in educational attendance systems.

These methods reduce manual effort and eliminate many limitations of traditional attendance systems. However, challenges such as illumination variations, occlusions, pose variations, and facial spoofing remain significant concerns.

July-September-Issue, Vol. 1, No. 2 (2026) | DOI: 10.66261/h211wr12

Table 1. Face Recognition Based Attendance Systems

Paper	Model	Advantages	Limitations
Schroff et al.	FaceNet	High-Recognition accuracy	Large training dataset required
Deng et al.	ArcFace	State-of-the-art accuracy	High computational cost
Taigman et al.	DeepFace	Human-level performance	Resource intensive
Howard et al.	MobileFaceNet	Lightweight deployment	Slight accuracy reduction

B. Anti-Spoofing and Liveness Verification Techniques

Face recognition systems are vulnerable to presentation attacks such as printed photographs, replay videos, masks, and deepfakes.

To address these threats, researchers have developed liveness detection methods based on:
- Eye blink analysis
- Head movement tracking
- Texture-based analysis
- Depth estimation
- CNN-based presentation attack detection
- Transformer-based anti-spoofing

Modern anti-spoofing systems analyze facial texture, reflection characteristics, depth information, and physiological movements to distinguish genuine users from spoofing attempts.

Table 2. Anti-Spoofing Techniques

Paper	Technique	Advantages	Limitations
Ming et al.	Texture Analysis	Simple implementation	Sensitive to lighting
Zhang et al.	CNN-based PAD	High detection accuracy	Dataset dependency
Keresh et al.	Vision Transformer	Better generalization	High computation
Kong et al.	Multi-modal PAD	Improved robustness	Complex deployment

July-September-Issue, Vol. 1, No. 2 (2026) | DOI: 10.66261/h211wr12

C. Deep Learning Based Attendance Frameworks

Recent attendance systems combine multiple AI components to improve recognition performance.

Deep CNN models automatically learn facial features and outperform traditional machine learning approaches.

Transfer learning using ResNet, EfficientNet, and MobileNet reduces training requirements and improves deployment feasibility.

Hybrid architectures combining CNNs with attention mechanisms have demonstrated superior performance in large-scale attendance environments.

Table 3. Deep Learning Attendance Frameworks

Paper	Architecture	Contribution	Limitation
ArcFace Framework	Deep CNN	Robust embeddings	Computational complexity
MobileFaceNet	Lightweight CNN	Fast inference	Reduced feature richness
ResNet50 Attendance	Transfer Learning	Improved accuracy	Memory requirement
Hybrid CNN-Attention	Deep Hybrid Model	Better robustness	Longer training time

D. Automated Dress Code Enforcement Techniques

Dress code compliance is an important requirement in many educational institutions.
Computer vision techniques have enabled automated detection of:
• Uniform compliance
• Shirt color verification
• Tie detection
• ID card detection
• Safety equipment verification

YOLO-based object detection models have become the most popular solution because of their real-time performance.

July-September-Issue, Vol. 1, No. 2 (2026) | DOI: 10.66261/h211wr12

Transfer learning approaches using ResNet and EfficientNet further improve clothing classification accuracy.

Table 4. Dress Code Detection Techniques

Paper	Technique	Advantages	Limitations
YOLOv5 Uniform Detection	Object Detection	Real-time monitoring	GPU requirement
ResNet Clothing Classification	Deep Classification	High accuracy	Dataset dependence
EfficientNet Uniform Verification	Lightweight DL	Better efficiency	Reduced robustness
YOLOv8 Dress Compliance	Real-time Detection	Fast inference	Training complexity

E. Integrated Smart Attendance Frameworks

Most existing solutions focus on a single problem domain.
Some systems implement facial recognition without liveness detection.
Others focus on anti-spoofing but do not support attendance management.
Very few frameworks combine:
• Face Recognition
• Anti-Spoofing Verification
• Dress Code Enforcement
within a single architecture.

Table 5. Integrated Framework Comparison

System	Face Recognition	Anti-Spoofing	Dress Code	Attendance
Traditional Attendance	No	No	No	Yes
Face Recognition System	Yes	No	No	Yes
Face + Liveness System	Yes	Yes	No	Yes

Proposed Framework	Yes	Yes	Yes	Yes

III. Popular Techniques in Smart Attendance Systems

A. Face Recognition Techniques

Face recognition systems generally employ:
• Face Detection
• Face Alignment
• Feature Extraction
• Face Matching
Popular architectures include FaceNet, ArcFace, DeepFace, MobileFaceNet, ResNet50, and Vision Transformers.

B. Anti-Spoofing Techniques

Popular approaches include:
• Texture Analysis
• Motion Analysis
• Blink Detection
• CNN-based PAD
• Vision Transformer Models
• Multi-modal Biometrics

C. Dress Code Enforcement Techniques

Popular techniques include:
• YOLO Object Detection
• Clothing Classification CNNs
• Transfer Learning
• Multi-Class Compliance Detection

Table 6. Popular Techniques Summary

Technique Category	Key Models	Strengths	Limitations
Face Recognition	ArcFace, FaceNet	High accuracy	Computational cost
Anti-Spoofing	CNN, ViT	Enhanced security	Dataset dependency
Dress Code Detection	YOLO, ResNet	Real-time monitoring	Environmental sensitivity

July-September-Issue, Vol. 1, No. 2 (2026) | DOI: 10.66261/h211wr12

Hybrid Frameworks	Multi-modal AI	Improved robustness	Increased complexity

IV. Existing Architecture of Face Recognition, Anti-Spoofing and Dress Code Based Smart Attendance Systems

Most smart attendance systems follow a layered architecture that captures facial images, verifies identity, performs liveness detection, checks dress code compliance, and finally records attendance. Recent studies indicate that modular architectures improve scalability, security, and deployment flexibility.
The overall framework can be divided into six major layers:

A. Image Acquisition Layer

The image acquisition layer is responsible for capturing student or employee images using surveillance cameras, webcams, smartphones, or IP cameras.
Modern attendance systems use:
• CCTV Cameras
• Smart Cameras
• Mobile Cameras
• IoT Enabled Cameras
The quality of image acquisition directly affects recognition performance. Poor illumination, low-resolution cameras, and improper camera angles reduce system accuracy.

Functions

- Capture facial images
- Capture dress appearance
- Collect video streams for liveness verification
- Provide real-time monitoring
-

B. Preprocessing Layer

Raw images often contain noise, shadows, illumination variations, and background interference.
The preprocessing layer performs:

- Image resizing
- Noise removal
- Histogram equalization
- Face alignment
- Color normalization
- Background suppression

Proper preprocessing improves feature extraction accuracy and reduces computational complexity.

Common Techniques

Technique	**Purpose**
Histogram Equalization	Improve contrast
Face Alignment	Standardize face orientation
Gaussian Filtering	Remove noise
Image Normalization	Improve consistency

C. Face Recognition Layer

This layer performs identity verification.
The process generally includes:
Face Detection → Feature Extraction → Feature Encoding → Identity Matching
Popular face recognition models include:

- FaceNet
- ArcFace
- DeepFace
- VGGFace
- MobileFaceNet
- Vision Transformers

Deep learning-based models automatically learn discriminative facial features and outperform traditional machine learning approaches.

Table 7. Face Recognition Models Used in Attendance Systems

Model	**Accuracy**	**Strength**
FaceNet	High	Compact embeddings
ArcFace	Very High	State-of-the-art recognition
DeepFace	High	Robust verification
MobileFaceNet	Moderate	Lightweight deployment
Vision Transformer	Very High	Better generalization

July-September-Issue, Vol. 1, No. 2 (2026) | DOI: 10.66261/h211wr12

D. Anti-Spoofing and Liveness Verification Layer

The liveness verification layer prevents proxy attendance and unauthorized access.
Common spoofing attacks include:

- Printed photographs
- Replay videos
- Deepfake videos
- 3D masks
- Screen display attacks

To counter these attacks, anti-spoofing mechanisms evaluate physiological and behavioral characteristics.

Popular Techniques

Motion-Based Verification

- Eye blink detection
- Lip movement analysis
- Head rotation tracking

Texture-Based Verification

- Local Binary Pattern (LBP)
- Reflection analysis
- Surface texture analysis

Deep Learning-Based Verification

- CNN-based PAD
- MobileNet Anti-Spoofing
- Vision Transformer PAD

Table 8. Anti-Spoofing Methods

Method	**Advantage**	**Limitation**
Eye Blink Detection	Simple implementation	Can be bypassed
Head Movement Detection	Low cost	Limited robustness
Texture Analysis	Fast detection	Sensitive to lighting
CNN-Based PAD	High accuracy	Dataset dependent
ViT-Based PAD	Better generalization	Computational overhead

July-September-Issue, Vol. 1, No. 2 (2026) | DOI: 10.66261/h211wr12

E. Dress Code Enforcement Layer

Dress code verification has emerged as an additional compliance component in educational institutions.

The system verifies:

- Uniform color
- Shirt type
- Tie presence
- ID card presence
- Lab coat compliance
- Safety equipment compliance

Object detection models identify dress-related components and compare them against predefined rules.

Popular Detection Models

- YOLOv5
- YOLOv8
- ResNet50
- EfficientNet
- MobileNetV

Table 9. Dress Code Detection Models

Model	Application	Strength
YOLOv5	Uniform detection	Real-time detection
YOLOv8	Multi-object detection	Higher accuracy
ResNet50	Clothing classification	Strong feature extraction
EfficientNet	Uniform verification	Efficient architecture
MobileNetV3	Edge deployment	Lightweight model

F. Attendance Management and Reporting Layer

After successful identity verification, liveness validation, and dress code compliance checking, attendance is recorded automatically. The reporting layer provides:

- Attendance reports
- Dress code violation reports
- Security alerts
- Student analytics
- Monthly attendance summaries

July-September-Issue, Vol. 1, No. 2 (2026) | DOI: 10.66261/h211wr12

Workflow Summary:

Image Acquisition
↓
Preprocessing
↓
Face Recognition
↓
Anti-Spoofing Verification
↓
Dress Code Verification
↓
Attendance Recording
↓
Dashboard & Reporting

V. Challenges in Smart Attendance Frameworks

Although face recognition attendance systems have achieved significant success, several challenges remain.

A. Dataset Limitations

Most datasets focus on facial recognition only.
There are very few publicly available datasets containing:

- Face images
- Spoofing attacks
- Uniform variations

simultaneously.
This limits the development of integrated frameworks.

B. Environmental Variability

Attendance systems operate in uncontrolled environments.
Factors affecting performance include:

- Illumination changes
- Shadows
- Camera angles
- Occlusions
- Crowd density

These variations reduce recognition accuracy.

C. Spoofing and Security Threats

Face recognition systems remain vulnerable to:

- Printed photographs
- Replay attacks
- Deepfake videos
- Synthetic facial images

Advanced anti-spoofing methods are still required for robust deployment.

July-September-Issue, Vol. 1, No. 2 (2026) | DOI: 10.66261/h211wr12

D. Computational Complexity

Deep learning models require:

- High processing power
- Large memory
- GPU resources

This limits deployment on low-cost devices.

E. Real-Time Processing Challenges

Attendance systems must simultaneously perform:

- Face detection
- Recognition
- Liveness verification
- Dress code checking

Real-time execution remains challenging in large classrooms.

F. Privacy and Data Security

Facial images are highly sensitive biometric data.
Major concerns include:

- Data leakage
- Unauthorized access
- Identity theft
- Privacy violations

Strong encryption and secure storage mechanisms are essential.

G. Explainability Issues

Most deep learning systems operate as black-box models.
Administrators often require explanations for:

- Attendance rejection
- Spoof detection
- Dress code violation alerts

Explainable AI remains an active research area.

H. Lack of Standard Evaluation Frameworks

Researchers use different datasets and evaluation metrics.
Common metrics include:

- Accuracy
- Precision
- Recall
- F1 Score
- APCER
- BPCER

July-September-Issue, Vol. 1, No. 2 (2026) | DOI: 10.66261/h211wr12

This makes fair comparison difficult.

Table 10. Challenges in Smart Attendance Systems

Challenge	Impact
Limited Datasets	Poor generalization
Environmental Variability	Reduced accuracy
Spoofing Attacks	Security risks
Computational Cost	Deployment limitations
Privacy Concerns	User acceptance issues
Lack of Explainability	Reduced trust
Real-Time Constraints	Scalability problems
Evaluation Differences	Difficult benchmarking

VI. Research Gap Analysis

Despite substantial progress, several research gaps remain

Table 11. Research Gap Analysis

Research Gap	Existing Limitation	Future Opportunity
Integrated Frameworks	Separate attendance modules	Unified attendance platform
Multi-Level Security	Single anti-spoofing layer	Multi-modal authentication
Dress Code Verification	Limited implementation	Real-time compliance monitoring

July-September-Issue, Vol. 1, No. 2 (2026) | DOI: 10.66261/h211wr12

Dataset Availability	No benchmark dataset	Public integrated dataset
Deepfake Resistance	Limited detection capability	Advanced PAD architectures
Privacy Protection	Centralized data storage	Federated learning
Explainable AI	Black-box systems	Transparent attendance decisions
Edge Deployment	Heavy models	Lightweight AI models
Analytics Integration	Limited reporting	Intelligent dashboards
Smart campus Integration	Isolated solutions	Campus-wide automation

VII. Future Research Directions

Although significant progress has been made in face recognition, anti-spoofing liveness verification, and automated dress code enforcement technologies, several research challenges remain. Future smart attendance systems should focus on improving security, scalability, interpretability, and deployment efficiency.

A. Emerging Technologies

Recent advancements in artificial intelligence and computer vision have opened new possibilities for attendance automation.

Future attendance systems are expected to incorporate:

- Vision Transformers (ViT)
- Multimodal Biometric Authentication
- Explainable Artificial Intelligence (XAI)
- Federated Learning
- Edge Artificial Intelligence
- Generative AI Resistant Anti-Spoofing Models

Vision Transformer architectures have demonstrated superior performance in both face recognition and presentation attack detection tasks by capturing long-range dependencies within facial features.

Similarly, multimodal biometric systems combining face recognition with voice, gait, or behavioral biometrics can significantly improve authentication security.

B. Improvement Areas

Several limitations observed in existing attendance systems require further investigation.

Robustness Against Environmental Variations

Future systems should be capable of operating under:

- Poor illumination
- Occlusions
- Crowded classrooms
- Variable camera angles
- Outdoor environments

Advanced data augmentation and domain adaptation techniques can improve model robustness.

Lightweight Model Development

Current deep learning models often require expensive hardware resources.

Future research should focus on:

- Lightweight CNN architectures
- Model compression
- Knowledge distillation
- Efficient transformer models

to support deployment on low-cost edge devices.

Enhanced Liveness Detection

Traditional anti-spoofing methods struggle against advanced attacks such as:

- Deepfakes
- AI-generated faces
- 3D mask attacks

Future anti-spoofing systems must incorporate multi-level authentication and behavioral biometrics.

C. New Models and Approaches

Future attendance frameworks may combine multiple deep learning techniques within a single architecture.

Examples include:

CNN–Transformer Hybrid Models

These architectures combine:

- CNN feature extraction
- Transformer attention mechanisms

to achieve improved recognition accuracy and spoof detection performance.

Multi-Task Learning Models

A single network can simultaneously perform:

- Face Recognition
- Liveness Verification
- Dress Code Classification

This reduces computational overhead and improves deployment efficiency.

Self-Supervised Learning

Self-supervised learning can reduce dependence on large labeled datasets by automatically learning facial representations from unlabeled data.

Explainable AI Frameworks

Explainable attendance systems can provide:

- Attendance verification explanations
- Spoof detection reasons
- Dress code violation justifications

thereby increasing user trust and system transparency.

July-September-Issue, Vol. 1, No. 2 (2026) | DOI: 10.66261/h211wr12

D. Integration Possibilities

Future attendance systems can be integrated with smart campus infrastructure.
Potential integrations include:

IoT-Based Smart Campus Systems

- Smart Classrooms
- Smart Entry Gates
- Smart Security Systems

Cloud-Based Attendance Platforms

Cloud computing enables:

- Centralized attendance storage
- Cross-campus analytics
- Remote monitoring

Learning Management Systems

Attendance data can be automatically synchronized with:

- Moodle
- Google Classroom
- Microsoft Teams
- ERP Systems

Predictive Analytics

Artificial intelligence can analyze attendance patterns to predict:

- Student absenteeism
- Academic performance
- Compliance trends

Such analytics can assist administrators in making informed decisions.

VIII. Conclusion

Smart attendance systems have evolved from simple attendance recording mechanisms to intelligent platforms capable of identity verification, security monitoring, and compliance enforcement.

This review analyzed recent developments in face recognition, anti-spoofing liveness verification, and automated dress code enforcement techniques published between 2020 and 2026. Face recognition technologies such as ArcFace, FaceNet, and Vision Transformers have demonstrated remarkable improvements in identification accuracy. Similarly, anti-spoofing approaches based on CNNs, Vision Transformers, and multimodal biometrics have enhanced system security against presentation attacks.

Automated dress code enforcement using YOLO-based object detection has further expanded the capabilities of attendance systems by enabling real-time compliance monitoring.

Despite these advancements, challenges related to dataset availability, deepfake attacks, computational complexity, privacy preservation, and explainability remain unresolved.

The proposed integrated framework combines attendance management, anti-spoofing verification, and dress code enforcement into a unified solution capable of supporting future smart campus environments. Future research should focus on lightweight AI models, federated learning, explainable AI, and multimodal biometric authentication to improve scalability, transparency, and security.

References

[1] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 44, no. 10, pp. 5962–5979, Oct. 2022.

[2] O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Deep Face Recognition," British Machine Vision Conference (BMVC), 2015.

[3] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," Proceedings of CVPR, pp. 1701–1708.

[4] A. Howard et al., "Searching for MobileFaceNet Architectures for Efficient Face Recognition," Proceedings of ICCV Workshops, 2019.

[5] K. Zhang et al., "Face Anti-Spoofing via Disentangled Representation Learning," European Conference on Computer Vision (ECCV), 2020.

[6] Z. Ming, M. de Marsico, A. Petrosino, and S. Ricciardi, "A Survey on Face Presentation Attack Detection with RGB Cameras," Pattern Recognition Letters, vol. 137, pp. 207–215, 2020.

[7] Y. Atoum, Y. Liu, A. Jourabloo, and X. Liu, "Face Anti-Spoofing Using Patch and Depth-Based CNNs," IJCB, 2020.

[8] P. Keresh and P. Shamoi, "Transformer-Based Self-Supervised Learning for Face Anti-Spoofing," IEEE Access, vol. 12, pp. 85123–85136, 2024.

[9] C. Kong, S. Kim, and A. Ross, "M3FAS: Multi-Modal Mobile Face Anti-Spoofing System," IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 5, no. 3, pp. 312–324, 2023.

[10] D. Saraswat, R. Kumar, and A. Sharma, "Anti-Spoofing Enabled Contactless Attendance Monitoring System Using Deep Learning," International Journal of Advanced Computer Science and Applications, vol. 14, no. 6, pp. 118–126, 2023.

[11] M. A. Hosen et al., "Face Recognition Based Attendance Management System with Anti-Spoofing Verification," International Journal of Computing and Digital Systems, vol. 12, no. 4, pp. 45–56, 2023.

[12] U. Supriatna, A. Kurniawan, and S. Putra, "Smart Attendance System Using Face Recognition and Anti-Spoofing Technology," Journal of Information Systems Engineering and Business Intelligence, vol. 8, no. 2, pp. 95–105, 2022.

[13] S. Sayed, M. Hassan, and A. Ibrahim, "Face Recognition Attendance System with MobileNetV3 Anti-Spoofing Detection," IEEE Access, vol. 13, pp. 21451–21465, 2025.

[14] B. Subagja, M. Putri, and A. Nugroho, "Minimizing Face Spoofing Attacks Using Deep Liveness Detection Models," Procedia Computer Science, vol. 245, pp. 175–184, 2025.

[15] Y. Pounikar, S. Verma, and R. Tiwari, "A Systematic Review of Face Recognition Attendance Systems: Security, Scalability and Automation," Artificial Intelligence Review, vol. 58, no. 2, pp. 1–32, 2025.

[16] S. Sarpotdar and K. Chavan, "A Novel Face Anti-Spoofing Neural Network for Real-Time Authentication Systems," International Journal of Intelligent Systems and Applications, vol. 14, no. 1, pp. 55–67, 2022.

[17] R. Faruque, M. Hasan, and A. Rahman, "YOLOv5 and ArcFace Based Mass Attendance Monitoring System," Proceedings of IEEE ICCIT, pp. 1–6, 2024.

[18] A. Redmon and J. Farhadi, "YOLO: Real-Time Object Detection for Visual Recognition," Proceedings of CVPR.

[19] M. Tan and Q. Le, "EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks," ICML, 2019.

[20] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," CVPR.

[21] H. Sharma and A. Gupta, "Automated Uniform Detection and Dress Code Monitoring Using Deep Learning," International Journal of Computer Vision Applications, vol. 11, no. 3, pp. 122–131, 2024.

[22] P. Mehta and R. Singh, "Real-Time Student Uniform Verification Using YOLOv8 Object Detection," Proceedings of International Conference on Smart Education Technologies, pp. 145–152, 2025.

[23] A. Jain and S. Verma, "Deep Learning Based Dress Code Compliance Monitoring in Educational Institutions," Journal of Intelligent Systems, vol. 33, no. 4, pp. 501–514, 2025.

[24] S. Patel, M. Shah, and D. Trivedi, "Smart Campus Management Using AI-Based Attendance and Behavioral Analytics," IEEE Access, vol. 12, pp. 92581–92595, 2024.

[25] M. Brown and T. Wilson, "Federated Learning for Privacy-Preserving Biometric Authentication Systems," Future Generation Computer Systems, vol. 151, pp. 125–138, 2025.

[26] R. Gupta, P. Sharma, and V. Mishra, "Explainable Artificial Intelligence for Secure Face Recognition Systems: A Survey," ACM Computing Surveys, vol. 58, no. 1, pp. 1–35, 2025.