https://doi.org/10.1051/itmconf/20268101017

A comprehensive review of AI-powered campus surveillance

Kumuda D P[1*], *Harshitha* B V[1], *Manikya* K[1], *Dhavan* H S[1], *Ankita* Awanti[1], *Swathi* H Y[1]

[1]Department of CSE(AI&ML), Malnad College of Engineering, Hassan 573202, India

Abstract. As education institutions face new security challenges, the integration of Artificial intelligence (AI) and computer vision with surveillance systems for real time monitoring and threat detection is becoming mainstream. The inefficiency of a traditional CCTV system, which rely on human monitoring, makes them susceptible to costly mistakes. This literature survey examines deep learning methodologies focused on Convolutional Neural Networks, YOLO based object detection, Haar Cascade classification, and Local Binary Pattern Histogram for campus surveillance and recognition systems used in the 46 works collected between 2020 and 2025. The survey tracks the advancements made towards systems that autonomously monitor and recognize faces, track vehicles, analyse crowds, and even detect behaviours, as AI systems attain the ability to automate processes. Although the systems in question boost recognition accuracy exceeding 95%, real time system flexibility, varying lighting conditions, occlusions, privacy, and system scalability remind touchy problems. The survey suggests that the AI powered systems of the future should work towards smart frameworks that integrate disparate surveillance systems and automated alert systems.

1 Introduction

Educational campuses are increasingly facing issues like theft, vandalism, trespassing, and student misconduct, all of which threaten safety and disrupt learning. Many institutions still rely on traditional CCTV systems that require operators to manually monitor footage. However, manual monitoring often leads to fatigue and reduced attention, especially as campus populations and surveillance areas grow. The growing use of artificial intelligence and computer vision has changed how campuses approach security. Instead of continuously watching the cameras, technology automatically checks the footages and then alerts authorities when something suspicious happens. In many cases, the systems identify potential threats more quickly and consistently than manual monitoring, and they can be expanded easily as the campus grows. With this shift, surveillance is no longer limited to simply recording events; it is becoming an active, automated process. This review explores how AI-based surveillance tools are being used in educational environments, particularly in areas such as facial recognition, object detection, and the analysis of human behaviour. The

* Corresponding author: dpkumuda12@gmail.com

discussion focuses on the current developments in the field, factors that influence system performance, and the key issues that need attention to create more reliable and integrated AI-supported security systems.

2 Literature review

AI-driven campus surveillance has progressed rapidly from 2020 to 2025, with most studies adopting deep learning models such as CNNs, YOLO, ResNet, VGG, FaceNet, and LightCNN, along with classical techniques like Haar Cascade, LBPH, HOG, SVM, and KNN.

Early work in this area largely focused on applying facial recognition to routine campus tasks such as marking attendance and controlling entry. Approaches based on enrolment databases, LBPH, Haar Cascade, and various CNN architectures frequently achieved accuracy levels above 95%. However, their performance tended to decline when lighting conditions varied, when faces were captured from non-frontal angles, or when concerns related to privacy arose. Then, transfer learning with models such as ResNet50, VGG16, InceptionV3, and GoogleNet helped to increase accuracy and reduce the training effort. Yet, running these systems in real time was still challenging because of the heavy GPU and hardware requirements. So, many early solutions worked well in controlled lab conditions but struggled when applied on actual campuses.

Real-time monitoring saw significant improvement with the adoption of YOLO models (YOLOv4, v5, v7, and v8), which made live face and object detection, alert generation, and behaviour tracking more practical. These systems generally performed well in identifying objects, children, rule violations, and even stray animals. However, their accuracy tended to drop in situations with poor lighting, class imbalance, occlusions, or inconsistent frame quality. IoT-based solutions built on Raspberry Pi or MERN pipelines provided affordable automation, but their performance was often limited by bandwidth restrictions, hardware capacity, and connectivity issues.

Techniques based on 3D-CNN, C3D, I3D, and transformer-driven architectures gave strong results in identifying unsafe movements, exam-hall violations, and other suspicious activities. However, these methods often performed poorly when applied to low-resolution CCTV footage.

Researchers also examined recognition tasks under more challenging conditions. Super-resolution techniques such as U-Net, along with models like ArcFace, FaceMaskNet-21, and several custom CNN variants, improved detection for masked faces, low-quality images, and partially obstructed views. Even with these improvements, performance still dropped when faces appeared at extreme angles, when scenes were crowded, or when lighting changed abruptly. Lightweight models, including LBPH, HOG combined with SVM, and CNN paired with KNN, offered more cost-effective options, but their reliability in real-world environments remained limited.

Large-scale facial recognition, regulatory compliance gaps, dataset transparency, privacy-preserving techniques like anonymization and federated learning, and the ethics and privacy concerns of specialized applications such as missing child identification, fall detection, biometric-based monitoring and child recovery work which has produced positive results, but are all still plagued with aging effects, appearance changes, and privacy concerns has all been previously documented.

Despite having integrated AI with sensors to increase efficiency and enable real-time response to alarm triggers, edge AI and IoT surveillance systems were still dependent on recalibration, and unfortunately, they still lacked standard metrics to evaluate their performance. Although low-cost surveillance provided good performances during tests with Arduino and PIR motion sensors, and Raspberry Pi, they were throttled by their low computational power, and they had very limited ranges of detection.

Across the literature, preprocessing steps such as alignment, normalization, histogram equalization, and contrast enhancement helped improve accuracy. Commonly used datasets included LFW, VGGFace2, SCface, YouTube Face, FaceScrub, CAD, and many custom campus datasets.

Even with reported performances of 85% to 99.9% accuracy, the systems performed poorly in the field due to poor lighting, obstacles, lack of detection of faces that were centered, small objects, and the limited detection range of the systems. Privacy and ethical surveillance systems, lack of generalization, scalability, and even systems to integrate them, were reported by every study. The computer science literature from closed campus AI based surveillance systems demonstrates great promise, but the literature still demonstrates the requirement of integrated multi-modal systems, faster AI systems that operate in real-time, richer datasets, and AI systems that operate with privacy to be effective campus surveillance systems.

3 Survey summary

Key research on CCTV based facial recognition has been tabulated with respect to each researcher's problem definition, methodology, and their results. This allows for a performance comparison that reveals the same methodologies, complex techniques used, and their performance results distributed over diverse implementations.

Table 1. Survey summary.

Ref. No	Problem Addressed	Authors' Approach / Method	Results
[1]	Tracking and logging individual entries/exits	Face registration + TensorCam with TensorFlow, Keras, Caffe2	Efficient face tracking; accuracy not quantified; limited to pre-registered users
[2]	Real-time attendance via CCTV	Face detection + LBPH; grayscale conversion and normalization	99.69% accuracy; reliable in controlled environments
[3]	Efficient attendance with limited training	Haar Cascade for detection + fine-tuned ResNet50/VGG16/InceptionV3	High accuracy; short training time; specific metrics not reported
[4]	Secure and scalable attendance marking	Deep CNN for recognition after face alignment	High accuracy claimed; exact value not provided
[5]	Enhancing campus safety with AI and IoT integration	YOLO for object detection; IoT for alerts and data flow	Improved response time; effectiveness dependent on network stability
[6]	Detecting violent	Deep learning + temporal	High accuracy in

https://doi.org/10.1051/itmconf/20268101017

	interactions in campus surveillance	analysis on human behavior	identifying violent events; real-time alerts supported
[7]	Summarizing long CCTV videos into key activity events	CNN with activity attention modeling on CAD dataset	Effectively summarizes academic activity videos; accurate filtering of key events
[8]	Improving face/mask detection during surveillance	HOG, SIFT, DNN, CNN; integrated using OpenCV and Dlib	Accurate face recognition; handles unusual face/mask detection
[9]	Recognizing individuals in real-time CCTV streams	PCA for features; CNN, KNN, RF for classification	CNN achieved 97.5% accuracy; PCA slower and less accurate
[10]	Real-time small-scale attendance system	LBPH with OpenCV; grayscale conversion + face detection	High accuracy for small datasets; real-time functionality in controlled setup
[11]	Real-time face recognition with limited hardware	CNN via Dlib; face alignment and cropping; compared with HoG	CNN achieved 98.3% accuracy; outperformed HoG; real-time on Raspberry Pi
[12]	Affordable IoT-enabled face recognition from CCTV	MTCNN + LBPH classifier; brightness & illumination normalization	73.41% accuracy; training ~309 sec; real-time alerts enabled
[13]	Face recognition using landmark-based morphometrics	HOG + Dlib landmark detection; Likelihood Ratio method	85.75% TPR, 25% FPR, cllr = 0.26; interpretable, forensic-friendly
[14]	Robust recognition in CCTV with occlusion/lighting	Histogram equalization + GoogleNet CNN + attention aggregation	98.55% accuracy on YouTube Face Dataset; 99.12% (no occlusion), 98.87% (occluded)
[15]	Face recognition under mask-wearing conditions	FaceMaskNet-21 (CNN + quadruplet loss); LFW, RMFRD datasets	88.92% overall accuracy; 100% for single-face video frames
[16]	Variations in face angles, lighting, and accessories	CNN + Haar, PCA, ICA, SVM; 400 images (students)	CNN+Haar: 98.95%; CNN: 97.83%; Haar: 78.95%; SVM: 93.95%
[17]	Ethical, legal, and privacy issues in facial recognition	Theoretical analysis; case studies (Clearview AI, AFR Locate)	No metrics; proposed legal oversight, transparency, and public consent
[18]	Qualitative evaluation of analog CCTV systems	Manual observation and interviews; no image data	Reduction in theft and vandalism; no smart analytics or digital features
[19]	Improving recognition in low-res CCTV frames	Super-resolution (U-Net, EDSR) + FR (ResNet50, MobileNetV2)	U-Net + ResNet50: 85% accuracy, 87% precision, 114 ms/image
[20]	Identifying children/strangers through face and object detection	YOLOv8 + CNN/LBPH/SVM; face classification by age/mask	YOLO mAP@0.5: 0.995; CNN most accurate; LBPH fastest
[21]	Comparing recognition methods for attendance	Reviewed 30 papers; CNN, LBPH, HOG, Eigenface, SVM	CNN: up to 99% accuracy; LBPH: 92%; CNN > others overall
[22]	Robust facial recognition under	MediaPipe Face Mesh + BlazeFace + DNN	Accuracy: 94.23%; robust to illumination and

	pose/illumination changes		background variation
[23]	Enhancing privacy using lensless camera data	FlatCam dataset; DCT transformation + VGG16, VGG-ATT	VGG-ATT + DCT: 87.71% accuracy; lower performance on raw sensor input
[24]	Security surveillance using real-time facial recognition from CCTV	Preprocessing with face detection and normalization; Deep CNNs + Haar Cascade	High accuracy in real-time face recognition; effective surveillance tracking
[25]	Recognizing faces in low-resolution CCTV footage	LightCNN, MobileNet-V2, ArcFace on LFW and SCface datasets	Achieved high accuracy in low-res conditions; ArcFace enhanced robustness
[26]	Classroom attendance using CCTV-based recognition	Used FaceNet for embeddings, KNN classifier	Achieved 92.85% accuracy in real-time attendance using CCTV
[27]	Suspect identification in security surveillance	HBA for feature selection + KNN on ORL and Yale datasets	Accuracy: 94.4% (ORL), 92.3% (Yale); promising for law enforcement use
[28]	Real-time detection and identification of criminal faces	Face detection via Haar, HOG for features, classified with SVM	Alerts on matches; accuracy metrics not detailed but system worked live
[29]	Difficulty identifying criminals in CCTV under occlusion	Face detection with MTCNN; recognition with ResNet	Achieved 92.56% accuracy; works well in occluded CCTV scenes
[30]	Face identification in law enforcement tasks	Haar Cascade + LBPH algorithm on law enforcement image set	High accuracy; supports field application with enhancements needed
[31]	Facial recognition in unconstrained, real-world settings	Modified VGGFace16 with GAP & PReLU; transfer learning	Achieved 99.9% accuracy, precision, recall, and F1-score on LFW, VGGFace2
[32]	Identifying missing children through facial recognition	CNN with transfer learning; real-world and law enforcement images	High precision and recall; exact values not provided
[33]	Locating missing children via face recognition	128-d embeddings using pre-trained CNNs; cosine/Euclidean comparison	Functional system; accuracy not quantified; works with mobile and CCTV
[34]	Detecting cheating behavior during exams	SSD for face, YOLOv5 for gesture, C3D for emotion analysis	98.8% overall accuracy; 99.2% for non-cheating detection
[35]	Real-time face recognition at airport checkpoints	Real-time capture via Raspberry Pi; unspecified recognition model	Functional testing completed; no specific accuracy metrics reported
[36]	Summary of face recognition using deep learning	Reviewed VGG16, FaceNet, AlexNet, MTCNN, YOLO, etc.	Reported accuracies from 95% to 99.85%; gaps in occlusion handling noted
[37]	Privacy risks in facial recognition systems	Survey of GANs, autoencoders, encryption, federated learning	No performance metrics; presents solutions for privacy-preserving recognition
[38]	Real-time surveillance without human	PIR/IR sensors + AI-based object and face recognition on	Improved efficiency and reduced false alarms;

 https://doi.org/10.1051/itmconf/20268101017

	monitoring	live feed	metrics not specified
[39]	Improving recognition accuracy and fall detection	FaceNet, ResNet, YOLOv8, 3D-CNN; fusion of multiple classifiers	KNN: 97.1% (face); YOLOv8: ~92% (fall); high accuracy across tasks
[40]	Low-cost real-time surveillance with anomaly detection	PIR sensors + Arduino + K-means clustering on motion events	Accuracy: 94.75%–98.75%; precision: up to 96.77%; scalable solution
[41]	Object/person detection in campus CCTV	YOLOv8 with MERN stack; Roboflow for annotation	~80.56% accuracy; real-time alerting for specific classes
[42]	Identifying violations (ID, shoes) in students	YOLOv7 for object detection; CNN for face recognition	YOLOv7: 90.4% accuracy; CNN testing accuracy: 92%
[43]	Securing wireless surveillance with optimal streaming	H.265 compression + NVR + QoS + motion triggers	Real-time access; 25–50% better data efficiency
[44]	Detecting anomalies in campus video using temporal modeling	I3D, C3D + Vision Transformer-based Temporal Self Attention (TSA)	TSA achieved 95.9% accuracy, 96.26% AP, F1: 79.5%, EER: 2.9%
[45]	Real-time object detection and anomaly detection in libraries	YOLOv4 with CSPDarknet53 backbone on annotated CCTV data	Precision: 92%, Recall: 90%, F1-score: 91%, mAP: 91.73%
[46]	Detecting unsafe behavior in crowds using visual cues	CNN + MRCDD (Masked Region-Centric Disparity Detection)	Precision: 96.15%, Classification Rate: 98.47%, False Detection Rate: 0.045%

From all studies, surveillance has moved on rapidly with the addition of deep learning surveillance techniques such as CNNs, YOLO, ResNet, VGG16, which surpass older techniques like LBPH or Haar Cascade by leaps and bounds. Other works emphasized the use of IoT and hybrid systems with CNNs and transfer learning to achieve 90–99.9% accuracy. Nevertheless, the challenges of lighting, occlusion, privacy, and computational cost still raise some of the most important concerns and are the most pertinent when designing reliable and accurate real-time surveillance systems.

4 Comparative analysis

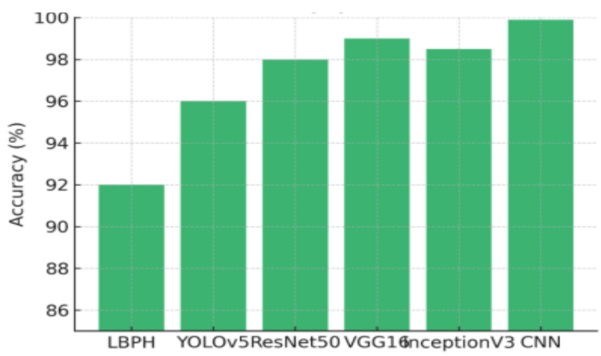

Fig. 1. Accuracy by AI Model

Depicted in Figure 1 are various deep learning models such as CNN, ResNet50, VGG16, Inception V3 achieving more than 98% accuracy, making them incredibly trustworthy for surveillance. YOLOv5 is also good for fast object recognition, while LBPH stands lower at approximately 92%. In general, deep models outperform classical approaches in most adaptability and real-world scenarios.

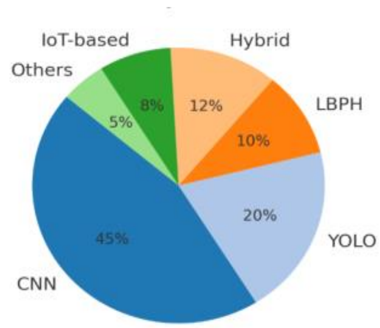

Fig. 2. AI Techniques Distribution

Depicted in Figure 2 are CNN based methods dominating the CNN based approaches in research at 45% usage due to its great feature extraction. YOLO also garners 20% for its real time object detection while LBPH and hybrid approaches cater to the lower resource niche. There is increasing interest in and smarter, integrated surveillance systems.

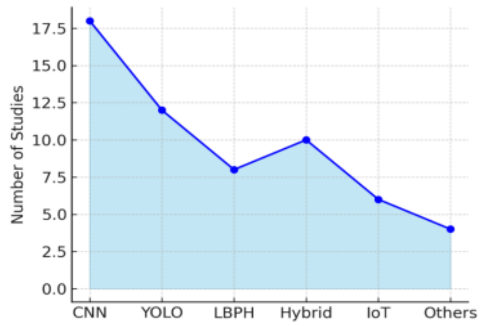

Fig. 3. Number of Model Studied

In Figure 3, almost all of the literature is focused on CNN frameworks, while YOLO and LBPH are gradually increasing in popularity for detection and recognition. Hybrid and IoT models are still uncommon, suggesting these are the earlier stages of research. The trend is indicating that more complex systems are going to replace the single model systems.

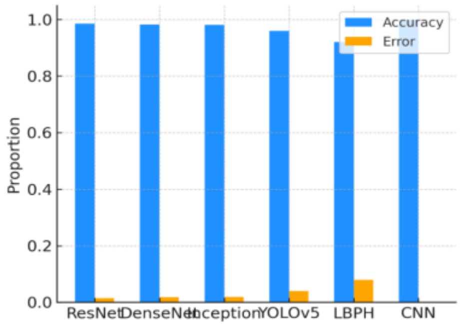

Fig. 4. Accuracy vs Error by Model Across Literature

Figure 4 has deep models such as ResNet, DenseNet, Inception, YOLOv5 and CNN almost defect free, whereas LBPH has more errors. The reason for the gap is primarily due to LBPH's lack of deep learning features. Overall, deep learning architectures generalize better in surveillance tasks.

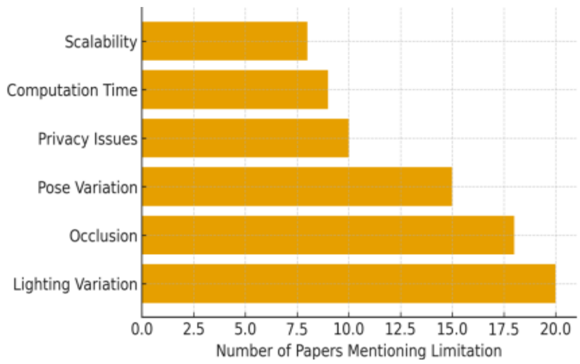

Fig. 5. Common limitations Identified in Reviewed Studies

The most prevalent limitations in the performance of surveillance systems in real-world settings are lighting changes and occlusions, as shown in Fig 5. After those are performance challenges like pose variation, privacy issues, costly computational demands, and limited scalability challenges. In real-world scenarios, most AI systems still struggle, even when labs prove the systems accurate.

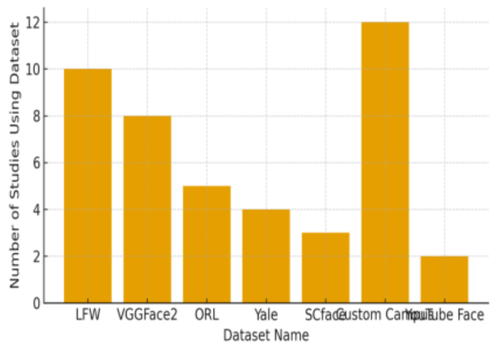

Fig. 6. Dataset Usage Frequency in Reviewed Studies

Heavy reliance on custom-created campus datasets is illustrated in Fig 6, in addition to continuing use of LFW and VGG-Face2 as benchmarking. For orphan datasets like ORL and Yale, the only use case is to conduct foundational tests, as they appear to be outdated. The trend shows the need to develop more diverse and contemporary datasets to help improve the robustness of models.

5 Research gap identified

Educational Over the years, many users of AI surveillance tech have been able to customize the software to specify the types of inputs the software is supposed to recognize, and then choose which inputs the software is expected to recognize. Most of these systems do not seem to recognize the complexities and challenges of configuring systems to recognize behaviors and recognize and correlate behaviors to moving people. Performance drops sharply in fast-paced environments, and many systems struggle in low-light situations, and move too fast to be captured for analysis. The systems these organizations are often renting or licensing are very reactive systems which means alerts for problematic situations are not configurable, so organizations become stuck in cycles where they can only react to problems when they occur for the first time, and every time after. Limited lighting, inclement weather, hardware updated, and many other factors also greatly weaken the detection and system overall. Scalability is another susceptible challenge, as many systems only implement one tool, and have very limited cross-functionality. This makes it nearly impossible to create a unified, other than educational, surveillance system. As a consequence of systemic fragmentation, instead of implementing a flexible, complete fusion of integration, automation, connectivity, and in real time systems are expected to do these tasks, greatly sophisticated and capable systems still unfulfilled lose efficiency.

6 Future scope

Developing systems that can simultaneously and seamlessly analyze faces, behaviors, and vehicle and adap-tively are the most important systems to design. Edge computing and federated learning will improve speed at the cost of enhanced user privacy by Explainable AI should be included to improve automated trust systems to gain trust in the systems built.

There is a strong need for richer and more diverse campus surveillance datasets so that models can better handle real-world variations. With the growth of IoT and 5G, faster data transfer and instant alerts will support more proactive and responsive monitoring. Finally, future systems must balance security with privacy by using privacy-preserving techniques and strong ethical governance frameworks to ensure responsible deployment in educational environments.

7 Conclusion

In conclusion, the AI-based surveillance systems that incorporate models such as CNN, YOLO, ResNet, and VGG had a positive impact on campus safety from 2020–2025 and improving face, behavior, and object recognition, which allowed campuses to go beyond simple CCTV recording and monitor their facilities in real time. However, poor lighting, occlusions, pose shifts, high computational needs, and privacy concerns continue to impact the challenge of broad deployment. Many systems also lack sufficient multimodal integration and real-time alerts.

Highlighted in this report, we are forecasting the future work to revolve around the design of edge computing driven, multi-purpose, and privacy-preserving surveillance systems. There are several surveillance systems that are more reliable and smarter. Such systems would have the ability to use edge computing in real time, multi-sensor fusion, autonomous patrolling robotics, and federated learning. There is also a need for closure of these gaps to empower educational setting to implement surveillance systems that are more reliable, scalable and AI driven. There also needs to be a balance of these frameworks gaps to ensure the governance of ethically and socially acceptable use.

References

1. P. Sarikonda, S. Bhutada, Customized campus surveillance system, *Int. Res. J. Eng. Technol.*, **7**(1), 737 (2020). IRJET
2. B. Sreekantha, S. A. Vijayalakshmi, H. B. Prasad, C. Hrithik, M. S. Nagajyothi, S. Rakshitha, Face-based CCTV attendance monitoring system using deep face recognition, *Int. Res. J. Eng. Technol.*, **8**(6), 3763 (2021). IRJET
3. K. Alhanaee, M. Alhammadi, N. Almenhali, M. Shatnawi, Face Recognition Smart Attendance System using deep transfer learning, *Proc. Comput. Sci.*, **192**, 4093–4102 (2021).
4. Nurkhamid, P. Setialana, H. Jati, R. Wardani, Y. Indrihapsari, N. M. Norwawi, Intelligent attendance system with face recognition using deep convolutional neural network, *J. Phys.: Conf. Ser.*, **1737**, 012031 (2021).

5. N. Junaid, M. Khalid, N. Saunshi, P. Mehta, M. N. Thippeswamy, Smart college camera security system using IoT, in *Lect. Notes Electr. Eng.*, pp. 295–309 (2021).
6. L. Ye, T. Liu, T. Han, H. Ferdinando, T. Seppänen, E. Alasaarela, Campus violence detection based on artificial intelligent interpretation of surveillance video sequences, *Remote Sens.*, **13**(4), 628 (2021).
7. W. Muhammad, I. Ahmed, J. Ahmad, M. Nawaz, E. Alabdulkreem, Y. Ghadi, A video summarization framework based on activity attention modeling using deep features for smart campus surveillance system, *PeerJ Comput. Sci.*, **8**, e892 (2022).
8. P. Keerthana, S. Prasath, S. Tamilmani, S. Veeragokulraj, Enhancing campus security through smart surveillance system, in *Proc. 2024 10th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, 14–15 March 2024, IEEE.
9. R. Ullah, H. Hayat, A. A. Siddiqui, U. A. Siddiqui, J. Khan, F. Ullah, S. Hassan, L. Hasan, W. Albattah, M. Islam, G. M. Karami, A real-time framework for human face detection and recognition in CCTV images, *J. Sensors*, 2022, Article ID 3276704 (2022).
10. E. Kagona, Facial recognition attendance scheme on CCTV cameras using Open Computer Vision and deep learning: A case study of International University of East Africa (IUEA), *Adv. J. Sci. Technol. Eng.*, **2**(1), 1–27 (2022).
11. M. Zamir, N. Ali, A. Naseem, A. A. Frasteen, B. Zafar, M. Assam, M. Othman, E. A. Attia, Face detection and recognition from images and videos based on CNN and Raspberry Pi, *Computation*, **10**(9), 148 (2022). https://doi.org/10.3390/computation10090148
12. S. Chattopadhyay, M. Rahaman, C. O. N. Susanto, N. Anwar, A. A.-H. Chen, Framework for face recognition in CCTV based on Internet of Things (IoT), *DSIM* (2021).
13. R. Verma, N. Bhardwaj, A. Bhavsar, K. Krishan, Towards facial recognition using likelihood ratio approach to facial landmark indices from images, *Forensic Sci. Int. Rep.*, **5**, 100254 (2021). https://doi.org/10.1016/j.fsir.2021.100254
14. S. Merikapudi, S. Math, C. Nandini, M. Rafi, Face recognition using CNN trained with histogram equalization based image enhancement scheme, *Eur. J. Mol. Clin. Med.*, **7**(8), 2940 (2020).
15. R. Golwalkar, N. Mehendale, Masked-face recognition using deep metric learning and FaceMaskNet-21, *Appl. Intell.*, **52**(11), 13268–13279 (2022). https://doi.org/10.1007/s10489-022-03569-2
16. A. Nurpeisova, A. Shaushenova, Z. Mutalova, Z. Zulpykhar, M. Ongarbayeva, S. Niyazbekova, A. Semenov, L. Maisigova, The study of mathematical models and algorithms for face recognition in images using Python in proctoring system, *Computation*, **10**(8), 136 (2022). https://doi.org/10.3390/computation10080136
17. M. Smith, S. Miller, The ethical application of biometric facial recognition technology, *AI Soc.*, **37**(1), 167–175 (2021). https://doi.org/10.1007/s00146-021-01157-3
18. E. W. Prasetyo, The effectiveness of surveillance system through CCTV in improving campus environment security, (2022).
19. A. R. P. Gondosiswojo, G. P. Kusuma, Low-resolution face recognition on CCTV images using a combination of super-resolution and face recognition models, *J. Theor. Appl. Inf. Technol.*, **101**(20), 6353 (2023).
20. G. Firmasyah, J. Joniwan, A. M. Widodo, B. Tjahjono, Preventing child kidnapping at home using CCTV that utilizes face recognition with YOLO algorithm, *J. Soc. Res.*, **2**(9), 3291–3304 (2023).
21. A. Budiman, F. Fabian, R. A. Yaputera, S. Achmad, A. Kurniawan, Student attendance with face recognition (LBPH or CNN): A systematic literature review, *Proc. Comput. Sci.*, **217**, 1370–1377 (2022).
22. S. Hangaragi, T. Singh, N. Neelima, Face detection and recognition using face mesh and deep neural network, *Proc. Comput. Sci.*, **218**, 741–749 (2023).
23. C. Henry, M. S. Asif, Z. Li, Privacy preserving face recognition with lensless camera, in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, IEEE (2022).
24. E. Irfan, C. Jacob, R. Resmi, Facial recognition and CCTV integration for enhanced security using deep learning techniques, in *Proc. IEEE Recent Adv. Intell. Comput. Syst. (RAICS)* (2024).

25. N. Surantha, E. Yose, S. M. Isa, Low-resolution face recognition for CCTV and edge-powered smart attendance systems, in *Proc. IEEE 46th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, 676–681 (2022).
26. N. Ambre, R. Pitale, P. Rao, H. Mote, S. Chavan, A-eye: Attendance monitoring using face detection and recognition from CCTV footage (2024).
27. S. A. Sari, M. D. Sulistiyo, Suspect identification based on facial recognition from CCTV using hybrid bat algorithm (2024).
28. C. Bhatt, M. Semwal, P. S. Aswal, V. Goswami, S. Rawat, R. Dhanalakshmi, Real-time surveillance criminal detection system, in *Proc. Second Int. Conf. Adv. Inf. Technol. (ICAIT)* (2024).
29. A. Singh, R. K. Tiwari, AIGuard: Criminal tracking in CCTV footage using MTCNN and ResNet, IEEE, 31–35 (2024).
30. S. S. Chittibomma, R. K. Surapaneni, A. Maruboina, Facial recognition system for law enforcement: An integrated approach using Haar cascade classifier and LBPH algorithm, IEEE, 1–6 (2024).
31. V. M. Rathod, A. M. Patil, H. S. Motekar, Automatic face recognition based on enhanced VGGFace-16 model in an unconstrained environment using transfer learning, *Multimed. Tools Appl.* (2025).
32. Sk. K. Basha, I. Malavika, V. H. Priyanka, B. K. Bhavitha, G. B. S. Kiran, Facial recognition and neural networks for missing child identification: A smart approach, *Int. J. Mod. Trends Sci. Technol.*, **11**(03), 397–407 (2025).
33. D. J. Sanju, B. R. Surya, S. Sudipta, T. G. Suhas, N. Suryakiran, Safenest: Finding and reuniting lost children using face recognition, *J. Emerg. Technol. Innov. Res.*, **12**(2), d298 (2025).
34. N. S. Arumugam, Deep learning-based smart invigilation system for enhanced exam integrity, *Proc. Eng. Technol. Innov.*, **29**, 99–115 (2025).
35. N. Norhashim, S. A. Shah, N. L. M. Kamal, Z. Sahwee, M. A. Azizan, M. I. A. A. Norizan, Face recognition system at the airport based on Internet of Things and cloud technologies, *KARYA*, **1**(1), 31–40 (2025).
36. A. Nemavhola, S. Viriri, C. Chibaya, A scoping review of literature on deep learning techniques for face recognition, *Hum. Behav. Emerg. Technol.* (2025).
37. L. Laishram, M. Shaheryar, J. T. Lee, S. K. Jung, Toward a privacy-preserving face recognition system: A survey of leakages and solutions, *ACM Comput. Surv.*, **57**(6), Article 147, 1–38 (2024).
38. M. Chahande, L. Yadav, B. Wadhibhasme, Creation of an automated video surveillance system using IoT and AI systems, *J. Interdiscip. Multidiscip. Res.*, **11**(2) (2025).
39. P. D. Anand, R. Umasankaran, N. Joshi, K. R. Mamtha, Optimized CCTV monitoring using biometrics and AI-driven surveillance, *J. Informetrics*, **19**(1) (2025).
40. O. D. Egbe, E. F. Anwaitu, O. M. Kepeghom, Development and optimization of a real-time campus security surveillance system using Arduino and CCTV camera, *BW Acad. J.* (2025).
41. H. Farooq, N. A. Khan, Safe-Campus: Leveraging AI for advanced surveillance and security enhancement, in *Proc. 4th Int. Conf. Innov. Comput. Sci. (ICONICS)*, Karachi, Pakistan, IEEE (2024).
42. R. Deepalakshmi, K. R. S. Murugan, R. S. Arunnachalam, M. B. Asif, Campus surveillance: Deep learning-based rules violation detection, in *Proc. 14th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Noida, India, IEEE (2024).
43. F. O. Ehiagwina, K. O. Kadiri, S. A. Yekeen, J. O. Azanubi, K. O. Mustapha, Design and implementation of a reliable and secure wireless CCTV camera network for the main administration building, Federal Polytechnic Offa, *Eng. Technol. J.*, **9**(9), 5007–5011 (2024).
44. S. Mishra, S. Jabin, Enhancing campus surveillance using temporal self-attention, *SSRN Electron. J.* (2024).
45. G. T. Olorunyomi, D. A. Babalola, A. T. Tiamiyu, B. A. Aliyu, D. Ojajuni, Exploring the integration of deep learning in CCTV systems for enhanced security measures in academic libraries, *J. Eng. Res. Rep.*, **27**(2), 310–323 (2025).
46. Y. Wu, S. Feng, Y. Wu, J. Wang, S. Zhou, M. Yuan, Z. Hu, C. Wu, Masked region disparity-based unsafe behavior detection via campus monitoring device images, *Knowl.-Based Syst.* (2025).