

A Comprehensive Review of Gait Speed Monitoring and Suspicious Behaviour Analysis for Automated Crime Detection in Video Surveillance Systems

Pratibha Pandey¹, Brajesh Mishra²

Dept. of CSE,

S R Institute of Management & Technology, (AKTU), Lucknow, India

Abstract— The rapid advancement of computer vision, artificial intelligence (AI), and deep learning has significantly transformed video surveillance systems, enabling automated monitoring and intelligent analysis of human activities for security and crime prevention. Traditional surveillance systems primarily depend on continuous human observation, which is time-consuming, labor-intensive, and prone to human error, fatigue, and delayed responses to potentially suspicious activities. In this context, gait speed monitoring and suspicious behaviour analysis have emerged as promising approaches for enhancing automated crime detection by identifying unusual movement patterns and behavioural deviations in surveillance videos. This paper presents a comprehensive review of existing methodologies, techniques, and emerging trends in gait-based human activity analysis and automated suspicious behaviour detection. It examines the role of gait speed estimation, human detection and tracking, pose estimation, trajectory analysis, spatiotemporal feature extraction, and behavioural pattern recognition in identifying potentially abnormal activities. Furthermore, the review explores the application of conventional machine learning algorithms, including Support Vector Machines (SVM), Random Forest, and clustering techniques, alongside deep learning architectures such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and Transformer-based models. Particular attention is given to the integration of gait speed variations with contextual information, movement trajectories, interactions between individuals, and temporal behavioural patterns to improve the reliability of automated surveillance systems. The paper also discusses major challenges, including occlusion, variations in lighting and camera angles, crowded environments, inconsistent walking speeds, individual behavioural differences, dataset limitations, false-positive detections, computational complexity, and privacy concerns. In addition, it investigates the importance of explainable AI, real-time processing, edge computing, and privacy-preserving video analytics for practical deployment. The review identifies key research gaps and outlines future research directions toward developing robust, scalable, and context-aware surveillance frameworks. By critically examining existing approaches and emerging technologies, this study aims to provide a comprehensive foundation for researchers and practitioners developing intelligent video surveillance systems that support early anomaly identification, security

monitoring, and crime prevention while preserving human oversight and minimizing unjustified suspicion.

Keywords— Gait Speed Monitoring, Suspicious Behaviour Analysis, Automated Crime Detection, Intelligent Video Surveillance, Computer Vision, Human Activity Recognition, Deep Learning, Human Pose Estimation, Anomaly Detection, Object Tracking, Spatiotemporal Analysis, Artificial Intelligence, Real-Time Surveillance, Explainable AI, Privacy-Preserving Surveillance.

I. INTRODUCTION

The rapid growth of urban populations, public transportation networks, commercial establishments, and interconnected public spaces has increased the demand for intelligent security and surveillance systems. Video surveillance has become an essential component of modern security infrastructure, supporting public safety, access control, traffic monitoring, and incident investigation. Conventional Closed-Circuit Television (CCTV) systems primarily rely on human operators to continuously observe video streams and identify potentially suspicious activities. However, the increasing volume of surveillance footage makes manual monitoring challenging because it requires sustained attention, significant human resources, and timely interpretation of complex behavioural patterns. Human operators may overlook critical events because of fatigue, distraction, visual complexity, and the simultaneous monitoring of multiple camera feeds. Consequently, automated video surveillance systems that can identify unusual movement patterns and potentially threatening activities have become an important research direction.

Advances in computer vision, machine learning, and deep learning have enabled surveillance systems to move beyond passive video recording toward automated scene understanding and intelligent event analysis. These systems can detect people, estimate body poses, track movement trajectories, recognize activities, and identify deviations from learned behavioural patterns. Research on video anomaly detection has demonstrated the potential of computational models to identify unusual events by learning normal patterns of activity and detecting deviations from those patterns [1], [2]. Furthermore, advances in human activity recognition have established effective approaches for analyzing spatial and temporal information in video sequences, providing a foundation for automated behaviour understanding [3].

Within this research domain, gait speed monitoring provides a useful behavioural indicator for examining human movement in surveillance environments. Gait speed refers to the rate at which an individual moves along a walking trajectory and can be estimated using successive observations of a tracked person, temporal displacement, camera calibration, and scene geometry. Variations in walking speed, sudden acceleration, abrupt deceleration, repeated changes in direction, irregular movement, and unusual stopping patterns may provide useful contextual evidence for identifying activities that warrant further examination. However, these characteristics are not inherently indicative of criminal intent. A person may run because of an emergency, walk slowly because of a physical limitation, or change direction because of ordinary navigation. Therefore, gait speed should be interpreted alongside contextual information, movement trajectories, surrounding activities, and temporal behaviour rather than being used as an independent indicator of criminality.

The motivation for integrating gait speed monitoring with suspicious behaviour analysis lies in the potential to combine measurable motion characteristics with higher-level behavioural interpretation. While conventional surveillance systems often focus on detecting predefined objects or activities, an intelligent surveillance framework can examine how individuals move, how their movement evolves over time, and whether their actions differ significantly from the expected patterns of a particular environment. Such an approach can support early identification of unusual events, prioritize video segments for operator review, and reduce dependence on continuous manual observation.

A. Role of Gait Speed Monitoring in Intelligent Surveillance

Gait analysis is an important research area in computer vision that investigates human locomotion through observable movement characteristics, including stride length, cadence, body posture, step frequency, and walking speed. Gait-based analysis has been extensively investigated for person recognition and behavioural understanding because human walking patterns contain spatial and temporal information that can be extracted from video sequences. Recent developments in deep gait recognition have demonstrated the effectiveness of deep learning models in learning representative features from human silhouettes, body poses, and motion sequences [4].

In video surveillance applications, gait speed monitoring differs from conventional gait recognition. Gait recognition primarily aims to identify or verify individuals based on their walking patterns, whereas gait speed monitoring focuses on quantifying movement dynamics and identifying deviations from contextually appropriate motion patterns. The two approaches can share several underlying techniques, including human detection, tracking, pose estimation, temporal feature extraction, and motion representation, but their objectives and evaluation criteria are different.

Gait speed can be estimated by measuring the displacement of a tracked individual over a specified time interval. A simplified formulation is expressed as

$$v_t = \frac{\| \mathbf{p}_t - \mathbf{p}_{t-\Delta t} \|}{\Delta t}$$

where v_t represents the estimated speed, $\mathbf{p}_t$ and $\mathbf{p}_{t-\Delta t}$ represent the person's positions at two different time instants, and Δt denotes the elapsed time. When positions are represented in image pixels, the resulting quantity is pixel displacement per unit time rather than physical walking speed. Estimating speed in metres per second requires appropriate camera calibration, perspective correction, or ground-plane mapping.

The temporal analysis of gait speed can reveal changes that may be overlooked by static image analysis. For example, a surveillance system may detect sudden acceleration, repeated pacing, rapid approach toward a restricted area, abrupt changes in direction, or unexpected movement relative to surrounding pedestrian flows. Nevertheless, these observations should be interpreted within the scene context. Running, stopping, or changing direction can occur during legitimate activities and must not automatically be classified as criminal behaviour.

Therefore, effective gait speed monitoring requires a combination of accurate person tracking, reliable motion estimation, contextual modelling, and temporal analysis. Errors in object detection, identity tracking, camera calibration, or trajectory estimation may lead to incorrect speed measurements and unreliable anomaly scores. These limitations make gait speed monitoring an important but technically challenging component of intelligent video surveillance.

B. Suspicious Behaviour Analysis Using Computer Vision and Deep Learning

Suspicious behaviour analysis involves identifying movement patterns or activities that deviate from expected behaviour within a specific environment. Unlike conventional object detection, which identifies predefined categories such as people, vehicles, or objects, behaviour analysis considers how entities interact with their surroundings and how their actions evolve over time. Relevant behavioural patterns may include prolonged presence in restricted areas, repeated movement around a location, unusual running or direction changes, aggressive physical interactions, unauthorized entry, and potentially dangerous crowd dynamics.

Anomaly detection provides a fundamental methodological framework for this task. Chandola et al. [1] presented a comprehensive survey of anomaly detection techniques and discussed their application to identifying observations that differ from expected data patterns. In video surveillance, such deviations may occur in spatial, temporal, appearance-based, or motion-related features. However, an anomaly is not necessarily a crime; its interpretation depends on environmental context, the operational objective, and the available evidence.

Deep learning has significantly expanded the capabilities of automated surveillance by enabling models to learn complex

representations directly from video data. Nayak et al. [2] reviewed deep learning-based video anomaly detection methods, highlighting different modelling strategies and the challenges associated with environmental variability, ambiguous anomalies, and limited datasets. Similarly, Duong et al. [3] examined deep learning techniques, preprocessing methods, feature engineering, and benchmark datasets for abnormal human activity detection in surveillance systems.

Several classes of computational techniques are relevant to suspicious behaviour analysis:

- Convolutional Neural Networks (CNNs): Extract spatial features from video frames, silhouettes, and human body representations.
- Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks: Model temporal dependencies and changes in human movement over successive frames.
- Pose estimation and skeleton-based analysis: Represent body joints and their movements to support the analysis of posture, gestures, and human interactions.
- Trajectory-based analysis: Examines movement paths, direction changes, acceleration, and spatial relationships between individuals.
- Transformer-based models: Capture long-range temporal dependencies and contextual relationships within video sequences.
- Unsupervised and semi-supervised anomaly detection: Learn normal behavioural patterns and identify deviations when labelled examples of suspicious activities are limited.

Research by Sultani et al. [5] demonstrated a weakly supervised approach to real-world surveillance video anomaly detection, addressing the difficulty of obtaining detailed frame-level annotations for unusual events. This research direction is particularly relevant because genuinely suspicious events are relatively diverse, context-dependent, and difficult to represent through a fixed set of predefined activity labels.

Despite these advances, suspicious behaviour analysis remains challenging because similar movements may correspond to different intentions. For instance, rapid movement may indicate an emergency response, an attempt to catch public transport, or another ordinary activity. Consequently, a reliable surveillance system should identify observable anomalies and communicate the evidence supporting an alert rather than making definitive accusations based solely on movement patterns.

C. Integration of Gait Speed Monitoring and Behavioural Analysis

Integrating gait speed monitoring with suspicious behaviour analysis provides an opportunity to develop more informative surveillance systems than those based on isolated motion features. Gait speed captures movement intensity, while trajectory analysis describes spatial progression and temporal behaviour modelling captures changes in activity over time. Combining these complementary signals can improve the characterization of unusual events.

II. LITERATURE SURVEY

The integration of gait speed monitoring, human activity recognition, and suspicious behaviour analysis has emerged as an important research direction in intelligent video surveillance. Traditional CCTV systems primarily record visual information for subsequent inspection, whereas modern surveillance frameworks employ computer vision, machine learning, and deep learning to identify individuals, track their movements, recognize activities, and detect deviations from normal behavioural patterns. The objective of automated surveillance research is to develop systems that can process large volumes of video data efficiently and assist security personnel in identifying potentially significant events.

Previous studies have investigated video anomaly detection, human gait analysis, spatiotemporal feature extraction, multi-object tracking, skeleton-based activity recognition, and deep learning-based behavioural classification. Although these research areas share several technical components, they address different aspects of surveillance intelligence. Gait analysis characterizes human locomotion, trajectory analysis examines spatial movement, and anomaly detection identifies deviations from learned or predefined patterns. Combining these capabilities may improve the contextual interpretation of unusual movements.

This literature review examines representative research contributions relevant to gait speed monitoring and suspicious behaviour analysis. It discusses their methodologies, contributions, limitations, and applicability to automated surveillance, with particular emphasis on identifying research gaps and opportunities for developing more reliable, context-aware systems.

A. Video Anomaly Detection in Surveillance Systems

Chandola et al. [1] established a broad foundation for anomaly detection by reviewing statistical, machine learning, and data-mining approaches for identifying observations that deviate from expected patterns. Their work provides a conceptual basis for surveillance applications in which abnormal events are detected by learning regular behavioural patterns. However, the study was not specifically designed for video-based gait analysis, and its general anomaly detection framework does not directly address the complexities of human movement in crowded surveillance environments.

Sultani et al. [6] proposed a weakly supervised framework for real-world anomaly detection in surveillance videos using a deep multiple-instance learning ranking model. Their approach learned from video-level labels rather than requiring detailed frame-level annotations for every anomalous event. The authors also introduced the UCF-Crime dataset, containing 1,900 long, untrimmed

surveillance videos covering 13 categories of anomalies alongside normal activities. This work is particularly relevant to automated crime detection because it demonstrates how models can learn to identify suspicious video segments from large-scale surveillance footage. Nevertheless, its anomaly scoring approach does not explicitly establish gait speed as a primary behavioural feature, and the distinction between unusual activity and actual criminal intent remains unresolved.

Nayak et al. [7] reviewed deep learning-based methods for video anomaly detection, examining neural architectures, feature extraction strategies, and the challenges associated with recognizing unusual events. Their analysis highlights the importance of learning spatial and temporal representations from video sequences. The review also indicates that environmental variability, limited anomalous training samples, and differences between training and testing scenarios can affect detection performance. For gait-based surveillance, these limitations imply that a model trained in one environment may not reliably identify unusual walking patterns in another without suitable adaptation.

A broader analysis by Nguyen et al. [8] examined anomaly analysis in images and videos, including computational approaches, datasets, evaluation methodologies, and outstanding research problems. Their review is relevant to suspicious behaviour analysis because it emphasizes the diversity of anomaly detection tasks and the need for appropriate experimental evaluation. However, general anomaly detection approaches do not necessarily explain which human movement characteristics contribute to a particular alert. Integrating interpretable gait speed, trajectory, and posture information could help address this limitation.

More recently, a review published in IEEE Access [9] examined deep learning approaches and benchmarks for video surveillance anomaly detection. It discussed the evolution from conventional computer vision methods to CNN-based models, sequential learning, transformers, and other deep architectures. The review identified continuing challenges associated with occlusion, perspective distortion, diverse anomalous events, computational cost, and real-time operation. These findings support the need for a surveillance framework that combines motion-based features with contextual information while balancing detection accuracy and computational efficiency.

B. Gait Analysis and Human Movement Characterization

Gait analysis provides a complementary foundation for understanding movement-related behaviour. Han and Bhanu [10] investigated individual recognition using the Gait Energy Image (GEI), which represents a walking sequence through an aggregate silhouette image. Their work demonstrated how gait sequences could be transformed into compact representations for automated analysis. Although GEI-based methods primarily address identity recognition rather than suspicious behaviour detection, they establish the importance of extracting meaningful motion information from successive video frames.

For gait speed monitoring, the central objective differs

from person identification. Rather than determining who an individual is, the system estimates how quickly that person moves and how their movement changes over time. Speed, acceleration, direction, stopping duration, and trajectory curvature can be used to describe locomotion. These features may contribute to identifying unusual movement patterns when interpreted in relation to the surrounding environment.

A key limitation is that image-space displacement does not directly correspond to physical walking speed. Camera perspective, the distance between a person and the camera, and the orientation of the walking trajectory can distort apparent motion. Consequently, reliable estimation of speed in metres per second requires calibration or a suitable mapping from image coordinates to the ground plane. Tracking errors can also introduce discontinuities that produce misleading speed estimates.

The literature therefore suggests that gait-based surveillance should distinguish between three related tasks: gait representation, quantitative movement estimation, and contextual behavioural interpretation. A model designed for gait recognition cannot automatically be assumed to estimate walking speed accurately, and a speed threshold alone cannot establish that a person is behaving suspiciously.

C. Crowd Behaviour and Trajectory-Based Anomaly Detection

Mehran et al. [11] proposed a social-force-based approach for detecting abnormal behaviour in crowded scenes. Their method modeled pedestrian interactions and crowd motion to identify deviations from expected collective behaviour. Instead of considering individuals exclusively in isolation, the approach examined how movement patterns differed from the surrounding crowd dynamics. This is relevant to suspicious behaviour analysis because a person's movement can be better understood by considering nearby pedestrians, local movement flow, and changes in collective activity. However, crowd-level anomaly detection may not reliably identify subtle individual behaviours, such as repeated pacing or a short-duration acceleration, unless these events produce a detectable deviation in the modeled motion patterns.

Trajectory-based methods offer another approach to surveillance analysis. By tracking individuals across successive frames, a system can construct movement paths and examine speed, direction, acceleration, turning frequency, and spatial relationships. These features can be used to identify unusual movement relative to a predefined route, restricted region, or learned pedestrian-flow pattern. Nevertheless, a trajectory that differs from the dominant movement pattern may reflect legitimate navigation rather than suspicious conduct.

The integration of individual trajectories with gait speed monitoring can provide a more detailed description of human movement. For example, a system can distinguish between a person moving rapidly along a direct path and a person repeatedly changing direction within a restricted area. Even in such cases, the resulting observations should be treated as contextual indicators for review rather than proof of wrongdoing.

Table 1. Comparative analysis of representative research studies

Ref.	Research focus	Methodology / contribution	Limitation relevant to this review
[6]	Real-world video anomaly detection	Weakly supervised multiple-instance learning and anomaly ranking	Does not explicitly center on gait speed estimation
[7]	Deep learning-based anomaly detection	Review of deep learning models and video anomaly detection techniques	General anomaly detection does not necessarily explain individual movement anomalies
[8]	Image and video anomaly analysis	Comprehensive review of anomaly detection methods, datasets, and evaluation	Broad scope rather than gait-specific behavioural modelling
[9]	Surveillance anomaly detection benchmarks	Analysis of deep learning architectures, datasets, and implementation challenges	Real-time scalability and diverse anomalies remain challenging
[10]	Gait representation	Gait Energy Image for individual recognition	Identity recognition is different from speed estimation
[11]	Abnormal crowd behaviour	Social-force-based modelling of pedestrian interactions	Individual-level behavioural deviations may require additional features
[12]	Skeleton-based activity recognition	Spatial-temporal graph convolutional networks	Pose estimation errors can affect downstream analysis
[13]	Skeleton graph representation	Extended graph topology and joint-relation modelling	Performance depends on pose quality and temporal information
[14]	Multi-object tracking	Motion prediction and appearance-based identity association	Occlusion and identity switches can distort speed estimates

[15]	Real-time anomaly detection	Weakly supervised learning with an emphasis on processing efficiency	Reliable event localization and generalization remain challenging
------	-----------------------------	--	---

III. ALGORITHMS

A. Algorithm Overview

The proposed algorithm integrates human detection, multi-object tracking, gait speed estimation, trajectory analysis, spatiotemporal behaviour recognition, and anomaly scoring to support automated video surveillance. Its primary objective is to identify unusual movement patterns and potentially suspicious activities by analyzing changes in walking speed, acceleration, direction, posture, and contextual movement patterns.

Unlike conventional surveillance approaches that rely on a single motion threshold, the proposed framework combines multiple behavioural indicators to assess whether an observed event deviates from expected behaviour. The algorithm is intended as a conceptual framework for the comprehensive review; its effectiveness must be established through implementation and experimental evaluation.

The algorithm consists of the following major stages:

1. Video acquisition and preprocessing.
2. Human detection and multi-object tracking.
3. Gait speed and acceleration estimation.
4. Trajectory and behavioural feature extraction.
5. Context-aware anomaly score calculation.
6. Suspicious-event flagging and human verification.

B. Proposed Algorithm: Gait Speed-Based Suspicious Behaviour Analysis

Algorithm 1: Integrated Gait Speed Monitoring and Behavioural Anomaly Detection

Input:

Surveillance video stream (V)

Frame rate (F)

Trained human detection model (D)

Multi-object tracking model (T)

Camera calibration parameters (H) , if available

Normal behaviour reference model (M)

Anomaly threshold (τ)

Temporal observation window (W)

Output:

Tracked person trajectories

Estimated gait speed and motion features

Anomaly scores and flagged video segments for human review

Pseudocode

C. Operational Workflow

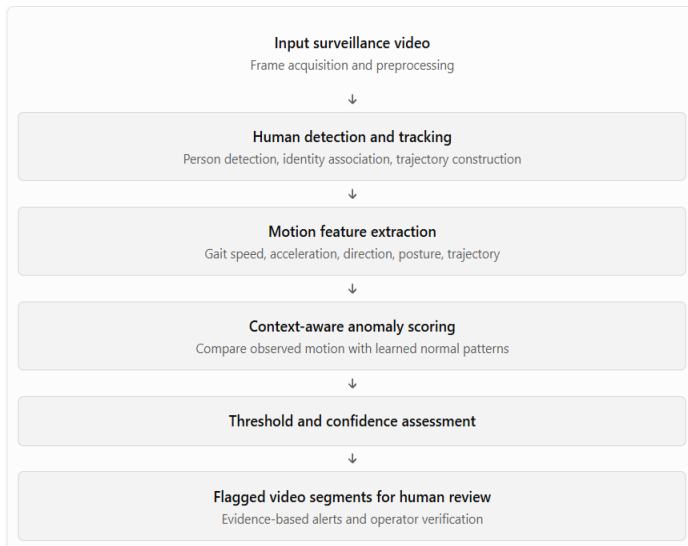


Figure 1: Operational Workflow

This workflow is consistent with established research directions involving spatiotemporal motion analysis, trajectory prediction, and velocity-aware anomaly detection. For example, Sun and Yang [16] investigated unsupervised video anomaly detection using multi-timescale trajectory prediction and velocity calculation, while Zhu et al. [17] studied abnormal running detection using spatiotemporal parameters and multi-target tracking.

IV. CONCLUSION

The integration of gait speed monitoring and suspicious behaviour analysis represents a promising research direction for developing intelligent, automated, and context-aware video surveillance systems. This review examined the fundamental concepts, methodologies, and technological developments associated with human movement analysis, gait speed estimation, trajectory tracking, human activity recognition, and video anomaly detection. The reviewed literature demonstrates that computer vision, machine learning, and deep learning techniques can support the automated identification of unusual movement patterns and reduce the dependence on continuous manual observation of surveillance footage.

The analysis highlights the complementary roles of gait speed estimation, multi-object tracking, pose estimation, spatiotemporal feature extraction, and contextual anomaly detection. Gait speed and acceleration provide quantitative information about movement dynamics, while trajectory analysis captures spatial behaviour and temporal models identify deviations from learned patterns. Integrating these features within a unified framework may improve the interpretation of unusual activities compared with approaches that rely exclusively on fixed speed thresholds or isolated visual features. Furthermore, CNNs, LSTM networks, graph convolutional networks, Transformer-based architectures, and weakly supervised learning approaches offer different capabilities for extracting meaningful behavioural representations from surveillance videos.

Despite these advances, several challenges remain, including inaccurate speed estimation caused by perspective distortion, tracking failures under occlusion, variations in lighting and

camera viewpoints, limited annotated datasets, high computational requirements, and the difficulty of distinguishing legitimate activities from genuinely concerning events. These limitations emphasize the importance of adaptive behavioural baselines, robust trajectory estimation, efficient real-time processing, explainable anomaly scores, and comprehensive experimental evaluation. Future research should focus on developing hybrid surveillance frameworks that combine motion-based features with scene context, interpersonal interactions, and temporal behavioural patterns while improving generalization across diverse environments.

Privacy, fairness, and responsible interpretation must also remain central to the design of automated surveillance systems. An unusual walking speed, abrupt direction change, or abnormal trajectory should not be considered independent evidence of criminal intent. Instead, the proposed approach should function as a decision-support mechanism that identifies potentially significant events, provides interpretable evidence, and enables authorized human operators to verify alerts before taking action.

In conclusion, gait speed monitoring combined with contextual suspicious behaviour analysis offers a valuable foundation for next-generation intelligent video surveillance systems. By integrating reliable movement estimation, spatiotemporal modelling, anomaly detection, and human-in-the-loop verification, future systems may improve the efficiency of surveillance monitoring and support earlier identification of unusual events. However, the practical effectiveness of such systems must be established through rigorous testing on representative datasets, using appropriate detection, localization, speed-estimation, computational-efficiency, and false-alarm metrics. This research direction provides opportunities for developing scalable, interpretable, and privacy-conscious surveillance technologies that support public safety without equating behavioural anomalies with criminal activity.

REFERENCES

- [1] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys*, vol. 41, no. 3, Art. no. 15, pp. 1–58, Jul. 2009, doi: 10.1145/1541880.1541882.
- [2] R. Nayak, U. C. Pati, and S. K. Das, "A comprehensive review on deep learning-based methods for video anomaly detection," *Image and Vision Computing*, vol. 106, Art. no. 104078, Feb. 2021, doi: 10.1016/j.imavis.2020.104078.
- [3] H.-T. Duong, V.-T. Le, and V. T. Hoang, "Deep learning-based anomaly detection in video surveillance: A survey," *Sensors*, vol. 23, no. 11, Art. no. 5024, May 2023, doi: 10.3390/s23115024.
- [4] A. Sepas-Moghaddam and A. Etemad, "Deep gait recognition: A survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 1, pp. 264–284, Jan. 2023, doi: 10.1109/TPAMI.2022.3151865.
- [5] W. Sultani, C. Chen, and M. Shah, "Real-world anomaly detection in surveillance videos," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Salt Lake City, UT, USA, 2018, pp. 6479–6488, doi: 10.1109/CVPR.2018.00678.

- [6] W. Sultani, C. Chen, and M. Shah, "Real-world anomaly detection in surveillance videos," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Salt Lake City, UT, USA, 2018, pp. 6479–6488. doi: 10.1109/CVPR.2018.00678.
- [7] R. Nayak, U. C. Pati, and S. K. Das, "A comprehensive review on deep learning-based methods for video anomaly detection," Image and Vision Computing, vol. 106, Art. no. 104078, 2021. doi: 10.1016/j.imavis.2020.104078.
- [8] K. Nguyen et al., "Anomaly analysis in images and videos: A comprehensive review," ACM Computing Surveys, vol. 55, no. 7, Art. no. 148, 2022. doi: 10.1145/3544014.
- [9] K. U. Duja et al., "Video surveillance anomaly detection: A review on deep learning benchmarks," IEEE Access, vol. 12, pp. 164811–164842, 2024. doi: 10.1109/ACCESS.2024.3491868.
- [10] J. Han and B. Bhanu, "Individual recognition using gait energy image," IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 2, pp. 316–322, Feb. 2006. doi: 10.1109/TPAMI.2006.38.
- [11] R. Mehran, A. Oyama, and M. Shah, "Abnormal crowd behavior detection using social force model," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Miami, FL, USA, 2009, pp. 935–942. doi: 10.1109/CVPR.2009.5206641.
- [12] S. Yan, Y. Xiong, and D. Lin, "Spatial temporal graph convolutional networks for skeleton-based action recognition," in Proc. AAAI Conf. Artif. Intell., vol. 32, no. 1, 2018. doi: 10.1609/aaai-v32i1.12328.
- [13] Q. Wang, K. Zhang, and M. A. Asghar, "Skeleton-based ST-GCN for human action recognition with extended skeleton graph and partitioning strategy," IEEE Access, vol. 10, pp. 41403–41410, 2022. doi: 10.1109/ACCESS.2022.3164711.
- [14] N. Wojke, A. Bewley, and D. Paulus, "Simple online and realtime tracking with a deep association metric," in Proc. IEEE Int. Conf. Image Process. (ICIP), Beijing, China, 2017, pp. 3645–3649. doi: 10.1109/ICIP.2017.8296962.
- [15] "Real-time weakly supervised video anomaly detection," in Proc. IEEE/CVF Winter Conf. Appl. Comput. Vis. (WACV), 2024. doi: 10.1109/WACV57701.2024.00670.
- [16] Q. Sun and Y. Yang, "Unsupervised video anomaly detection based on multi-timescale trajectory prediction," Computer Vision and Image Understanding, vol. 227, Art. no. 103615, 2023. doi: 10.1016/j.cviu.2022.103615.
- [17] B. Zhu et al., "Detection and recognition of abnormal running behavior in surveillance video," Mathematical Problems in Engineering, 2012, Art. no. 296407. doi: 10.1155/2012/296407.