

Optimized CCTV Monitoring using Biometrics and AI-driven Surveillance

DR. K. R. MAMATHA, PRIYANKA ANAND D, RISHITA UMASANKARAN, NIDHI JOSHI
Information Science and Engineering
BMS College of Engineering
1908, Bull Temple Road
BANGALORE

Abstract: - Traditional surveillance systems are becoming inadequate for modern security and health monitoring needs. This survey explores the integration of AI and ML in next-generation CCTV systems, transforming them from passive monitors to intelligent, proactive solutions. Key advancements include biometric authentication for secure identification, behavior analysis for detecting suspicious activities, and health monitoring for emergencies like falls or medical distress. To address privacy concerns, the study reviews encryption, data anonymization, and customizable monitoring parameters to ensure compliance with ethical standards. Using real-time analytics and adaptive designs, AI-driven surveillance is reshaping security and healthcare in public spaces, workplaces, and medical environments, fostering safer communities while respecting privacy.

Key-Words: - cctv monitoring, intelligent surveillance, facial recognition, anomaly detection, privacy protection, artificial intelligence

Received: May 18, 2024. Revised: March 19, 2025. Accepted: April 21, 2025. Published: July 16, 2025.

1 Introduction

In our increasingly interconnected world, the rapid advancement of artificial intelligence (AI) and machine learning (ML) is reshaping security and healthcare monitoring systems. While traditional CCTV setups serve basic surveillance needs, they often fall short in responding to the complex demands of modern environments, especially where real-time intervention is critical. Conventional systems operate passively, requiring manual footage review and offering limited analytical capabilities, leading to missed incidents and overwhelming data.

To address these gaps, this study explores various AI-driven methodologies for intelligent surveillance and proposes a modular architecture that enhances real-time efficiency, accuracy, and privacy. The proposed Smart CCTV Monitoring System demonstrates sub-second frame processing, reduced false positives through reappearance-based facial tracking, and secure AES-encrypted face-data storage. It supports flexible deployment (on-premises or cloud-based) and is designed to integrate easily with existing infrastructure.

By incorporating anomaly detection, facial recognition, fall detection, and health monitoring, the system transforms surveillance from a reactive tool to a proactive safety mechanism. AI techniques allow the differentiation between routine and suspicious behaviors, such as unauthorized access or unusual gatherings, and trigger timely alerts to the relevant authorities. The system also supports healthcare applications, such as monitoring patient status or detecting fever symptoms in epidemic-prone zones.

Importantly, this solution is based on privacy. Through data anonymization, encryption, and customizable monitoring parameters, it ensures legal and ethical data handling while maintaining operational effectiveness.

In summary, the proposed AI-powered CCTV architecture represents a step toward smarter and more responsive surveillance. By combining real-time analytics with ethical data practices, it offers a scalable solution for safeguarding public, institutional, and healthcare environments.

2.1 Objectives

- (1) The development of an integrated solution of surveillance that prides itself on blending biometric identification, behavioral analysis, and health monitoring into a unique whole. The applicability is for hospitals, public safety, commercial offices, and educational institutions.
- (2) Real-time audit of advanced identification such as facial recognition and cancellable biometric templates to ensure safe, privacy-preserving identity verification. Instantly detects and alerts security teams of suspicious behaviors, newcomers, or breach in security in real time.
- (3) Implements an AI-based motion analysis and speech frequency monitoring, capable of detection of medical emergencies, such as falls or irregularity in breathing, giving alarm to emergency services with real-time precise location when detected.
- (4) Use encryption with access to recorded data like video and audio to prevent unauthorized access. Effective data-retention and data-reviews mechanisms that would comply with privacy rules and build user trust.
- (5) Formulate intuitive users' interfaces to monitor and control. Compatibility with installed IP cameras and with Network Video Recorders (NVRs) will guarantee common use and wide acceptance

2.2 Scope

- (1) **Integrated Surveillance Architecture**
This study proposes a unified AI-driven surveillance system that merges biometric identification, behavioral analysis, and health anomaly detection, ensuring broad applicability across public institutions, hospitals, commercial facilities, and educational sectors.
- (2) **Real-Time Threat Detection and Response**
The system is designed for real-time detection of suspicious behavior, unauthorized access, and the reappearance of unknown individuals. This allows

immediate alerts to security personnel, minimizing risks and enabling proactive incident management.

- (3) **AI for Health and Emergency Monitoring**

The architecture includes motion analysis and audio frequency evaluation to identify critical events, such as falls or abnormal breathing. This is especially beneficial for elderly care, hospital monitoring, and high-risk environments.

- (4) **Privacy-Preserving Data Handling**

A strong emphasis is placed on data security and compliance, with mechanisms for encrypted video/audio storage and restricted access. This ensures alignment with GDPR and HIPAA-like regulations in health and surveillance sectors.

- (5) **Industrial Applications**

In industrial contexts, the system supports:

- Workplace safety monitoring (e.g., fall detection in hazardous areas).
- Intrusion detection in restricted or high-risk zones.
- Compliance verification for PPE usage and worker behavior.
- Predictive maintenance uses surveillance to detect machine anomalies.

- (6) **Advanced Technological Stack**

The solution leverages modern AI models such as YOLOv8, ResNet, FaceNet, and 3D-CNNs, integrated with NVR/IP camera infrastructure and optionally backed by cloud-based analytics platforms for scalability and big data processing.

- (7) **Cross-Platform Usability**

The system is designed for use across desktop and mobile platforms, ensuring wide accessibility for surveillance teams, medical personnel, and emergency responders.

- (8) **Scalability and Adaptability**

The framework supports both on-premises and cloud deployment, making it adaptable for settings of various scales, from small offices to smart cities, while maintaining performance under varying environmental and lighting conditions.

2 Literature Survey

The first study analyzed presents an AI-based intelligent video surveillance system designed to monitor over 1000 cameras in real time using advanced computer vision techniques like YOLOv8 and difference detection algorithms [1]. The system automates event detection, classifies alarms by priority, and enables targeted monitoring through predefined regions of interest (ROI), significantly reducing the reliance on human operators. It is highly scalable, allowing additional cameras and processing scripts to be integrated based on available computing resources. Key features include real-time person detection, change detection in video frames, and a web-based interface for camera management and event review. The system supports diverse hardware configurations and adapts to various camera types, ensuring operational flexibility. Demonstrated through a use case in railway station security, the technology proves effective for public safety, with broader applicability in military, commercial, healthcare, and residential surveillance contexts.

The next paper presents a deep learning-based Human Action Recognition (HAR) system for video surveillance, combining the KTH dataset with a custom real-time dataset to enhance model robustness [2]. It employs Convolutional Neural Networks (CNNs) with a two-phase architecture: training on preprocessed KTH data and testing on real-time video input. Key preprocessing steps include noise removal and data augmentation. The CNN effectively extracts spatiotemporal features for classifying six human actions. The system achieves an impressive average accuracy of 98.8%, with boxing reaching 99.8%, demonstrating its high reliability for real-time surveillance applications.

This paper proposes an anomaly detection algorithm for video surveillance using an improved ResNet-18 convolutional neural network [3]. A self-made dataset simulating five types of surveillance anomalies (e.g., blur, overexposure, noise) was used for training and testing. The model was trained using the SGD optimizer with cross-entropy loss and validated using cross-validation techniques. Results show a high average detection accuracy of

94.8%, outperforming traditional algorithms in classifying and detecting anomalous scenes. The method eliminates the need for manual feature extraction and shows promise for real-world deployment in intelligent security systems.

This paper proposes a privacy-preserving security framework for CCTV systems that use facial recognition [4]. To protect biometric data, techniques like facial area detection, mosaic/scrambling, and encryption are applied so unauthorized users can't access raw facial images. The framework ensures secure communication between CCTV components (camera, server, and client) and introduces reverse scrambling for authorized recovery during investigations. It addresses privacy threats (e.g., tapping, unauthorized access, misuse) and provides countermeasures such as session keys, device authentication, and access control. This system maintains surveillance efficiency while safeguarding personal data integrity in networked environments.

This paper explores the design and capabilities of intelligent video surveillance systems that leverage artificial intelligence and computer vision for real-time security monitoring [5]. It covers key modules such as object detection, tracking, and classification, and discusses different camera types (PTZ, IP, thermal) and video management systems (DVR, NVR) for deployment. Intelligent systems reduce manual effort, improve accuracy, and support automated threat detection in indoor and outdoor environments. The paper also emphasizes video analytics for recognizing abnormal behaviors and optimizing storage through event-based recording. A tiered evaluation model (image acquisition to event understanding) is proposed to assess system performance and deployment efficiency.

This study presents real-time elderly fall detection system using YOLOv8, integrating video feeds, wearable sensors, and AWS services for alerting and analytics [6]. The system achieved 92% accuracy, 88% precision, 90% recall, and a 5-second response time, outperforming YOLOv7 and other models. AWS SNS enabled instant notifications, while AWS Glue supported continuous improvement via data insights. The system's architecture ensures

scalability, adaptability, and future integration with smart home technologies for enhanced elderly care and safety.

This paper presents a face recognition system for low-resolution CCTV footage using a custom CNN6 deep learning model [7]. The system detects faces using Haar cascade classifier and classifies them through a 6-layer CNN trained on 6,667 images from 62 subjects over 500 epochs. The CNN6 achieved 99.99% training, 98.45% validation, and 96.03% testing accuracy, outperforming VGG16 and LHBP models. It also showed 94.55% accuracy on the TinyFace benchmark dataset, demonstrating its robustness for low-resolution surveillance applications.

This paper proposes BFace, a lightweight privacy-preserving face recognition system that uses Bloom filter encoding to securely represent face data for IoT and CCTV applications [8]. Unlike traditional models which protect only stored datasets, BFace ensures privacy even at edge devices by converting facial features (via SVD) into non-reversible Bloom filter space, allowing analytics like SVM classification without exposing raw images. Evaluated on the YaleB dataset, the system achieved up to 92% classification accuracy, outperforming the raw image baseline of 80%, while maintaining low computational overhead suitable for real-time CCTV surveillance.

This paper reviews key challenges and advancements in building fast and efficient surveillance systems using face detection, recognition, image/video processing, and pattern matching techniques [9]. It highlights that existing CCTV setups lack real-time intelligence and require human monitoring. Deep learning models like CNN improve detection accuracy, while techniques like Eigenfaces and SVD help in low-light or wet face recognition. Edge computing enhances processing efficiency for IoT systems. However, issues remain with illumination, pose variation, and night-time visibility. The study concludes that combining the best algorithms across domains is vital for creating smart, privacy-aware, and scalable surveillance systems.

This paper presents a criminal identification system using MTCNN for face detection, FaceNet for embeddings, and various machine learning classifiers for identity verification on the NIST mugshot dataset [10]. Among the tested models, K-Nearest Neighbors (KNN) achieved the highest accuracy at 97.18%, followed by Naive Bayes (94.37%) and Random Forest (91.55%), while Decision Tree performed the worst at 52%. Key evaluation metrics like precision, recall, and F1 score confirm KNN's superior performance. The system proves effective in accurately identifying faces in surveillance applications using deep learning and lightweight classification techniques.

This paper explores the use of deep learning and transfer learning (AlexNet) for fall detection using CCTV footage under realistic, varying environmental conditions [11]. The pre-trained AlexNet CNN was fine-tuned to classify frames into fall or non-fall using a dataset of 30 video records, achieving 99% accuracy and Cohen's kappa of 0.93 for known conditions. For unseen conditions, the model maintained high accuracy, but the kappa dropped to 0.60, indicating reduced generalization. Despite class imbalance, the model showed high specificity (0.99) and good sensitivity (0.93/0.61). Future improvements include temporal frame sequencing and dataset enrichment to reduce false positives.

This paper proposes an enhanced CCTV security system that integrates Object Recognition (using TensorFlow), Twilio API for SMS/calls, OpenCV for image processing, and MySQL for user authentication. Unlike traditional CCTVs that only record footage, the system detects intrusions, captures images of intruders, sends email alerts, SMS notifications, and even makes calls to the owner [12]. Access is secured via a random OTP-based login system, improving security without requiring memorized passwords. It can work with any CCTV hardware via IP address, supports automatic alarm activation, and includes real-time object labeling. Future enhancements include smartphone app support and face identification with demographics, aiming for cost-effective, automated, and widely deployable surveillance.

2 Proposed System Design

The proposed Smart CCTV Monitoring System has been tested under diverse lighting, motion, and occlusion conditions to ensure robustness. The system integrates advanced deep learning models and AI-powered logic to deliver intelligent surveillance, real-time alerts, privacy-preserving data handling, and health event detection. Threaded video streams maintain fluidity and reduce latency, while exception handling ensures uninterrupted operation.

(1) Video Surveillance Module

The Video Surveillance Module serves as the core of the intelligent CCTV system, handling real-time video capture, pre-processing, and analysis. It uses a threaded camera class for non-blocking video stream acquisition, which ensures minimal latency and high frame stability. This module is architected with two major subcomponents:

Anomaly Detection Submodule:

This component employs YOLOv8 for real-time object detection, enabling the identification of people, vehicles, and contextual objects within the environment. Detected bounding boxes and class labels are passed to a CNN-LSTM (Convolutional Neural Network + Long Short-Term Memory) pipeline, which performs temporal sequence modeling. This hybrid model allows the system to detect complex behavioral patterns such as loitering, sudden gatherings, or unauthorized entry into restricted zones. Additionally, environmental context—such as abandoned objects or prolonged stationary presence—is evaluated using Scene-Aware CNNs, which add spatial awareness to standard detection logic. These combined techniques enable the system to go beyond static detection, providing meaningful behavioral insight through both frame-level and sequence-level analysis.

Fall Detection Submodule:

The Fall Detection Module is designed to identify human falls in real time using a hybrid approach that combines object detection with human pose

estimation. It utilizes the YOLOv8 model to detect human figures within video frames, and then applies MediaPipe Pose to analyze joint movements and postural orientation.

- Once a person is detected, the system evaluates two primary indicators of a fall:
- Bounding Box Shape – If the person's bounding box becomes abnormally horizontal (i.e., width-to-height ratio exceeds a threshold), and the person appears close to the floor, it suggests a fall.

Torso Angle via Pose Estimation – Using joint landmarks such as shoulders and hips, the system computes the torso angle. A sharp angle beyond a defined limit, combined with a shoulder height closer to the floor, indicates a fall.

To ensure robustness, the module tracks each detected person (referred to as a "track") over time and accumulates fall signals across multiple frames. A fall is only confirmed if these signals persist for several consecutive frames (fall_frames), reducing false positives caused by temporary postures like sitting or bending. Recovery is similarly confirmed over a threshold number of frames (recover_frames).

When a fall is detected, the system sends an email alert to predefined recipients using SMTP. The alert includes the track ID and a timestamp, providing context for the incident. Additionally, bounding boxes are drawn around individuals, labeled as either "FALL" or "OK", offering visual feedback on the live frame.

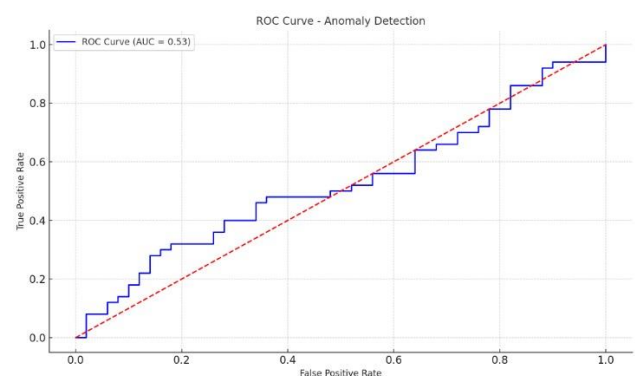


Fig 2.1

Although the module is functional, the ROC curve of the anomaly detection component indicates a modest AUC of 0.53 (refer Fig 2.1). This suggests room for improvement in distinguishing fall events from normal activities. Enhancing model precision through better training data, fine-tuning thresholds, or incorporating temporal models (e.g., LSTMs or Transformers) could significantly improve performance. Together, these submodules provide a highly responsive and intelligent layer of surveillance, capable of detecting not only physical presence but also contextually meaningful behavior.

(2) Biometric Facial Recognition Module

This module forms the identification backbone of the smart surveillance system, enabling both secure access control and persistent individual tracking. This module uses a multi-modal approach to overcome the limitations of conventional face recognition systems, especially in crowded or obstructed environments.

Face Encoding using ResNet-50:

Faces are first detected using MTCNN or Haar cascades, after which ResNet-50-based deep face embedding models convert the face into a 128-dimensional vector representation. This encoding is robust to lighting variations, facial expressions, and angular displacement. These encodings are then compared with the known user database using cosine similarity or Euclidean distance to determine identity with high precision.

Periocular Recognition for Occlusion Handling:

In real-world scenarios such as hospitals or during pandemics, full facial visibility is often obstructed due to masks or gear. To handle this, the system includes a periocular biometrics pipeline. Using fine-tuned CNNs (such as VGG or MobileNet variants trained on periocular datasets), the system extracts and matches localized features from the eye region—including eyelid curvature, interocular distance, and eyebrow contour. This allows for partial face recognition with reasonable accuracy.

Facial Reappearance and Threat Scoring:

Individuals not found in the registered database are labeled as "unknown" and tracked across sessions using facial re-identification (ReID) techniques. A lightweight Triplet-Loss Network ensures that repeated appearances of the same unknown individual are logged with unique IDs. A threat scoring algorithm is implemented to monitor reappearance frequency and location, escalating alerts if a potentially suspicious pattern emerges (e.g., repeated presence near entry points or sensitive zones).

This module's adaptability to various face visibility conditions and its layered verification model makes it suitable for sensitive locations such as airports, hospitals, data centers, and government facilities, where both identification accuracy and privacy preservation are critical.

(3) Alert Notification Module

The Alert Notification Module acts as the core communication bridge between the intelligent surveillance system and the responding personnel, ensuring that any anomaly, fall, or unauthorized access is swiftly escalated. It employs a real-time event queue architecture that captures critical incidents as soon as they are detected by upstream modules. These alerts are routed through multiple channels depending on the configuration and severity of the event. Standard delivery methods include email notifications via SMTP, SMS alerts using third-party APIs (e.g., Twilio), and instant dashboard pop-ups within the system interface for administrators and security teams. The system logs each alert with a comprehensive payload—containing the event type (e.g., "fall", "intrusion", "unknown face detected"), precise timestamp, associated user (if identified), and the camera or zone in which the event occurred. This structured alerting framework enhances the responsiveness of security or medical personnel, especially in time-sensitive emergencies. Future work also considers integration with mobile applications for push notifications, enabling decentralized and on-the-go monitoring capabilities.

(4) Data Privacy Module

In recognition of the increasing emphasis on ethical surveillance and legal compliance (such as GDPR and India's Digital Personal Data Protection Act), the Data Privacy Module plays a crucial role in safeguarding individual identities and maintaining data integrity. This module ensures that all raw face images and video clips are protected using AES-256 encryption, applied immediately upon capture before any storage action. Moreover, the system implements automatic face anonymization—blurring or masking the facial data of individuals who are not recognized as part of the trusted database ("unknown" category). Access to original, unblurred logs is strictly limited to authorized administrators through a secure role-based login system. Decryption operations are permitted only within admin interfaces using protected keys, ensuring end-to-end security of sensitive footage. By integrating these mechanisms, the system adheres to privacy-by-design principles and minimizes the risk of data misuse or identity breaches.

(5) Advanced Data Storage and Scalability

To manage the vast amounts of video and metadata generated in real-time, the system utilizes a hybrid storage architecture that balances local performance with cloud scalability. At its core, a MongoDB database stores structured metadata such as user profiles, facial embeddings, timestamps, and anomaly labels. For large binary files like images and video clips, GridFS is used—a MongoDB-specific mechanism that segments large files into chunks and stores them efficiently. In parallel, critical video clips (such as fall incidents or unauthorized access events) are automatically backed up to cloud-based blob storage services like Azure Blob Storage. These backups are encrypted and include metadata for quick retrieval. The system is designed for modular deployment: smaller setups can run on local servers (e.g., for offices or retail stores), while larger deployments (e.g., city surveillance or hospitals) can leverage cloud-based VMs with load-balancing to handle high traffic and ensure high availability. This architecture ensures both data redundancy and scalability,

accommodating growing surveillance demands over time.

(6) Report Generation Module

The Report Generation Module compiles and visualizes operational statistics to aid in monitoring system performance, auditing events, and supporting administrative decisions. Reports are generated either periodically (daily, weekly) or on-demand by users with appropriate access rights. The system aggregates logs and metrics into structured summaries, highlighting key figures such as the total number of falls detected, accuracy of facial recognition matches, frequency and patterns of unknown person reappearances, and average system response time to alerts. Additionally, graphical plots and time-series analytics are integrated into the dashboard, offering a clear picture of surveillance trends, anomaly heatmaps, and detection hotspots over time. These reports are exportable as PDF or CSV formats and can also be emailed automatically to stakeholders. By maintaining detailed records and metrics, this module enhances system transparency, facilitates compliance auditing, and empowers stakeholders with actionable insights.

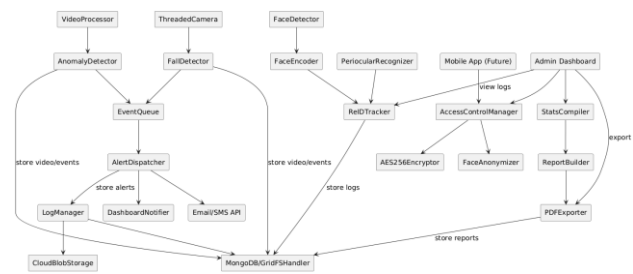


Fig. 2.2

This component diagram (Fig. 2.2) illustrates the modular architecture of a Smart CCTV Monitoring System designed for real-time surveillance, anomaly detection, biometric authentication, and privacy-aware data handling. The system is composed of interconnected components that collectively ensure proactive monitoring, timely alerting, secure storage, and administrative oversight.

Component diagram description

(1) Video Surveillance Module

ThreadedCamera and VideoProcessor handle real-time video acquisition.

These feed data to:

- FallDetector (3D-CNN + Pose Estimation) for detecting human falls.
- AnomalyDetector (YOLOv8 + CNN-LSTM) for recognizing suspicious activities.

Both modules send detected events to the Alert Notification Module and log data into storage.

(2) Biometric Facial Recognition Module

FaceDetector (MTCNN/Haar) and FaceEncoder (ResNet-50) perform facial recognition.

PeriocularRecognizer (CNN-Based) adds fallback recognition for partially visible faces (e.g., masked).

ReIDTracker (Triplet Loss + Threat Score) tracks unknown individuals over time and assigns threat scores.

Outputs are logged for auditing and linked to the alert and report modules.

(3) Alert Notification Module

Uses an EventQueue to buffer events.

AlertDispatcher routes notifications to:

- Email/SMS API
- DashboardNotifier
- Alerts are also stored through the LogManager into cloud and database storage.

(4) Advanced Data Storage

Uses:

- MongoDB/GridFSHandler for structured logs, biometric data, and metadata.
- CloudBlobStorage for large video clip storage.
- LogManager to unify access and manage logs from all modules.

(5) Report Generation Module

StatsCompiler analyzes system data.

ReportBuilder generates insights such as:

- Fall count
- Recognition success rate
- Alert frequency

PDFExporter produces admin-ready reports which are stored and accessible through the dashboard.

(6) Data Privacy Module

Enforces role-based access via AccessControlManager (roles: Admin, Operator, User, Auditor).

Applies AES256Encryptor for video/image encryption.

Uses FaceAnonymizer to blur/obfuscate unknown faces before display or storage.

(7) User Interfaces

Admin Dashboard and future Mobile App interact with:

- Privacy controls
- Report generation
- Real-time alerts

Access is strictly governed through the Data Privacy Module.

4 Conclusion

The proposed Smart CCTV Monitoring System showcases how AI can transform traditional surveillance into an intelligent, responsive, and privacy-conscious solution. By integrating modules for real-time anomaly detection, facial recognition, fall detection, and secure data handling, the system ensures accurate monitoring and timely alerts across diverse environments. Leveraging models like YOLOv8, ResNet-50, and 3D-CNN, it achieves high accuracy while maintaining compliance with privacy standards through encryption and anonymization. Scalable and modular in design, this system offers a robust framework for modern security needs and lays the groundwork for future advancements in proactive and ethical surveillance.

References:

- [1] V. Ilić, "The Integration of Artificial Intelligence and Computer Vision in Large-Scale Video Surveillance of Railway Stations," Zooming Innovation in Consumer Technologies Conference (ZINC), 2024, pp. 42–47.
- [2] R. Sathya, M. Mythili, S. Ananthi, R. Asitha, V. N. Vardhini and M. Shivaani, "Intelligent Video Surveillance System for Real-Time Effective Human Action Recognition using Deep Learning Techniques," 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), 2023, pp. 1826–1831.
- [3] H. Yang, D. Chen and X. Feng, "Abnormality Monitoring and Recognition of Surveillance Video Based on ResNet Residual Network," 3rd International Conference on Artificial Intelligence and Computer Information Technology (AICIT), 2024, pp. 1–4.
- [4] B.-J. Han, H. Jeong and Y.-J. Won, "The Privacy Protection Framework for Biometric Information in Network-Based CCTV Environment," IEEE Conference on Open Systems, 2011, pp. 86–90.
- [5] V. Chundi, J. Bammidi, A. Pegallapati, Y. Parnandi, A. Reddithala and S. K. Moru, "Intelligent Video Surveillance Systems," International Carnahan Conference on Security Technology (ICCST), 2021, pp. 1–5.
- [6] V. Papan and M. S., "Intelligent Fall Detection and Alert System for the Elderly using YOLOv8 and Cloud-based Analytics," 5th International Conference on Electronics and Sustainable Communication Systems (ICESC), 2024, pp. 1–6.
- [7] S. Powale, S. Kawale, A. Dhanawade, N. L. Chutke, S. Bagwe and S. Chavan, "Person Identification in Low Resolution CCTV Footage using Deep Learning," 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2020, pp. 236–240.
- [8] W. Xue, W. Hu, P. Gauranvaram, A. Seneviratne and S. Jha, "An Efficient Privacy-Preserving IoT System for Face Recognition," IEEE Workshop on Emerging Technologies for Security in IoT (ETSecIoT), 2020.
- [9] R. Moorthy, V. Upadhyay, V. V. Holla, S. S. Shetty and V. V. Tantry, "Challenges Encountered in Building a Fast and Efficient Surveillance System: An Overview," Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2020.
- [10] S. T. Ratnaparkhi, P. Singh, A. Tandasi and N. Sindhwani, "Comparative Analysis of Classifiers for Criminal Identification System Using Face Recognition," 9th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO), 2021.
- [11] L. Anishchenko, Real-Time Healthcare Video Monitoring using Biomedical AI Technologies, Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBREIT), 2018.
- [12] H. S. Kanyal, M. Goel, A. S. Tomar, H. K. Yadav, K. Singh, Object Recognition and Security Improvement by Enhancing the Features of CCTV, 2020 9th International Conference on System Modeling and Advancement in Research Trends (SMART), 2020.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0

https://creativecommons.org/licenses/by/4.0/deed.en_US