Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Smart Security Surveillance System for Real-Time Unknown Person Detection and Instant Alert Mechanism

Mrs. Sneha Ashtankar [1], Gunjali Y. Rewatkar [2], Paras G. Doye [3], Priyadarshee P. Waghmare [4], Yashaswi S. Patharkar [5]

[1] Professor, Department of Computer Technology, KITS Ramtek
[2,3,4,5]U. G. Student, Department of Computer Technology, KITS Ramtek

Abstract

Ensuring safety in the residential and public environments become increasingly challenging due to rising numbers of security threats. Conventional surveillance systems primarily depend on continuous human monitoring, which can result in delayed responses and reduced effectiveness. This paper presents smart security surveillance system designed to automatically identify unfamiliar individuals and enhance real-times security management. The proposed software processes live video streams, detects human faces and compares them with authorized records stored in a database. When an unknown person is recognized, the system immediately generates an alert and shares the captured image with user, enabling rapid action. By minimizing manual supervision and improving detection efficiency, the system offers a reliable and practical solution for modern surveillance needs. The developed approach focuses on accuracy, quick response and ease of deployment, making it suitable for homes, offices and institutional environments.

Keywords: Smart Surveillance System, Automated Security Monitoring, Unknown Individual Detection, Facial Recognition Technology, Real-Time Alerting, Video Analytics, Image-Based Identification, Threat Detection, Digital Security Solution.

1. Introduction

The growing need for effective security has led to increased adoption of surveillance technologies across residential, commercial and institutional environments. As urban areas expand and security concerns continue to rise, traditional monitoring methods are no longer sufficient to ensure continuous protection. Conventional CCTV systems require constant human observation, which is both time-consuming and prone to error. Fatigue, distraction and limited attention spans can cause critical events to go unnoticed, reducing the overall reliability of manual surveillance.

Recent advancements in computer vision and image processing have enabled the development of intelligent monitoring solutions capable of analyzing visual data automatically. Smart surveillance systems u software- based technologies to detect human presence, recognize faces and identify individuals without requiring uninterrupted human involvement. Such automation not only improves

response time but also enhances accuracy of the threat detection.

This research focuses on the design and implementation of a smart security surveillance system that detects unknown individuals in real-time and generates immediate alerts with captured images.

2. LITERATURE REVIEW

2.1 AI-DRIVEN VIDEO SURVEILLANCE FOR AUTOMATED THREAT DETECTION

Recent studies show that artificial intelligence has significantly improved effectiveness of surveillance systems by enabling automated detection of suspicious behavior. Deep Learning models can analyze video streams in real-time and identify unusual activities without continuous human monitoring, reducing response time and operational workload. Research also highlights that AI-based systems enhance situational awareness and allow faster decision-making in public safety environments.

2.2 DEEP LEARNING TECHNIQUES FOR VIDEO ANOMALY RECOGNITION

Modern surveillance research increasingly focuses on anomaly detection using neutral networks trained on large datasets. These models learn patterns of normal behavior and flag deviations such as violence, theft or unauthorized entry. Studies indicate that deep learning approaches perform traditional rule-based methods because they can capture complex spatial and temporal relationships within video data.

2.3 EDGE COMPUTING FOR REAL-TIME SURVEILLANCE PROCESSING

Emerging architectures combine surveillance cameras with edge computing to process data closer to the source rather than relying entirely on cloud servers. This approach reduces latency, supports faster alerts and minimizes bandwidth consumption. Researchers emphasize that edge-enabled systems are particularly suitable for smart cities where continuous video streaming can overload centralized infrastructure.

2.4 PRIVACY-AWARE SMART SURVEILLANCE FRAMEWORK

As surveillance technologies expand, protecting personal data has become a major research priority. Recent frameworks integrate encryption, access control and anonymization techniques to prevent unauthorized use of recorded footage. Scholars note that balancing security benefits with ethical considerations is essential for public acceptance and long-term deployment of intelligent surveillance networks.

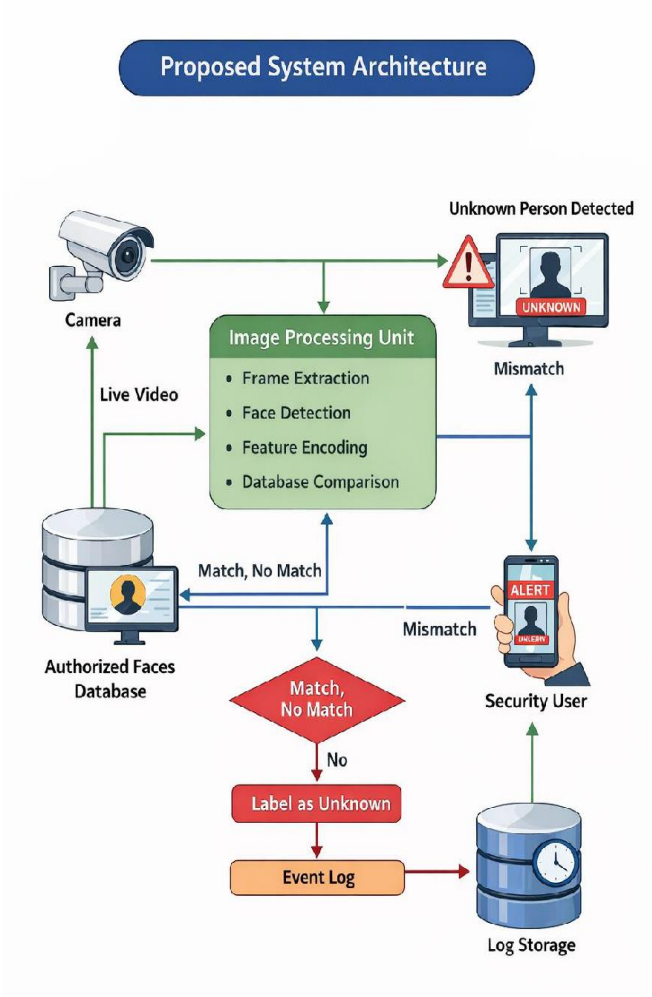
3. METHODOLOGY

This research describes the systematic process used to design and develop smart security surveillance system. The proposed system focuses on automatically detecting unfamiliar individuals and generating immediate alerts improves security response and reduce manual monitoring.

3.1 SYSTEM ARCHITECTURE

The surveillance system is structured as software-based solution that captures live video through a camera and processes the visual data using image analysis techniques. The architecture consists of video acquisition, face detection, feature extraction, database comparison and alert generation modules. Each component works sequentially to ensure accurate identification and timely notification.

Fig. 1 System Architecture



3.2 VIDEO CAPTURE AND DATA ACQUISITION

The process begins with continuous video streaming from a connected camera. Individual frames are extracted from the live feed at regular intervals to enable real-time analysis. This step ensures that the system maintains constant observation of the monitored environment without requiring human supervision.

3.3 FACE DETECTION

Once frames are obtained, the system locates human faces within the images using computer vision algorithms. This stage isolates relevant visual regions and removes unnecessary background information, which improves processing efficiency and detection speed.

3.4 FEATURE EXTRACTION AND ENCODING

After detecting face, distinctive facial characteristics are converted into numerical representations. These encoded features act as digital identifiers that allow the system to differentiate between authorized users and unfamiliar individuals. The transformation of visual data into structured pattern enhances comparison accuracy.

3.5 DATABASE MATCHING

The generated facial encoding is compared with records stored in a predefined database of authorized persons. If a match is found within the acceptable similarity threshold, the individual is classified as recognized. Otherwise, the system labels the person as unknown and proceeds with the alert mechanism.

3.6 UNKNOWN PERSON DETECTION AND ALERT GENERATION

When an unfamiliar face is identified, the system automatically captures the image and sends a notification to the user or security personnel. This alert may include the detected photograph along with the time of occurrence, enabling rapid assessment and response to potential threats.

3.7 DATA STORAGE AND LOGGING

All detection events are recorded for future reference. Maintaining logs helps users review past activities, analyze security patterns and improve system reliability over time.

4. RELATED WORK

Recent advancements in intelligent surveillance system have focused on improving automated threat detection, behavioral analysis and real-time monitoring capabilities. In 2025 study proposed an AI-driven surveillance framework designed to analyze crowd behavior using deep learning architecture such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) and transformers. The research highlighted the importance of supervised and unsupervised learning strategies to enhance anomaly detection accuracy while addressing challenges such as data set bias and limited training data. Another 2025 research effort introduced real-time intelligent surveillance system that integrates YOLOv8 with Deep Learning to identify suspicious behavior and analyze facial emotions. The system demonstrates how combining as object detection with facial analytics can improve response time and support proactive security operations in public environments. Furthermore, an advanced deep learning model for anomaly-based surveillance emphasized the importance of automated video analytics the volume of recorded footage continues to grow rapidly, making manual inspection inefficient.

5. PROPOSED APPROACH

The proposed approach implements an intelligent, software-driven surveillance framework designed for automated identification of unauthorized individuals in real time. The system continuously acquires live video streams and processes individual frames using computer vision algorithms to detect and localize human faces. Following detection, the extracted face regions are transformed into high-dimensional feature vectors through facial encoding techniques. These feature vectors serve as unique biometric descriptors that enable reliable identity discrimination under variations in illumination, pose and facial expression. The generated encodings are compared against a pre-established database of authorized users using a defined similarity metric and threshold value. If the compared similarity score satisfies the acceptance criteria, the individual is classified as authenticated. Otherwise, the subject is designated as unknown. In such cases, the system captures the corresponding image frame, records the detection timestamp and stores the data for documentation and analysis. An automated alerting module is triggered upon detection of an unrecognized individual. The notification, containing relevant visual evidence, is

transmitted to the designated user or security personnel to facilitate immediate response.

6. RESULT AND DISCUSSION

Figure 6.1 demonstrates the system's SMS-based alert mechanism, where real-time notifications are transmitted through integration with the Twilio API. Each message contains detection details, including the number of individuals identified and associated object information. The recurring alerts indicate continuous monitoring and event-driven message generation. This functionality ensures immediate user notification via mobile networks, enabling rapid awareness of security events independent of email or internet access.

Fig. 6.1 SMS based alert mechanism

Figure 6.2 shows the intrusion detection system's output, where captured images of unidentified individuals are automatically stored in a dedicated folder. Each file is labeled with a timestamp to ensure accurate event tracking and documentation. This structured storage mechanism confirms the system's ability to detect, classify and log potential security threats in real time.

Fig. 6.2 Intrusion Detection System

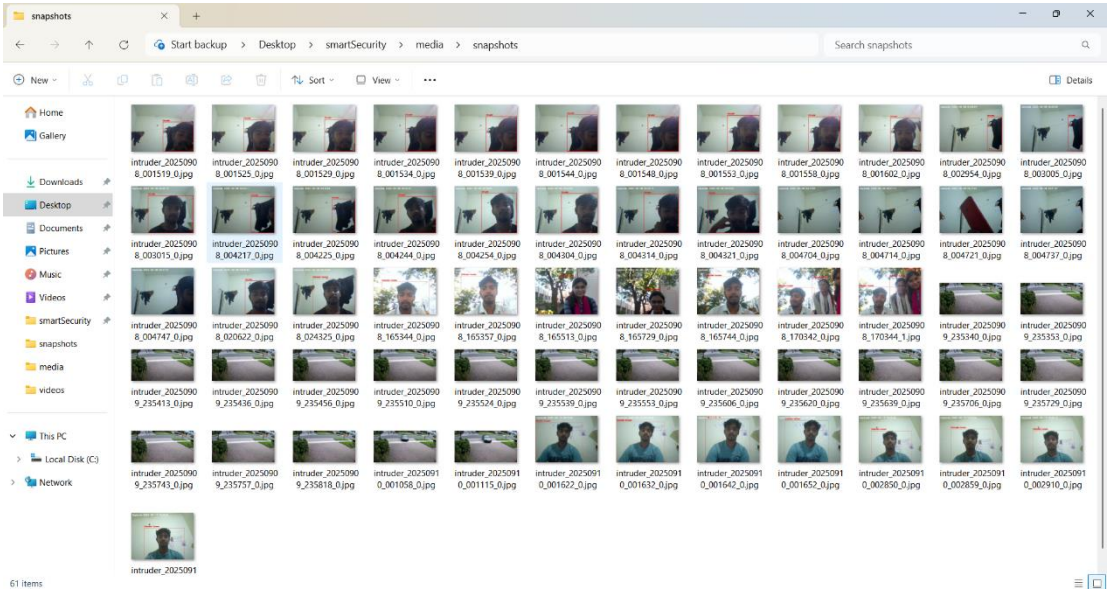


Figure 6.3 depicts a system-generated log file that records surveillance events in a structured textual

format. Each entry includes a precise timestamp, the count of detected individuals and any additionally identified objects within the frame. The sequential records demonstrate continuous monitoring, human detection capability and basic object recognition functionality. This log file acts as an adult trail, ensuring traceability and supporting post-event analysis of system activity.

Fig. 6.3 Log files

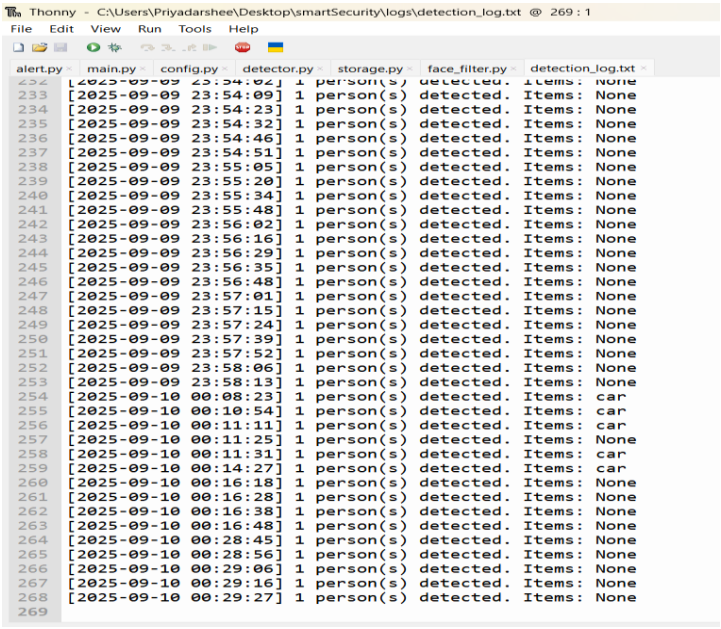


Figure 6.4 illustrates an automated email notification generated by the surveillance system upon detecting an unauthorized individual. Each alert includes a standardized subject line, detection details such as the number of persons identified and relevant object information. The system also attaches a captured image as visual evidence, demonstrating its capability to deliver real-time intrusion alerts with supporting data to the user via email.

Fig. 6.4 Email Notification

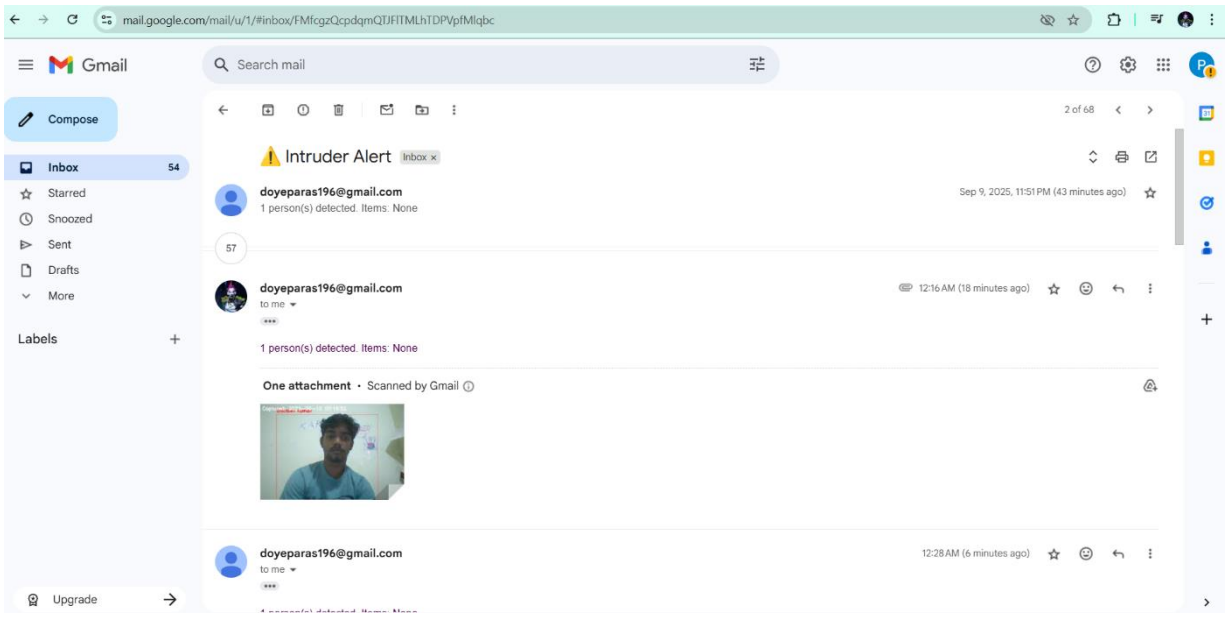
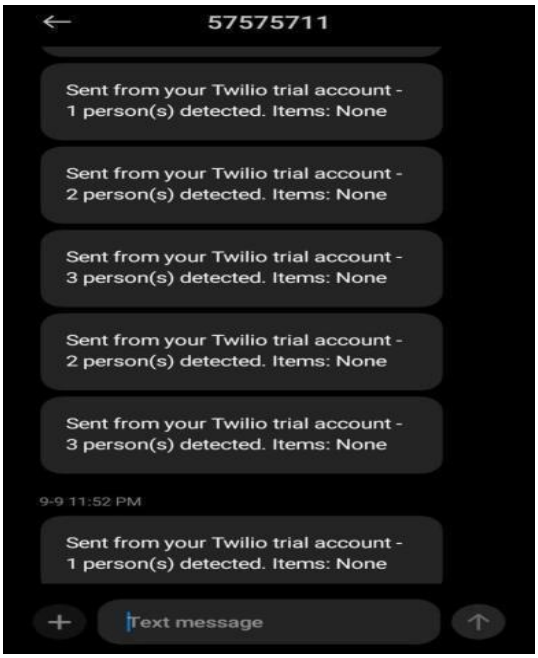


Figure 6.5 demonstrates the system's SMS-based alert mechanism, where real-time notifications are transmitted through integration with the Twilio API. Each message contains detection details, including the number of individuals identified and associated object information. The recurring alerts indicate continuous monitoring and event-driven message generation. This functionality ensures immediate user notification via mobile networks, enabling rapid awareness of security events independent of email or internet access.

Fig. 6.5 SMS-based alert mechanism



7. Conclusion

The Smart Security Surveillance Systems presents an effective approach to modern security by combining automated detection with intelligent alert mechanisms. The system successfully identifies unknown individuals and immediately notifies authorized users with captured images, reducing the need for continuous human monitoring and enabling faster response to potential threats. The software-driven design ensures cost efficiency and easy deployment without relying heavily on complex hardware infrastructure. Its scalable architecture allows future enhancements such as cloud integration, advanced analytics and multi-camera connectivity, making it adaptable to evolving security requirements. Although environmental conditions and image quality can affect recognition accuracy, these challenges can be addressed through improved algorithms and expanded training datasets. Overall, the proposed system demonstrates that intelligent surveillance solutions can significantly strengthen safety, improve monitoring efficiency and support proactive security management across various environments.

References

1. Sarker, M.A.B.; Hossain, S.M.S.; Venkataswamy, N.G.; Schuckers, S.; Imtiaz, M.H. An Open-Source Face-Aware Capture System. *Electronics* 2024, Vol. 13, No. 7, pp. 1178.
2. Kukade, J.; Panse, P. Advanced Deep Learning Model for Anomaly Detection Based Video Surveillance System. *International Journal of Intelligent Systems and Applications in Engineering*

2023, Vol. 12, No. 5s, pp. 477–485.
3. Li, C. Advancements and Challenges of Deep Learning in Facial Recognition. *Applied and Computational Engineering* 2024, Vol. 82, pp.45–53.
4. Shathik, J.A.; Saroliya, A.; Suhasini, G.; Borase, S.; Noor Alleema, N.; N.A.R. Smart Vision Systems for Public Safety: Real-Time Crowd Monitoring and Anomaly Detection Using Deep Learning and Edge Computing. *International Journal of Applied Mathematics* 2024.
5. Agustiyar, A.; Isnanto, R.R.; Widodo, C.E. Face Recognition for Attendance Systems: A Bibliometric Review of Research Trends and Opportunities. *Jurnal Sisfokom* 2025, Vol. 15,No. 1.
6. Soltani Nejad, S.; Haque, A. Weakly-Supervised Anomaly Detection in Surveillance Videos Based on Two-Stream I3D Convolution Network. *arXiv* 2024.
7. Shaik, A.N.; Villarini, B.; Argyriou, V. A Deep Learning Approach for Facial Attribute Manipulation and Reconstruction in Surveillance and Reconnaissance. *arXiv* 2025.
8. Otroshi Shahreza, H.; et al. SDFR: Synthetic Data for Face Recognition Competition. *Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition* 2024.
9. Noiret, S.; Ravi, S.; Kampel, M.; Florez-Revuelta, F. Fairly Private: Investigating the Fairness of Visual Privacy Preservation Algorithms. *arXiv* 2023.
10. Adjabi, I.; Ouahabi, A.; Benzaoui, A.; Taleb- Ahmed, A. Past, Present, and Future of Face Recognition: A Review. *Electronics* 2020, Vol. 9, No. 8, pp. 1188.
11. Li, S.Z.; Jain, A.K. Handbook of Face Recognition. *Springer* 2011.
12. Wang, W.; Yang, D.; Chen, Y. Video Surveillance Using Deep Learning: A Systematic Review. *IEEE Access* 2020, Vol. 8, pp. 134–152.
13. LeCun, Y.; Bengio, Y.; Hinton, G. Deep Learning. *Nature* 2015, Vol. 521, No. 7553, pp. 436–444.
14. Simonyan, K.; Zisserman, A. Very Deep Convolutional Networks for Large-Scale Image Recognition.
International Conference on Learning Representations (ICLR) 2015.
15. Redmon, J.; et al. You Only Look Once: Unified, Real-Time Object Detection. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* 2016.