E-ISSN: 2664-603X
P-ISSN: 2664-6021
IJPSG 2025; 7(7): 127-131
www.journalofpoliticalscience.com
Received: 10-06-2025
Accepted: 11-07-2025

Jaswant Singh Rathore
Research Scholar, MDSU, Ajmer, Rajasthan, India

Corresponding Author:
Jaswant Singh Rathore
Research Scholar, MDSU, Ajmer, Rajasthan, India

AI-based police surveillance system

Jaswant Singh Rathore

DOI: https://www.doi.org/10.33545/26646021.2025.v7.i7b.599

Abstract
This article aims to design and implement an AI-based surveillance system that can process video data, identify important events, and automatically make informed decisions in real-time. This will substantially impact the working of all the pillars of Police Administration- Investigation, Prosecution, Training and Prisons. This automated system will also automatically warn the police sentry at the police station as well as the district police control room when some suspicious activity is observed by the camera.

Keywords: AI, Police, surveillance, audio-video, electronic communication, enquiry, investigation, tool, policing, detection, crime

Introduction
In a true sense, AI enables automated machines to perform cognitive tasks, including perception, learning, and reasoning, which are generally linked to human abilities. McCarthy stated, "The science and engineering of developing intelligent machines and sophisticated computer programs is artificial intelligence". However, the emergence of genuine artificial intelligence is likely to be decades away. Though computers excel in tasks such as separating, computation, memorizing, indexing, and pattern recognition, abilities like emotion identification, face recognition, and conversational engagement remain uniquely human. However, AI can substantially improve machine performance to mimic human capabilities, prominent instances of AI applications encompass:

- AI-generated forecasts by Google (e.g., Google Maps)
- Ride-hailing applications (e.g., Uber, Ola)
- Autopilot systems employed in commercial aviation, spam identification in electronic mail
- Facial recognition technology
- Recommendations for searches on e-commerce platforms and web browsers
- Speech recognition services
- Intelligent virtual assistants (e.g., Siri, Alexa)
- Systems for the detection and prevention of fraud.

In essence, Artificial intelligence (AI) helps create computers, robots, and software that can think like humans. This involves studying how people think, learn, make decisions, and solve problems. By understanding these processes, developers can build advanced software and systems.

Artificial Intelligence (AI) in policing
The field of law enforcement is increasingly looking to harness the potential of artificial intelligence (AI) and machine learning (ML) technologies. Various applications are currently being developed and explored within this context, each focusing on enhancing different aspects of policing and public safety. However, the availability and implementation of these AI and ML solutions often hinge on their current stage of development. Some applications are fully developed and operational, providing real-time analytics and decision support to law enforcement agencies. Others are still in the research phase, undergoing analysis and refinement to improve their efficacy and reliability. Additionally, a number of innovative concepts are simply being explored, with researchers working to assess their feasibility and potential impact on law enforcement practices.

As this field continues to evolve, the successful integration of AI and ML into law enforcement will depend not only on technological advancements but also on careful consideration of ethical implications, data privacy, and the ability to maintain public trust.

Identified Problem: Dependence on Human Surveillance
Conventional surveillance systems engaging human operators to oversee video feeds at law enforcement facilities may encounter obstacles that we may address. The manual nature of this method may induce operator fatigue, potentially causing key facts to be forgotten or reactions to situations to be delayed. The above scenario underscores the necessity for creative and effective surveillance systems that improve reliability.

- **Efficacy and Agility:** Manual monitoring may be insufficient, especially over extended periods, leading to delayed responses to safety-related issues.
- **Constant Surveillance:** Human operators need intervals, and continuous monitoring may result in attentional lapses. Hence, surveillance systems must deliver uninterrupted monitoring to guarantee the safety and security of public areas and essential infrastructure.
  Security in Police Detention Facilities: The limits of human continual surveillance pose a substantial risk of neglecting suspicious activity or events in lockups. Therefore, the deployment of AI-driven Surveillance cameras in police stations, including detention facilities, is crucial for augmenting security.
- **Real-Time Decision-Making:** When it comes to decision-making, systems that are operated by humans may face delays; on the other hand, an artificial intelligence system can provide speedier responses. The goal is to give the artificial intelligence system the ability to make decisions in real-time based on the analysis of videos.

Solution Overview

- **AI-Powered surveillance system:** Develop an advanced system that leverages artificial intelligence to analyze live video feeds, enabling it to make rapid and accurate decisions in real-time situations.
- **Implementation of sophisticated algorithms:** Integrate cutting-edge algorithms into high-tech camera systems designed to differentiate between typical behaviors and potentially suspicious activities. This capability will allow for focused responses while significantly reducing the number of false alarms, ultimately enhancing overall security measures.
- **Identification of dangerous items:** The system will be equipped to recognize various risky items, such as blades, metallic objects, and potentially harmful edibles, thus ensuring proactive monitoring of potential threats.
- **Detection of suspicious movements:** It will also have the capacity to spot alarming actions, such as individuals attempting to climb over walls, drill into surfaces, or hide items within their clothing or surroundings actions that could signify illicit behavior.
- **Incorporation of machine learning techniques:** By utilizing machine learning, the AI model will be able to learn from its environment and user feedback, continuously improving its decision-making abilities. This commitment to ongoing enhancement will build confidence in the system's reliability and effectiveness.
- **Real-Time Triggers for Suspicious Activities**: The system must be capable of recognizing suspicious behaviors and generating immediate alerts, allowing for prompt intervention in real-time security situations.

Conceptual Framework
The AI system will be meticulously programmed to detect and react to suspicious movements by establishing a series of triggers or predetermined conditions. These triggers will function as early warning signals, facilitating swift action against potential security threats.

Examples of Triggers

- Detection of unusual movements or behaviors among individuals within a monitored area.
- Notable anomalies in the interactions between different individuals, such as between the accused and others, which could indicate suspicious activity.
- This comprehensive approach aims to create a robust security system that not only monitors but also effectively responds to emerging threats in a timely manner.ops.
- Any actions that seem out of the ordinary or possibly problematic.

Real-Time Decision-Making: Upon detecting something suspicious based on the triggers, the AI system will immediately make decisions to enhance security measures. This rapid response capability ensures that potential threats are addressed promptly, minimizing the risk of security breaches.

Autonomous Analysis: The AI system will automatically examine the video streams without human intervention.

Case Study: Cracking of heist case in Churu, Rajasthan[1]
On November 30, 2024, a daring heist unfolded at a jewelry showroom in Ratangarh, nestled in the Churu District of Rajasthan, where thieves executed a jaw-dropping scheme that resulted in the stolen loot worth ₹2.73 crore. This wasn't just any robbery; it was a carefully orchestrated operation typical of a high-stakes heist movie. The gang, displaying remarkable precision, made their entrance by breaking through the roof tiles, deftly disabling CCTV cameras, and utilizing gas cutters to access safes all while steering clear of main roads and surveillance. In an innovative response, the Churu Police turned to sophisticated AI software to sift through other CCTV footage. By analyzing distinguishing features such as eye shapes and skin tones of the masked criminals, the AI not only unveiled the original registration number of the getaway vehicle but continued to track it even after the thieves attempted to alter the number plates. The AI's capabilities didn't stop at facial recognition; it crafted detailed profiles of the suspects that matched known criminals from Uttar Pradesh. The investigation took a significant turn as the police scrutinized CCTV images and discovered a suspicious Ertiga car that had journeyed through critical locations including Jhunjhunu and

[1] https://timesofindia.indiatimes.com/city/jaipur/rajasthan-police-uses-ai-to-solve-273-crore-jewellery-heist-three-arrested/articleshow/116185735.cms
https://www.ndtv.com/india-news/ai-to-the-rescue-how-cops-busted-rs-2-7-crore-jewllery-theft-in-rajasthan-7222217

Kuchaman City in Nagaur. Thanks to the power of AI, the police traced the vehicle back to its registered owner, comparing generated images of the suspects against eyewitness descriptions. On December 09, 2024, this relentless pursuit culminated in the capture of three thieves of the notorious 'Battery Gang' from Uttar Pradesh: Bhagirath (42) and Yadram (52) from Auraiya district, alongside Ajmer Singh (48), who had connections to Jaipur's Jhotwara area yet was residing in Kuchaman City. Also, authorities recovered the stolen vehicle along with a portion of the missing jewelry. The 'Battery Gang' is notorious for their elaborate preparations. These meticulous criminals would spend up to 20 days scouting potential targets and plotting escape routes, showcasing a level of sophistication typically reserved for Hollywood thrillers. So, this case not only marks a significant triumph for the Churu Police but also heralds a new era in crime-fighting, demonstrating the transformative power of advanced technology in law enforcement. This initiative sets a remarkable precedent in crime detection, underscoring a pivotal shift toward more innovative policing methods in the fight against crime.

Applications of artificial intelligence based surveillance
Artificial Intelligence-based Facial Recognition
Automated Facial recognition technology is increasingly utilized by law enforcement authorities for the identification of persons of interest. This technique employs automated biometric software that evaluates and contrasts facial characteristics. It examines the contours, configurations, and ratios of an individual's visage. AI-driven facial recognition enables law enforcement to rapidly scan databases of faces and compare them with identified faces in real time. This innovative technology provides optimism for enhanced law enforcement methodologies. Key uses:

- **Identification and tracking of criminals:** Advanced facial recognition technology enables law enforcement agencies to effectively identify and monitor individuals with a history of criminal activity. By matching facial features against extensive databases, authorities can quickly locate suspects and track their movements, enhancing public safety.
- **Detecting Suspicious Behavior:** These systems are designed to analyze real-time footage and identify unusual behaviors that may indicate criminal intent. By recognizing patterns of suspicious activity, the technology can alert security personnel, potentially preventing crimes before they occur and assisting in the investigation of potential suspects.
- **Detecting and Preventing Violence: F**acial recognition can play a crucial role in public safety by identifying individuals who exhibit aggressive or violent behavior. By monitoring locations such as public events or transportation hubs, the technology helps intervene proactively to diffuse situations that could escalate into violence.
- **Identifying unclaimed objects:** Through visual detection capabilities, facial recognition systems can flag unclaimed bags or items in crowded spaces. This functionality enhances security measures, allowing authorities to investigate suspicious objects promptly and mitigate possible threats.
- **Finding missing children or persons:** The compassionate application of facial recognition technology can significantly aid in the search for missing individuals. By scanning public areas and matching faces against databases of the missing, this technology provides valuable support to search efforts and helps reunite families.
- **Preventing illegitimate intrusion or trespassing:** In sensitive or restricted environments, AI-powered facial recognition serves as a robust security measure. By monitoring entrances and identifying authorized personnel, the system can effectively prevent unauthorized access, thereby safeguarding critical areas.
- **Searching for Lost or Stolen Vehicles:** The application of facial recognition extends beyond individuals to assist in the recovery of lost or stolen vehicles. By scanning license plates and matching them with reported thefts or losses, law enforcement can efficiently track down vehicles.
- **Identification of Deceased Individuals:** In unfortunate circumstances, facial recognition technology can assist medical examiners and law enforcement in identifying deceased individuals. By comparing facial features with databases, authorities can bring closure to families and aid in the investigation of unidentified remains.

Facial recognition using artificial intelligence: What Is It?
Facial recognition technology leverages artificial intelligence (AI) to analyze and identify individual faces. Each person's face consists of various data points, including the distance between the eyes, the height of the cheekbones, and the distance between the eyes and the mouth. Advanced AI techniques can also consider dynamic features, such as facial expressions and other characteristics, along with static ones. AI-powered facial recognition software works by scrutinizing these data points and adjusting for differences that may arise, such as the distance from the camera or slight changes in the angle of the face. This technology can identify a person's face without requiring any physical contact. The system runs algorithms that compare the facial data of an individual to images stored in a database. If a match is found, law enforcement authorities are alerted.
The intelligent creation of criminal databases is being handled by advanced facial recognition systems that use artificial intelligence. When an image or face needs to be added to the database, the software evaluates and creates multiple versions of the image with different angular poses and variations, such as a dim image, a partial image, and changes caused by ageing. This allows for faster and more efficient comparisons with the input.

Video & Image Processing: One way to get smart in computer vision is to process videos. Computers, like humans, have eyes (via cameras), but they can't perceive the world the way we can. We can close the gap using video image processing. To do this, we can think of video frames as images and apply image processing techniques to them. In this way, we can view video processing as a set of image processing jobs. As an example, if you think of a series of N video frames as images and take the statistical average of the continuous image sequence, you can remove the background from the foreground. Video processing is really the culmination of several smaller processes. In video processing, the video is read frame by frame, and features are extracted from each frame via image processing. A plethora of image filters are required for feature extraction.

Mathematical functions carry out all of these operations. A face recognition system has many stages of operation. The first step is to use a model that has been trained on hundreds of photos to detect faces in the frame. Once face detection is complete, each image undergoes pose estimation to guarantee a high-quality frontal view. After making sure we are getting a good view of the front face the key points on the faces are identified. These points are eyes, nose, lips and jaw line. These points help us to identify a person. For each person identified in the frame we compare each person's facial points with points of the individuals in the database. Since these points are decimals thousands of comparisons can be done in a matter of milliseconds.

Object Detection: Similar to face detection, AI models are also being taught to identify bags and weapons. Since the model has been trained on various image types, there is no need to specify the object's shape, color, size, or sort of the object in order to recognize it.

AI enabled CCTV Cameras: Cameras equipped with advanced AI chips have significantly enhanced their functionality beyond traditional capabilities. These intelligent systems enable real-time monitoring and proactive surveillance, allowing for immediate detection of suspicious activities and potential criminal behavior. With integrated algorithms, these cameras can analyze patterns, distinguish between ordinary movement and anomalies, and generate alerts to notify security personnel or law enforcement. This proactive approach to crime detection and prevention not only improves safety but also optimizes the effectiveness of surveillance operations, making them a vital tool in modern security strategies.

AI enabled Drones: The cutting-edge integration of artificial intelligence revolutionizes the way machines operate, enabling them to engage intelligently with their environment. Similarly, powerful synergy between drones and AI not only meets diverse demands in aerial imaging but also marks a transformative leap in aerial technology through advanced computer vision and sophisticated neural networks. Patrol Drones infused with AI technology are incredibly versatile, catering to a myriad of applications such as:

- Object detection, counting, segmentation, and tracking
- Real-time monitoring and tracking of individuals or animals
- Accurate crowd counting for event management and safety
- Advanced thermal detection for various scenarios
- Ensuring compliance with face mask usage in public and workplace environments
- Detection of personal protective equipment like goggles and helmets
- Facial detection and recognition for security applications
- Early fire and smoke detection to safeguard lives and property
- License plate recognition for traffic management and security purposes
- Assessment of crack damage on structures for maintenance and safety
- License plate reading

Robotic Birds: Birds are omnipresent, yet they often go unnoticed by the majority of people. This observation has sparked interest in utilizing avian forms for surveillance purposes. Modern robotic birds are designed for autonomy and can remain airborne for extended periods. As technology advances, increasingly sophisticated bird robots are being developed to fulfil specific functional requirements.

Smart glasses: Smart glasses are an innovative tool that can be used for surveillance purposes, offering an advanced method of monitoring citizens. These high-tech glasses are equipped with sophisticated facial recognition software, allowing them to scan faces in real-time and match individuals to a database of persons of interest within mere seconds. This capability significantly enhances the efficiency of law enforcement agencies when it comes to identifying potential threats or suspects. The augmented reality (AR) eyewear is designed not only for functionality but also for comfort, making it lightweight and easy to wear for extended periods. Each pair comes with a front-facing camera that captures video and images of the surrounding environment, alongside a motion tracker that allows for seamless interaction with digital interfaces. Additionally, the display integrated into each lens provides real-time information and alerts to the wearer, enabling law enforcement personnel to stay informed while on patrol. Overall, smart glasses represent a significant advancement in surveillance technology, blending augmented reality with practical law enforcement capabilities.

Body-Worn Cameras: Body-worn cameras are vital tools for police departments, empowering them to assess the effectiveness of officers' responses during emergencies. These advanced cameras excel even in low-light conditions, capturing crucial visuals that can be pivotal in conflict situations. The important recordings are securely stored on police station computer systems, ensuring they are accessible for future review. With cutting-edge artificial intelligence, these devices provide mobile surveillance that not only records but also actively identifies criminals and missing persons in crowds, as well as recognizing stolen vehicles. They enable real-time alerts to authorities about wanted individuals, vehicles, or abducted children, promoting swift and decisive action when it is most critical.

Use of AI in cyber sphere

- **Proactive Social Media Monitoring:** AI tools monitor social media to analyze information, sentiments, and relationships, aiding law enforcement in tracking suspects and criminals.
- **Sentiment and Hate Speech Analysis:** AI helps predict and manage movements that may threaten peace, security, or law and order by analyzing public sentiments.
- **Fake News Detection:** AI algorithms are developed to identify and mitigate the spread of fake news on social media, which can negatively impact individuals and society.
- **Fake Profile Identification:** Machine learning and NLP techniques classify social media profiles to distinguish between genuine and fake accounts, improving detection accuracy over time.
- **Phishing Link Identification:** AI methods are being researched to detect phishing links and alert users, helping to protect sensitive personal information from

attackers.

- **Deep and Dark Web Monitoring:** Machine learning tools are being created to analyze data from the dark web, assisting law enforcement in combating criminal activities prevalent in hidden online spaces.

Conclusion

In today's rapidly evolving digital landscape, law enforcement agencies, including the police, face increasing challenges from technology-driven crimes such as cyber-attacks, identity theft, and online fraud. To effectively combat these sophisticated criminal activities, it is essential for these agencies to adopt a proactive approach. This involves not only enhancing their investigative techniques but also integrating advanced scientific tools like artificial intelligence (AI) into their operations. By leveraging AI, law enforcement can improve their surveillance capabilities, analyze vast amounts of data for patterns and anomalies, and ultimately increase their efficiency in preventing and solving crimes. Embracing these innovations will empower police forces to stay one step ahead of criminals who exploit technology for illicit gain.

References

1. Harel Y, Ben Gal I. Cyber security and the role of intelligent systems in addressing its challenges. ACM Trans Intell Syst Technol. 2017;8(4).
2. Jadhav EB, Sankhla MS, Kumar R. Artificial intelligence: Advancing automation in forensic science and criminal investigation. J Seybold Rep, 2020 Aug, ISSN: 1533-9211.
3. UNICRI, Interpol. Artificial intelligence and robotics for law enforcement [Internet], 2019 [cited 2024 Oct 25]. Available from: http://www.unicri.it/news/files/artificial_intelligence_robotics_law%20enforcment_web.pdf
4. UNICRI, Interpol. Towards responsible AI innovation: Second INTERPOL and UNICRI report on artificial intelligence for law enforcement [Internet], 2020 [cited 2024 Oct 25]. Available from: https://www.interpol.int/es/content/download/15290/file/AI%20Report%20INTERPOL%20UNICRI.pdf
5. Dilek S, Çakır H, Aydın M. Applications of artificial intelligence techniques to combating cyber crimes: A review. Int J Artif Intell Appl. 2015;6(1):21-39.
6. NITI Aayog. Discussion paper, National strategy for artificial intelligence [Internet], [Cited 2024 Oct 25].
7. Axon. Axon announces AI in car licence plate reader [Internet], 2018 [Cited 2024 Oct 25]. Available from: https://www.axon.com/news/ethics/axon-announces-ai-powered-in-car-license-plate-reader
8. Naik B, Mehta A, Yagnik H, Shah M. The impacts of artificial intelligence techniques in augmentation of cybersecurity: A comprehensive review. Springer, 2021 Aug.
9. Dupont B, Stevens Y, Westermann H, Joyce M. Artificial intelligence in the context of crime and criminal justice. A report for the Korean Institute of Criminology, 2018 Dec.
10. INNEFU. Face recognition solution, AI Vision for Delhi Police [Internet], [Cited 2024 Oct 25]. Available from: https://www.innefu.com/CaseStudy_DelhiPolice.pdf
11. Bureau of Police Research and Development. Crime forecasting: A machine learning and computer vision approach to crime prediction and AI in the service of law enforcement.
12. IBM. Artificial intelligence: Study material-Teacher instruction manual.
13. BBC. How AI is helping to fight crime [Internet], 2019 Feb 28 [cited 2024 Oct 25]. Available from: https://www.bbc.com/future/article/20190228-how-ai-is-helping-to-fight-crime
14. Emerj. Artificial intelligence in policing, Use-cases, ethical concerns, and trends [Internet], [Cited 2024 Oct 25]. Available from: https://emerj.com/ai-sector-overviews/artificial-intelligence-in-policing