A Comprehensive Review of AI-Driven Intelligent Surveillance System for Criminal Identification and Missing Person Detection with Privacy Preservation and Blockchain Integration

Prof. Bharti Bandgar[1], Rahul Satyendra Tiwari[2], Atharva Wakchaure[3]
[1,2,3]*Department of Computer Engineering, KJ College of Engineering and Management Research, Pune-411048, Maharashtra, India*

***Abstract*— The rapid expansion of urban surveillance infrastructure has increased the reliance on video monitoring systems for public safety, criminal identification, and missing person detection. However, traditional surveillance approaches largely depend on manual observation, resulting in limited scalability, delayed response, and reduced accuracy in complex environments. Recent advancements in artificial intelligence and computer vision have enabled automated face detection, recognition, and activity analysis, significantly improving detection performance. Existing research explores a wide range of techniques, including classical machine learning methods, deep learning-based facial recognition, real-time multi-camera systems, and image enhancement approaches. While these methods demonstrate improved accuracy under controlled conditions, several critical challenges remain unresolved. Current systems often struggle with cross-camera tracking, long-term identification of missing individuals, and robustness under occlusion, illumination variation, and appearance changes. Furthermore, most solutions lack mechanisms for privacy preservation, secure data sharing, tamper-proof evidence management, and transparent auditing. Emerging approaches such as federated learning and blockchain have been introduced to address some of these concerns; however, their integration with intelligent surveillance pipelines remains limited. This paper presents a comprehensive review of existing AI-driven surveillance systems, analyzing their methodologies, strengths, and limitations across multiple dimensions, including accuracy, scalability, privacy, and trust. The study identifies key research gaps and highlights the need for integrated, multi-modal, and privacy-preserving surveillance frameworks. The findings emphasize that future intelligent surveillance systems must combine advanced artificial intelligence techniques with secure and transparent data management to support reliable and legally accountable public safety applications.**

***Index Terms*—Artificial Intelligence, Intelligent Surveillance, Multi-Camera Tracking, Face Recognition, Blockchain-Based Security**

I. INTRODUCTION

The rapid growth of urban populations, smart city initiatives, and public safety demands has led to a significant expansion in video surveillance systems across public and private spaces. Modern environments such as transportation hubs, commercial complexes, and urban streets are increasingly equipped with large-scale camera networks to monitor activities and enhance security. While these systems generate vast amounts of visual data, traditional surveillance methods still rely heavily on human operators to observe and interpret video streams. Such manual monitoring is inherently limited by human attention span, fatigue, and the inability to process multiple feeds simultaneously, resulting in missed incidents, delayed responses, and reduced overall effectiveness. To address these limitations, artificial intelligence (AI) and computer vision technologies have been widely adopted to automate surveillance tasks. Early approaches focused on classical machine learning techniques for face detection and recognition; however, these methods struggled to perform reliably under real-world conditions. The introduction of deep learning, particularly convolutional neural networks, has

significantly improved the accuracy and robustness of facial recognition systems by enabling automatic feature extraction and better handling of variations in lighting, pose, and background. As a result, AI-driven surveillance systems are now capable of identifying individuals, detecting suspicious activities, and assisting law enforcement agencies in real time. In recent years, the scope of intelligent surveillance has expanded beyond single-camera setups to include multi-camera systems capable of tracking individuals across different locations. These systems aim to provide continuous monitoring and improve situational awareness in complex environments. However, challenges such as occlusion, appearance changes, and inconsistent data across cameras continue to affect tracking performance. Additionally, the widespread deployment of AI-based surveillance has raised serious concerns regarding privacy, data security, and ethical use. Centralized systems often require the collection and storage of sensitive video data, increasing the risk of misuse, unauthorized access, and regulatory non-compliance. Although numerous research efforts have addressed specific aspects of intelligent surveillance, such as face recognition, masked face detection, real-time processing, and data security, most existing solutions focus on isolated components rather than providing a unified and scalable framework. There remains a lack of comprehensive analysis that integrates advancements in deep learning, multi-camera tracking, privacy-preserving techniques, and secure data management mechanisms such as blockchain. This paper presents a comprehensive review of AI-driven intelligent surveillance systems for criminal identification and missing person detection, analyzing existing methodologies, identifying key limitations, and highlighting the need for integrated, secure, and privacy-preserving surveillance frameworks for modern public safety applications.

II. FUNDAMENTALS OF INTELLIGENT SURVEILLANCE SYSTEMS

Intelligent surveillance systems integrate computer vision and machine learning to automatically analyze video data for identification, recognition, and tracking tasks. A standard pipeline includes face detection, feature extraction, recognition, and tracking. Face detection identifies facial regions in images or video frames using methods such as Haar Cascade, CNN, or MTCNN. After detection, deep learning models generate compact feature representations known as embeddings, which capture unique facial characteristics. Recognition is then performed by comparing these embeddings with stored database records using similarity measures such as cosine similarity or Euclidean distance. In multi-camera systems, tracking and re-identification methods match the same person across video frames and multiple camera perspectives by analyzing visual appearance and movement patterns. Modern surveillance systems largely rely on CNN-based architectures due to their superior accuracy, robustness, and scalability. The effective integration of these components forms the foundation of intelligent surveillance and determines system performance under real-world conditions

III. REVIEW OF EXISTING METHODS

The evolution of intelligent surveillance systems spans from traditional machine learning approaches to deep learning and distributed security frameworks. Existing methods can be grouped based on their core objectives and technologies.

A. Traditional Methods

Early systems used Haar Cascade for face detection and LBPH, PCA, SVM, or KNN for recognition. These methods are computationally efficient and suitable for small datasets, but their accuracy declines under illumination changes, pose variation, and large-scale deployment.

B. Deep Learning-Based Face Recognition

CNN-based models such as FaceNet, ArcFace, and MobileNet significantly improved recognition accuracy through automated feature extraction and embedding generation. These systems perform well in varied conditions but require large datasets, higher computation, and remain vulnerable to heavy occlusion.

C. Missing Person Identification Systems

Several studies applied facial matching for missing person detection using database comparison, KNN classifiers, or CNN+SVM hybrids. These systems reduce manual search effort but are mainly limited to

static matching and do not support long-term appearance changes or continuous tracking.

D. Real-Time Surveillance and Multi-Camera Systems

Real-time surveillance systems based on YOLO, SSD, and OpenVINO enable faster detection from live video streams. Although suitable for practical deployment, most systems provide limited cross-camera tracking and lack behavioral risk analysis or predictive capabilities.

E. Occlusion and Masked Face Recognition

To handle masks and partial faces, researchers introduced embedding-based matching and masked face datasets. These methods improve recognition under moderate occlusion, but performance decreases when facial visibility is severely restricted.

F. Image Enhancement and Super-Resolution

Super-resolution techniques such as SRCNN, FSRCNN, and SRGAN improve low-quality surveillance images and indirectly enhance recognition accuracy. However, these methods focus only on image quality and do not provide higher-level intelligence.

G. Blockchain-Based Surveillance Systems

Blockchain technology has been adopted in surveillance systems to enable secure evidence storage, protected data sharing, and transparent audit trails. Although these approaches improve data integrity and trustworthiness, they are frequently isolated from AI-driven processing pipelines and can introduce additional computational and communication delays

H. Privacy-Preserving Approaches

Federated learning enables collaborative model training without sharing raw surveillance data, helping address privacy concerns. However, current approaches still face challenges in trust verification, heterogeneous data handling, and real-time integration.

Overall, existing systems solve specific problems individually, but few provide a unified framework combining recognition, tracking, privacy preservation, and secure evidence management.

IV. COMPARATIVE ANALYSIS

A comprehensive comparison of existing surveillance approaches is essential to understand their capabilities and limitations across different dimensions. Table I summarizes key characteristics of representative methods discussed in the literature, including accuracy, real-time capability, multi-camera support, privacy considerations, and major limitations.

Table I

Method / Approach	Accuracy	Real-Time	Multi-Camera	Privacy Support	Key Limitations
Traditional ML (Haar, PCA, KNN, SVM)	Low–Moderate	Yes	No	No	Sensitive to lighting, poor scalability, low robustness
LBPH-based Recognition	Moderate	Yes	No	No	Limited feature representation, struggles with occlusion
CNN-based Recognition	High	Partial	No	No	Requires large datasets, computationally expensive
FaceNet / ArcFace (Embedding-based)	Very High	Partial	Limited	No	Performance drops under occlusion and disguise

CNN + SVM Hybrid Models	High	No	No	No	Static matching, not suitable for real-time tracking
Missing Person Systems (Database Matching)	Moderate–High	No	No	No	No long-term tracking, no age progression
YOLO / SSD Real-Time Systems	High	Yes	Limited	No	Weak cross-camera tracking, lacks behavior analysis
OpenVINO Edge Systems	High	Yes	Partial	No	Limited scalability, lacks privacy mechanisms
Masked Face Recognition Systems	Moderate–High	Yes	No	No	Accuracy drops under extreme occlusion
Super-Resolution Techniques (SRGAN, FSRCNN)	Indirect (Enhancement)	No	No	No	Improves image quality only, no intelligence
Blockchain-Based Surveillance	High (Data Integrity)	No	Yes	Partial	High latency, weak AI integration
Federated Learning-Based Systems	High	Partial	Yes	Yes	Lack of trust validation, complex deployment

A. Analysis of Existing Approaches

The comparative analysis reveals that different research efforts focus on specific components of intelligent surveillance systems rather than providing a holistic solution. Traditional machine learning methods offer computational efficiency and real-time capability but fail to achieve high accuracy in complex environments. Deep learning-based approaches significantly improve recognition performance; however, they often require substantial computational resources and large datasets. Systems designed for missing person identification primarily rely on static image matching and database comparison, limiting their ability to support real-time tracking and long-term identification. Real-time surveillance frameworks using models such as YOLO and SSD demonstrate strong performance in detection tasks but lack robust mechanisms for cross-camera tracking and behavioral analysis. Approaches addressing occlusion, such as masked face recognition systems, improve performance under partial visibility but remain unreliable in extreme conditions. Similarly, super-resolution techniques enhance image quality but do not contribute to higher-level intelligence such as tracking or decision-making.

B. Security and Privacy Considerations

Blockchain-enabled surveillance systems offer enhanced data integrity and traceability by providing secure evidence storage and transparent audit mechanisms, thereby reducing the risk of tampering. However, these solutions are commonly developed independently of AI processing frameworks and may introduce additional latency during data handling and verification. In contrast, federated learning supports

privacy preservation by avoiding centralized data collection and enabling decentralized model training. Despite these advantages, it still faces challenges related to model validation, trust management, and ensuring the integrity of contributions from participating entities.

C. Identified Gaps

The analysis highlights several critical gaps across existing research:

- Lack of unified systems integrating detection, tracking, and prediction
- Limited support for robust multi-camera tracking in real-world environments
- Inadequate handling of occlusion, appearance changes, and long-term identification
- Absence of integrated privacy-preserving and secure data-sharing mechanisms
- Weak linkage between AI-based analytics and trust frameworks such as blockchain

V. RESEARCH GAPS AND CHALLENGES

Despite major progress in intelligent surveillance, existing systems remain fragmented and do not fully satisfy practical public safety requirements. Most research improves individual components while neglecting complete system integration, scalability, privacy, and trust.

A. Lack of Multi-Camera Coordination

Many systems operate at a single-camera level and provide limited cross-camera re-identification. Reliable tracking across different locations, viewpoints, and lighting conditions remains a major challenge.

B. Weak Performance Under Occlusion

Recognition accuracy still decreases under masks, partial faces, and appearance changes. Existing methods often depend only on facial features and do not effectively use gait, pose, or body cues.

C. No Long-Term Missing Person Tracking

Most missing person systems rely on static image matching and cannot handle aging or long-term appearance variation. Age progression and temporal identity modeling are rarely addressed.

D. Limited Behavior Prediction

Current systems mainly perform reactive detection and recognition. Suspicious activity analysis, threat prediction, and early crime prevention remain insufficiently explored.

E. Privacy Risks in Centralized Systems

Centralized architectures require collection and storage of sensitive surveillance data, creating risks of misuse, leakage, and regulatory non-compliance. Privacy-preserving alternatives are still limited.

F. Lack of Tamper-Proof Evidence

Most surveillance platforms do not provide secure evidence logging, chain-of-custody tracking, or transparent auditing, reducing legal reliability.

G. Lack of Unified Frameworks

Existing approaches usually solve recognition, tracking, privacy, or security separately. There is a clear need for integrated and scalable systems combining AI analytics with secure data governance.

Overall, these gaps justify the development of next-generation surveillance frameworks that are intelligent, privacy-aware, trustworthy, and suitable for real-world deployment.

VI. FUTURE DIRECTIONS

The evolution of intelligent surveillance systems is expected to move toward more integrated, scalable, and trustworthy solutions capable of addressing real-world complexities. Based on the limitations identified in existing research, several promising directions can guide future developments in this domain.

A. Multi-Modal Biometric Integration

Future surveillance systems are likely to rely on multi-modal biometric approaches that combine multiple sources of identity information, such as facial features, gait patterns, voice signals, and soft biometrics (e.g., height and clothing attributes). Integrating these complementary modalities can significantly improve identification accuracy, especially in scenarios where facial data is partially occluded or unavailable. Multi-modal systems also enhance robustness against spoofing attacks and

enable more reliable tracking across diverse environments.

B. Integration of Artificial Intelligence and Blockchain

The combination of artificial intelligence with blockchain technology presents a strong foundation for building secure and transparent surveillance systems. Future research should focus on tightly integrating AI pipelines with blockchain frameworks to enable real-time, tamper-proof logging of surveillance events, secure sharing of identity data across multiple entities, and automated enforcement of access control policies through smart contracts. Optimizing blockchain performance to reduce latency and support high-throughput environments will be essential for large-scale deployment.

C. Explainable Artificial Intelligence (XAI)

With the growing adoption of AI-based surveillance systems, ensuring transparency and interpretability has become essential. Explainable AI (XAI) methods offer clear insights into the reasoning behind system decisions, allowing operators and legal authorities to better understand and trust the generated outcomes. Integrating explainability into surveillance frameworks can also assist in detecting biases, enhancing fairness, and ensuring adherence to ethical principles and regulatory requirements.

D. Privacy-Preserving Artificial Intelligence

Protecting user privacy will remain a critical requirement for future surveillance systems. Advanced privacy-preserving techniques, including federated learning, secure multi-party computation, homomorphic encryption, and differential privacy, can be leveraged to minimize the exposure of sensitive data. Future research should focus on improving the efficiency and reliability of these methods while ensuring seamless integration with real-time surveillance pipelines.

E. Real-Time and Large-Scale Deployment

Scaling intelligent surveillance systems to operate in large urban environments remains a significant challenge. Future systems must support real-time processing across hundreds or thousands of cameras while maintaining high accuracy and low latency. This will require advancements in edge computing, distributed architectures, and efficient model optimization techniques. Ensuring interoperability between different surveillance infrastructures and enabling continuous operation in connectivity-limited environments will also be key factors for practical deployment.

Overall, future intelligent surveillance systems must move toward unified, multi-modal, and privacy-aware frameworks that combine advanced AI capabilities with secure and scalable system design. These developments will play a crucial role in enhancing public safety while maintaining ethical and legal standards.

VII. CONCLUSION

This paper presented a comprehensive review of intelligent surveillance systems for criminal identification and missing person detection, covering a wide range of methodologies from traditional machine learning techniques to advanced deep learning, real-time multi-camera systems, and emerging privacy-preserving and blockchain-based approaches. The analysis shows that while significant progress has been made in improving face recognition accuracy and real-time processing capabilities, most existing solutions remain limited in scope and fail to address critical real-world requirements. Traditional methods offer simplicity and efficiency but lack robustness and scalability, whereas deep learning-based approaches achieve high accuracy at the cost of computational complexity and dependency on large datasets. Systems developed for missing person detection and real-time surveillance offer valuable capabilities; however, they frequently function independently and do not effectively support continuous tracking, coordination across multiple cameras, or behavior analysis. In addition, technologies like federated learning and blockchain help improve privacy protection and data security, but they have not yet been fully incorporated into comprehensive surveillance systems. The review highlights the growing need for unified and intelligent surveillance systems that combine accurate detection, robust multi-camera tracking, behavior understanding, privacy preservation, and secure evidence management within a single architecture. Such integration is essential to overcome the limitations of

fragmented approaches and to enable reliable, scalable, and trustworthy surveillance solutions. From a broader perspective, intelligent surveillance systems play a critical role in enhancing public safety, supporting law enforcement, and enabling faster response to security threats. However, their deployment must be guided by principles of transparency, accountability, and ethical use to ensure public trust. Future advancements should focus on developing integrated, privacy-aware, and legally compliant systems capable of addressing the evolving challenges of modern surveillance environments.

ACKNOWLEDGMENT

The authors gratefully acknowledge the guidance of Prof. Bharti Bandgar and the Department of Computer Engineering, K. J. College of Engineering and Management Research, Pune, for their invaluable support.

REFERENCES

[1] B. Vinavatani, M. R. Panna, P. H. Singha, and G. J. W. Kathrine, "AI for detection of missing person," in Proc. Int. Conf. Applied Artificial Intelligence and Computing (ICAAIC), IEEE, 2022, pp. 66–73.

[2] L. Al-Sahan, F. Al-Jabiri, N. Abdelsalam, A. Mohamed, T. Elfouly, and M. Abdallah, "Public security surveillance system using blockchain technology and advanced image processing techniques," in Proc. IEEE Int. Conf. Public Security Surveillance Systems, 2020, pp. 104–111.

[3] A. Ajay and M. J. Ahamed, "Computer vision and convolutional neural networks for advanced face detection and recognition," in Proc. Int. Conf. Machine Learning and Autonomous Systems (ICMLAS), IEEE, 2025, pp. 989–993.

[4] K. P. Teja, G. D. Kumar, and T. Prem Jacob, "Face detection and recognition for criminal identification," in Proc. 8th Int. Conf. Communication and Electronics Systems (ICCES), IEEE, 2023, pp. 1431–1435.

[5] A. Ponmalar et al., "Finding missing person using artificial intelligence," in Proc. Int. Conf. Computer, Power and Communications (ICCPC), IEEE, 2022, pp. 562–565.

[6] S. Divya, T. Jeevika, and A. V. A. Geo, "Innovative approaches to criminal identification using real-time facial recognition," in Proc. 6th Int. Conf. Mobile Computing and Sustainable Informatics (ICMCSI), IEEE, 2025, pp. 1694–1700.

[7] L. Ma, "Face recognition of intelligent building based on super-resolution reconstruction of visual image," in Proc. 5th Int. Conf. Intelligent Computing and Control Systems (ICICCS), IEEE, 2021, pp. 895–900.

[8] D. A. Maharani, C. Machbub, L. Yulianti, and P. H. Rusmin, "Improving the capability of real-time face masked recognition using cosine distance," in Proc. 6th Int. Conf. Interactive Digital Media (ICIDM), IEEE, 2020.

[9] S. T. Ratnaparkhi, A. T. Andasi, and S. Saraswat, "Face detection and recognition for criminal identification system," in Proc. 11th Int. Conf. Cloud Computing, Data Science & Engineering (Confluence), IEEE, 2021, pp. 773–777.

[10] S. Shilaskar et al., "Robust criminal identification system for recognition of obscure and hidden faces," in Proc. 2nd Int. Conf. Futuristic Technologies (INCOFT), IEEE, 2023, pp. 1–6.

[11] S. K. Teoh, Y. H. Wong, L. Y. Tan, and C. F. Leong, "Face detection and face re-identification system using deep learning and OpenVINO," in Proc. 2nd Int. Conf. Artificial Intelligence and Data Sciences (AiDAS), IEEE, 2021.

[12] X. Zhao, "Research and implementation of face recognition in remote intelligent monitoring system," in Proc. 2nd Int. Conf. Smart Electronics and Communication (ICOSEC), IEEE, 2021, pp. 1013–101.