JOURNAL
of INTERDISCIPLINARY
KNOWLEDGE

DOI: https://doi.org/10.37497/jik.v8iknowledge.1633

ARTICLE

Privacy-Preserving Approaches in Smart Surveillance Systems Using the YOLO Algorithm

Abordagens de Preservação da Privacidade em Sistemas Inteligentes de Vigilância: Aplicações do Algoritmo YOLO em Detecção de Objetos em Tempo Real

Yashvi Yashi Srivastava
Department of Computer Science – United University Prayagraj (India).
E-mail: phd21008@iiml.ac.in

ABSTRACT | Purpose: This paper investigates privacy-preserving approaches in smart surveillance systems, focusing on maintaining the balance between public security and individual privacy rights. With the proliferation of surveillance technologies and artificial intelligence (AI), ensuring data confidentiality while maintaining operational efficiency has become a key concern. The study emphasizes the role of the YOLO (You Only Look Once) algorithm in enabling privacy-conscious, real-time object detection and its integration with advanced cryptographic and federated learning methods. **Design/Methodology/Approach:** The research employs a conceptual and analytical approach, reviewing recent technological developments in AI-based surveillance, particularly the application of YOLO for secure, real-time object detection. Privacy-preserving methods such as anonymization, edge computing, encryption, and federated learning are analyzed for their potential to reduce data exposure and risks of misuse. Case references, including the deployment of AI-driven surveillance during the Maha Kumbh Mela 2025 in India, illustrate real-world implications of privacy-centered frameworks. **Findings:** The findings demonstrate that integrating YOLO with privacy-preserving techniques enhances surveillance efficiency without compromising user privacy. Federated learning enables decentralized data training, while secure convolutional operations protect sensitive information through encryption. Despite YOLO's advantages in speed and accuracy, challenges remain in detecting small or overlapping objects and in managing computational demands on edge devices. **Research Limitations/Implications:** Future research should focus on optimizing YOLO models for low-power environments and on developing standardized privacy protocols suitable for large-scale surveillance systems. Originality/Value: This study contributes to the discourse on ethical AI by presenting a holistic framework for privacy-preserving smart surveillance that combines real-time operational efficiency with robust data security principles.

Keywords | Privacy preservation, YOLO algorithm, Smart surveillance, Federated learning, Data security

Received: 02 March 2025
Revised: 4 April 2025
Accepted: 3 May 2025
e-ISSN: 3086-0016

Associate editor: Altieres Silva – Alumni.In Publisher

How to cite this article: Srivastava, Y. Y. (2025). Privacy-Preserving Approaches in Smart Surveillance Systems Using the YOLO Algorithm. *Journal of Interdisciplinary Knowledge*, 8(knowledge), e01633. https://doi.org/10.37497/jik.v8iknowledge.1633

RESUMO | Objetivo: Analisar abordagens de preservação da privacidade aplicadas a sistemas inteligentes de vigilância, com ênfase no uso do algoritmo YOLO (*You Only Look Once*) como ferramenta de detecção de objetos em tempo real, buscando equilibrar eficiência operacional, segurança pública e proteção dos direitos individuais. **Método:** O estudo adota uma abordagem conceitual e analítica, fundamentada em revisão da literatura recente sobre vigilância baseada em inteligência artificial. São examinadas técnicas de preservação da privacidade, como anonimização de dados, computação em borda, criptografia, aprendizado federado e convoluções seguras, bem como sua integração com arquiteturas YOLO. Exemplos práticos e contextuais, incluindo a aplicação de sistemas inteligentes de vigilância no evento Maha Kumbh Mela 2025, na Índia, são utilizados para ilustrar implicações reais dessas abordagens. **Resultados:** Os achados indicam que a integração do YOLO com técnicas de preservação da privacidade melhora significativamente a eficiência da vigilância sem comprometer a confidencialidade dos dados pessoais. O aprendizado federado permite o treinamento descentralizado de modelos, reduzindo a exposição de dados sensíveis, enquanto métodos criptográficos protegem informações durante o processamento. Apesar das vantagens em velocidade e precisão, o YOLO apresenta limitações na detecção de objetos pequenos ou sobrepostos, além de desafios relacionados à carga computacional em dispositivos de borda. **Conclusão:** Conclui-se que a adoção de abordagens de preservação da privacidade associadas ao YOLO constitui um caminho promissor para o desenvolvimento de sistemas de vigilância inteligentes, éticos e eficientes, sendo necessária a evolução de protocolos padronizados e modelos otimizados para ambientes de grande escala.

Palavras-chave | Vigilância inteligente; Preservação da privacidade; YOLO; Detecção de objetos; Inteligência artificial; Computação em borda.

INTRODUCTION

Smart surveillance systems has experienced a rapid increase in its use in the urban areas to enhance security and monitor activities. Still, these systems have potential risks to privacy due to the collection, storage, and analysis of sensitive private and personal data .Our Privacy-preserving approaches aim to bring a balance in the need for surveillance with the protection of a person's rights, ensuring data security while maintaining system efficiency. To enhance the smart surveillance system we can use object detection technology or technique such as YOLO algorithm. If we look at future and present times, Modern surveillance technologies have made rapid advancements. Race security requires the best surveillance for breaches and facility infringements which is why , user surveillance is necessary. To manage the rapid growth of surveillance technologies, surveillance-based security measures need to be balanced out with user's right to privacy.

As technology continues to develop, future strategies that protect privacy will incorporate sophisticated methods of cryptography, AI-powered data redaction, and user-oriented design. These innovations will be key in managing the conflicting need for surveillance and individual privacy. But for now we will be discussing in this study about YOLO algorithm.

OVERVIEW

When we discuss about Object detection technology we know that it plays a very important role in improving smart surveillance systems by automating the identification and tracking of objects in real-time which means they have a strong connection.

I. Importance of Object Detection Technology in Smart Surveillance System

a) **Automated monitoring:** With the help of object detection , surveillance systems can automatically check video feeds , identify and track the objects for example: people , vehicles or any activities etc.This will lead us to quicker response time.

b) **Real Time Warning for Security:** systems if they use object detection, they can give alerts when they find out something fishy or suspicious . For example: if there is an unattended bag or suitcase left in a public area for a long time, the security personnel will get immediately notified.

c) **Management of Traffic:** Object detection technology is very important for traffic monitoring. It can assess the flow of vehicles , detect heavy traffic and can provide support. For example: Mahakumbh 2025 witnessed heavy traffic jams , in such situations we definitely need surveillance systems but with the help of object detection we can detect things in real time .

For all these things we got introduced to an algorithm known as YOLO (You look only once) algorithm which is an object detection technique. It has capability of detecting and identifying multiple objects simultaneously that too quickly and accurately.

II. Importance of YOLO algorithm for privacy preservation

The YOLO (You Only Look Once) algorithm is crucial for privacy-preserving methods, especially object detection. Its efficiency in operation and architectural design makes it suitable for strengthening privacy across numerous applications. Some of the important points about how YOLO helps privacy-preserving techniques follow:

a) **Real-Time Processing and Efficiency:** YOLO is optimized for real-time object detection, making it possible to quickly and efficiently process images. The speed is essential in applications like video monitoring or autonomous vehicles, where prompt feedback is required. Through the detection in a single network pass, YOLO reduces the volume of data to be transmitted or stored, potentially lowering the chances of sensitive information exposure during processing.

b) **Federated Learning Integration:** One of the most promising integrations of YOLO with privacy-protecting approaches is its fusion with federated learning (FL). FL enables models to learn on decentralized data from multiple devices without sending the raw data to a central point. This process is especially valuable in sensitive contexts, like healthcare, where patient information needs to be kept secret. YOLO's effectiveness makes it appropriate for deployment in FL environments, allowing joint model training while preserving local datasets as private. It basically sends the model to the data , instead of sending data to the model.

c) **Secure Convolutional Techniques:** New developments have integrated secure convolutional techniques into the YOLO system to improve its object detection capabilities while keeping data confidential. They entail encrypting and processing data without decrypting it, hence

protecting sensitive data during the detection process. This feature is crucial in cases where data confidentiality is essential[5].

III. Applications in Sensitive Domains

Its relevance is illustrated by the use of YOLO in privacy-critical applications—like healthcare diagnosis or individual monitoring. For example, medical images can be used to enhance diagnostic models in hospitals without revealing patient records directly. Institutions can strengthen their models while being compliant with stringent privacy policies[3] by utilizing the capabilities of YOLO within a federated learning system.

IV. Privacy-Preserving Techniques

a) **Anonymize Data:** Anonymization techniques are applied to obscure personally identifiable information (PII) but enable effective monitoring. Examples include blurring faces or reconfiguring identifiable features from video streams prior to processing with YOLO algorithms.

b) **Edge Computing:** Deploying edge computing enables processing to take place nearer to the source, reducing raw data transmission over networks. This minimizes the chances of interception and unauthorized access since only required information is transmitted to central servers for analysis.

c) **Encrypted Video Streams:** Certain systems use encrypted streams in which features are derived from encrypted video data. This ensures that sensitive information is protected during transmission and processing, enabling YOLO algorithms to process non-sensitive features without violating privacy.

d) **Hybrid Surveillance Models:** Hybrid models combine conventional surveillance methods with state-of-the-art AI approaches such as YOLO, allowing selective monitoring according to pre-specified privacy parameters. These models may adjust operation dynamically according to levels of detected activity or particular triggers (e.g., outlier movement patterns) without compromising user anonymity.

V. Applications of YOLO in Smart Surveillance

a) **In Hospitals:** YOLO-based systems are used to monitor patient activities, detect falls, and ensure safety in elderly care environments. These systems send alerts to administrators upon detecting unusual behavior or incidents like falls or intrusions, improving situational awareness.

b) **Smart Homes:** YOLO has been integrated into smart home surveillance systems to detect infiltrators and improve security. By using transfer learning and quantization techniques, these systems achieve high accuracy while reducing computational requirements

c) **In situations like Mahakumbh 2025:** The use of smart surveillance systems, specifically those having AI and the YOLO algorithm, was being implemented at the Maha Kumbh Mela in Prayagraj, India, to enhance safety and crowd management during this massive religious gathering. This shows how useful and secure these approaches can be if implemented correctly.

VI. Real Life situation

Maha Kumbh Mela 2025, which is one of the large-scale religious events in Prayagraj, integrated cutting-edge smart surveillance systems to boost security and cope with the arrival of more than 400 million devotees. The application of technology, especially artificial intelligence (AI), plays a crucial role in facing the specific challenges of such a massive event. And when we use Surveillance System in such extent , we definitely have to ensure that we also protect the privacy of an individual's data .

VII. Significance of Privacy

Though the deployment of smart surveillance systems is meant to provide safety during the Maha Kumbh Mela, it still raised some major privacy issues:

a) **Data Security:** Collection and storage of individual data through facial recognition needs to be handled cautiously so that misuse or unauthorized access is avoided. Data handling needs to be ensured to meet privacy regulations. Data breaches can destroy the reputation and would be very wrong .

b) **Consent and Transparency:** Pilgrims ought to be informed of the purpose for which their data is collected and offered an option to consent to monitoring mechanisms. Transparency can assist in instilling trust among participants.With that a lot of trust can also be gained .

c) **Safety and Privacy Balancing:** Government agencies must find a balance between maintaining public security and honoring citizens' right to privacy. This entails enacting stringent security practices without impeding personal freedom.

In summary, the use of smart surveillance systems at Maha Kumbh 2025 is a major step towards the modernization of security measures at mass gatherings. But it is important to address privacy issues in advance to ensure public trust in these technologies while providing a secure environment for all attendees. And in order to do that we can go ahead with our privacy preserving approaches.

VIII. Approaches To Ensure Privacy

a) **Real Time Object Detection:** Real-time object detection via the YOLO (You Only Look Once) algorithm has the potential to greatly improve privacy by allowing processing on the device, thus removin the need for raw video or image data to be sent to remote servers and consequently limiting exposure to data breaches. Selectively detecting only a particular

object of interest for example, a vehicle or animal—while disregarding sensitive identifiers such as faces, YOLO prevents the collection of excessive data. In addition, privacy-friendly methods like blurring the object can be implemented in real-time for detected objects, making sure sensitive data stays anonymous before storage or transmission.

b) **Federated Learning Integration:** Federated learning and secure convolutional methods can be used to improve privacy in the YOLO algorithm by resolving data security issues during training and inference. Federated learning allows decentralized training on multiple devices or nodes without exchanging raw data. Rather, it combines locally trained model updates, keeping sensitive data on individual devices. This is especially useful for YOLO, which is based on large datasets for object detection operations. With federated learning, organizations are able to train YOLO models jointly while maintaining user privacy and reducing risks that come with centralizing data storage, including data breaches or exploitation.

c) **Secure convolutional Techniques:** Secure convolutional methods also enhance privacy in YOLO's architecture by encrypting intermediate computations within the convolutional neural network (CNN) operations. These methods, like homomorphic encryption or secure multi-party computation, make it possible for YOLO to execute object detection operations on encrypted data without decrypting it. This guarantees that confidential data contained in images or videos remains safe during the detection process. Coupled with federated learning, secure convolutional approaches build a strong privacy-preserving YOLO implementation framework, which is appropriate for usage in surveillance or autonomous cars where data confidentiality is a priority**.**

X. Drawbacks of the YOLO Algorithm in Smart Surveillance Systems

While the YOLO algorithm is one of the fastest method of object detection, it comes with several drawbacks when it is used in smart surveillance systems:

a) **Difficulty with Small Objects:** Given the small object's distance from the camera, classifying pedestrians as small objects can be difficult because of the zoomed-out view. Small items such as traffic lights can be misclassified as well and this can be a major problem due to the grid strctured nature of YOLO.

b) **Lacking Ability to Classify Overlapping Objects:** Recognition of heterogeneous people in the same group is where YOLO image recognition fails

c) **Sensitivity to Environmental Lighting:** Worst results in dim light, moving blur, and extreme-angle conditions.

d) **Computational Load on Edge Devices:** Newer YOLO versions require significant processing power, limiting their use on low-power devices like mobile devices, IoT systems, and embedded vision applications.

XI. Solutions for Enhancing YOLO in Intelligent Surveillance

a) **Employment of Sophisticated Loss Functions:** Adding loss functions such as CIoU, DIoU, and GIoU can enhance object localization and detection accuracy.

b) **Transformer-Based Improvements:** Adding transformer-based models can enhance feature extraction and detection accuracy, as in YOLOv8.

c) **Multi-Scale Feature Extraction:** Methods such as Feature Pyramid Networks (FPN) and Spatial Pyramid Pooling (SPP) assist in object detection across varying sizes, enhancing performance across different surveillance contexts.

d) **Optimized Model Versions:** The use of optimized models such as YOLOv7 or YOLOv8, with improved speed and accuracy balance, can provide improved real-time surveillance capabilities

XII. CONCLUSION

The study illustrates that the use of synthetic datasets for training the YOLO system can accomplish proper object detection with a reduced risk of leaking private information. In the end, it is clear that such approaches concerning preservation of privacy are essential for smart surveillance systems using the YOLO algorithm. As surveillance technologies become Widespread in public safety, urban management, and various fields, ensuring the privacy of the people is crucial. As we can see that with time there is a rapid increase in crimes and security threats , which is why it has become a trend now to use surveillance system and with growth in technology it because smart surveillance system . But because of those surveillance systems we are somewhere also having this fear of data leak and data misuse .

So to prevent that issue we really need some approach to ensure privacy , for that we came across the YOLO algorithm. Definitely it's not just YOLO that would help us but for now and seeing the present conditions we can definitely make the best use of this object detection technique.

XIII. REFERENCES

Beugin, Y., Jiang, P., Ergu, D., Liu, F., & Ma, B. (n.d.). *Building a privacy-preserving smart camera system: A review of YOLO algorithm development.*\

El Majdoubi, D., El Bakkali, H., Sadki, S., Maqour, Z., & Leghmid, A. (2022). The systematic literature review of privacy-preserving solutions in smart healthcare environment. *Journal of Healthcare Engineering, 2022*, Article 3072856. https://doi.org/10.1155/2022/3072856

Gowda, K. R. A., Athul Kumar, S., V. R., Gujrati, R., Rashmi, & Gulati, U. (2023). A study on impact of service quality on customer satisfaction with low-cost carriers in India. *Journal of Information and Optimization Sciences, 44*(8), 1665–1684. https://doi.org/10.47974/JIOS-1483

Kadyan, S., Sharma, Y., Agarwal, K., Gujrati, R., Rashmi, R., & Koul, M. (2023). Linking workplace incivility with employee turnover intention and job satisfaction: The mediating role of self-efficacy of employees in telecom sector in NCR. *Journal of Information and Optimization Sciences, 44*(8), 1595–1611. https://doi.org/10.47974/JIOS-1479

Lavanya, G. S. D. P. (n.d.). *Enhancing real-time object detection using YOLO algorithm*.

Mir, A. Y., Arora, M., Gujrati, R., Rashmi, J., A. K., Uygun, H., & Dixit, I. (2023). An empirical study on correlation of the factors of the perception: Service delivery and patient satisfaction about service quality in selected public and private hospitals of the Raipur city. *Journal of Information and Optimization Sciences, 44*(8), 1715–1728. https://doi.org/10.47974/JIOS-1487

Öztürk, C., Denizhan, S., Gujrati, R., & Denizhan, B. (2024). Vocational education and candidate performance analysis. *Journal of Information and Optimization Sciences, 45*(5), 1401–1420. https://doi.org/10.47974/JIOS-1725

Patil, H. P., Pawar, N. R., Sawant, A. T., & Sonawane, M. (2022). Smart surveillance system. *International Journal of Creative Research Thoughts (IJCRT), 10*(3), 587–592. https://doi.org/10.5281/zenodo

Popuri, S. S., Shaik, M. I., & Siddiq, A. (2024). *Smart security surveillance system using IoT*. Vignan University.

Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2015). You only look once: Unified, real-time object detection. *arXiv preprint* arXiv:1506.02640. https://arxiv.org/abs/1506.02640

Sao, A., Hatipoglu, C., Pathak, D., Vijh, G., Gujrati, R., & Patnaik, B. (2025). Unveiling the dynamic duo: How AI acts as the moderator between human intelligence and consumer buying behavior in automobile industry. *Journal of Information and Optimization Sciences, 46*(3), 879–892. https://doi.org/10.47974/JIOS-1953