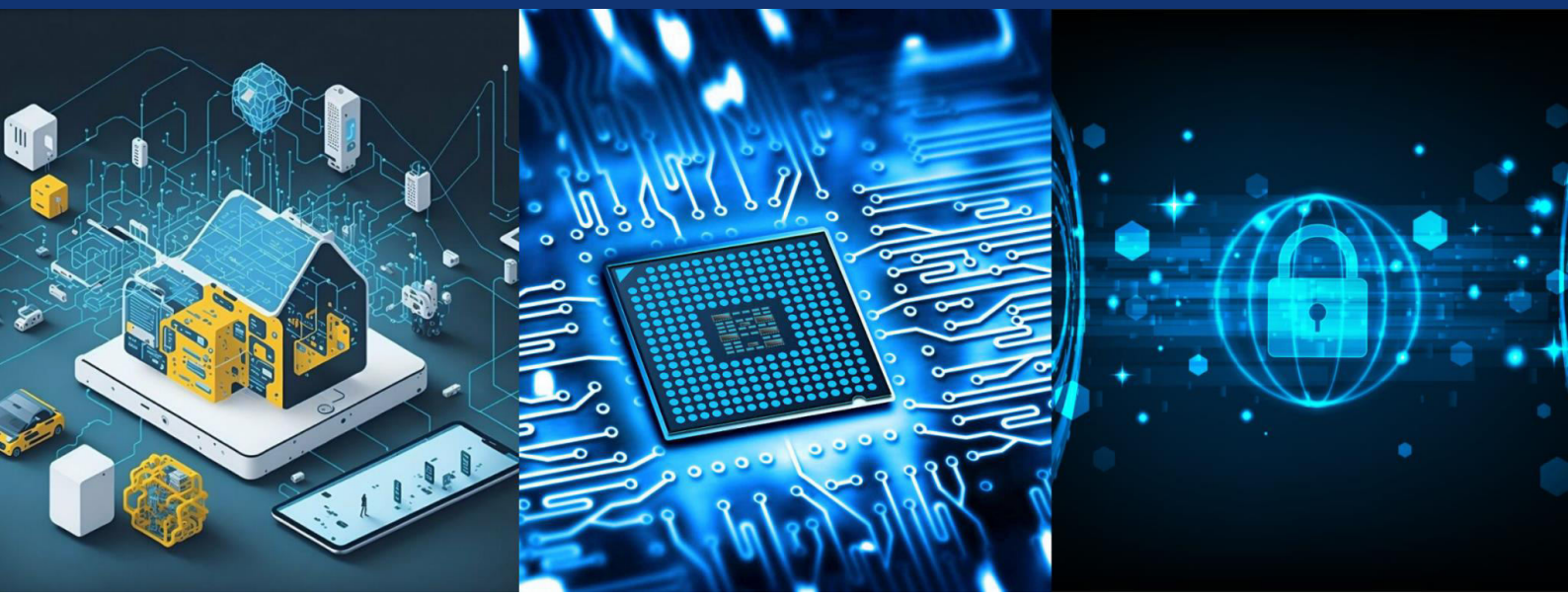
IJIRCCE

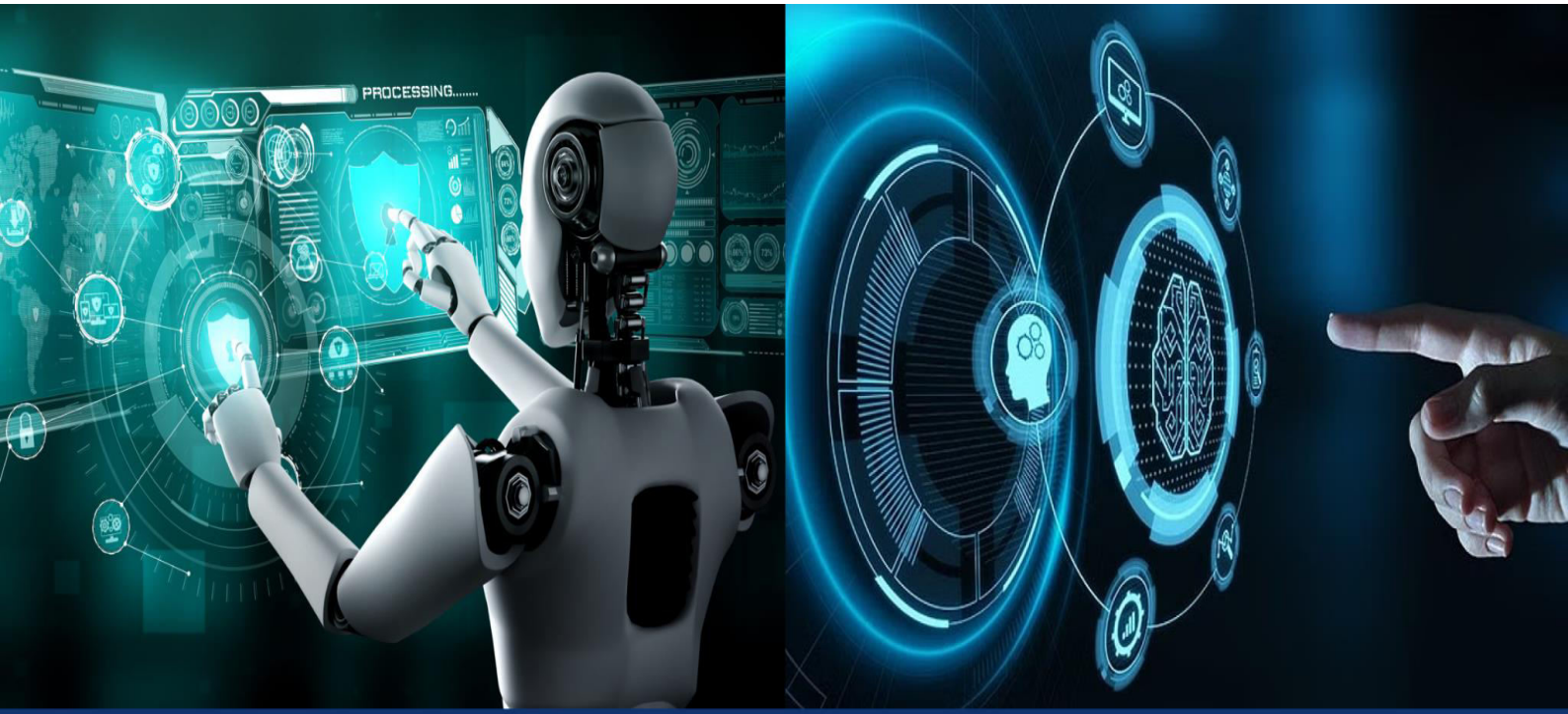
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 3, March 2025

© 2025 IJIRCCE | Volume 13, Issue 3, March 2025| DOI: 10.15680/IJIRCCE.2025.1303115

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Surveillance for Threat Detection using Yolo

Shubha Shree. G N, Dr. V. Sangeetha

III-B. Sc., Department of Computer Science with Data Analytics, Dr. N.G.P. Arts and Science College, Coimbatore, India

Assistant Professor, Department of Computer Science with Data Analytics, Dr. N.G.P. Arts and Science College, Coimbatore, India

ABSTRACT: Surveillance for threat detection involves identifying and analyzing potential threats in visual data. This paper presents a system that detects and classifies threats in video footage using the YOLO (You Only Look Once) object detection algorithm. The system processes video frames to identify suspicious activities or objects, such as weapons, violence, or abnormal behaviours. The detection process involves applying YOLO for real-time localization and classification of threats. Once detected, the system marks the threat regions with bounding boxes, highlighting the areas of concern. The proposed approach enables automated, efficient, and accurate surveillance monitoring, reducing the need for manual intervention and enhancing security measures.

KEYWORDS: Threat detection, YOLO, Object detection, Surveillance, Real-time monitoring, Security analysis.

I. INTRODUCTION

Surveillance for threat detection is a crucial application in modern security systems, aiming to automatically identify and classify potential threats in real-time video footage. This process involves detecting suspicious activities, objects, or behaviors, such as weapons, violence, or unauthorized access, to enhance security and prevent incidents.In this system, the YOLO (You Only Look Once) object detection algorithm is employed for real-time threat detection. YOLO efficiently processes video frames, localizing and classifying threats with high accuracy. The system marks detected threats with bounding boxes, enabling security personnel to respond promptly.

Threat detection through surveillance has various real-world applications, including monitoring public spaces, transportation hubs, and critical infrastructure. It helps in identifying criminal activities, ensuring public safety, and supporting law enforcement operations.The paper is organized as follows: Section II describes the threat detection process using YOLO, including video frame processing and object classification. Section III explains the visualization and marking of detected threats using bounding boxes. Section IV presents the experimental results and performance analysis of the system. Finally, Section V concludes the paper with insights and future directions.

II. RELATED WORK

Threat detection through surveillance has gained significant attention in recent years, with various methods proposed for real-time monitoring and analysis. The YOLO (You Only Look Once) algorithm, introduced by Redmon et al. [1], revolutionized real-time object detection by providing accurate localization and classification in a single pass through the network. This one-stage detection model significantly improved speed and efficiency compared to traditional two-stage approaches like Faster R-CNN.

In [2], the authors implemented YOLOv3 for real-time detection of suspicious objects, such as firearms and knives, in surveillance videos. The model demonstrated high accuracy and low latency, making it suitable for real-world applications. Another work by Bochkovskiy et al. [3] introduced YOLOv4, which enhanced detection accuracy and performance by incorporating data augmentation techniques and improved backbone architectures.

Several studies have explored the use of deep learning models, including CNNs and RNNs, for threat recognition. In [4], the authors combined YOLO with LSTM to track and classify threats over multiple frames, improving the reliability of the detection system. Furthermore, in [5], researchers applied object tracking algorithms alongside YOLO

© 2025 IJIRCCE | Volume 13, Issue 3, March 2025| DOI: 10.15680/IJIRCCE.2025.1303115

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

to follow identified threats across video sequences, ensuring continuous monitoring.The system presented in this paper builds on these prior works by utilizing YOLO for real-time threat detection. The approach efficiently detects and marks threat regions with bounding boxes, enabling rapid identification of potential dangers in surveillance footage.

III. METHODOLOGY

The proposed threat detection system uses the YOLO algorithm for real-time surveillance analysis. The methodology consists of several stages. First, the input video is processed by extracting individual frames, which are then resized and preprocessed to match the YOLO model's input dimensions. Next, each frame is passed through the YOLO model, which performs object detection and localization. The algorithm outputs bounding boxes, class labels, and confidence scores for the identified objects. Suspicious objects or behaviors, such as weapons or acts of violence, are flagged.

The detected threats are then highlighted with bounding boxes, indicating their location within the video frame. Confidence scores are displayed alongside the bounding boxes to reflect the accuracy of the detection. To enhance the system's reliability, post-processing and tracking are applied. Detected threats are monitored across consecutive frames, ensuring consistent identification. Object tracking algorithms, such as SORT or DeepSORT, are used to maintain consistent labeling of moving threats.

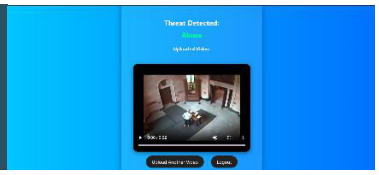
The proposed system ensures efficient and accurate threat detection in real-time, making it suitable for surveillance applications in public spaces, transportation hubs, and security-sensitive areas.

IV. EXPERIMENTAL RESULTS

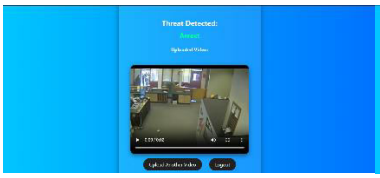
The figures illustrate the results of threat detection and classification using the YOLO model. (a) Represents the **Login** page. (b) Displays the **Video Upload** interface, where smaller objects below a predefined threshold are filtered out. Only regions with significant area and dimensions related to potential threats are retained.

(a) Login

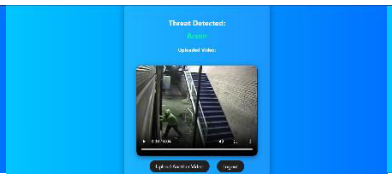
(b)Upload Video



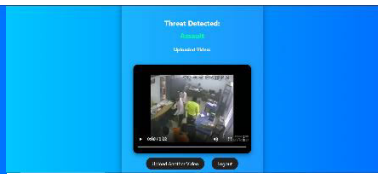
(i) Predicted Video



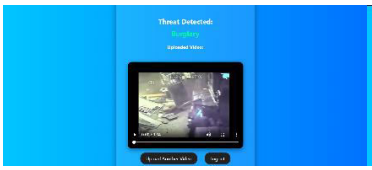
(ii) Predicted Video type(Arrest)



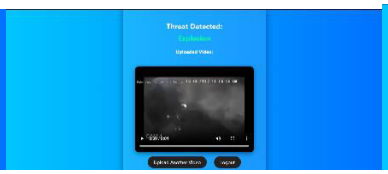
(iii) Predicted Video type(Arson)



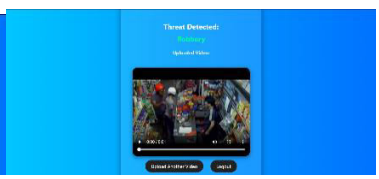
(iv) Predicted Video type(Assault)



(v) Predicted Video type(Burglary)



(vi) Predicted Video type(Explosion)



(vii) Predicted Video type(Robbery)

Threat Detection using YOLO

(a) Displays the **Login** page.

(b) Shows the **Video Upload** interface.

(i) to (vii) Display the predicted video types, including:

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- (i) Abuse
- (ii) Arrest
- (iii) Arson
- (iv) Assault
- (v) Burglary
- (vi) Explosion
- (vii) Robbery

V. CONCLUSION

We have implemented an automated **threat detection system** using the **YOLO model** for surveillance video analysis. The system effectively detects and classifies suspicious activities by identifying potential threat regions in video frames. The algorithm was tested on multiple surveillance clips and accurately detected various threat types, demonstrating its reliability and efficiency in real-world scenarios.

REFERENCES

[1] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You Only Look Once: Unified, Real-Time Object Detection," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 779-788, 2016.
[2] G. Jocher, A. Chaurasia, and A. Qadir, "YOLOv8: Real-Time Object Detection," *Ultralytics*, 2023.
[3] J. Deng, W. Dong, R. Socher, L. Li, K. Li, and L. Fei-Fei, "ImageNet: A Large-Scale Hierarchical Image Database," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 248-255, 2009.
[4] A. Dosovitskiy, L. Beyer, A. Kolesnikov, et al., "An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale," *International Conference on Learning Representations (ICLR)*, 2021.
[5] T.-Y. Lin, M. Maire, S. Belongie, et al., "Microsoft COCO: Common Objects in Context," in *European Conference on Computer Vision (ECCV)*, pp. 740-755, 2014.
[6] H. Law and J. Deng, "CornerNet: Detecting Objects as Paired Keypoints," in *European Conference on Computer Vision (ECCV)*, pp. 734-750, 2018.
[7] A. Howard, M. Sandler, G. Chu, et al., "Searching for MobileNetV3," in *Proceedings of the IEEE International Conference on Computer Vision (ICCV)*, pp. 1314-1324, 2019.
[8] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 770-778, 2016.
[9] L. Bottou, "Large-Scale Machine Learning with Stochastic Gradient Descent," in *Proceedings of COMPSTAT*, pp. 177-186, 2010.
[10] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," in *Advances in Neural Information Processing Systems (NeurIPS)*

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details