IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Suspicious Human Activity detection using AI and ML

Meghana C, Monika Kadam N, Preethi N, Priyanka P
Under the Guidence of
Mrs.Pratibha S
Asst. prof, Dept of CS&E
PES Institute of Technology and Management Shimoga, India

Abstract: With the rise in anti-social activities, the need for robust security measures has become paramount. Closed-Circuit Television (CCTV) systems are commonly deployed for continuous surveillance, but the manual monitoring of extensive footage is impractical. This paper proposes an innovative approach by integrating YOLOv3 and Mobile LSTM into surveillance systems to efficiently identify abnormal activities with precision and speed. YOLOv3's object detection capabilities are leveraged to enhance the system's ability to detect concerning behaviors such as aggression, unauthorized access, and erratic movements. Additionally, Mobile LSTM is introduced for its proficiency in sequential data processing, enabling precise temporal analysis within video streams. By combining YOLOv3 and Mobile LSTM, the proposed model effectively captures both spatial and temporal information, enhancing the system's overall surveillance capabilities. This integration not only improves the accuracy of abnormal activity detection but also expedites decision-making processes, thus addressing the challenges posed by manual monitoring and bolstering security measures.

Keywords: Artificial intelligence, YOLOv3 model, Mobile LSTM, video surveillance, abnormal activity detection

Introduction

Human activity detection for video surveillance system is an automated way of processing video sequences and making an intelligent decision about the actions in the video. It is one of the growing areas of Computer vision and artificial intelligence. A lot of cameras are installed in many places for surveillance, but the surveillance is done by human, and it is done only if there is a report of anomaly behavior, otherwise the videos are kept as archives, and never use. Developing algorithms for automatic detection of Human movements, and making appropriate decision when there is any suspicious behavior, it will result to real time processing of Human activities in public places. It will help in security, and ensuring public safety.

1. Literature Survey

A. Suspicious Human Activity Recognition for Video Surveillance System

Authors: Prateek Agrawal, Ahmad Salihu Ben Musa, and Sanjay Kumar Singh.

In this research work Suspicious Human Activity Recognition for Video Surveillance System, we detected cheating activities in examination hall. We used SURF (Speed Up Robust Features) to extract interest points, and use SURF method to match and find the corresponding features. We used some algorithms to classify the suspicious activities. We also use Viola Jones object detectors for finding the faces and labelling the activities. We also use tracking algorithms to track detectors in the input video.

They have implemented Suspicious Human activity Recognition Surveillance System, which will be useful in detecting and recognizing cheating activities in the examination hall using SURF.

B. Methodology For Human Suspicious Activity Detection

Authors: Tejashri Subhash Bora, Monika Dhananjay Rokade

The crime is increasing day by day. So for the security, the demands for surveillance cameras are also increased. Surveillance cameras are more and more being used in public places e.g. streets, intersections, banks, shopping malls, etc. However, the monitoring ability of law enforcement agencies has not kept pace. The outcome is that there is a deficiency in the utilization of surveillance cameras and an unworkable ratio of cameras to human monitors. One critical task in video surveillance is detecting anomalous events such as traffic accidents, crimes or illegal activities. Such systems require frequent rule-base updates and signature updates, and are not capable of detecting unknown attacks. The result of the

proposed system will be able to detect whether any anomaly action is taking place or not. And most of the previous researches had lower accuracy in determining the abnormal behavior.
Therefore, in this a new approach CNN is used for better results.

C. Suspicious Activity Detection in Surveillance Footage

Authors: Prasanna Sumathipala, Gayashan Kariyawasam, Sathyajit Loganathan.

Suspicious activities are of a problem when it comes to the potential risk it brings to humans. With the increase in criminal activities in urban and suburban areas, it is necessary to detect them to be able to minimize such events. Early days surveillance was done manually by humans and were a tiring task as suspicious activities were uncommon compared to the usual activities. Breaking down complicated tasks and detecting sub tasks which lead to potential crimes are one way to simplify an activity to be automated. We focus on two main potential leads to crimes which we attempt to detect through our models. The method proposed for detecting abandoned baggage is computationally efficient and our findings indicate that, while achieving an extremely low false alarm rate, we detected most of the abandoned items effectively.

D. Deep Learning Approach for Suspicious Activity Detection from Surveillance Video Authors: Amrutha C.V, C. Jyotsna, Amudha J.

Video Surveillance plays a pivotal role in today's world. The most unpredictable one is human behaviour and it is very difficult to find whether it is suspicious or normal. Deep learning approach is used to detect suspicious or normal activity in an academic environment. AIML it also uses the latent sematic analysis. It all emphasis on the keywords which are present and the subject and the course which were available. The proposed deep learning approach for detecting suspicious or normal activity in an academic environment using video surveillance data has several advantages. The model can monitor student behavior in a campus and prevent potential crimes or incidents.

2. Algorithm Used

Integrating Mobile LSTM with YOLO for gun detection in security and surveillance systems enhances the capabilities of both algorithms significantly.

Grid Division: YOLO divides the image into a grid, and Mobile LSTM augments this by providing temporal context to the predictions made by each grid cell. This allows for a more nuanced understanding of the evolving scene, improving the system's ability to detect guns accurately amidst complex surroundings.

Bounding Box Prediction: YOLO's bounding box prediction benefits from Mobile LSTM's ability to analyze sequential data. By considering the temporal evolution of objects, Mobile LSTM helps refine the parameters of the bounding boxes, resulting in more precise localization of guns within the video stream.

Class Prediction: Mobile LSTM enriches YOLO's class prediction by incorporating temporal dependencies between frames. This enables the system to better differentiate between objects, reducing false positives and improving the accuracy of identifying guns amidst varying environmental conditions.

Confidence Score: The confidence scores assigned by YOLO are enhanced by Mobile LSTM's contextual understanding. By analyzing the consistency of object trajectories over time, Mobile LSTM adjusts confidence scores dynamically, improving the reliability of gun detection while minimizing false alarms.

Non-Max Suppression: Non-Max Suppression: Mobile LSTM aids in refining non-maximum suppression by considering temporal coherence between detections. This ensures that redundant or overlapping detections are filtered more effectively, resulting in cleaner and more accurate final outputs.

Thresholding: YOLO's thresholding mechanism is improved by Mobile LSTM's ability to adapt to changing contexts. By analyzing the temporal evolution of confidence scores, Mobile LSTM optimizes thresholding parameters, striking a balance between sensitivity and specificity in gun detection.

Post- Post-Processing: Mobile LSTM contributes to post-processing by validating detection outputs based on temporal coherence. This ensures that detected guns are accurately characterized and seamlessly integrated into the broader surveillance narrative, enhancing the overall effectiveness of the system.

In essence, the integration of Mobile LSTM with YOLO enhances gun detection in security and surveillance systems by providing a deeper understanding of both spatial and temporal aspects of the scene. This synergy results in more accurate, robust, and adaptable detection capabilities, ultimately improving safety and security.

3. Existing System

Existing systems often struggle to comprehend complex contextual information, leading to misinterpretations of activities. Understanding nuanced behaviors in different settings remains a challenge. Achieving real-time analysis of higher resolution video streams requires significant computational power, leading to latency issues and resource-intensive processing.

4. Proposed System

Input: The system takes input from various sources such as CCTV cameras, image feeds, or video streams.

Pre-processing: In addition to standard pre-processing steps, such as resizing and normalization, Mobile LSTM analyzes the temporal sequence of pre-processed frames to extract contextual information over time. This temporal analysis enriches the input data, providing the YOLOv3 algorithm with a more comprehensive understanding of the scene dynamics.

YOLOv3 Algorithm: The YOLOv3 algorithm, enhanced with Mobile LSTM, not only predicts bounding boxes, class probabilities, and confidence scores but also incorporates temporal context from neighboring frames. This fusion of spatial and temporal information enables more precise localization and classification of guns in the input images or frames.

Model Deployment: The integrated YOLOv3 model with Mobile LSTM is deployed within the system's architecture, leveraging dedicated hardware for optimized performance. Mobile LSTM's lightweight architecture ensures efficient execution on resource-constrained devices, facilitating real-time analysis of video streams.

Detection and Alerting: Upon detecting a gun, the system generates alerts using Mobile LSTM's contextual insights to improve the accuracy and reliability of notifications. These alerts are transmitted to relevant personnel through visual indicators, audible alarms, or mobile notifications, enabling swift responses to detected threats.

Integration with Security Systems: The integrated gun detection system seamlessly integrates with existing security systems, surveillance networks, and access control systems. Mobile LSTM's compatibility with diverse hardware and software environments ensures smooth communication and coordination between different components of the security infrastructure.

Customization and Fine-tuning: The system allows for customization and fine-tuning of both the YOLOv3 and Mobile LSTM components based on specific deployment requirements and environmental conditions. This includes adjusting detection thresholds, optimizing model hyperparameters, and incorporating real-world feedback to enhance detection accuracy and minimize false alarms.

Scalability and Flexibility: Designed to be scalable and flexible, the system accommodates additional cameras, expands coverage areas, and adapts to evolving security needs. Mobile LSTM's efficiency enables seamless scalability without compromising performance, making it suitable for deployment in various settings, from schools to high-security facilities.

Continuous Monitoring and Maintenance: The integrated system undergoes continuous monitoring and maintenance to ensure optimal performance and reliability. This includes regular updates to the YOLOv3 and Mobile LSTM models, software patches, hardware maintenance, and performance evaluations to assess detection accuracy and system efficiency over time.

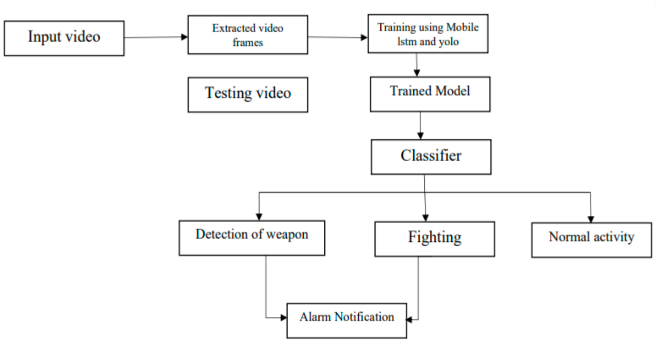

Fig. 1. Block diagram

5. Results and Discussion

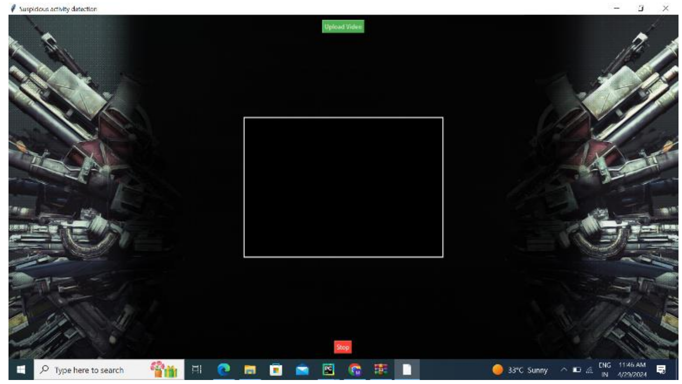

Fig. 2.1 GUI showing project.

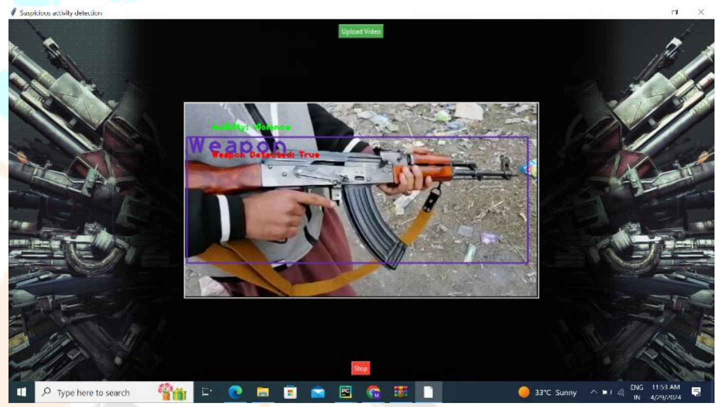

Fig. 2.2 Detection of gun

The above figure shows the detected area highlighted and the weapon is detected in the provided video.

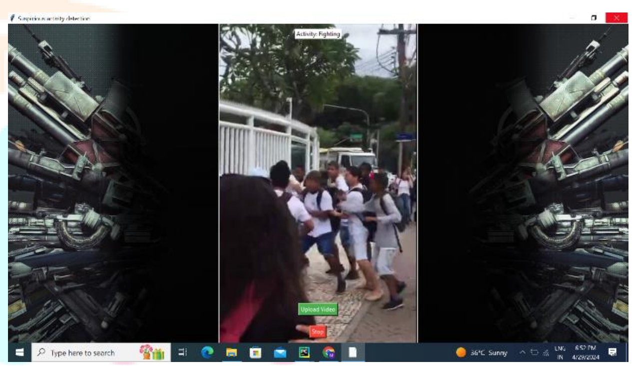

Fig. 5.3 Detection of fighting.

The above figure shows that fighting is detected in the given video stream.

6. Conclusion

In conclusion, our approach provides a reliable and efficient method for using AI to find suspicious behavior. The outcomes demonstrate its potential as an effective tool for boosting security across a range of sectors. Our strategy could have a big impact on public safety and security with further development and incorporation into actual systems. The result of the proposed system will be able to detect whether any anomaly action is taking place or not. The necessity to develop such a security system is increasing with the increasing number of violence that are happening everyday.

References

[1] P.Bhagya Divya, S.Shalini, R.Deepa, Baddeli Sravya Reddy, "Inspection of suspicious human activity in the crowdsourced areas captured in surveillance cameras", International Research Journal of Engineering and Technology (IRJET), December 2017.

[2] U.M.Kamthe,C.G.Patil "Suspicious Activity Recognition in Video Surveillance.System", Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018.

[3] Amrutha CV, Jyotsna C, Amudha J (2020) Deep learning approach for suspicious activity detection from surveillance video. In: 2020 2nd international conference on innovative mechanisms for industry applications (ICIMIA), pp 335–339. IEEE

[4] G. Sreenu and M. A. Saleem Durai "Intelligent video surveillance: a review through deep learning techniques for crowd analysis" , Journal Big Data ,2019.

[5] Anishchenko, L (2018) Machine learning in video surveillance for fall detection. In: 2018a ural symposium on biomedical engineering, radioelectronics and information technology (usbereit), pp 99–102. IEEE.

[6] A. O Oredein, "Checking Examination Malpractice in Nigerian Schools, Nigerian Journal of Educational Research and Evaluation", Vol: 5, No: 1, pg: 82-90, 2004.

[7] K. Kavikuil and Amudha, J., "Leveraging deep learning for anomaly detection in video surveillance", Advances in Intelligent Systems and Computing,2019.