AI Powered Automated Suspicious Activity Survilance

Anuja Gaikwad
MCA(JSPM UNIVERSITY)

Dr. Khan Arahiya Anjum
Asst.Prof.JSPM UNIVERSITY

ABSTRACT:

In this study, we investigate the use of deep learning models, such as convolutional neural networks recurrent neural networks, and their variations, for the automated detection of suspicious activity in a variety of contexts, such as video surveillance, network security, and financial transactions.

Large datasets of pertinent data are first gathered and preprocessed by the proposed system, which may comprise camera footage, network traffic logs, or financial transaction records. These datasets are then used to train deep learning models to discover trends and anomalies connected to shady activity.

KEYWORDS;

Object detection, visual data, background extraction, intelligent camera surveillance, CCTV camera.

INTRODUCTION :

Automated suspicious activity detection is a crucial tool in today's digital landscape, enabling the protection of sensitive information and critical assets.[2] It uses advanced technologies like artificial intelligence, machine learning, and data analytics to identify anomalies and respond to irregular behavior. This proactive approach offers benefits such as safeguarding financial transactions, protecting sensitive information in healthcare and banking, securing critical infrastructure, and enhancing cybersecurity in personal devices.[5] Automation minimizes human error and enables quicker and more precise threat mitigation. As the digital realm continues to evolve, implementing automated suspicious activity detection is essential for maintaining digital security.

LITRATUER SURVEY

Through the use of real-time object detection, the "Suspicious Activity Detection from Videos Using YOLOv3" project takes a novel approach to enhancing security and surveillance by spotting and reacting to suspicious activity in video footage. While raising significant ethical and privacy issues, this technology has the potential to increase public safety and security across a variety of domains[1]By fusing the strength of deep learning with specially designed features, this project seeks to develop a reliable violence detection system for video sequences, ultimately enhancing safety and security in various domains[2] The objective of the project is to create a sophisticated method of spotting and flagging potentially suspicious

actions or behaviours in surveillance video footage. This project leverages Convolutional Neural Networks (CNNs), a deep learning architecture known for its effectiveness in image and video analysis[3] Project represents a technological solution to tackle the issue of academic dishonesty. By combining cutting-edge technology and robust algorithms, it aims to create a secure and fair examination environment, ultimately benefiting both students and educational institutions[4].Event Detection in Surveillance Videos: A Review" offers a valuable resource for researchers, practitioners, and policymakers interested in surveillance technology and video analysis. It provides an in-depth overview of the current state of event detection in surveillance videos, shedding light on both the progress made and the challenges that lie ahead in this important domain[5].This project focuses on the development of a sophisticated deep learning-based system for recognizing suspicious activities in video sequences. By combining the power of DarkNet-NasNet for feature extraction, it aims to enhance the accuracy and efficiency of anomaly detection in video surveillance[6].This project leverages deep learning techniques to develop a robust system for the automated detection of suspicious activities in surveillance videos, contributing to enhanced security and safety in various contexts[7]. The main goal of this project is to contribute to the development of surveillance and security systems that can automatically detect violent actions, thus enhancing public safety and security in real-time video monitoring scenarios[8].The project emphasized that the choice of machine learning technique should be tailored to the specific requirements and characteristics of the surveillance system. A combination of supervised and unsupervised methods, along with advanced feature extraction and real-time processing, can contribute to more robust and effective suspicious behaviour recognition in intelligent surveillance systems. Future research could focus on improving the adaptability of models to evolving threats and reducing false positives to enhance the practicality of these systems[9]. The project "Crowd Density Analysis and Suspicious Activity Detection" aims to develop a system that uses computer vision and machine learning techniques to monitor and analyze crowd behaviour in public spaces. This system will be capable of calculating crowd density, identifying anomalous crowd behaviours, and detecting suspicious actions in real-time. By processing video feeds from surveillance cameras, it can provide valuable insights for security and crowd management in various settings, such as airports, stadiums, and urban areas. The project's primary objectives include enhancing security, improving crowd flow management, and ensuring the safety of public spaces through intelligent video analysis[10].

4. EXISTING SYSTEM

In Existing System, They Used SVM Algorithm for Suspicious Activity Detection. They Uses Text Data for Detect Suspicious Activity.

where each word or term can be considered a feature. This is particularly beneficial when dealing with text data for suspicious activity detection.[6]

•Robust to Overfitting: SVMs are less prone to overfitting compared to some other machine learning algorithms, thanks to the margin maximization concept. This can result in better generalization performance.

•Versatile Kernels: SVMs allow the use of different kernel functions (e.g., linear, polynomial, radial basis function) to handle complex decision boundaries. This flexibility can help capture non-linear patterns in the data.

•Effective for Binary Classification: SVMs are well-suited for binary classification tasks, which are common in suspicious activity detection (normal vs. suspicious).

5. PROPOSED SYSTEM

The system uses a video dataset for input and employs modules for preprocessing, feature extraction, and classification. The first input is a video dataset, which is preprocessed to remove blur and image imperfections. The system then extracts parameters or features in the extraction section. The classification process uses the CNN algorithm for suspicious activity detection.

5.1 PROJECT MODULES :

The obtained data may require preprocessing to clean, normalize, and present it suitably. This step ensures that the data is in a usable state for analysis.

Relevant characteristics or traits are taken from the data during data analysis. These qualities or trends in the data are indications of potential suspicious conduct.

5.2 METHODOLOGY(ARCHITECTURE)

Video Input & Frame Segmentation Capture real-time video stream or pre-recorded footage.as shown in fig 1

Segment into frames at a chosen rate (e.g., 10–15 FPS); group frames into segments—for instance, 3 seconds = 30 frames—for higher-level**Background Modeling & Subtraction** Generate a **background model** using approaches like Gaussian Mixture Models (GMM), ViBe, or the Teknomo–Fernandez algorithm for initial background frame Perform pixel-wise **subtraction** between current frames and background to extract **foregrounmasks**[2]Optionally as shown in fig 2 enhance segmentation by combining classic BGS with **real-time semantic segmentation** (CNN-based) for refined mask**Foreground Extraction & Object Segmentation**Clean masks via morphological operations to refine object blobs.Use connected-component analysis to identify individual moving objects; optionally deploy a lightweight CNN to distinguish human vs. non-human foregrounds (e.g., luggage Track objects across frames to build continuous **object trajectories**.**Feature Extraction & Sequence Encoding**[3]For each object or frame segment, extract:

Spatial features: CNN-based deep features (ResNetInception) from bounding**Temporal features**: motion trajectories, optical flow histograms (HOF), tracking dynamicAggregate features across grouped frames into sequences for input to temporal models.**Suspicious vs Normal Activity Detection**Train classification models to distinguish between “normal” and “suspicious” events (e.g., running, loitering, fighting, trespassing, theft) using labeled data sets Implement ensemble or rule-informed filtering to improve reliability and reduce false alarms.

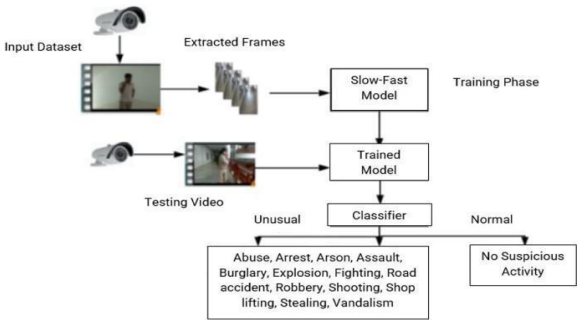

Fig 1 (flow chart)

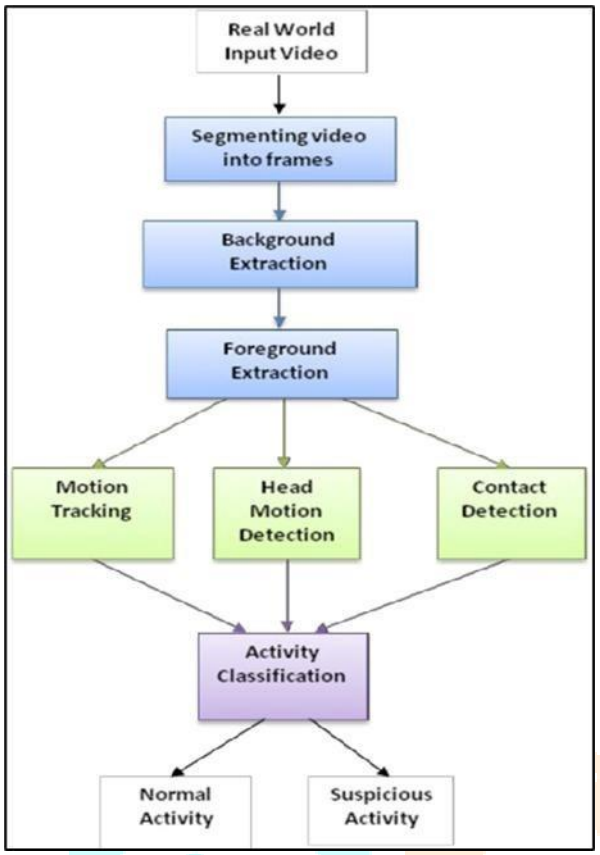

Fig 2(system architecture)

5.3ALGORITHMS USED

Suspicious activity detection in videos is a complex and specialized field that uses Convolutional Neural Networks (CNN) to automatically extract features from visual data. The algorithmic steps involve data collection and preparation, frame preprocessing, feature extraction, temporal analysis, model training, detection threshold, inference, post-processing, alert generation, evaluation and fine-tuning, deployment, and scalability. Data is collected from surveillance cameras or other sources, divided into frames or clips, and resized to a common size. Pre-trained CNN models like VGG, ResNet, and Inception are used for feature extraction. Temporal analysis is considered by considering a sequence of frames as inputs. Model training involves fine-tuning the pre-trained CNN model on an annotated dataset of normal and suspicious activities. The detection threshold is set based on factors like the model's confidence score or other domain-specific criteria. The model is then applied to analyze video frames or sequences, calculates the probability of containing suspicious activity, applies post- processing techniques to reduce false positives and improve detection accuracy, and generates alerts or notifications when identifying suspicious activity beyond the threshold.

RESULT AND DISCUSSION

Real-Time Detection: Intelligent surveillance systems equipped with advanced software can analyze video feeds in real-time to identify behaviors such as sudden movements, loitering, or unusual interactions. in public safety applications. **Pattern Recognition**: Machine learning algorithms, particularly those utilizing unsupervised learning, have shown promise in detecting anomalies without predefined rules. By analyzing large datasets, these systems can identify subtle patterns indicative of suspicious activities, thereby reducing false positives and enhancing detection accuracy

Behavioral Analytic Incorporating behavioral analytics allows for a more nuanced understanding of user actions. By establishing baseline behaviors and monitoring deviations, organizations can proactively identify potential threats, whether they stem from insider actions or external breache**Privacy Concerns**: The deployment of surveillance systems raises significant privacy issues. It's essential to balance security needs with individual rights, ensuring that monitoring practices are transparent and comply with legal standards.**False Positives**: Despite advancements, detecting suspiciousbehavior without generating false alarms remains a challenge. Continuous refinement of detection algorithms is necessary to minimize these occurrences.

CONCULSION

challenges persist, the ongoing development and implementation of sophisticated detection systems are pivotal in safeguarding environments from potential threats. By addressing privacy concerns, minimizing false positives, and embracing technological advancements, organizations can enhance their security frameworks and respond effectively to suspicious activities.

REFERENCES:

[1]P. Bhagya Divya, S. Shalini, R. Deepa, and 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] "Suspicious Movement Detection and Tracking of Human Behaviour and Object with Fire Detection Using A Closed Circuit TV (CCTV) cameras," International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 5 Issue XII December 2017.

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

[4] Zahraa Kain, Abir Youness, Ismail El Sayad, Samih Abdul-Nabi, Hussein Kassem, " Detecting Abnormal Events in University Areas ", International conference on Computer and Application,2018.

[5] Tian Wanga, Meina Qia, Yingjun Deng, Yi Zhouc, Huan Wangd, Qi Lyua, Hichem Snoussie, "Abnormal event detection based on analysis of movement information of video sequence",Article-Optik,vol-152,January-2018.

[6] Nipunjita Borodoloi, Anjan Kumar Talukadr, Kandarpa Kumar Sarma "Suspecious Activity Detection from Video YOLOv3,Department of electronic and communication engineering Gauahati University . Feb. 2020

[7] Nipunjita Borodoloi, Anjan Kumar Talukadr, Kandarpa Kumar Sarma "Suspecious Activity Detection from Video YOLOv3" ,Department of electronic and communication engineering Gauahati University . Feb. 2020

[8] Nipunjita Borodoloi, Anjan Kumar Talukadr, Kandarpa Kumar Sarma "Suspecious Activity Detection from Video YOLOv3" ,Department of electronic and communication engineering Gauhati University . Feb. 2020

[9] Amrutha C.V, C. Jyotsna, Amudha J. , "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video", International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020)

[10]Abdolamir Karbalaie · Farhad Abtahi ·M˚arten Sj¨ostr¨om "Event detection in surveillancevideos:areview",MULTIMEDIA TECHNOLOGYFORSECURITYANDSURVEILLANCEIN DEGRADEDVISION, jan-2021

[11] Musa Dima Genemo "Suspicious activity recognition for monitoring cheating in exams", International Conference on Data Engineering and Communication Technology, pp. 525–533 2020

[12] Li, C., Han, Z., Ye, Q., Jiao, J.: Abnormal behaviour detection via sparse reconstruction analysis of trajectory. In: Proceedings- 6th

International Conference on Image and Graphics, ICIG 2011. pp. 807810 (2011)

[13] Lu, C., Shi, J., Jia, J.: Abnormal event detection at 150 fps in matlab. In: 2013 IEEE International Conference on Computer Vision.
pp. 27202727 (Dec 2013)

[14] Mahadevan, V., Li, W., Bhalodia, V., Vasconcelos, N.: Anomaly detection in crowded scenes. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) pp. 19751981 (2010)

[15] Medel, J.R.: Anomaly Detection Using Predictive Convolutional Long Short-Term Memory Units. Masters thesis, Rochester Institute of Technology (2016), accessed from http://scholarworks.rit.edu/theses/9319

[16] Mehran, R., Oyama, A., Shah, M.: Abnormal crowd behaviour detection using social force model. In: 2009 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, CVPR Workshops 2009. pp. 935942 (2009)

[17] Mo, X., Monga, V., Bala, R., Fan, Z.: Adaptive sparse representations for video anomaly detection. IEEE Transactions on Circuits and Systems for Video Technology 24(4), 631645 (2014

[18] Patraucean, V., Handa, A., Cipolla, R.: Spatio-temporal video autoencoder with dierentiable memory. International Conference On Learning Repaer sentations (2015), 110 (2016), http://arxiv.org/abs/1511.06309

[19] Piciarelli, C., Micheloni, C., Foresti, G.L.: Trajectory-based anomalous event detection. IEEE Transactions on Circuits and Systems for Video Technology 18(11), 15441554 (2008)