Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 3, No. 2, March : 2024

SUSPICIOUS ACTIVITY DETECTION IN VIDEO SURVEILLANCE USING CONVOLUTIONAL NEURAL NETWORK

Mrs. Dr. Saleha Sudagar, Mrs. Ruchira Tare, Assistant Professor, Dept. Of Computer Engineering, Trinity College of Engineering and Research, Pune, India.
Mr. Pratik Garkar, Mr. Suyash Shishupal, Mr. Tohid Inamdar, Mr. Tejas Dalvi, Student of Computer Engineering, Trinity College of Engineering and Research, Pune, India.

Abstract
Video surveillance systems have become an integral part of ensuring public safety and security are a concern in multiple areas, such as transportation, retail, and critical infrastructure. Detecting suspicious activities within vast amounts of video data is a challenging task, necessitating the development of sophisticated methods. A new strategy is proposed in this study to detect suspicious activity in video surveillance using Convolutional Neural Networks (CNNs).
The proposed system leverages the deep learning capabilities of CNNs to automatically extract relevant features from video frames and identify unusual or suspicious behaviours. Key steps in the methodology include data preprocessing, frame extraction, and CNN model training. By utilizing a large dataset of labelled video clips, the CNN model learns to recognize patterns associated with suspicious activities, such as loitering, violence, or trespassing.
Keywords: Video Surveillance, Security, Machine Learning, Internet of Things, sensors.

I. Introduction

Suspicious activity detection intended to detect various types of suspicious activities including human behavior. Any observed behavior that indicates a person may be involved in a crime or about to commit a crime is called suspicious activity. Surveillance video monitoring requires the detection of human suspicious activity, which is an important task. The task of monitoring a large video dataset can be both time-consuming and complex. This causes the detection of suspicious activity to be missed. Automating video dataset monitoring and detecting suspicious activity in surveillance systems is of great importance, as shown by this.

Fig. Suspicious Activity Detection

The challenges in HAR include simultaneous activities, interleaved activities, ambiguity of prediction, multiple people, and various technical challenges like occlusion, illumination, and variations in object size. By using a 63-layer CNN model, pre-training, and feature optimization, the proposed solution aims to tackle these challenges through a deep feature extraction methodology.

II. Literature

A description is given by the author is comprehensive overview of the existing literature on human activity recognition. They discuss various approaches, including handcrafted feature extraction methods and deep learning techniques. Previous works in the field and the significance of HAR in various applications, such as healthcare, human-robot interaction, surveillance, and others, are highlighted by them.
The research in [1], Suspicious Activity Detection from Videos using YOLOv3 in 2020 by Nipunjita Bordoloi 1, Anjan Kumar Talukdar2 developed Suspicious activity detection is This paper discusses

the use of YOLOv3, a popular deep learning algorithm, for detecting suspicious activities in video sequences. Suspicious activity detection is an important area in computer vision and artificial intelligence, especially for security and surveillance applications. The paper highlights the challenges in human detection due to non-rigid body shapes and varying environmental conditions, such as poor lighting and pose variations.

The paper provides an overview of related work in the field of suspicious action detection, citing different approaches and methods used by various researchers. These methods range from multiple instances learning to background subtraction and deep neural networks.

The research in [2], Suspicious Activity Recognition Using Proposed Deep L4-Branched-Actionnet with Entropy Coded Ant Colony System Optimization in 2021 The developed framework is first transformed into a pre-trained framework by conducting its training on an object detection dataset called CIFAR-100 with the SoftMax function.

The research in [3], Crowd Density Analysis by Shriya Akella, Priyanka Abhang The paper addresses the need for intelligent surveillance systems to distinguish between normal and suspicious behavior in public and private spaces. The proposed system utilizes the YOLOv3 algorithm for object detection, trained on the COCO dataset. It consists of two main components: feature computation from images and activity classification based on detected features. The system calculates crowd density by counting the number of people in a frame and identifies suspicious objects like isolated bags, knives, and guns.

The paper [4], Novel Deep Neural Network for Suspicious Activity Detection and Classification by Ms. A. M. Bhugul1, Dr. V. S. Gulhane in 2023 The commitment to one's job and the protection of children have undeniably become paramount concerns, particularly in industrialized nations. As societal demands evolve, so does the need to safeguard our loved ones, and this extends to the broader public as well. Unfortunately, the modern world has witnessed a surge in incidents involving the use of weapons, resulting in the tragic loss of innocent lives. Robberies, especially at banks and ATMs, have become disturbingly common occurrences. While the deployment of CCTV surveillance systems has proliferated, it is disheartening to observe that crimes, particularly those involving weapons, continue to escalate.

The existing monitoring systems, although a significant step towards ensuring security, possess a fundamental limitation—they often lack the inherent capability to autonomously detect suspicious activities. In the field of computer science, this problem must be solved. The main concerns are on recognizing distinctive human behaviors and developing the capacity to distinguish between what is considered normal and what is obviously wrong, especially in the diverse range of public and private contexts.

The detection of suspicious conduct in private situations is the main emphasis of this work. such as the all-too-frequent robberies in banks or the potential for violence in public places, including ATMs, and other financial institutions. Each of these environments presents a distinctive array of abnormal behaviors, making it crucial to develop sophisticated and effective methods to detect and respond to potential threats. In an era where safety is an increasing concern, this research takes a significant step towards enhancing security measures and ensuring the safety of our communities.

The paper [5], Performance Evaluation of Automatic Suspicious Activity Detection Method in 2023 by Dr. Sachin S. Gurav The paper addresses the challenge of video monitoring when dealing with large surveillance video datasets. Monitoring such datasets can be a cumbersome task, and errors in monitoring and detecting suspicious activities can lead to missed detections. Automation of suspicious activity detection has become a necessity in this context. This research evaluates the effectiveness of an approach that integrates many methods, such as GLCM, Harries corner detection, and speeded up robust features (SURF), for suspicious activity identification in video data. The results demonstrate an average accuracy of 96% in detecting suspicious activities on a self-designed dataset.

The need for automating video dataset monitoring and suspicious activity detection is underscored, as manual monitoring of large video datasets can be time-consuming and complex, often resulting in missed detections. The automation algorithm primarily focuses on human suspicious activity

detection, where human movement within frames is a central point of interest. The paper outlines a method that reduces the complexity of identifying human objects within multiple frames, thus streamlining the processing task.
The literature survey conducted in the paper provides insights into various techniques and methods used in the field of video surveillance and human activity detection. These incorporate the utilize of highlights like speeded up vigorous highlights (SURF), neighbourhood double design (LBP), histogram-based action discovery, and more. These strategies are aiming to extend the exactness and productivity of video checking and discovery of suspicious movement.
The proposed work comprises of a four-stage preparing approach for suspicious action location. The strategy begins with the location of suspicious outlines, lessening the handling stack compared to dissecting all outlines within the video. Feature extraction, including GLCM-based features and entropy-based features, is carried out on these suspicious frames. The paper too examines the utilize of Harries corner location and SURF include extraction within the consequent stages of confirmation. The research presents a novel approach to improving the accuracy of suspicious activity detection by combining multiple methods in a sequential manner. This multi-stage processing enhances the performance of the system, resulting in a 96% average accuracy in detecting suspicious activities. The approach is comprehensive, addressing the challenges in monitoring large video datasets and automating the detection of suspicious activities, which is vital for enhancing security and surveillance efforts.
The object detection in manga images are done through convolutional neural network[6]. The right comparison between R-CNN , Speedier R-CNN and SSD are done here. The panel layout of manga images are better identified through R-CNN while the speech balloon identified through Faster R-CNN.
In [7] author has implemented intrusion detection through deep learning where preprocessing is done through 1-hot encoding method which is one of the CNN method. The feature selection is done through marine predator algorithm which is nature inspired marine creature strategy. Legitimate highlights will offer assistance increment the productivity of suspicious movement location which is appeared within the result through matlab utilizing VeReMi. Encourage they have compared the proposed strategy with existing machine learning classification calculation.
In [8] author has delved into the importance of anomaly detection and explores how SVM and CNN-based methods are reshaping the landscape of security and safety in public spaces.
In [9] The author has examined the issue of malpractice during examinations, whether it's online or offline. Activities such as copying from neighbouring candidates or external materials, exchanging answer scripts, and other forms of cheating have threatened the integrity of examination systems. Such behaviours typically involve deviations from the normal posture and movements observed in candidates during the initial stages of the examination. This review explores a groundbreaking solution that utilizes real-time edge computing and video analytics to identify and prevent suspicious activities related to examination malpractice.
In [10] author introduces a system that assesses the accuracy of fight detection in surveillance videos using two distinct approaches the 3DCNN (Three-Dimensional Convolutional Neural Arrange) and CNN-LSTM (Convolutional Neural Arrange - Long Brief Term Memory organize).
In [11] Within the proposed work, the creators centre on programmed following and recognizing unordinary developments in closed-circuit recording. The method starts by changing over video film into person outlines. From these outlines, human subjects are distinguished employing a foundation subtraction strategy. The following step includes the extraction of highlights from these distinguished people employing a Convolutional Neural Arrange (CNN).
In [12] The study's reenactment comes about uncover that the integration of CNN with PNN, alluded to as CNN-PNN, has driven to significant changes in question location when connected to video gushing and video observation frameworks. The results grandstand higher rates of precision, f-measure, and decreased rate mistake compared to other existing strategies.

In [13] The framework leverages Profound Learning models, particularly lightweight models like MobileNetV2 and ResNet50V2, to distinguish possibly undermining exercises inside video outlines. Three particular datasets, counting UCF wrongdoing, real-life viciousness circumstances, and UBI-fights, are utilized for preparing and testing. The framework identifies signs of savagery inside video outlines and evaluates exactness in doing so. this framework grandstands the control of profound learning, particularly CNNs like MobileNetV2 and ResNet50V2, to upgrade observation and security in ranges prepared with CCTV cameras.

In [14] The creator presents an imaginative approach utilizing exchange learning, utilizing VGG16 as a highlight extractor and a convolutional neural arrange (CNN) as a classifier. The essential centre of this inquire about is on techniques for optimizing the input highlights and preparing the demonstrate to classify three unmistakable human practices: running, strolling, and waving. The ponder compares comes about accomplished through different approaches.

III. Discussion:

The paper highlights the increasing importance of intelligent visual surveillance systems, especially in public places, where ensuring safety is crucial. It acknowledges that traditional surveillance methods have limitations and outlines the need for more advanced systems to detect and respond to suspicious activities.

The core of the paper is the introduction of the "L4-BranchedActionNet," a deep CNN model designed for feature extraction and classification in suspicious activity recognition. This model is based on an altered version of the AlexNet architecture, with added branches for feature enhancement.

The paper mentions the creation of a dataset consisting of five suspicious activities from existing datasets, such as HMDB51 and AIDER, to train and test the proposed model.

The CNN show is pre-trained on a isolated dataset (CIFAR-100) utilizing the SoftMax work. After pre-training, profound highlights are extricated for the suspicious action acknowledgment dataset. Include subset optimization is connected, utilizing entropy and an subterranean insect colony framework (ACS) calculation to choose the foremost instructive highlights.

The paper utilizes different classification models, counting Back Vector Machines (SVM) and k-Nearest Neighbours (KNN), to classify the extracted highlights. The cubic SVM is detailed to realize the most noteworthy exactness execution of 0.9924.

The proposed demonstrate is assessed on a isolated dataset, the Weizmann activity dataset, accomplishing an precision of 0.9796, which is considered promising.

The paper's commitments incorporate the improvement of the L4-BranchedActionNet demonstrate, the creation of a dataset for suspicious movement acknowledgment, the application of include extraction and optimization procedures, and the assessment of the model's execution on a real-world dataset.

The paper recognizes different challenges in human action acknowledgment and observation, such as impediment, light, varieties in question measure and appearance, and computational time. The proposed demonstrate points to address these challenges and progress the exactness of suspicious movement location.

The paper gives a comprehensive audit of existing investigate in human action acknowledgment and observation frameworks, counting different methods and approaches.

IV. Conclusion

In conclusion, the paper presents a well-structured and comprehensive approach to improving suspicious activity detection in surveillance environments. The proposed CNN-based model, along with feature optimization and classification, shows promise in accurately identifying and classifying suspicious activities. The research addresses important challenges in the field of surveillance and contributes to enhancing public safety and security.

References

[1] N. Bordoloi, A. K. Talukdar and K. K. Sarma, "Suspicious Activity Detection from Videos using YOLOv3," 2020 IEEE 17th India Council International Conference (INDICON), New Delhi, India, 2020, pp. 1-5, doi: 10.1109/INDICON49873.2020.9342230.

[2] T. Saba, A. Rehman, R. Latif, S. M. Fati, M. Raza and M. Sharif, "Suspicious Activity Recognition Using Proposed Deep L4-Branched-Actionnet With Entropy Coded Ant Colony System Optimization," in IEEE Access, vol. 9, pp. 89181-89197, 2021, doi: 10.1109/ACCESS.2021.3091081.

[3] S. Akella, P. Abhang, V. Agrharkar and R. Sonkusare, "Crowd Density Analysis and Suspicious Activity Detection," 2020 IEEE International Conference for Innovation in Technology (INOCON), Bangluru, India, 2020, pp. 1-4, doi: 10.1109/INOCON50539.2020.9298315.

[4] A. M. Bhugul and V. S. Gulhane, "Novel Deep Neural Network for Suspicious Activity Detection and Classification," 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2023, pp. 1-7, doi: 10.1109/SCEECS57921.2023.10063130.

[5] A. S. Kulkarni, N. E, M. Swetha and S. M. Kusuma, "Automated System for Detection of Suspicious Activity in Examination Hall," 2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 2021, pp. 01-05, doi: 10.1109/CONECCT52877.2021.9622599.

[6] S. M, G. S, J. R. Fenitha and S. R, "Fight Detection in surveillance video dataset versus real time surveillance video using 3DCNN and CNN-LSTM," 2022 International Conference on Computer, Power and Communications (ICCPC), Chennai, India, 2022, pp. 313-317, doi: 10.1109/ICCPC55978.2022.10072291.

[7] An Amalgamated Novel IDS Model for Misbehaviour Detection using VeReMiNet, Saleha Saudagar, Rekha Ranawat,

[8] Violence detection for surveillance systems using lightweight CNN modelsN. Suba; A. Verma; P. Baviskar; S. Varma

[9] A. S. Kulkarni, N. E, M. Swetha and S. M. Kusuma, "Automated System for Detection of Suspicious Activity in Examination Hall," 2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 2021, pp. 01-05, doi: 10.1109/CONECCT52877.2021.9622599.

[10] S. M, G. S, J. R. Fenitha and S. R, "Fight Detection in surveillance video dataset versus real time surveillance video using 3DCNN and CNN-LSTM," 2022 International Conference on Computer, Power and Communications (ICCPC), Chennai, India, 2022, pp. 313-317, doi: 10.1109/ICCPC55978.2022.10072291.

[11] A. B. A., P. P. and V. S., "Detection of Suspicious Human Activity based on CNN-DBNN Algorithm for Video Surveillance Applications," *2019 Innovations in Power and Advanced Computing Technologies (i- PACT), Vellore, India, 2019, pp. 1-7, doi: 10.1109/i-PACT44901.2019.8960085.*

[12] D. B, R. K. K, R. S and R. R, "Improved Object Detection in Video Surveillance Using Deep Convolutional Neural Network Learning," *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC),* Palladam, India, 2021, pp. 1-8, doi: 10.1109/I-SMAC52330.2021.9640894.

[13] N. Suba, A. Verma, P. Baviskar and S. Varma, "Violence detection for surveillance systems using lightweight CNN models," *7th International Conference on Computing in Engineering & Technology (ICCET 2022)*, Online Conference, 2022, pp. 23-29, doi: 10.1049/icp.2022.0587.

[14] A. A. Tiriya and M. A. Zaveri, "Human Behaviour Classification for Video Surveillance Using CNN," 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 2020, pp. 769-774, doi: 10.1109/ICACCCN51052.2020.9362771.