iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.60244

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Deep Learning Approach for Suspicious Activity Detection from Video Surveillance

Harshal Khalkar[1], Nikita Nikam[2], Saloni Titame[3], Manas Mali[4], Prof. Abhay R. Gaidhani[5]
Information Technology, SPPU

Abstract: ***Video surveillance is getting more important as technology improves. New systems use artificial intelligence to tell the difference between normal and suspicious behaviour in live video. Since people can be unpredictable, it's hard to know for sure if something is suspicious. This system uses deep learning to identify suspicious activity in schools, like classrooms or hallways. If the system sees something suspicious, it can alert security or the police.***
Here's how it works: The system breaks down the video into individual pictures, one after another. Then, it uses a special program to decide if what's happening in the pictures is suspicious or normal.
Keywords: suspicious activity, video surveillance, deep learning.

I. INTRODUCTION

In the ever-expanding world of video surveillance, traditional methods are reaching their limits. Human analysts face the daunting task of sifting through hours of footage, struggling to distinguish between normal and suspicious activity. This is where deep learning steps in, offering a powerful new approach to suspicious activity detection.

Deep learning, a subfield of artificial intelligence, is particularly adept at analyzing complex patterns. This makes it ideal for deciphering the intricacies of human behavior captured in video surveillance footage. Unlike traditional methods that rely on predefined rules, deep learning can learn and adapt over time. This allows the system to identify even subtle anomalies in human movement or interactions that might go unnoticed by the human eye.

Here's how a deep learning approach for suspicious activity detection works: The system first breaks down the video footage into individual frames, essentially creating a series of snapshots. Then, it goes to work on each frame, extracting key features that could be indicative of suspicious behaviour.These features might include a person's posture, their movement speed, or even the objects they are carrying. Finally, a powerful classifier, trained on a massive dataset of labeled videos, analyzes these extracted features and determines whether the observed behaviour falls within the normal range or deviates into suspicious territory.

The real-world implications of this technology are significant. By automating the detection of suspicious activity, deep learning can significantly reduce the workload placed on human security personnel. Additionally, the ability to identify anomalies in real-time allows for quicker intervention and potentially prevents dangerous situations from escalating. However, it's important to remember that deep learning models are still under development, and ethical considerations regarding privacy and potential biases need to be addressed before widespread adoption.

II. LITERATURE SURVEY

The rise of deep learning has spurred significant research in automating suspicious activity detection within video surveillance systems. This technology holds immense promise for improving security and public safety. A vast body of literature explores various deep learning architectures for this purpose. Convolutional Neural Networks (CNNs) are a popular choice due to their proficiency in extracting spatial features from video frames. Studies have investigated the effectiveness of pre-trained models like VGG-16 and YOLOv3, fine-tuned for identifying suspicious objects and human actions. Additionally, Recurrent Neural Networks (RNNs) are being explored for their ability to analyze the temporal relationships between consecutive frames, providing valuable context for understanding ongoing activities. Research is ongoing to optimize these deep learning models for specific environments and activities, with a focus on improving accuracy, reducing false alarms, and handling challenging scenarios like cluttered backgrounds or low-resolution footage.

However, the literature also acknowledges the limitations and challenges associated with deep learning approaches. The requirement for large, well-labeled datasets for training these models remains a hurdle. Additionally, ensuring the fairness and generalizability of the models across diverse environments and populations is crucial. Researchers are actively exploring techniques to address these concerns, such as data augmentation and domain adaptation methods.

Overall, the deep learning literature on suspicious activity detection from video surveillance paints a picture of a rapidly evolving field with immense potential for real-world applications.

III. SYSTEM OVERVIEW

Video surveillance is becoming increasingly prevalent, but manually sifting through footage for suspicious activity is a cumbersome and time-consuming task. Deep learning offers a powerful solution through its ability to automate suspicious activity detection. Here's an overview of how this approach works:

1) *Data Preprocessing:* The first step involves preparing the video data for the deep learning model. This includes tasks like segmenting the video into individual frames, resizing them to a standard format, and potentially applying techniques to normalize lighting variations or enhance specific features.
2) *Feature Extraction:* This is where the deep learning magic happens. A Convolutional Neural Network (CNN) takes center stage. CNNs are adept at extracting features from visual data like video frames. The CNN architecture typically involves multiple convolutional layers that act like filters, scanning each frame and identifying features like shapes, edges, and motion patterns. These layers progressively build a hierarchy of increasingly complex features that represent the visual content of the scene.
3) *Classification:* Once features are extracted, the system needs to interpret them and determine if they represent suspicious activity. This is where the fully connected layers of the CNN come into play. These layers analyze the extracted features from the previous stage and make a final classification. The network is trained on a massive dataset of labeled video examples, allowing it to learn the visual patterns associated with normal and suspicious behaviors. Based on this training, the final layer outputs a probability score, indicating the likelihood of the observed activity being suspicious.
4) *Alerting and Response:* If the classified behavior surpasses a predefined threshold for suspicion, the system can trigger an alert. This alert might be sent to security personnel or initiate further automated actions like zooming in on the suspicious area or initiating recording at a higher resolution. The specific response will depend on the system's configuration and the nature of the suspicious activity detected.

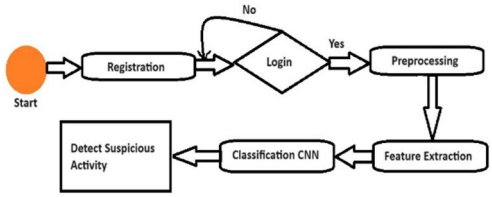


Fig.1.System Overview

IV. RESULT ANALYSIS

Evaluating the effectiveness of a deep learning approach for suspicious activity detection in video surveillance goes beyond simply looking at the video output. Researchers rely on a combination of metrics and analysis techniques to assess the system's performance.

Fig.2.GUI

One crucial aspect is accuracy. Metrics like True Positives (correctly identified suspicious activities) and False Positives (normal activities flagged as suspicious) help gauge the system's ability to differentiate between normal and suspicious behaviors. A confusion matrix provides a visual representation of these results, highlighting areas where the model might be struggling. This allows researchers to pinpoint weaknesses and make adjustments, such as refining the CNN architecture or gathering more training data for specific types of suspicious activities.

Fig.3.Registration Form

Another key consideration is the balance between precision and recall. Precision, measured as the proportion of genuine suspicious activities among all alerts, ensures the system doesn't overwhelm security personnel with unnecessary notifications. Recall, on the other hand, reflects how well the system catches actual suspicious events.

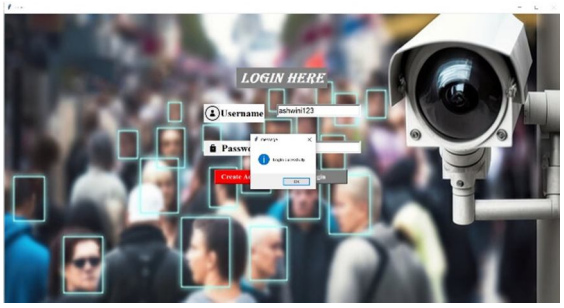


Fig.4.Login Page

To bridge the gap between detection and response, email alerts can be integrated into the system. These emails are triggered when the probability of suspicious activity exceeds a predefined threshold. This threshold is carefully chosen to minimize false alarms while ensuring timely notification of potential threats. Emails typically include details like timestamps, video snippets from the suspicious event, and the specific location within the frame. This information equips security personnel with the necessary context to quickly assess the situation and take appropriate action.

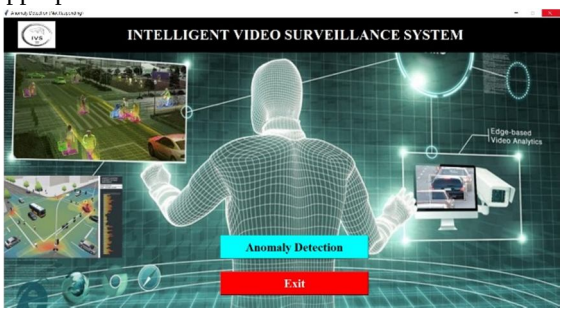


Fig.5.Upload Video

The deep learning approach doesn't stop at initial deployment. By analyzing the results after the system is live, researchers can further refine the model. Techniques like data augmentation, where variations of existing training data are artificially generated, can improve the model's ability to handle diverse scenarios and reduce false alarms. Through continuous analysis and improvement, the deep learning approach can become a powerful tool for enhancing security and safety in video surveillance systems, with email alerts acting as a critical bridge between detection and real-world response.

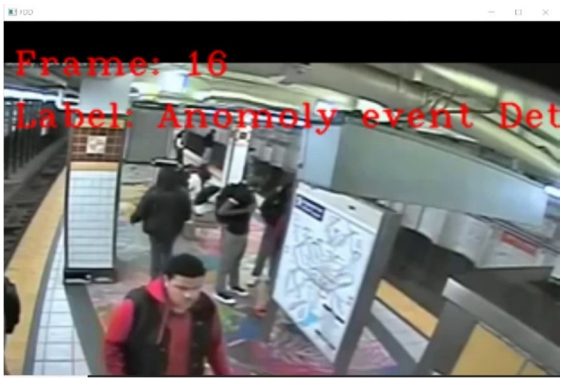
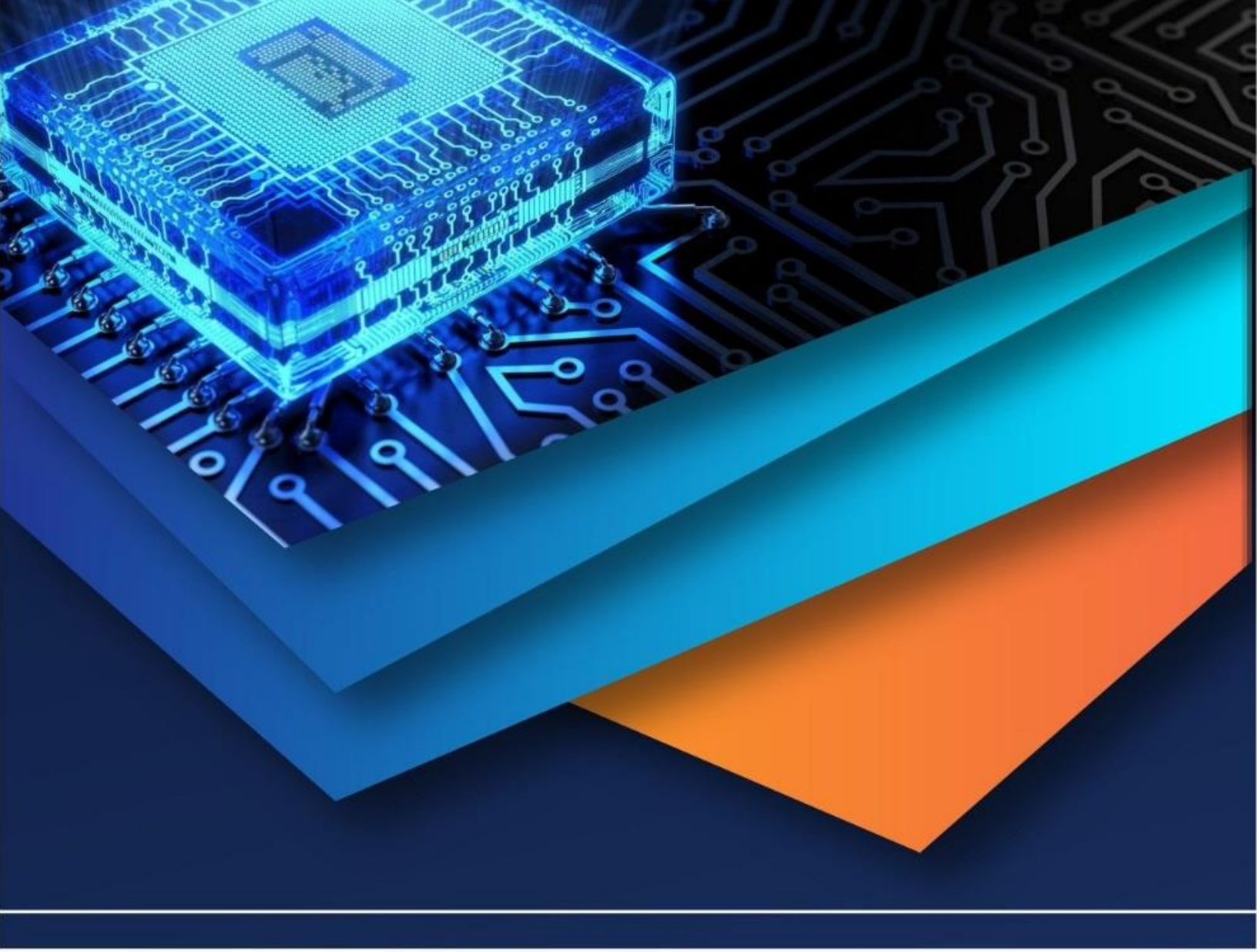


Fig.6.Detect Suspicious Activity

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] Asma Al Ibrahim, Gibrael Abosamra, Mohamed Dahab "Real-Time Anomalous Behavior Detection of Students in Examination Rooms Using Neural Networks and Gaussian Distribution", International Journal of Scientific and Engineering Research, October 2018.
[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,vol152,January-2018.
[6] Elizabeth Scaria, Aby Abahai T and Elizabeth Isaac, "Suspicious Activity Detection in Surveillance Video using DiscriminativeDeep Belief Netwok", International Journal of Control Theory and Applications Volume 10, Number 29 -2017.
[7] Dinesh Jackson Samuel R,Fenil E, Gunasekaran Manogaran, Vivekananda G.N, Thanjaivadivel T , Jeeva S , Ahilan A, "Real time violence detection framework for football stadium comprising of big data analysis and deep learning through bidirectionalLSTM",The International Journal of Computer anD Telecommunications Networking,2019.
[8] Kwang-Eun Ko, Kwee-Bo Sim"Deep convolutional framework for abnormal behaviour detection in a smart surveillancesystem."Engineering Applications of Artificial Intelligence ,67 (2018).
[9] Yuke Li "A Deep Spatiotemporal Perspective for Understanding Crowd Behavior", IEEE Transactions on multimedia, Vol. 20,NO. 12, December 2018.
[10] Labelimg. (2015) Tpzutalin Accessed: jul 10, 2020. [online].
[11] J.jing,D Zhuo,H Zhang,Y.Liang and M.Zheng "Fabric defect detection using the improved YOLOv3 model",2020 journal of engineered fibers and fabrics, vol 15.
[12] J. Redmon and A. Farhadi "YOLOv3: An Incremental Improvement,"Arxiv.org 2018.
[13] U.M.Kamthe,C.G.Patil "Suspicious Activity Recognition in Video Surveillance System", Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018.
[14] Javier Abellan-Abenza, Alberto Garcia-Garcia, Sergiu Oprea, David Ivorra-Piqueres, Jose Garcia-Rodriguez "Classifying Behaviours in Videos with Recurrent Neural Networks", International Journal of Computer Vision and ImageProcessing,December 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY