As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 9(07): 07-11, 2023

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0907002
Available online at: http://www.ijmtst.com/vol9issue07.html

An Effective Suspicious Activity Detection Model on CCTV Camera Footage using Machine Learning

[1]Dr.D.Suneetha, [2]N.Swarna Latha

[1]Professor & HOD, Department of CSE, NRI Institute of Technology, Agiripalli, Andhra Pradesh
[2] M.Tech Student, Department of CSE,

To Cite this Article
Dr.D.Suneetha and N.Swarna Latha. An Effective Suspicious Activity Detection Model on CCTV Camera Footage using Machine Learning. International Journal for Modern Trends in Science and Technology 2023, 9(07), pp. 07-11. https://doi.org/10.46501/IJMTST0907002

Article Info
Received: 28 May 2023; Accepted: 23 June 2023; Published: 27 June 2023.

ABSTRACT

Now a days we have seen a dramatic increase in criminal activity, making security measures a top priority. A key concern of any society today is providing safety to an individual. The main reason behind this concern is due to the constantly increasing activities causing threats, starting from deliberate ferocity to an injury caused through an accident. Simple installation of a traditional closed circuit television(CCTV) is not sufficient as it requires a person to continuously stay alert and monitor the cameras, which is quite inefficient. This call for the requirement to develop an security system which is fully automated system that recognizes anomalous activities in real time and brings instant help to the victims. Hence we proposed a system which will examine and detect the suspicious human action from real-time CCTV footage with help of machine learning techniques. This necessitates the automation of similar processes. Also, it's important to highlight the exact frame and region of interest that house the anomalous behavior, so that a more informed conclusion may be reached about whether or not it's abnormality. To do this, we first divide the video into individual frames and then examine the contents of those frames to determine what people are doing. Wide acceptance is made possible with the use of machine learning and deep learning algorithms and methodologies.

KEY WORDS: Video Surveillance, Anomaly detection, Machine learning, Convolutional neural networks, Image processing

1. INTRODUCTION

The human face and human behavioral patterns are both crucial components in the identification process of individuals. The identification process relies heavily on information of a visual kind. Such visual information may be obtained through surveillance recordings, which can either be watched as live films or played back for use as a reference at a later time. Even the relatively new phenomenon known as "automation" is having an effect on the area of video analytics. Video analytics have a broad range of potential applications, including the detection of motion, the prediction of human activity, the recognition of deviant behavior, the identification of individuals and vehicles, the counting of people in congested areas, and other similar tasks. Face recognition and gait recognition are the technical terms for the two aspects of a person's identity that are used in this particular field for the purpose of identifying that individual. In comparison to these two methods, face recognition is the more flexible option for carrying out automatic person identification using surveillance recordings. The recognition of a person's face may be used to make predictions about the position of a person's head, which can then be used to make predictions about the behavior of a person. The combination of motion recognition and facial recognition is very beneficial in a wide variety of applications, including the verification of a person, the identification of a person, and the detection of the presence or absence of a person at a certain location and time. In addition, human interactions such as subtle touch between two people, head motion detection, hand gesture identification, and estimate are used in the development of a system that is able to properly discover and recognize suspicious behavior among pupils in an examination hall. The purpose of this study is to provide an approach for the identification of suspicious human activities using facial recognition. The primary applications for video processing are surveillance and scientific investigation. A gadget like this one monitors live videos with the help of clever algorithms. When developing a real-time system, some of the most important considerations include computational complexity as well as temporal complexities. The system that employs an algorithm that has a relatively lower time complexity, uses less hardware resources, and produces good results will be more useful for time-critical applications such as the detection of bank robberies, the monitoring of patients, the detection and reporting of suspicious activities at train stations, and other similar applications. It is standard practice in every region of the globe to do both manual monitoring of examination rooms by means of invigilators and manual monitoring of examination rooms using surveillance footage. The monitoring of an examination room is a particularly difficult undertaking in terms of the amount of man power required. During human supervision, the manual monitoring of examination rooms presents the possibility of human mistake. Not only would the implementation of such a system as a "automated suspicious activity detection system" assist in the identification of suspicious actions, but it will also assist in the reduction of the frequency of such activities. In addition, the likelihood of making a mistake will be drastically reduced. This method will be helpful for educational institutions in serving as a monitoring mechanism for such institutions. This article provides a description of a system in which real-time videos are analyzed and utilized for human activity analysis in an examination hall. This helps to identify whether or not the behaviour of a specific individual is suspicious. The system that was built can detect unusual head movements, which eliminates the possibility of copying. Additionally, it indicates a student who has moved out of his place or who has switched places with another student. Finally, the system is able to identify interaction between pupils, which stops students from exchanging potentially damning information with one another. In the course of our study, we have made a contribution toward the development of a system that is capable of intelligently processing live footage of examination rooms including students and classifying the behaviors of those students as either suspicious or not suspicious. An intelligent algorithm is proposed as a result of this research. This algorithm has the capability to monitor and analyze the activities of students within an examination room. Additionally, this algorithm has the capability to alert the administration of an educational institute on account of any malpractices or suspicious activities. During the course of an examination, the goal of the Suspicious Human Activity Detection system is to detect the pupils who engage in unethical actions or activities that raise questions about their motives. The technology can automatically identify potentially malicious behavior and sends a warning to the administrator.

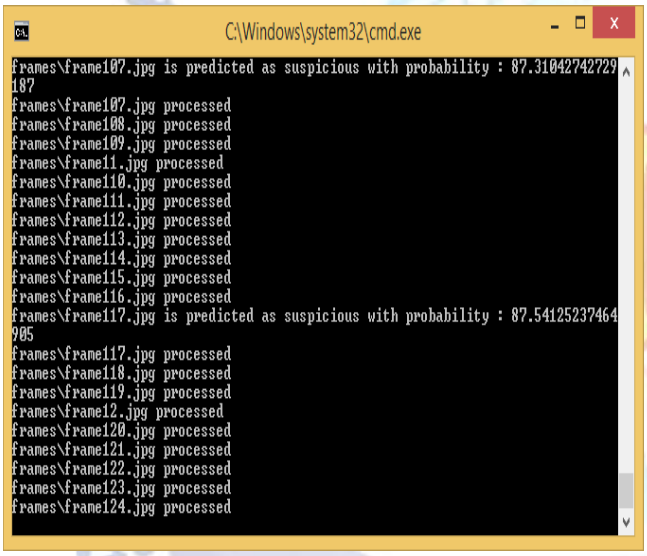
2. LITERATURE SURVEY

According to [1], sparse coding has developed anomaly detection that has demonstrated superior performance. The theories that are included in this construction are feature learning, sparse representation, and dictionary learning. In this research study, a novel neural network called AnomalyNet is developed for the purpose of detecting anomalies. This network achieves feature learning, sparse representation, and dictionary learning all inside three joint neural processing blocks. To be more specific, the authors build a motion fusion block together with a feature transfer block in order to learn enhanced features. This allows them to enjoy the advantages of removing background noise, capturing motion, and enhancing data insufficiency all at the same time. As stated in [2], [2] A suspicious activity is any observable behavior that may indicate a person is participating in a crime or is going to conduct a given criminality. Suspicious activities may be seen in a variety of contexts. The practice of identifying potentially suspicious behavior is known as anomaly detection. When it comes to the problem of maintaining safety in a variety of settings, surveillance cameras are among the most effective solutions. Because it is so difficult to detect illegal activities and deviant behavior, the modern system requires a significant amount of manpower dedicated to its surveillance. Consequently, the purpose of this study is to conduct a survey on anomaly detection for the purpose of video surveillance employing a variety of various ideas, such as deep learning and RNN. Then The difficulty in automating the identification of anomalous activities within large video series, as discussed in research article [3], is related to the lack of clarity around the definition of such occurrences. The authors approach the issue by developing generative models that can find abnormalities in films while only receiving little supervision. Convolutional Long Short-Term Memory (Conv-LSTM) networks are projected to be end-to-end trainable complex networks that are able to forecast the evolution of a video sequence from a tiny number of input frames. According to the research [4], the authors were motivated by the potential of sparse coding based suspicious detection. As a result, they projected a Temporally-coherent Sparse Coding (TSC), in which they implemented identical surrounding frames to be encoded with same reconstruction coefficients. After that, we mapped the TSC using a unique configuration of stacked recurrent neural networks (sRNN). The following are some of the advances that the work makes: I it proposes a TSC that is capable of being recorded to a sRNN, which makes it easier to optimize the parameters and speeds up the uncertain prediction. ii) Create a very big dataset that is even greater than the total of all the other datasets that are currently available in order to search for unusual behavior. A method that is useful for detecting abnormalities in movies was detailed in a research article published by Springer [5]. Recent applications of convolutional neural networks have highlighted the capabilities of convolutional layers for object identification and recognition, particularly in the context of photographs. Convolutional neural networks, on the other hand, are supervised, meaning they need labels as a kind of learning signal. A spatiotemporal architecture for the identification of suspicious activity in movies including crowded settings has been presented by the authors as well as others. The end-to-end trainable complex Convolutional Long Short-Term Memory (Conv-LSTM) networks were suggested in the publication [6]. [Citation needed] These Conv-LSTM networks are able to anticipate the progression of a video sequence based on a very small number of the frames that were used as input. The reconstruction errors of a collection of estimates are used to create consistency ratings, with irregular video sequences generating lower regularity scores as they distance more and further from the real sequence over time. The models make use of a composite structure and investigate the unique implications that conditioning has on the process of learning representations with more significance. According to [7], the solution to this challenge may be found by first developing a generative model for consistent motion patterns. This model should make use of many resources and should have very little supervision. In particular, the study presents two approaches that are based on autoencoders because of their capability to function with a little amount of or even no supervision at all. The first strategy is to investigate the fully linked autoencoder after first using the usual handmade spatio-temporal local features. The second step is to build an end-to-end learning structure that consists of a fully convolutional feed-forward autoencoder. This will allow the local features and the classifiers to be learned concurrently. The model that has been suggested is capable of capturing the regularities that are present in a variety of datasets. The authors of the work [8] have presented a method for the identification and localisation of anomalies in real time that take place in crowded settings. Each movie is properly defined as a collection of distinct cubic places that do not overlap with one another, and its meaning is articulated via the use of both local and global descriptors. The video assets from various stages are captured here by the descriptions that are being utilized. We are able to differentiate normal occurrences from abnormalities in movies by incorporating simple Gaussian classifiers that are efficient in terms of cost. Then the primary focus of the research study referred to as [9] is on the intrinsic redundancy of video structures. The authors provide an efficient framework for sparse combination learning. It achieves respectable performance in the detection phase without sacrificing the quality of the results in any way. The novel approach reduces the complexity of the initial difficult issue so that it may be solved using fewer, less expensive stages of small-scale least square optimization. As a result, the low running time is guaranteed to be error-free. When calculating on a typical desktop PC with MATLAB, the method achieves good detection rates on benchmark datasets.

3.PROPOSED SYSTEM

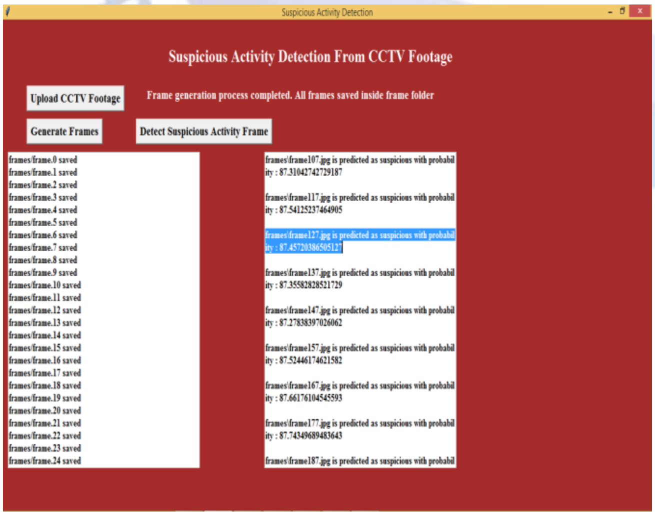
In our proposed system, for detecting anomalous behavior, the CNN i.e. convolution neural network have been used. For effective classification of anomalous activities, it is essential to recognize the temporal data in the video. Recently, CNN is mostly used for extracting key features from each frame of the video. CNN is only the algorithm best suited for this purpose. For classifying the given input successfully it is necessary that the features get extracted from CNN, therefore CNN should be capable of knowing and extracting the needed features from the frame of videos.

4. RESULTS



```
frames\frame107.jpg is predicted as suspicious with probability : 87.31042742729
187
frames\frame107.jpg processed
frames\frame108.jpg processed
frames\frame109.jpg processed
frames\frame11.jpg processed
frames\frame110.jpg processed
frames\frame111.jpg processed
frames\frame112.jpg processed
frames\frame113.jpg processed
frames\frame114.jpg processed
frames\frame115.jpg processed
frames\frame116.jpg processed
frames\frame117.jpg is predicted as suspicious with probability : 87.54125237464
905
frames\frame117.jpg processed
frames\frame118.jpg processed
frames\frame119.jpg processed
frames\frame12.jpg processed
frames\frame120.jpg processed
frames\frame121.jpg processed
frames\frame122.jpg processed
frames\frame123.jpg processed
frames\frame124.jpg processed
```

Figure 1: Activity Detection


Suspicious Activity Detection
Suspicious Activity Detection From CCTV Footage
Upload CCTV Footage
Generate Frames
Detect Suspicious Activity Frame

Frame generation process completed. All frames saved inside frame folder

```
frames/frame.0 saved
frames/frame.1 saved
frames/frame.2 saved
frames/frame.3 saved
frames/frame.4 saved
frames/frame.5 saved
frames/frame.6 saved
frames/frame.7 saved
frames/frame.8 saved
frames/frame.9 saved
frames/frame.10 saved
frames/frame.11 saved
frames/frame.12 saved
frames/frame.13 saved
frames/frame.14 saved
frames/frame.15 saved
frames/frame.16 saved
frames/frame.17 saved
frames/frame.18 saved
frames/frame.19 saved
frames/frame.20 saved
frames/frame.21 saved
frames/frame.22 saved
frames/frame.23 saved
frames/frame.24 saved
```

```
frames\frame107.jpg is predicted as suspicious with probabil
ity : 87.31042742729187

frames\frame117.jpg is predicted as suspicious with probabil
ity : 87.54125237464905

frames\frame127.jpg is predicted as suspicious with probabil
ity : 87.45720386505127

frames\frame137.jpg is predicted as suspicious with probabil
ity : 87.35582828521729

frames\frame147.jpg is predicted as suspicious with probabil
ity : 87.27838397026062

frames\frame157.jpg is predicted as suspicious with probabil
ity : 87.52446174621582

frames\frame167.jpg is predicted as suspicious with probabil
ity : 87.66176104545593

frames\frame177.jpg is predicted as suspicious with probabil
ity : 87.74349689483643

frames\frame187.jpg is predicted as suspicious with probabil
```

Figure 2: Suspicious Activity Detection from CCTV Footage

4. CONCLUSIONS:

The research suggests employing a convolutional neural network for feature extraction and a discriminative deep belief network for action classification to detect suspicious behavior from surveillance video. By using a deep-learning-based model, the suggested approach achieves better categorization than earlier efforts. To begin, we divided video into frame segments and used CNN to extract features from the background and foreground. The output is then input into a trained one, which classifies the recognized behaviors as normal or suspicious.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

References

[1] Joey Tianyi Zhou, Jiawei Du, Hongyuan Zhu, Xi Peng, Rick Siow Mong Goh," Anomaly Net: An Anomaly Detection Network for Video Surveillance, 2019.

[2] Monika D. Rokade and Tejashri S. Bora, "Survey on Anomaly Detection for Video Surveillance" 2021 International Research Journal of Engineering and Technology (IRJET). Technique Dataset Accuracy Joey T. Z. UFC Crime Dataset 76% Proposed System UFC Crime Dataset (Two classes anomalous and non-anomalous) 85% Vol-7 Issue-3 2021 IJARIIE-ISSN(O)-2395-4396 14261 www.ijariie.com 694

[3] Jefferson Ryan Medel, Andreas Savakis, "Anomaly Detection in Video Using Predictive Convolutional Long Short-Term Memory Networks" under review.

[4] W. Luo, W. Liu, and S. Gao, "A revisit of sparse coding-based anomaly detection in stacked rnn framework," in The IEEE International Conference on Computer Vision (ICCV), Oct 2017

[5] Y. S. Chong and Y. H. Tay, "Abnormal event detection in videos using spatiotemporal autoencoder," in International Symposium on Neural Networks. Springer, 2017, pp. 189–196.

[6] J. R. Medel and A. Savakis, "Anomaly detection in video using predictive convolutional long short-term memory networks," arXiv preprint arXiv:1612.00390, 2016.

[7] M. Hasan, J. Choi, J. Neumann, A. K. Roy-Chowdhury, and L. S. Davis, "Learning temporal regularity in video sequences," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 733–742.

[8] M. Sabokrou, M. Fathy, M. Hoseini, and R. Klette, "Real-time anomaly detection and localization in crowded

scenes," in The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, June 2015.

[9] C. Lu, J. Shi, and J. Jia, "Abnormal event detection at 150 fps in matlab," in Proceedings of the IEEE international conference on computer vision, 2013, pp. 2720–2727.

[10] H. Mousavi, M. Nabi, H. K. Galoogahi, A. Perina, and V. Murino, "Abnormality detection with improved histogram of oriented tracklets," in International Conference on Image Analysis and Processing. Springer, 2015, pp. 722–732.

[11] Monika D.Rokade, Dr. Yogesh Kumar Sharma, "MLIDS: A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset", International Conference on Emerging Smart Computing and Informatics (ESCI), IEEE 2021.

[12] Monika D.Rokade, Dr. Yogesh Kumar Sharma, "Identification of Malicious Activity for Network Packet using Deep Learning ", in 2020.

[13] Monika D.Rokade, Dr. Yogesh Kumar Sharma, "Deep and Machine Learning Approaches for Anomaly-Based Intrusion Detection of Imbalanced Network Traffic", IOSR Journal of Engineering, 2019.

[14] Y. K Sharma, S Khatal Sunil, " Health Care Patient Monitoring using IoT and Machine Learning", IOSR Journal of Engineering, 2019.

[15] S Khatal Sunil, Y. K Sharma, "Analyzing the role of heart disease prediction system using IOT and machine learning", International Journal of Advanced Science and Technology, 2020.