TEST Engineering & Management

May-June 2020
ISSN: 0193-4120 Page No. 5134-5138

Security Surveillance Video using CNN With SMS Alert

[1]Anirudha A Nayak, [2]Ambika B J, [3]A Rajesh Reddy, [3]Kushal P, [5]Jagadesh K
[2]Assistant Professor
[1,2,3,4,5]Department of Computer Science(C&IT), REVA University, Bangalore, India
[1]anirudhnayak007@gmail.com, [2]ambikabj@reva.edu.in
[3]rajeshreddyandhra185@gmail.com, [4]kushalrajup@gmail.com, [5]jagadesh.bharath@gmail.com

Article Info
Volume 83
Page Number: 5134-5138
Publication Issue:
May-June 2020

Article History
Article Received:*19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *16 May 2020*

Abstract
In recent times cameras have been mounted in many different locations for security and surveillance purposes. The inspection of the data that is captured using the surveillance system can play an vital role in predicting an incident in particular situations, to monitor online for security reasons and also for an objective driven evaluation of applications such as anomaly and intrusion detection. Presently many AI (Artificial Intelligence) based techniques are been used to detect anomalous activities among which Convolutional Neural Networks (CNN or ConvNets) using deep learning techniques has improved the precision significantly. The main aim of this project is to recommend a new model based on CNN a class of deep neural networks to detect anomaly in the video captured by surveillance cameras. This method has been trained and evaluated using the UCSD dataset and has showed an increase in the accuracy of the anomaly detection model.

Keywords: *CNN, deep learning, anomaly detection, surveillance cameras, SMS alert.*

1. Introduction

Detection and classification of anomaly based on supervised or unsupervised deep neural networks such as CNN [5] is stillan undeveloped deliberation in the field of Deep learning and Artificial Intelligence. The word Anomaly means something that deviates from what is standard or normal occurrence of events or behavioral pattern which are irregular, unusual, unpredictable and unexpected and thus unlike any current samples or patterns [1,5].The detection of anomalies or irregularities in any situation is completely dependent on the environment, context and the scenario[3,4]. The design of the anomaly detection system is divided into three keys parts: the training and testing model component and the data preprocessing component. The model's role is to interface with Tensor Flow, a popular machine learning, open source AIlibrary, as well as manage a number of trained models. The preprocessing component's role is to interact with the file system, storing and organizing the videos in a dataset. The Anomaly Detection class uses both components in order to train, test, and run the anomaly detection model. The process to detect an anomalous activity or any irregularities is completely reliant on the environment, the context or the situation and the scenario and it will vary depending on the various situations. Current deep learning methods for anomaly detection such as simple CNN based methods require labels which are difficult to attain because the data is of high dimension as well as volume [8].High dimension of data affects representation and creation of a model. In this paper, detection of anomaly is based on videos that is the data obtained through the use of security cameras. The intricacy increases if the procedure is online. Using deep learning is one the best methodology. The benefits of these sorts of procedures, which typically have dimensional information or data, can be traced back to the existence of an end-to-end system. End-to-end systems deliver a complete functional solution which in turn automates extraction of features from the video [7]. The detection of irregularities or anomalies in videos is more difficult than in any other form of data since it involves

Published by: The Mattingley Publishing Co., Inc.

May-June 2020
ISSN: 0193-4120 Page No. 5134-5138

detection methods and also requires video pre-processing as well and the problems that arise are-

- Depending upon the environment and different situations the anomalies that occur are different
- The handling of the data produced by the surveillance cameras poses serious challenges and difficulties such as speed of the data produced, volume and variety of data etc.
- To make use of deep learning technique in all the phases
- The anomalies that are perceived are completely reliant on the context, situation, scenario and the background environment
- Automatic controlling and monitoring of the System

Surveillance or Reconnaissance cameras have become a part of our society and daily life. As we see them in nearly every in every houses buildings, Restaurants or any public spaces such as streets, parking, parks etc. However, hiring people to monitor all the surveillance video is time consuming as well as expensive. The main objective of our project is to implement an algorithm that will detect irregular activity such as robbery, accident, etc. and alert the concerned authorities. The scope of this project is to create a system that will detect anomalous events in images and videos consuming deep learning. In the subsequent release, we will design a classification method to classify the event, after that, we will design an alert system to alert the corresponding person about anomalous event.

2. Literature Survey

Because of the presence of rich and analytical information in videos and the ease of accessing such data, scientific researchers have been captivated in the examination and handling of these types of data. Identification and detection of objects such as animals, tools etc. in video frames is one of the major challenges in analysis of video data [9]. Additionally, detection of anomalies in videos has been one of the debated research topics within the recent times. In the last couple of years, deep learning methodologies have been adapted for implementing video based anomaly detection method. In all the current anomaly detection approaches, learning is attained exclusively through regular data. Another significant point with respect to the irregularities is that strange occurrences are typically uncommon and rare that occurs relatively less than normal events [2].

The difficulties for distinguishing abnormalities in videos include speed and volume of the data produced, online alerts, and localization of the abnormality. It ought to be mentioned that localization of anomaly is very decisive and most of the existing models and data lack it. To increase the accuracy of the process in some methods the localization is done in the preprocessing step which is usually based on comparison of video frames [10, 11]. Currently most of the present methodologies and their accessible datasets only specify the occurrences of anomaly and not their location [12]. The current methods also lack appropriate training of data and the correct description of the anomalies along with their high cost of extracting features which directly affect detection process [6]. One of the extensively utilized strategies for detecting anomalies is the use of a binary classifier which contains two classes i.e. normal and abnormal. The normal class contains data whose frequency of occurrence is high, while the other abnormal class contains infrequent and unnoticed events in compliance with the data pattern [2].

As in any other machine learning based methods, deep learning based anomaly detection techniques can also be categorized into three categories of supervised learning, semi-supervised learning and unsupervised learning. Supervised anomaly detection needs labeled data which is difficult because of the volume and dimension of data. In a supervised learning approach, the main operation is decision rule based or model based which can distinguish between two classes [13]. And also unsupervised methods need complex computing as there no labeled data provided to the model [2]. Unsupervised methods are also known as data driven anomaly detection [13].

Objectives

- The main intention of our project to detect the irregular activities which occurs in the videos.
- The model will analyze the data and detect the threatening object.
- Automatic notification will be sent to the control station about detection of abnormal event.
- Challenges that are faced in uncovering anomalies in videos are (i) speed of detection, (ii)localization of the anomaly and (iii)online alerts to concerned party

3. Methodology

The subsequent modules given show the work flow of our project and speak of some the significant sections in our project.

Data Collection: This module represents the collection of datasets to train and test our project. We use the UCSD (University of California and San Diego) dataset to help train and test our model. The UCSD dataset in of the well-known crime detection.

Data Preprocessing: In this module there are 4 steps

- Converting the video into images /frames.
- Resizing the frame i.e. to change the width & height of the image without changing the amount of data in it.
- The next step is Feature Extraction, We use C3D [14,15,16] by Facebook AI Research and Visual Learning Group
- C3D is an upgraded version of BVLC caffe to support 3D convolution and pooling. The main features include:

a) Training or fine-tuning 3D convolutional nets.

Published by: The Mattingley Publishing Co., Inc.

May-June 2020
ISSN: 0193-4120 Page No. 5134-5138

b) Extracting video features with pre trained C3D models.

The C3D model can recognize many features such as human, fire etc. Each feature is represented as a feature vector with real numbers.

In a frames with anomalies in it are assigned a score 1 and frames without anomalies are assigned a score 0. We use the Numpy library in python to handle the large multidimensional array generated due to the feature vector and the assigned score.

Training: We train the model by using CNN (Convolutional Neural Network).

- CNNs use image acknowledgment and characterization so as to identify objects, perceive faces, and so forth. They are comprised of neurons with learnable loads and inclinations. CNNs are principally used to characterize pictures, group them by likenesses, and afterward perform object acknowledgment.
- CNN has an imbibed feature known as max pooling which helps in reducing the dimensionality and preserve the main feature which helps in reducing over fitting which occurs when too much irrelevant information is given in an image.

Testing: In this module a video with or without an anomaly is taken to evaluate the accuracy.

- Firstly, the video is converted into frames and resized.
- We check for anomalies in the video frames by grouping 16 frames at a time if the score generated is higher than the threshold value set by us (0.5 in our case) then the program will reconstruct the video where anomaly is present.
- Now, to send the alert to owner and the concerned authorities in charge we use SMS GATEWAY CLOUD which will alert them to take prompt action in the situation.

Validation: We separate our data set in to two parts: The separated datasets for both the parts i.e. training and testing contain anomalous activities at different locations in the videos at different time intervals. Moreover some of the videos have multiple anomalies. The testing part of the video is compare to the trained part to estimate the accuracy of the model. The assessment of the model by using the ROC (Receiver operating characteristics) curve.

Application

This system can be used in

1. Can be used in jewelry shops, Colleges, ATM, Restaurant's, Banks or any public places to maintain Law and Order.
2. To monitor home, streets, private properties for security purposes.

The following flow chart depicts the important modules and their work flow

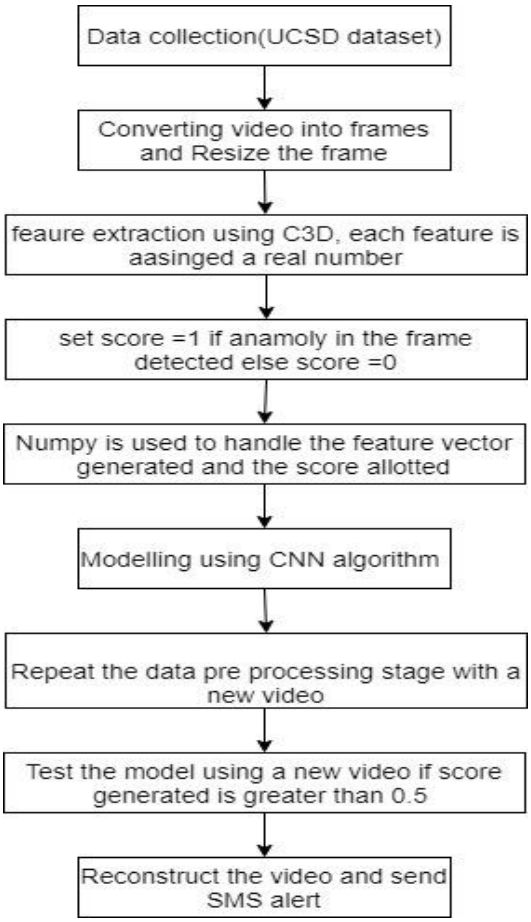

Figure 1: Workflow Diagram

4. Evaluation Results

The following graph shows us that our proposed method has an Accuracy of 96% in training.

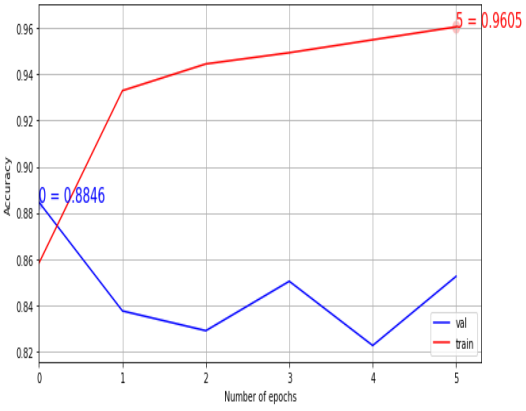

Figure 2: Training accuracy

The following graph shows us that our proposed model has an average Accuracy of 83% in testing.

May-June 2020
ISSN: 0193-4120 Page No. 5134-5138

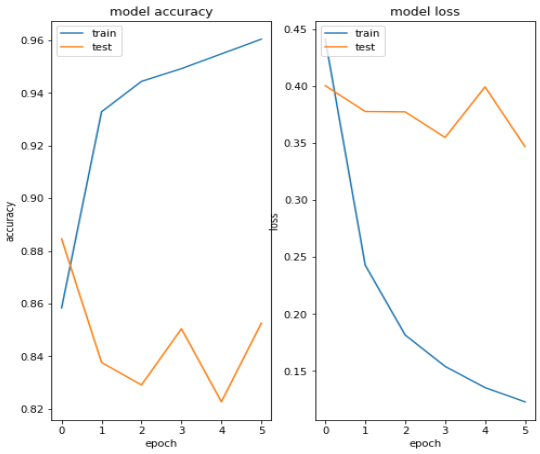

Figure 3 & 4: Model accuracy and Model loss

Model loss is nothing but an indication of how bad the prediction was on a single example.
Epoch is the number of times the model has been trained by the full dataset. We use the **ROC curve** which describes the accuracy of a classifier. The following graph shows us the performance of our project.

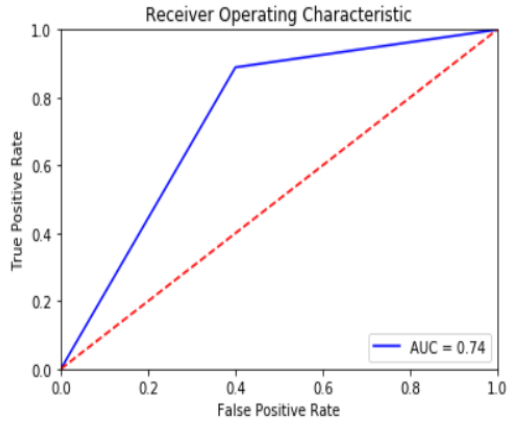

Figure 5: ROC Curve

5. Conclusion &Future Works

The main benefit of using the proposed method is the use of ConvNets (Convolutional Neural Networks) in both the training and testing constituent of the project. The fundamental parts of this strategy are assessed dependent on certain measurements and the use of the UCSD(University of California and san Diego) dataset which is one of the most acknowledged crime detection dataset. The other advantage of this method is the seclusion of the training phase from the testing phase. So that a preprocessing network can be used for future works. For the future development it gives an opportunity to enhance by adding a recognition classifier or we can also try to add an component which will classify the anomaly and with the goal that it can detect an anomaly so that separate specialists, for example, local group of fire-fighters, police, emergency vehicle and so forth can be called dependent on the circumstance.

We are proposing a Convolutional Neural Network (CNN) which is a class of deep learning method to identify real world anomalies such as assault, abuse, arson etc. in surveillance videos. Owing to the intricate nature of the anomalies using only the standard data only is not optimal for anomaly detection. To avoid the provisional annotations of segments which can be very labor intensive in the training videos. We learn a universal model to detect anomalous data using the deep learning framework. To authenticate the future approach, a new important data set consisting of a of real world situations and scenarios introduced. We exhibit the handiness of our dataset for the task of anomalous activity identification.

This research work can be extended to be develop a faster and better responsive system which can detect anomalies in real time in case of any harmful or threatening emergency. This will assist with building better model which can be helpful in detecting the crime and alerting promptly which will help to reduce the anti-social activities in our society. This model will also help in building better models which can process the video stream live and make use of the cloud/Internet and will be able to inform the concerned authorities as soon as possible in real time and also help them to take a prompt and decisive action. This model can be further trained to classify the anomaly based on the situation which will help the authorities take better preventive measures.

References

[1] Dinesh Kumar Saini, Dikshika Ahir and Amit Ganatra, “Techniques and Challenges in Building Intelligent Systems: Anomaly Detection in Camera Surveillance”, Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems, Springer International Publishing Switzerland, 2016

[2] B Ravi Kiran, Dilip Mathew Thomas, Ranjith Parakkal, “An overview of deep learning based methods for unsupervised and semisupervised anomaly detection in videos”, MDPI Journal of Imaging, arXiv:1801.03149v1, 2018

[3] Ryota Hinami, Tao Mei, and Shin’ichi Satoh, “Joint Detection and Recounting of Abnormal Events by Learning Deep Generic Knowledge”, arXiv:1709.09121v1, 2017

[4] M. Ribeiro, A.E.L., and H. S. Lopes, “A study of deep convolutional auto-encoders for anomaly detection in videos”, Pattern Recognition Letters, ELSEVIER, 2017

[5] Ali Khalegi, Mohammed Shahram Moin. “Improved anamoly detection in surveillance based on a deep learning method”, 2018 8th Conference of AI & Robotics.2018

Published by: The Mattingley Publishing Co., Inc.

May-June 2020
ISSN: 0193-4120 Page No. 5134-5138

[6] Hung Vu, "Deep Abnormality Detection in Video Data", Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence, 2017

[7] M. Sabokroua, M.F., M. Fathyc, Z. Moayedd and R. Kletted, "Deep- Anomaly: Fully Convolutional Neural Network for Fast Anomaly Detection in Crowded Scenes", Journal of Computer Vision and Image Understanding, 2017

[8] Qaisar Abbas, Mostafa E. A. Ibrahim, M. Arfan Jaffar1, "Video scene analysis: an overview and challenges on deep learning algorithms", Multimedia Tools and Applications, Springer, 2017

[9] Revathi, A. R., Kumar, Dhananjay "An efficient system for anomaly detection using deep learning classifier", Signal, Image and Video Processing, Springer, 2016

[10] Hung Vu, Tu Dinh Nguyen, Anthony Travers, Svetha Venkatesh And Dinh Phung, "Anthony Travers, Energy-Based Localized Anomaly Detection in Video Surveillance", Springer International Publishing AG, 2017

[11] Siqi Wanga, E.Z., Jianping Yin, "Video anomaly detection and localization by local motion based joint video representation and OCELM", Neurocomputing, 2017

[12] M. Sabokrou, M. Fathy, M. Hoseini., "Video anomaly detection and localisation based on the sparsity and reconstruction error of autoencoder", ELECTRONICS LETTERS, IEEE, 2016.

[13] Yong Shean Chong, Yong Haur Tay, "Modeling Video-based Anomaly Detection using Deep Architectures: Challenges and Possibilities", Control Conference (ASCC), IEEE, 2015

[14] D. Tran, L. Bourdev, R. Fergus, L. Torresani, and M. Paluri, Learning Spatiotemporal Features with 3D Convolutional Networks, ICCV 2015, PDF.

[15] Y. Jia, E. Shelhamer, J. Donahue, S. Karayev, J. Long, R. Girshick, S. Guadarrama, and T. Darrell, Caffe: Convolutional Architecture for Fast Feature Embedding, arXiv 2014.

[16] A. Karpathy, G. Toderici, S. Shetty, T. Leung, R. Sukthankar, and L. Fei-Fei, Large-scale Video Classification with Convolutional Neural Networks, CVPR 2014.