"Deep Learning Approach for Suspicious Activity Detection from Surveillance Video"

Mr. M. R. Kharde, Miss. Shraddha Jadhav, Miss. Pratiksha Jagdhane, Miss. Sara Kadam, Miss.Jayshri Gaikwad
Deparatment. of Computer Engineering, Pravara Rural Engineering College Loni, Maharashtra

Abstract

Suspicious Activity is predicting the body part or joint locations of a person from an image or a video. Human suspicious activity is one of the key problems in computer vision that has been studied for more than 15 years. It is important because of the sheer number of applications which can benefit from activity detection. For example, human pose estimation is used in applications including video surveillance, animal tracking and behavior understanding, sign language detection, advanced human-computer interaction, and marker less motion capturing. Low cost depth sensors have limitations like limited to indoor use, and their low resolution and noisy depth information make it difficult to estimate human poses from depth images. Hence, we plan to use neural networks to overcome these problems. Suspicious human activity recognition from surveillance video is an active research area of image processing and computer vision. Through the visual surveillance, human activities can be monitored in sensitive and public areas such as bus stations, railway stations, airports, banks, shopping malls, school and colleges, parking lots, roads, etc. to prevent terrorism, theft, accidents and illegal parking, vandalism, fighting, chain snatching, crime and other suspicious activities.

Keywords— *neural networks, image processing, suspicious activities, theft*

INTRODUCTION

We plan to build an application for detection of suspicious activity of people in public places in real time. Our application can be used in surveillance at places like malls, airports, railway stations, etc. where there is a risk of robbery or a shooting attack.
We will be using deep learning and neural networks to train our system. This model will then be deployed as a mobile and desktop app which will take real time CCTV footage as input and send an alert on the administrator's device if some suspicious pose is found. Human suspicious activity is related to identifying human body parts and possibly tracking their movements. Real life applications of it vary from gaming to AR/VR, to healthcare and gesture recognition. Compared to image data domain, there is relatively little work on applying CNNs to video classification. This is because, a video is more complex than images since it has another dimension temporal. Unsupervised learning exploits temporal dependencies between frames and has proven successful for video analysis. Some suspicious activity approaches use CPU instead of GPU so that suspicious activity can run on low cost hardware like embedded systems and mobile phones. Low cost depth sensors are another new technology in computer vision. They are present in gaming consoles like the Kinect for Xbox 360. They are motion sensors which allow the user to interact with the console without a game controller, through just hand gestures. These are RGB-D sensors that obtain depth information by structured light technology. The structured light sensors infer the depth values by projecting an infrared light pattern onto a scene and analyzing the distortion of the projected light pattern. However, these sensors are limited to indoor use, and their low resolution and noisy depth information make it difficult to estimate human poses from depth images.

MOTIVATION

Human suspicious activity is one of the key problems in computer vision that has been studied for more than 15 years. It is important because of the sheer number of applications which can benefit from suspicious activity. For example, human suspicious activity is used in applications including video. Surveillance, animal tracking and behavior understanding, sign language detection, advanced human computer interaction, and marker less motion capturing. Low cost depth sensors have limitations like limited to indoor use, and their low resolution and noisy depth information make it difficult to estimate human poses from depth images. Hence, we plan to use neural net- works to overcome these problems. Suspicious human activity recognition from surveillance video is an active research area of image processing and computer vision. Through the visual surveillance, human activities can be monitored in sensitive and public areas such as bus stations, railway stations, airports, banks, shopping malls, school and colleges, parking lots, roads, etc. to prevent terrorism, theft, accidents and illegal parking, vandalism, fighting, chain snatching, crime and other suspicious activities. It is very difficult to watch public places continuously, therefore an intelligent video surveillance is required that can monitor the human activities in real-time and categorize them as usual and unusual activities; and can generate an alert. Mostly, of the research being carried out is on images and not videos. Also, none of the papers published tries to use CNNs to detect suspicious activities

LITURATURE SURVEY

Smart surveillance systems in public and private places to logically differentiate between normal and abnormal behavior. This system makes use of the YOLOv3 algorithm for object detection. The COCO dataset, which is a large-scale object detection, segmentation and captioning dataset, has been used for training this model. Depending on the object detected, the algorithm classifies a frame as suspicious or normal. Crowd density has been calculated by detecting the number of people in a frame and suspicion detection has been performed by analyzing. The objective of this project is to equip the user with information regarding a frame by analyzing it from time to time. A real-time analysis also equips the various law enforcing bodies to have more informed insight and makes surveillance smart and efficient. Crime rates have been on a rise in recent times. There are not enough measures in place to actively work on emergency dispatch for combating crime. The objective of this project is to equip the user with information regarding a frame by analysing it from time to time. Such analysis can help in early detection of a rather grave situation and prevent it from happening. [1] The excessive use of Instant Messaging Applications (IMA) and Social Networking Sites (SNS) has tremendously increased the suspicious information sharing activity which in turn is effectively used for evil purposes. These words cannot be detected by an earlier OSMD surveillance tool, resulting in the concealment of suspicious messages. For detecting suspicious messages, the SFC program is proposed for OSMD. Even though many methodologies to detect cyberbullying among which deceptive Phishing in IMs for text-related messages being developed, there remains some inefficiencies in the detection process of suspicious words in the IM & SNS. The criminal minds had indulged in the usage of SNS for sending suspicious messages, criminal activities, and plans. The tracing of such e-criminals becomes extremely difficult for the e-crime department to identify them from SNS, due to the bulk of messages communicated through social networks from one group of users to another group of users. [2] Computer vision is one of the fields which aims in building smart applications that understands the contents of images and videos as the understanding of humans. In this paper, YOLOv3 is used to detect different suspicious activities like bag-snatching, lock breaking etc. The video surveillance is said to be effective when it detects any abnormal/suspicious activities efficiently. Most of the current surveillance systems are human operated. So our main motive is to create an automatic computerized system for human action recognition for suspicious movements that will be robust and can work fast and accurately in every environment. [3] With increasing crime rates it becomes a problem if they are not identified in time and necessary precautionary actions taken. This paper uses a deep neural network model that can detect handguns in images and a machine learning and computer vision pipeline that detects abandoned luggage. Breaking down complicated tasks and detecting sub tasks which lead to potential crimes are one way to simplify an activity to be automated. We focus on two main potential leads to crimes which we attempt to detect through our models. [4] Human behavior recognition in the real-world environment finds plenty of applications including intelligent video surveillance, shopping behavior analysis. This is more generic because the process of feature extraction is fully automated. From the image pixels, convolutional neural network (CNN) can learn visual patterns directly. Currently, the tracking has been performed by human. Since we are dealing with huge amount of video data, this is easy to make people feel tired and the manual intervention will also produce omissions. It greatly affects the efficiency of the system. Analyzing abnormal events from video is an emerging topic in the domain of automated video surveillance systems. [5]

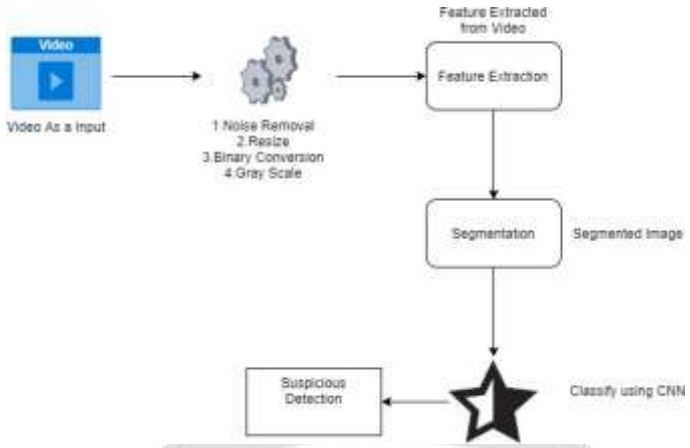
AIM & OBJECTIVES

- Detect the Suspicious Activity.
- Any one can use this application easy.
- A system to process real-time CCTV footage to detect any suspicious activity will help to create better security and less human intervention.
- It is very difficult to watch public places continuously, therefore an intelligent video surveillance is required that can monitor the human activities in real-time and categorize them as usual and unusual activities; and can generate an alert.

SYSTEM ARCHITECTURE

- This system accepts input in the form of video dataset. We know that we're doing data processing and trained dataset on the system, therefore we're employing modules: Preprocessing, Feature extraction, and classification, all of which use our CNN algorithm.
- So First Input as an video dataset, then preprocessed the dataset (pre-processing step is clean the Image and Remove Blur part) After that, then the system extracts the parameters or features of the in the extraction section.

- Then, in classification, where we utilize our CNN algorithm to Suspicious Activity Detection.



APPLICATION

- The success of deep learning methods in various applications consequently caused the rise of such methods in anomaly detection.
- The abnormalities in videos are crucial for applications ranging from automatic quality control to visual surveillance.
- The time-series modeling and has proved its performance in applications such as speech translation and handwriting recognition.
- Detection and recognition are widely used in most of the applications such as security and surveillance, traffic control etc.

SYSTEM REQUIREMENTS

Software Used:

- Spyder

Hardware Used:

- System: Intel I3 Processor and above.
- Hard Disk : 20 GB
- Ram : 8G

MODULES SPLIT UP

The software development cycle is a combination of different phases such as designing, implementing and deploying the project. These different phases of the software development model are described in this section. The SDLC model for the project development can be understood using the following figure. The chosen SDLC model is the waterfall model which is easy to follow and fits bests for the implementation of this project.

- **Requirements Analysis:** At this stage, the business requirements, definitions of usecases are studied and respective documentations are generated.
- **Design:** In this stage, the designs of the data models will be defined and different data preparation and analysis will be carried out.

- **Implementation:** The actual development of the model will be carried out in this stage. Based on the data model designs and requirements from previous stages, appropriate algorithms, mathematical models and design patterns will be used to develop the agent's back-end and front-end components.

- **Testing:** The developed model based on the previous stages will be tested in this stage. Various validation tests will be carried out over the trained model.

- **Deployment:** After the model is validated for its accuracy scores its ready to be deployed or used in simulated scenarios.

- **Maintenance:** During the use of the developed solution various inputs/scenarios will been countered by the model which might affect the models overall accuracy. Or with passing time the model might not fit the new business requirements. Thus, the model must be maintained often to keep its desired state of operation.

CONCLUSION

A system to process real-time CCTV footage to detect any suspicious activity will help to create better security and less human intervention. Great strides have been made in the field of human suspicious Activity, which enables us to better serve the myriad applications that are possible with it. Moreover, research in related fields such as Activity Tracking can greatly enhance its productive utilization in several fields.

REFERENCES

1. Shriya Akella, Priyanka Abhang, Vinit Agrharkar, Dr. Reena Sonkusare Department of Electronics and Telecommunication Sardar Patel Institute of Technology, Mumbai, India shriya.akella@spit.ac.in, priyanka.abhang@spit.ac.in, vinit.agrharkar@spit.ac.in, reena kumbhare@spit.ac.in

2. Mohd. Mahamood Ali Department of CSE MJCET, Osmania University Hyderabad, Telangana, India mahmoodedu@gmail.com Mohd. Abdul Rasheed Department of IT MJCET, Osmania University Hyderabad, Telangana, India marasheed634@gmail.com Md. Khaleel Ahmed Khan Department of CSE M.Tech Student, MJCET Hyderabad, Telangana, India khaleelahmed076@gmail.com

3. Nipunjita Bordoloi1 , Anjan Kumar Talukdar2 , Kandarpa Kumar Sarma3 123Dept. of Electronics and Communication Engineering Gauhati University, Guwahati, Assam, India 1nipunjitabordoloi@gmail.com,2 anjantalukdar@gauhati.ac.in, 3kandarpaks@gauhati.ac.in

4. Sathyajit Loganathan Dept. of Information Technology Sri Lanka Institute of Information Technology Malabe, Sri Lanka sathyajit.loganathan@my.sliit.l Gayashan Kariyawasam Dept. of Information Technology Sri Lanka Institute of Information Technology Malabe, Sri Lanka it16014350@my.sliit.lk Prasanna Sumathipala Dept. of Information Technology Sri Lanka Institute of Information Technology Malabe, Sri Lanka prasanna@sliit.lk

5. Amrutha C.V, C. Jyotsna, Amudha J. Dept. of Computer Science & Engineering, Amrita School of Engineering, Bengaluru, Amrita Vishwa Vidyapeetham, India amruthacvvtk@gmail.com, c_jyotsna@blr.amrita.edu, j_amudha@blr.amrita.edu