Journal of ISMAC (2020)
Vol.02/ No.04
Pages: 216-221
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.4.005

Suspicious Human Activity Detection System

Pankaj Bhambri[1*], Sachin Bagga[2], Dhanuka Priya[3], Harnoor Singh[4], Harleen Kaur Dhiman[5]

[1,2]Assistant Professor, Department of Information Technology, Guru Nanak Dev Engineering College, Ludhiana, Punjab, India.

[3,4,5]Research Scholar, Department of Information Technology, Guru Nanak Dev Engineering College, Ludhiana, Punjab, India.

[*]Email: pkbhambri@gmail.com

Abstract In collaboration with machine learning and artificial intelligence, anomaly detection systems are vastly used in behavioral analysis so that you can help in identity and prediction of prevalence of anomalies. It has applications in enterprise, from intrusion detection to system fitness tracking, and from fraud detection in credit score card transactions to fault detection in running environments. With the growing crime charges and human lack of confidence globally, majority of the countries are adopting precise anomaly detection systems to approach closer to a comfy area. Visualizing the Indian crime index which stands at 42. 38, the adoption of anomaly detection structures is an alarming want of time. Our own cannot be prevented with the aid of CCTV installations. These systems not simplest lead to identification on my own, but their optimized versions can help in prediction of unusual activities as properly.

Keywords: Anomaly Detection, Suspicious Human Activities

1.Introduction

In this project, we developed an application for detecting suspicious human behaviour activities in images, videos and CCTV (Close Circuit TeleVision). As in today's world everybody wants to live in a secure environment and there is a need of techniques that can enhance the safety tiers of humans. So through this task we suggest an automated system using deep learning algorithms to detect suspicious human behaviour. Deep learning is an advanced version of machine learning. Machine learning is classed into two wide categories first is supervised learning (calls for type) and other is unsupervised studying (does no longer require records class). We are using the supervised learning approach and CNN (Convolution Neural Networks) to detect the unusual activities. CNN comprises of two phases. The first one is the train network and the second one is detection classifier. The train network deals with the feature extraction step and the detection classifier takes up the decision of whether there is an anomalous activity or not by taking the final decision. By using this approach, the application is appropriate to detect the unusual human activities and to provide safe and secure environment.

1.1 Project Category

Suspicious Human Activity Detection system falls under the category of PoC (Proof of Concept) and implementation. Proof of concept is a consciousness of a positive technique or concept with a view to reveal its feasibility or a demonstration in precept with the purpose of verifying that some idea or idea has practical potential after which enforcing it.

1.2 Sustainability related to technology used

Sensors, data acquisition systems, communications and processing units require sustainable power for a truly autonomous operation. The sustainable operation of the Intelligent Sensor Network Platform is determined by the interrelation of three components: 1) Maximum energy utilization of the sensor node components, 2) Energy harvesting/generation capability, and 3) Rechargeable power of the battery. If the peak energy usage of the sensor will gradually exhaust the capacitor, the device is known to be inefficient. Intelligent hardware and software protocols are therefore required to achieve energy and service balance in order to enable continuous sensing operations. There are three main components that consume power within the smart sensor nodes: a) RF (Radio Frequency) communication chip; b) smart processing core; and c) analog front end sensor. Smart sensors not only improve signal processing capacities, they also minimize data transmission. This is possible as smart sensors tend to contact either when there is an error or when an investigation request comes from the central server. Sustainability requires not only energy harvesting, but also efficient power management.

ISSN: 2582-1369 (online)
Submitted: 28.09.2020
Accepted: 22.10.2020
Published: 31.10.2020

1.3 Objectives

Major set of objectives are as below:

- To identify suspicious human activities in surveillance videos: Robbery, Fight and fire etc. from images, videos and CCTV by using deep learning algorithms.
- To develop Graphical User Interface or a smart phone friendly application.
- To enhances the security of the society by predicting the unusual scenarios and reduce human efforts.

1.4 Problem Formulation

With the increasing crime rates and human insecurity globally, majority of the nations are adopting precise anomaly detection systems to approach towards a secure space. They are highly used in intrusion detection, fraud detection, fault detection systems, health monitoring, event detections and detecting ecosystem disturbances. Visualizing the Indian Crime Index which stands at 42.38, the adoption of anomaly detection systems is an alarming need of time. Activities like abuse, burglary, explosion, accidents, shooting and stealing etc. alone cannot be prevented by CCTV installations. There is a need of upgrading them into smart and efficient systems by adopting anomaly detection systems. These systems not only lead to identification alone, but their optimized versions can help in prediction of unusual activities as well. This can prove a significant aid to prevent any kind of destruction.

1.5 Identification of Need

To formulate this automated system the approach we followed there was a need to have prior knowledge of Python language and machine learning where we used CNN. Considering the project requirements, there was a need to identify and lists down all the suspicious human activities and work upon the detection of primary activities from them.

2. Detailed Design

Detailed design of the project is elaborated in multiple numbers of steps as described below:

2.1 Data Classification

Datasets of surveillance in video (mp4 format) are gathered and classified on the basis of types of human suspicious activities present in them. We have gathered datasets for violence, robbery and fire. They contain real life scenarios of suspicious activities from different locations.

2.2 Frame Extraction

The videos are divided into frames using python script. The suitable frames which portray the clear and accurate action of suspicion are selected manually to be used. The extracted frames are from multiple videos of different locations, activities, environments and persons. About 250-300 frames are selected per activity.

2.3 Training and Testing Sets

The selected frames are further classified into training dataset and testing dataset by splitting the entire data into a fixed ratio for every activity. For this application, we reserved 70% of the frames for training dataset and rest 30% for the test dataset. No frames in classified training and testing datasets belong to the same video i.e. both datasets are exclusive of each other.

2.4 Labelling

The accuracy of our application highly depends upon how well the data has been labelled. Training and test datasets are labelled using the xml python module. Each frame is labelled by the name of the indicated suspicious human activity by carefully selecting the region of occurrence via square box label. The frames after labelling are saved in the form of.xml files.

2.5 Data Conversion and CNN

In case of image classification, we have used simple CNN model, the input for which were datasets in .jpg format. Using Python Scripts, the .xml files are converted to CSV files and further their files are converted to TF Records format. The tf.data files are fed to the faster RCNN Inception v2 (COCO) Model for video classification.

ISSN: 2582-1369 (online)
Submitted: 28.09.2020
Accepted: 22.10.2020
Published: 31.10.2020

2.6 Training

The model is trained using Graphical Processing Unit (GPU) and data from all the activities is collaborated and trained in one segment. The time consumed by the system to train the model is proportional to the amount of data fed.

2.7 Output

After the accomplishment of training, the application detects the suspicious human activities by indicating colored labelled boxes around the area of occurrence for video input. In case of image inputs, the output is reflected on the GUI with results and percentage.

3. Structured Analysis of Structured Design

The various stages of structured analysis of system design are categorized as below:

3.1 Flowchart

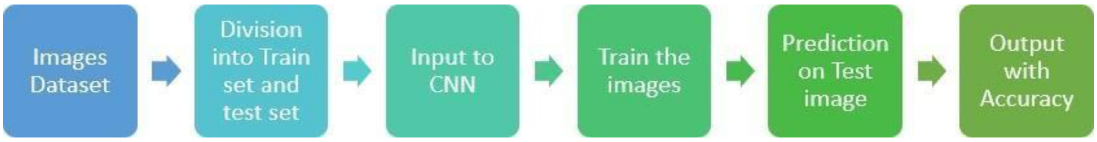


Figure 3.1: Flowchart of Anomaly Detection System for Images

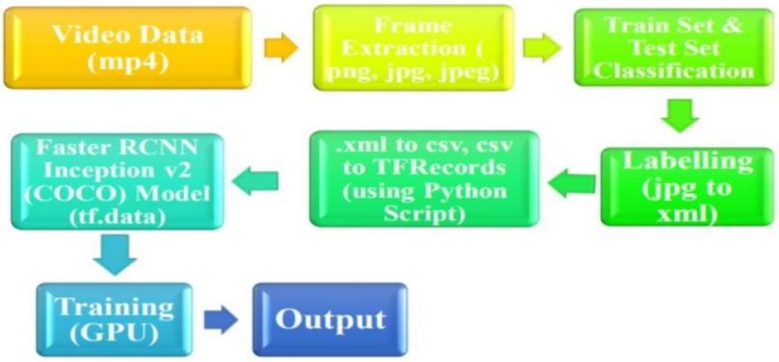

Video Data (mp4)
Frame Extraction (png, jpg, jpeg)
Train Set & Test Set Classification
Labelling (jpg to xml)
.xml to csv, csv to TFRecords (using Python Script)
Faster RCNN Inception v2 (COCO) Model (tf.data)
Training (GPU)
Output

Figure 3.2: Flowchart of Anomaly Detection System for Videos

Figure 3.1 and Figure 3.2 represents a diagram of the sequence of working project. It symbolizes the data transfer and format during various stages of the project formulation.

3.2 Data Flow Diagram

Figure 3.3 represents the detailed flow of data in training and test modules of the project.

4. Image Resizer

Image resizing refers to scaling of images. Scaling comes handy in many image processing as well as machine learning applications. It helps in reducing the number of pixels from an image and that has several advantages e.g. it can reduce the time of training of a neural network as more is the number of pixels in an image more is the number of input nodes that in turn increases the complexity of the model. It also helps in zooming in images. Many times we need to resize the image i.e. either shirk it or scale up to meet the size requirements. OpenCV provides us several interpolation methods for resizing an image.

ISSN: 2582-1369 (online)
Submitted: 28.09.2020
Accepted: 22.10.2020
Published: 31.10.2020

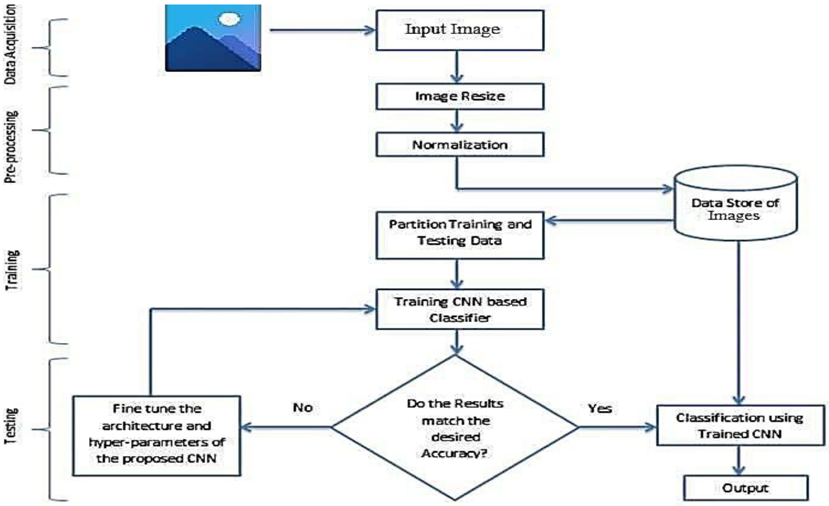

Data Acquisition
Pre-processing
Training
Testing
Input Image
Image Resize
Normalization
Data Store of Images
Partition Training and Testing Data
Training CNN based Classifier
Do the Results match the desired Accuracy?
No
Yes
Fine tune the architecture and hyper-parameters of the proposed CNN
Classification using Trained CNN
Output

Figure 3.3: DFD of Anomaly Detection System for Images

5. Training Module

Training module refers to the training the images with CNN and videos with inception v2 model so that it yields the required results. We train a model until it starts to represent minimum error. The better trained the module; more efficient will be the results when applied on real life human activity anomaly detection.

6. Graphical User Interface

The user friendly GUI enables us to provide output in the form of images and videos and displays the predicted output with detection percentage on it.

6.1 Robbery Detection

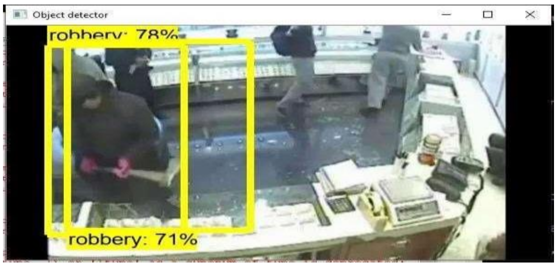


Figure 6.1: Robbery Detection-1

6.2 Fire Detection

Fire is a natural anomaly which may or may not be human induced. The application detects any kind of fire in surveillance. The presence of a little spark can alert the user and save the area from loss on time. And also, if the fire is human induced, the culprits can be detected. Hence, enhance the security level in the environment.

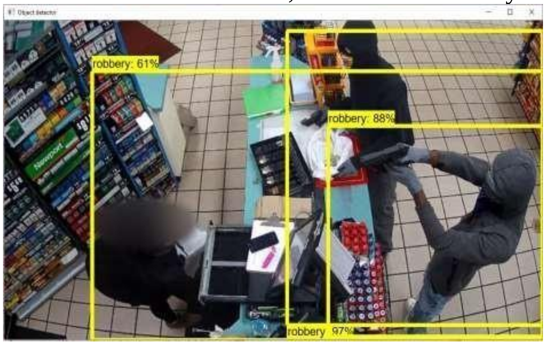


Figure 6.2: Robbery Detection-2

ISSN: 2582-1369 (online)
Submitted: 28.09.2020
Accepted: 22.10.2020
Published: 31.10.2020

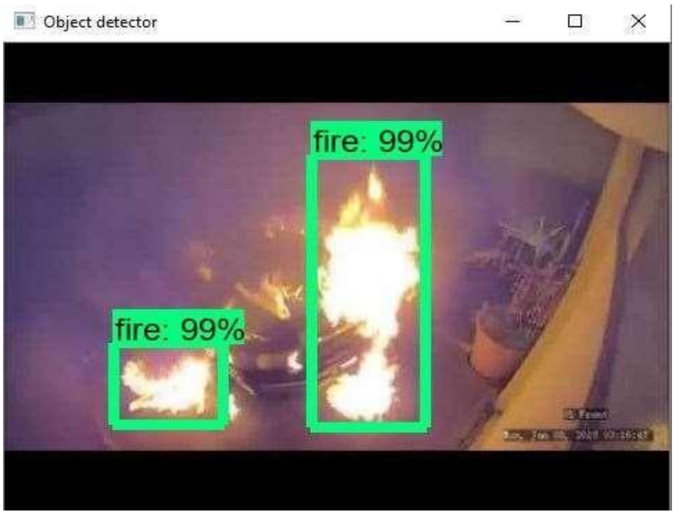


Figure 6.3: Fire Detection-1

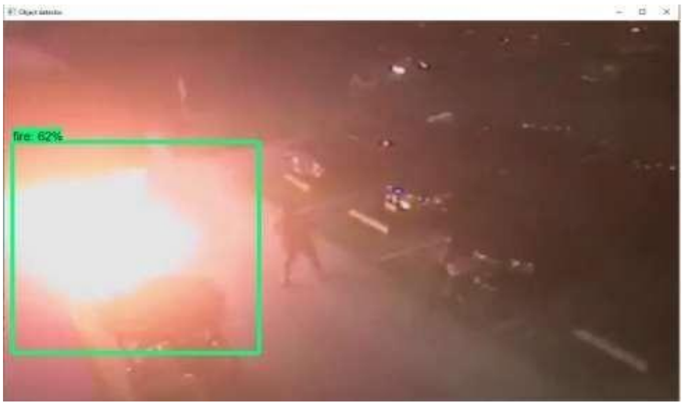
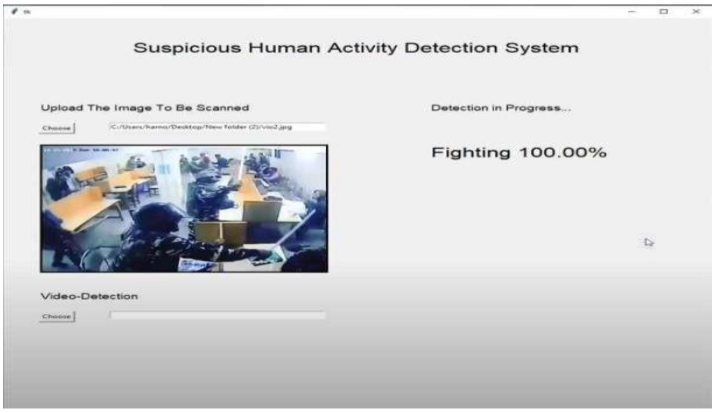


Figure 6.4: Fire Detection-2

6.3 Violence

The system detects activities in which entities indulge in any type of fight or physical violence.



Suspicious Human Activity Detection System

Upload The Image To Be Scanned

Choose C:/Users/hamo/Desktop/New folder (2)/vio2.jpg

Detection in Progress...

Fighting 100.00%

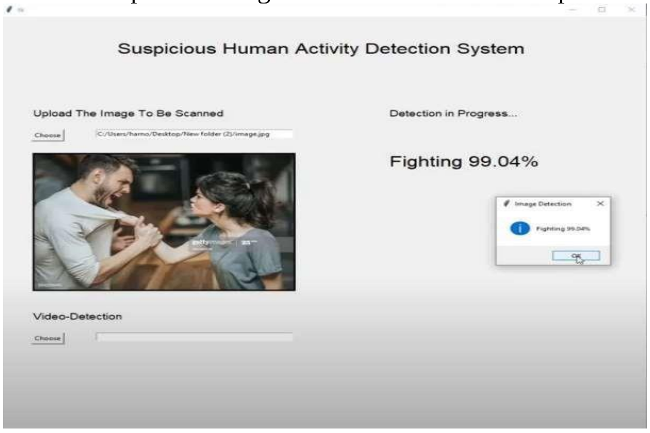
Video-Detection

Choose

Figure 6.5: Violence Detection-1

7. Conclusion and Future Scope

In this study, we have applied a supervised learning method to the Suspicious Human Behaviour Detection Framework focused on Neural Networks. We concentrated on phenomena that exist in outdoor environments, recognizing the difficulty of publicly accessible anomaly detection datasets. The fundamental benefit of our methodology is the usage of CNN for picture recognition and the fast-start v2 pattern.



Suspicious Human Activity Detection System

Upload The Image To Be Scanned

C:/Users/harno/Desktop/New folder (2)/image.jpg

Detection in Progress...

Fighting 99.04%

Image Detection

Fighting 99.04%

Video-Detection

Figure 6.6: Violence Detection-2

We have demonstrated the effectiveness and robustness of the proposed approach, demonstrating the competitive performance of existing methods. Further work directions should involve integrating feedback with richer temporal and qualitative knowledge and integrating the extraction function with the final judgment on anomaly. In addition, we can learn to design more sophisticated frameworks from deep neural network frameworks for object detection and classification tasks in order to represent multiple patterns from input video. Due to the complexity of realistic anomalies, using only normal data on its own may not be optimal for anomaly detection. We're able to manipulate both regular and anomalous images. A new large-scale anomaly dataset consisting of a variety of real-world anomalies is introduced to validate the proposed approach. The experimental findings that our suggested anomaly detection strategy performs far more than the reference approaches. In fact, we have shown the utility of our sample for the identification of unusual behavior activities. The future scope of our project lies in the following:

- Formulation of a more optimized GUI.
- Formulating the project as a smart phone friendly application which enables the user to keep a check of surveillance from their phones.
- Associating the application with "alarms" that warn the user of the suspicious patterns and reduce human efforts to check the system from time to time completely.
- Addition of more activities will lead to a more precise and secure system which can be deployed for professional purposes as well.

References

[1] https://medium.com/@everisUS/video-analysis-to-detect-suspicious-activity-based-on-deep-learning-fee2032ea14a
[2] http://www.svcl.ucsd.edu/projects/anomaly/dataset.htm
[3] https://www.kaggle.com/jubaerad/weapons-in-images-segmented-videos
[4] https://www.kaggle.com/ritupande/fire-detection-from-cctv
[5] https://www.kaggle.com/mohamedmustafa/real-life-violence-situations-dataset
[6] S.K. Panda, G.S.M. Reddy, S.B.Goyal, T.K., P. Bhambri, M.V. Rao, A.S. Singh, A.H. Fakih, P.K. Shukla, P.K. Shukla, A.B. Gadicha, and C.J. Shelke, "Method for Management of Scholarship of Large Number of Students based on Blockchain", Indian Patent issue 36/2019, application 201911034937, (2019), September 06.
[7] W. CHU, K.T. LEE, W. LUO, P. Bhambri, and S. Kautish, "Predicting the Security Threats of Internet Rumors and Spread of False Information Based On Sociological Principle", Computer Standards & Interfaces, (2020), ISSN 0920-5489, https://doi.org/10.1016/j.csi.2020.103454.