e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:07/July-2021 Impact Factor- 5.354 www.irjmets.com

ADVANCE SUSPICIOUS ACTIVITY DETECTION

Ms. Archana R. Ghuge[*1], Mr. Rushikesh S. Wakchaure[*2], Mr. Sagar D. Wagh[*3], Mr. Parag S. Hude[*4], Ms. Aishwaraya V. Pingale[*5]

[*1]Information Technology, Pres Svit, Nashik, Maharashtra, India.

Guide, Department Of Information Technology, Pres Svit, Nashik, Maharashtra, India.

[*2,3,4,5]Information Technology, Pres Svit, Nashik, Maharashtra, India

Students, Department Of Information Technology, Pres Svit, Nashik, Maharashtra, India.

ABSTRACT

Video surveillance is an old process used for security purposes. Using Artificial Intelligence & Machine Learning with any existing technologies is causing a greater impact on society. We can merge Machine Learning with Video Surveillance to improve capabilities of Security Systems. This approach will have several stages, first being collection & selection of frames, next one being able to apply an predetermined, pretrained machine learning model which can identify, predict or as necessary detect some activities or malicious, unethical phenomenons happening around. We trained a Machine Learning model based on Convolutional Neural Network which will improve ability to secure a premise. It serves two major features, first, it identifies and recognises faces which means we can track suspicious persons of crime or persons related to criminal activities, second, the network is trained on identifying suspicious activities.

Keywords: Video Surveillance, Artificial Intelligence, Machine Learning, Etc.

I. INTRODUCTION

Artificial Intelligence is a pretty old concept, but in use from nearly 2 decades ago due to evolution of low cost hardware, improvised software and a vast amount of data. Data is the driving fuel for Artificial Intelligence, this data can be anything in any format, in structured or unstructured way. Machine learning works on a principle that if we provide data to machines such that data is labeled into useful and not useful format, for example, data which distinguish between cat and dog such as images of cats & dogs, then machines can identify some underlying patterns in between data. Machines then can use this identified pattern to distinguish between cats & dogs on images that are new for machines. We can use this same approach for various purposes such as to identify faces, to identify suspicious activities and others. In cases of faces we can train models to identify faces that security personnel want to locate, such as persons with criminal activities or persons that are suspects in crimes. In cases of suspicious activities we not only have to train our model to identify activities but also to train our model to identify which activity is suspicious and which activity is normal for our society. For example, leaving a bag with no owner at a public place is definitely a suspicious activity while, leaving a bag inside a dustbin is not a suspicious activity.

II. MOTIVATION

In daily life we are using manual processes for our security purpose. Manually operating everything is not a great idea, as many mistakes can take place by negligence or carelessness behaviour of humans. Machines are better at identifying patterns, doing calculations & other things. We can also program or teach them to do the same work. Machines are better at doing repetitive tasks. We can use machines in daily life for doing repetitive tasks as well as tasks that involve the lives of many people directly or indirectly such as Security. Surveillance can be done manually as well as with machines using Video Surveillance as an example. Machines with the help of Humans can be a better partner to solve some of our major security concerns.

III. LITERATURE SURVEY

We studied a paper by Piyush Kakkar, Mr. Vibhor Sharma, International Journal of Advance Research in Computer Engineering (IJARCCE): Criminal Identification System Using Face Detection and Recognition in which they proposed a model that can detect guns in still frames(images), the demerit was the model was less effective in low light conditions and angel of the face not properly inclined towards the camera.[1]

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:03/Issue:07/July-2021 Impact Factor- 5.354 www.irjmets.com

We also studied a paper by Rajesh Kumar Triparti,Anand Singh Dalal, Int. J. of Innovative Science and Eng. Jan-Feb 2017: Suspicious Human Activity Recognition. The objective of that paper was to provide the literature review of six different suspicious activity recognition systems with its general framework to the researchers of this field.[2]

IV. PROPOSED SYSTEM

In this paper we proposed a system which is capable of doing 2 main tasks, 1st being identifying faces of given suspects, 2nd identifying suspicious activities such as people holding weapons or abandoned bags in public places. For our 1st goal our system uses convolutional neural networks along with picam to use cameras for recording frames. These frames are then used to locate faces. Neural network is trained using HAAR Cascade for fast and easy tuning. Patterns are already extracted which are helping detect unknown faces. These faces are then matched with previously processed images and if any match found system displays an alert on screen.

For our 2nd goal, a set of frames are extracted to find out what's really happening inside the frame. We are using a similar approach with convolutional neural networks but this time to identify or categorize between normal activities from suspicious ones as we already discussed. This both networks are independent of each other, can work simultaneously if necessary, to improve reach of security personnel. Suspicious activity detection works in 2 stages, 1st to identify an activity then to label the activity based on experience of machine learning model 1 out of 2 available labels (Normal Activity & Suspicious Activity).

V. RESULT DISCUSSION

Following are the screenshots of our system trained on identifying a face our team member,

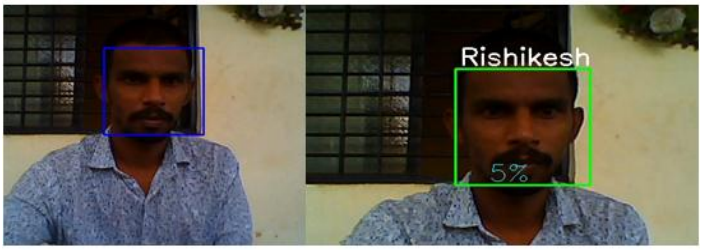

Fig: System Identifying a team member.

VI. CONCLUSION

In this paper we proposed a system based on Deep Neural Networks using Convolutional Neural Network algorithm which can classify suspicious activities as well as identify faces which can be trained to identify faces of suspects in criminal activities. The method we propose for detecting abandoned baggage is computationally efficient and our findings indicate that, while achieving an extremely low false alarm rate, we detected most of the abandoned items effectively. We managed to solve shortcomings like having a long-standing individual being identified as a left behind object by adding one extra step to validate our results from the stationary Object Detector. Because of the considerably smaller computational time for each frame, this technique can be said for any implementation in Real-Time.

VII. REFERENCES

[1] Open Computer Vision Library Reference Manual.Intel Corporation,USA, 2001.

[2] Hui-Xing, J., Yu-Jin, Z.: Fast Adaboost Training Algorithm by Dynamic Weight Trimming. Chinese Journal of Computers(2009).

[3] Bureau of Justice Statistics, U.S. Department of Justice, April 1990), pp. 43-66; SEARCH Group, " Legal and Policy Issues Relating to Biometric Identification Technologies ".

[4] Real time face recognition using PiCam : https://towardsdatascience.com/real-time-face-recognition-an-end-to-end-project-b738bb0f7348

[5] Suspicious_human_activity_recognition: https://www.researchgate.net/publication/314126434_Suspicious_human_activity_recognition_a_review