International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 589-592 www.ijaem.net ISSN: 2395-5252

Ai Based Instant Cctv Malicious Activity Detection Server Using Raspberry Pi

Jayanthi M G, Lavanya M E, Pooja S, Revathi A, Tejal Mahesh Desai
Associate Professor Cambridge Institute ofTechnology Bengaluru, India
Computer Science dept. Cambridge Institute of Technology Bengaluru, India
Computer Sciencedept. Cambridge Institute ofTechnology Bengaluru, India
Computer Sciencedept. Cambridge Institute of Technology Bengaluru, India
Computer Science dept.Cambridge Institute of Technology Bengaluru, India
Corresponding author: Jayanthi M G

Date of Submission: 26-07-2020 Date of Acceptance: 05-08-2020

ABSTRACT:
Artificial Intelligence (AI) technology is proliferati ng rapidly all over the world. To identify individuals, objects and events. AI for surveillance uses computer software programs that analyse images from video surveillance cameras. The Internet of Things (IoT) allows humans to wirelessly communicate and monitor everyday activity and make their lives more convenient. The Raspberry Pi is a thin, lightweight and inexpensive single board computer that can fit on the palm of humans. Closed- circuit television (CCTV) is one of the devices used to monitor any intruders to the protected area. This CCTV based on AI detects malicious activities by detecting intruders and intimating the person concerned about such activities. The proposed Raspberry Pi is connected to a webcam and internet access, so that the whole system can be programmed to perform the monitoring tasks.

I. INTRODUCTION

Surveillance system in security is crucial in today's fast growing world. The flow of individuals is growing consistently annually with the event of urbanization. It's important to watch crowd during a timely manner to stop from malicious activity and security threats. The manual security system continuously observes the visual screens for detecting any event of interest, which becomes challenging to tackle all the time. This is often the motive behind automated malicious activity detection. There has been extensive research done in the area of anomaly detection by computer vision and signal processing communities. Many models are developed using deep learning algorithms to avoid any complex handcrafted feature extraction and processing methods. Despite substantial research add this area, yet there are deficiencies like unavailability of cameras, adverse weather, visual modality issues etc. The remaining of the paper is organized as follows: Section 2 is about the proposed system while Section 3 describes the methodology of the proposed idea.
Section 4 gives implementation details, Section 5 draws conclusion and discusses future research directions for further improvements.

A. Objectives

The objective is to detect the malicious activity happening around through a CCTV camera and provide alert signals to the user. To give security to the people. To minimalism the malicious activity happening. To detect the weapons or objects that cause malicious activity. The main objective is to make minimal use of human input by using AI concepts.

II. PROPOSEDSYSTEM

The drawback of the existing system is that it does not distinguish discriminative features of the activity and does not accurately predict the desired results.

AI based instant CCTV malicious activity system focus on capturing of video from Raspberry Pi and converting it into images frames and after classification signals the burglar alarm. Raspberry Pi 3 is a credit card sized computer which has the Linux operating system and its available at lower cost. The web camera is mounted over to the raspberry pi module which captures the image and stores to on the raspberry pi server. These input images are then further processed.

The image frames are preprocessed using image preprocessing technique and the images are labeled after preprocessing then the images are made ready for training and preparing the model.
The images are then treated with CNN algorithms to train the model on the training dataset and the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 589-592 www.ijaem.net ISSN: 2395-5252

model is constructed and save the model. The model is used for classifying the activity. After the comparison the image which is malicious, that is the image which has lot of movements that image is predicted as a malicious and sends signal to alarm.

The Convolution neural networks algorithm is implemented using python programming language by Open CV package. The model is created using machine learning packages which is suitable for CNN and desired results are predicted for the tested data provided by the user.

The proposed Crime Classification scheme based on one of the features of the common convolutionary neural network (CNN). We use CNN which will be able to isolate, understand and identify features automatically. Compared to other algorithms for the image classification, CNNs use very little preprocessing. This means the network is thinking about the filters that are in. The proposed framework should manage all the data with ease and the model's accuracy is very good. The proposed systems effectively remove the limitations of the current system and provide strong data protection.

III. SYSTEMDESIGN

ThesystemconsistsofRaspberryPimodule,Pi camera and a buzzer sensor.

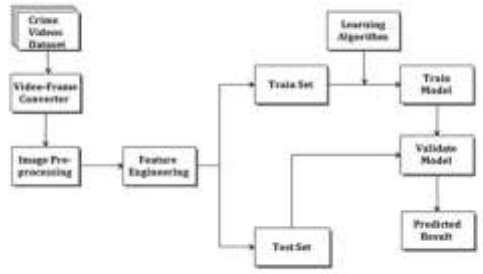

Fig. 1 Block diagram of system design

a. Raspberry Pi:

Fig. 2 Raspberry Pi

The 3rd generation Raspberry Pi 3 Model B is a Raspberry Pi that is single board computer sized by credit card can be used for many applicationsandreplacesRaspberryPiModelB+andRaspberryPi 2 Model B. While maintaining the popular Raspberry Pi 3 Model board format B brings you a more powerful, 10x faster processor than the first-generation Pi toRaspberry.

b. PiCamera:

Fig. 3 Pi Camera

It could be used to catch Raspberry Pi camera module Photograph and take footage in high definition. You should put it to use the camera libraries to create results. Photography Module has a fixed- focus 5-megapixel sensor Supports Modes 1080p30, 720p60 and recording. It interconnects via 15 cm ribbon cable to Raspberry Pi's CSI connection. The Camera fits with all Raspberry Pi 1 versions, as well as Pi2-Pi2. It is accessible through MMAL (Multi-Media) AbstractionLayer),Linuxvideoframeworkinterfacetosoftwareand there are several third parties Libraries built for it, such as the Pi camera library Python. The camera module is used extensively for building surveillance applications and camera traps inwildlife

c. Active Buzzer Alarm Module:

Fig. 4 Buzzer module

For Arduino an Active Buzzer Alarm Module is an audio signaling system that may be mechanical. This is durable in operation, using top-

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 589-592 www.ijaem.net ISSN: 2395-5252

quality material. An activated buzzer rings out as long as it is electrified. It is a bit costly but easier to control as opposed to a passive buzzer. Typical uses of buzzers include warning systems, timers and user input validation like a mouse click or keystroke.

Transistor drive module uses 8550. With fixed bolt hole- easy installation- 2.6mm aperture. Operating voltage 3.3V-5V. PCB Dimensions: 34.28 mm (L) * 13.29 mm (W) * 11.5 mm (H).

Crime events such as snatching and trying to kill an individual or an unusual occurrence in a community, even if we have a servlet camera, it is impossible for a human to track such an occurrence. So, a program that uses Machine Learning Technique to identify the event whether it is normal or abnormal. If this is an irregular occurrence it sends a warning message to the department concerned. A novel method is proposed for the classification of crime based on one of the common convolutionary neural networks (CNN features).

CNN which can automatically extract, learn and classify features CNNs use very little pre-processing compared to other algorithms for the classification of the images. Such freedom from previous information and human intervention in feature design is a major advantage in the classification of images. The image frames are pre-processed using image pre-processing technique and the images are labelled after pre-processing, then the images are prepared for training and model preparation. The images are then handled with CNN algorithms to train the model on the training dataset and the model is constructed and saved. Upon comparing the malicious picture, that is the picture that has several motions that the image is predicted as malicious and sends an alarm signal.

IV. IMPLEMENTATION

The implementation of this system provides malicious activity, detection of intruders by using an automated system without manual labors.

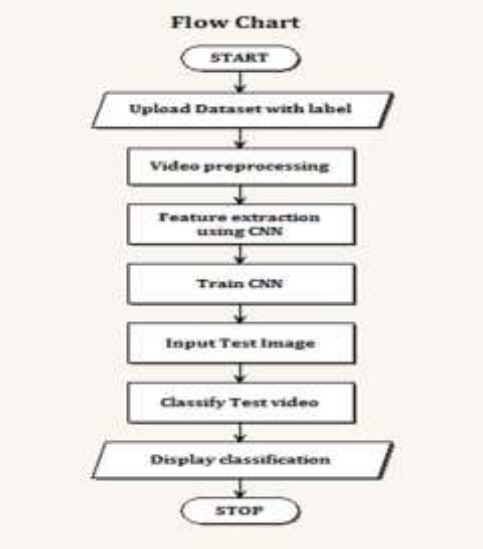

Fig. 8 Flow chart of machine learning model

This system provides alerts to the users by classifying the event as malicious or not. The objective of the system is as follows:

- Capturing the video of the particular area where the system the system is deployed with the help of PI cam.
- Sending this data to the software model where the video is pre-processed and classified as malicious activity or non-malicious.
- If found malicious, the system alerts the user with a buzzer sound which is connected to the system.
- If found non-malicious the system performs goes back to perform the same task of monitoring the area.

The system works as follows, when an intruder is trying to enter into a monitored place with a weapon or if an intruder is trying to break open a door, the PI cam captures this activity and feeds this input to raspberry pi which contains the testing model. The testing module which is trained on various datasets of malicious and non-malicious activity classifies the event. If the output is malicious the alarm is triggered immediately alerting the user, to take necessary step, if not the system starts monitoring the environment without triggering the alarm.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 3, pp: 589-592 www.ijaem.net ISSN: 2395-5252

V. RESULT

Fig. 9 Object Recognition

VI. CONCLUSION

CCTV cameras are implemented in all places where security is given much importance. Manual surveillance is a very tedious and time consuming task.So we need a computerization system to speed up the process. We can do this surveillance by using Raspberry Pi and camera modules which are cost-effective surveillance mechanism.A complete system that will monitor a specific area by identifying any malicious activities in the surrounding. In case of any malicious activity the system will alert the client.To identify the malicious activity, we use various image processing techniques to filter the image and train the model and feature extraction using CNN to extract the features.

ACKNOWLEDGEMENT

We express our gratitude to our guide Prof. Jayanthi M.G. who guided us in the project, clarified all our doubts and gave solution for the problems we faced. She extended her full support for the improvement of the project. A special thanks to all the teammates who worked really hard to complete the project successfully.

REFERENCES

[1]. C. Chen, R. Jafari, and N. Kehtarnavaz, “Action recognition from depth sequences using depth motion maps-based local binary patterns,” in Proc. IEEE Win. Conf. Appl. Comput. Vis., 2015, pp. 1092–1099.

[2]. J. Yu and J. Sun, “Multiactivity 3-D human pose tracking in incorporated motion model with transition bridges,” IEEE Trans. Syst., Man, Cybern.,Syst., to be published.

[3]. W. Chi, J. Wang, and M. Q.-H. Meng, “A gait recognition method for human following in service robots,” IEEE Trans. Syst., Man, Cybern.,Syst., to be published.

[4]. G. Liang, X. Lan, J. Wang, J. Wang, and N. Zheng, “A limb-based graphical model for human pose estimation,” IEEE Trans. Syst., Man,Cybern., Syst., vol. 48, no. 7, pp. 1080–1092, Jul. 2018.

[5]. Y. Guo, D. Tao, W. Liu, and J. Cheng, “Multiview Cauchy estimator feature embedding for depth and inertial sensor-based human action recognition,” IEEE Trans. Syst., Man, Cybern., Syst., vol. 47, no. 4, pp. 617–627, Apr. 2017.

[6]. S. Zhang, C. Gao, F. Chen, S. Luo, and N. Sang, “Group sparse-based mid-level representation for action recognition,” IEEE Trans. Syst., Man,Cybern., Syst., vol. 47, no. 4, pp. 660–672, Apr. 2017.

[7]. H. Wang, A. Kläser, C. Schmid, and C.-L. Liu, “Action recognition by dense trajectories,” in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., 2011, pp. 3169–3176.

International Journal of Advances in Engineering and Management
ISSN: 2395-5252

IJAEM

Volume: 02 Issue: 01 DOI: 10.35629/5252

www.ijaem.net
Email id: ijaem.paper@gmail.com