Chapter 6
Smart Surveillance System Using Deep Learning Approaches

Uma K. V.
Thiagarajar College of Engineering, India

Aakash V.
Thiagarajar College of Engineering, India

Deisy C.
Thiagarajar College of Engineering, India

ABSTRACT

In modern days, CCTVs are being used for monitoring, and most shops have surveillance cameras up and running during the night times, but still, robberies are happening since the surveillance footage is being checked only after a robbery on the next day. To overcome the problems of having manual security and cost wastage along with automating the monitoring of the surveillance during the night times once the shops are closed, the authors propose the smart surveillance system. Deep learning algorithms and computer vision techniques are used to detect the presence of humans/intruders in a given video. The smart surveillance system along with the reduction in the cost of manual securities also provides robust nighttime monitoring, and it provides immediate notification to the authority as soon as it spots the intruder in the specified monitoring time, thereby reducing the robberies and the business impact caused.

INTRODUCTION

Video analytics and pedestrian detection is a vastly growing domain that has multiple application in various domains like self-driving cars, behavioral analysis, crowd management as well as surveillance purpose. The absence of real time monitoring of surveillance footage is the main cause of the robberies that are taking place during the night times in the shop.

Below were real time robbery images where the robbery took place in-spite of surveillance camera. Figure 1 show the real time robberies that happens despite of having CCTVs.

DOI: 10.4018/978-1-7998-8892-5.ch006

Figure 1. Showing the real time robberies despite the presence of CCTV camera.

We still need to monitor the CCTV by humans to make some kind of decision. In this project we propose the end-to-end automated surveillance monitoring system during the night times to prevent the robberies and to reduce the cost of human securities using the convolutional neural networks and computer vision techniques. The convolution neural networks are being used as the start-of-art image classification algorithm and for image processing in the modern days. The problem of intruder detection comes under the task of human detection binary classification. A binary classification CNN model can be trained with images of two classes (image with humans and image without humans). Using computer vision techniques, the CCTV footage video can be processed in frames and can be converted into RGB matrices. These processed RGB frames of the surveillance footage can be passed onto the trained CNN model to detect intruders. A properly trained CNN model can able to detect intruders even if they wear mask on their face. This system alerts and notifies the using a python notification and calling library as soon as it detects the intruders thereby preventing the loss incurred due to the robbery.

Video analytics represent a middle thing of many wi-fi offerings that require processing of voluminous information streams emanating from hand-held devices. MultiAccess Edge Computing (MEC) is a promising answer for helping such resourcehungry offerings, however there's a plethora of configuration parameters affecting their overall performance in an unknown and probably timevarying fashion. To triumph over this obstacle, we recommend an Automated Machine Learning (AutoML) framework for at the same time configuring the provider and wi-fi community parameters, in the direction of maximizing the analytics` accuracy problem to minimal body charge constraints. Our experiments with a bespoke prototype screen the risky and system/data dependent overall performance of the provider, and encourage the improvement of a Bayesian online mastering set of rules which optimizes on the fly the provider overall performance. We show that our answer is assured to discover a nearoptimal configuration the use of secure exploration, i.e., without ever violating the set body charge thresholds. Use the testbed to in addition examine this AutoML framework in numerous eventualities with real-international datasets (Galanopoulos, 2021).

New video analysis tasks based on deep learning require computationally intensive neural networks and powerful computing resources in the cloud to achieve high accuracy. Due to latency requirements and limited network bandwidth, edge cloud systems adaptively compress data to find a balance between overall analytical accuracy and bandwidth consumption. However, when the data deteriorates, another