INFORMATICS INSTITUTE OF TECHNOLOGY

INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

"SECUREFLOW"

A Transfer Learning Approach to Detect Suspicious Criminal Behaviors at an Early Stage

A dissertation by

Mr. Shenal Pelpola

Supervised by

Mr. Pumudu Fernando

Submitted in partial fulfilment of the requirements for the BSc in Computer Science degree at the University of Westminster.

April 2022

Abstract

In recent years, public security has emerged as a critical problem in modern society since it is intimately tied to social stability and economic development. Due to human limitations in visual focus of attention, real-time manual surveillance video analysis has become a time-consuming process, and for this reason, automated video surveillance has been one of the most sought-after research topics in the computer vision domain. Suspicious criminal behavior detection is a subset of suspicious behavior detection, also known as anomaly behavior, and is a subdomain of automated surveillance systems. Most suspicious behavior detection systems in the literature are focused on detecting the crime while it is taking place, providing a limited window of opportunity to prevent the crime. Detecting criminal behavior at an early stage aims to detect the crime using the person's pre-crime behavior, providing a large opportunity to prevent the crime.

Based on the literature, the pre-crime behavior segment in a crime video can be defined as the time between when the person first appears in the crime scene and finally commits the crime. Throughout the pre-crime behavior segment, the person exhibits non-verbal behavior identified in the literature as social signals. The research aims to develop a semi-automated system which aids the monitoring person to detect these social signals to identify shoplifting, stealing and robbery related crimes at the earliest possible stage. By considering the methodology of pre-crime behavior and social signals which happens during shoplifting, stealing and robbery a new dataset was proposed. A transfer learning approach was proposed which allows to develop the solution with a limited amount of data.

Three state-of-the-art architectures, including ResNet3D, ResNetMixed, and ResNet(2+1)D, were experimented with different hyperparameter optimizations to develop the most optimal approach for the problem. ResNet3D architecture achieved an AUC score of 96.7%, which performed the best out of the three architectures and outperformed the previous research in detecting suspicious criminal behaviors at an early stage.

Keywords: Automated Video Surveillance, Suspicious Human Behavior detection, Video Anomaly Detection, Transfer Learning