Chapter 13
Learning Algorithms for Anomaly Detection from Images

Tarem Ahmed
BRAC University, Bangladesh

Al-Sakib Khan Pathan
International Islamic University Malaysia, Malaysia

Supriyo Shafkat Ahmed
BRAC University, Bangladesh

ABSTRACT

Visual surveillance networks are installed in many sensitive places in the present world. Human security officers are required to continuously stare at large numbers of monitors simultaneously, and for lengths of time at a stretch. Constant alert vigilance for hours on end is difficult to maintain for human beings. It is thus important to remove the onus of detecting unwanted activity from the human security officer to an automated system. While many researchers have proposed solutions to this problem in the recent past, significant gaps remain in existing knowledge. Most existing algorithms involve high complexities. No quantitative performance analysis is provided by most researchers. Most commercial systems require expensive equipment. This work proposes algorithms where the complexities are independent of time, making the algorithms naturally suited to online use. In addition, the proposed methods have been shown to work with the simplest surveillance systems that may already be publicly deployed. Furthermore, direct quantitative performance comparisons are provided.

1. INTRODUCTION

Physical security is unfortunately of prime concern today, and an extensive network of multimodal surveillance and security sensors is prevalent in many places in the world. They range from analogue closed-circuit television (CCTV) systems to sophisticated networks of infra-red and motion sensors in sensitive areas such as banks and museums. The London Underground and London Heathrow Airport have more than 5000 cameras for the purposes of physical security, for example (Valera & Velastin, 2008). Images

DOI: 10.4018/978-1-5225-0983-7.ch013

from these systems are typically transmitted to a control room, where human security officers constantly watch the monitors to guard against physical intruders attempting unauthorized access. As events such as burglary attempts rarely occur, the security officers typically must continuously stare at monotonous images for long stretches of time. Constant alert vigilance for days on end is humanly difficult to maintain. Studies have shown that the optimal concentration spans for a person ranges between 25 and 30 minutes (Noyes & Bransby, 2002). This consequently increases the risk of suspicious activity going unnoticed. In the most unfortunate of situations, given the labour cost involved with hiring the requisite number of human operators to monitor a visual surveillance network, the feeds may be monitored only sparingly, or not at all, often merely serving as an archive to retroactively refer back to once an untoward incident in known to have occurred (Ko, 2008). It is thus important to remove the onus of detecting unwanted intruders from the human security officers with cognitive limits, to an automated system. *This was the objective of the first author's doctoral dissertation (Ahmed, 2013), on which the conference version of this paper was based (Ahmed et al., 2014), and thereby subsequently so is this extension*.

The first author's PhD thesis (Ahmed, 2013) proposed four algorithms where the computational, storage, and memory complexities are independent of time, making them suitable for online use. The thesis proposed the Kernel-based Online Anomaly Detection (KOAD), Kernel Estimation-based Anomaly Detection (KEAD), Kernel Principal Component Analysis (KPCA) and One-Class Neighbour Machine (OCNM) algorithms. This work is the first application of the stated algorithms to the problem of automated surveillance. KOAD (Ahmed et al., 2007) and KEAD (Ahmed, 2009) were initially developed with the problem of online anomaly detection in backbone IP (Internet Protocol) networks in mind. OCNM and KPCA were adapted in (Ahmed, 2013) for intruder detection in surveillance networks.

Results obtained during various stages of progress of this research were reported through timely publications (Ahmed et al., 2010; Ahmed, 2011; Ahmed et al., 2011; Ahmed & Pathan, 2012a; Ahmed et al., 2012; Ahmed & Pathan, 2012b; Ahmed et al., 2013a; Ahmed et al., 2013b; Ahmed & Pathan, 2013; Ahmed et al., 2013; Ahmed et al., 2014). *Being a dissertation paper based on the first author's doctoral research, results from these prior publications are summarised here.*

This paper proceeds as follows. Section 2 introduces the basic mathematical principles. Section 3 presents our proposed algorithms. Section 4 describes our experimental setup and Section 5 presents results. Section 6 concludes the paper alongside suggesting future works.

1.1. Related Work and Our Contribution

As was concluded in (Ahmed, 2013), "the field of automated visual surveillance has attracted a lot of recent attention, with many large research projects such as an European Erasmus Mundus project (Erasmus Mundus, n.d.) granted on the subject. Some of the most recent research works on outlier detection in image sequences are being performed at the Computer Vision Laboratory at the Swiss Federal Institute of Technology (ETH) Zurich, Switzerland (Breitenstein et al., 2009; Schuster et al., 2010), and at the Center for Sensor Web Technologies at Dublin City University in Dublin, Ireland (Kuklyte et al., 2009; Kuklyte et al., 2011)."

Aziz et.al. presented an Intrusion Detection Systems (IDS) in (Abdel-Aziz et al., 2013a) using genetic algorithms and principal component analysis to detect anomalies and classify anomalies. They showed that in general J48 gave better results than other classifiers, while for certain attacks Naïve Bayes gave the best results. Subsequently in (Abdel-Aziz et al., 2013b), Aziz et al. proposed an anomaly detector generation approach using genetic algorithm in combination with several feature selection techniques,