Advanced Science and Technology Letters
Vol.42 (Mobile and Wireless 2013), pp.1-4
http://dx.doi.org/10.14257/astl.2013.42.01

Automated Surveillance in Distributed, Wireless Visual Networks: A Comparative Study

Tarem Ahmed[1], Supriyo Ahmed[1], and Al-Sakib Khan Pathan[2]

[1]Department of Electrical and Electronic Engineering,
BRAC University, Dhaka, Bangladesh
[2]Department of Computer Science,
International Islamic University Malaysia, Kuala Lumpur, Malaysia
{tarem,supriyo}@bracu.ac.bd,sakib@iium.edu.my

Abstract. A number of algorithms have been recently proposed for automatic intruder detection from CCTV images. Past researchers have tested these algorithms on centralized networks where all images are transmitted to a central control room. This paper demonstrates the applicability of a selection of such algorithms to a distributed network of wireless visual sensors. An empirical comparative study of the most popular of such algorithms on a simulation of a wireless sensor network is presented. In addition, this paper provides further evidence in support of the most effective of such algorithms to the problem of anomaly detection in image streams.

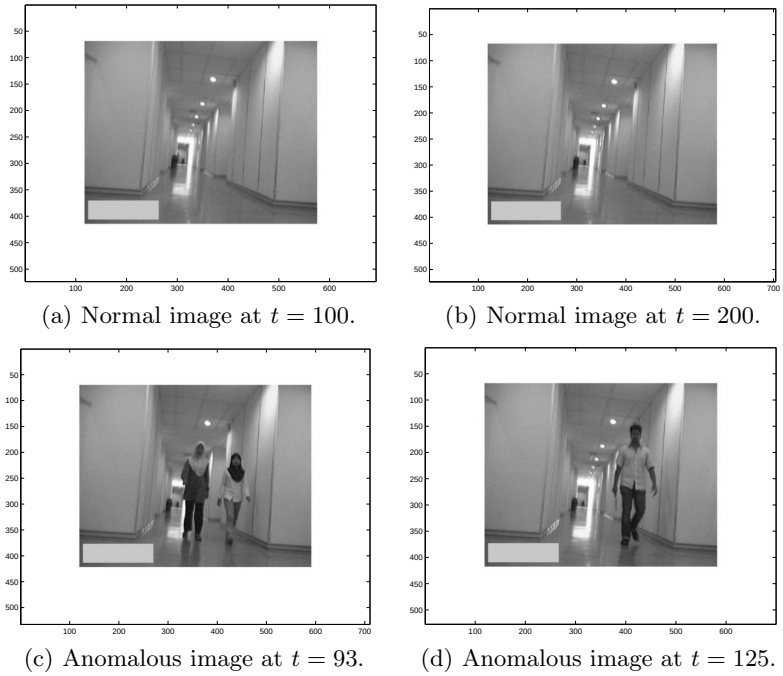
Keywords: wireless sensor networks, machine learning, kernel methods

1 Introduction

Physical security is unfortunately of prime concern in today's world, and an extensive network of multimodal surveillance networks is prevalent in many places. Ahmed et al. have recently proposed three schemes based on kernel machines to perform automated detection of unnatural activity in visual surveillance systems [1]. Ahmed et al. have compared their proposed algorithms with two representative schemes selected from two families of methods popularly used in automated surveillance. They have tested on an infrastructure consisting of a centralized network of archaic CCTV cameras around a poorly-lit building.

Here, we argue the applicability of the algorithms introduced in [1] to a distributed network of wireless visual sensors. Minimizing communication costs is imperative in a mobile and wireless network, unlike in a static, centralized network that can use backbone wired connections such as an indoor LAN. We simulate a network of wireless visual sensors by using a network of high-resolution webcams deployed randomly inside a building, and apply the algorithms discussed in [1] in a distributed manner at each node. This paper also provides a comparative empirical study of the algorithms discussed in [1] on a *complementary* setting, thus providing further evidence in support of said algorithms to the general problem of automated intruder detection in surveillance networks.

ISSN: 2287-1233 ASTL



(a) Normal image at $t = 100$. (b) Normal image at $t = 200$.

(c) Anomalous image at $t = 93$. (d) Anomalous image at $t = 125$.

Fig. 1. Images captured during four example timesteps at Node 1. Two timesteps show usual images while two show situations where humans appear.

2 Algorithmic Bases

We apply the Kernel-based Online Anomaly Detection (KOAD) [2, 3], Kernel Estimation-based Anomaly Detection (KEAD) [4], and the Kernel Principal Component Analysis (KPCA) [1] algorithms. By virtue of being schemes built using Kernel Machines, KOAD, KEAD and KPCA look for patterns in a richer feature space, and are able to exploit higher order correlations between pixels in the sequence of images. We then provide direct quantitative comparisons with the standard Principal Component Analysis (PCA) technique and the Normalized Compression Distance (NCD) measure between images first proposed by Au et al., two schemes on which many existing autonomous intruder detection systems have been based [5, 6]. Due to space constraints, the reader is referred to [5] for algorithmic descriptions and implementation details.

3 Experiments

Four high-resolution Logitech^{TM} webcams were randomly deployed in a junction of hallways at the International Islamic University Malaysia (IIUM) to simulate a distributed network of visual sensors. Laptop computers connected to the webcams were programmed to take still snaps every 15-seconds. The detection algorithms were then run individually at each node in a distributed fashion. The

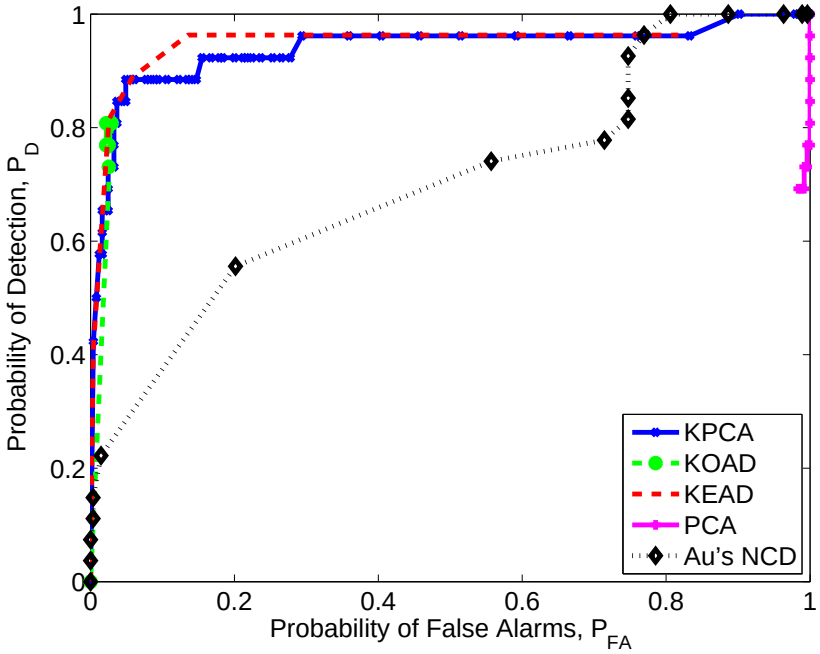


Fig. 2. ROC curves showing performances of KPCA, KOAD, KEAD, PCA and Au's NCD-based algorithms.

total data set consisted of 300 timesteps, of which 27 were manually identified as potential anomalies. Figure 1 shows pictures from Camera 1 corresponding to four example timesteps, with (a) and (b) showing regular (normal) scenarios, and (c) and (d) showing instances of human forms appearing.

Figure 2 compares the performances of KOAD, KEAD and KPCA with PCA and Aus NCD-based algorithms. Receiver Operating Characteristic (ROC) curves are presented, demonstrating the tradeoff between the Probability of False Alarms (P_{FA}) and the Probability of Detection (P_D). It is evident that the performances of all of KPCA, KOAD and KEAD are significantly superior to those of PCA and NCD-based algorithms. Moreover, all kernel-based algorithms easily achieve near-perfect detection rates at low false alarm rates.

4 Conclusions and Future Directions

Ahmed et al. have recently proposed three adaptive algorithms to perform automated detection of unnatural activity in visual surveillance networks [1]. They have compared their algorithms with two representative schemes selected from two families of methods popularly used in automated surveillance, and tested on a centralized network of archaic CCTV cameras around a poorly-lit area.

This paper has demonstrated the applicability of the algorithms introduced in [1] to a distributed network of wireless visual sensors. In addition, this paper has also provided a comparative empirical study of the said algorithms on a

complementary setting, thus providing further evidence in support of the kernel-based algorithms first advocated in [1] to the general problem of automated intruder detection in surveillance networks.

Our future work will concentrate on applying other machine learning algorithms such as the One-Class Neighbor Machine (OCNM) [7–9] to the problem at hand, and applying the algorithms discussed here to intrusion detection problems in other networks such as ad hoc and P2P networks [10, 11].

References

1. T. Ahmed, X. Wei, S. Ahmed, and A.-S. K. Pathan, "Efficient and effective automated surveillance agents using kernel tricks," *SIMULATION: Transactions of The Society for Modeling and Simulation International*, vol. 89, no. 5, pp. 562–577, May 2013.
2. T. Ahmed, Sabrina Ahmed, Supriyo Ahmed, and M. Motiwala, "Real-time intruder detection in surveillance systems using adaptive kernel methods," in *Proc. IEEE Int. Conf. on Communications (ICC)*, Cape Town, South Africa, May 2010.
3. T. Ahmed, M. Coates, and A. Lakhina, "Multivariate online anomaly detection using kernel recursive least squares," in *Proc. IEEE Int. Conf. on Computer Communications (INFOCOM)*, Anchorage, AK, USA, May 2007.
4. T. Ahmed, "Online anomaly detection using KDE," in *Proc. IEEE Global Communications Conf. (GLOBECOM)*, Honolulu, HI, USA, Nov. 2009.
5. ——, "Effficient and effective automatic surveillance approaches," Ph.D. dissertation, International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia, Sep. 2013.
6. T. Ahmed and R. Rahman, "Survey of anomaly detection algorithms: Towards self-learning networks," in *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, A.-S. K. Pathan, Ed. Auerbach Publications, CRC Press, USA, Sep. 2010, pp. 65–89.
7. T. Ahmed, B. Oreshkin, and M. Coates, "Machine learning approaches to network anomaly detection," in *Proc. ACM/USENIX Workshop on Tackling Computer Systems Problems with Machine Learning Techniques (SysML)*, Cambridge, MA, USA, Apr. 2007.
8. T. Ahmed, X. Wei, S. Ahmed, and A.-S. K. Pathan, "Intruder detection in camera networks using the one-class neighbor machine," in *Proc. American Telecommunications Systems Management Association (ATSMA) Networking and Electronic Commerce Research Conf.*, Riva del Garda, Italy, Oct. 2011.
9. ——, "Automated intruder detection from image sequences using minimum volume sets," *International Journal of Communication Networks and Information Security*, vol. 4, no. 1, pp. 11–17, Apr. 2012.
10. X. Wei, T. Ahmed, M. Chen, and A.-S. K. Pathan, "PeerMate: A malicious peer detection algorithm for P2P Systems based on MSPCA," in *Proc. IEEE Int. Conf. on Computing, Networking and Communications (ICNC)*, Lahaina, HI, USA, Jan. 2012.
11. X. Wei, J. Fan, M. Chen, T. Ahmed, and A.-S. K. Pathan, "SMART: A subspace based malicious peers detection algorithm for P2P systems," *International Journal of Communication Networks and Information Security*, vol. 5, no. 1, pp. 1–9, Apr. 2013.

