Intruder Detection in Camera Networks using the One-Class Neighbor Machine

Tarem Ahmed
Dept of CS,
Int. Islamic Univ Malaysia (IIUM)
Kuala Lumpur,
Malaysia
tarem@ieee.org

Xianglin Wei
Dept of CSE,
PLA University of Science & Tech.
Nanjing,
China
wei_xianglin@ieee.org

Supriyo Ahmed
Dept of EEE,
BRAC University
Dhaka,
Bangladesh
supriyo@bracu.ac.bd

Al-Sakib Khan Pathan
Dept of CS,
Int. Islamic Univ Malaysia (IIUM)
Kuala Lumpur,
Malaysia
sakib@iium.edu.my

Abstract

We propose a new algorithm based on machine learning techniques for automatic intruder detection in surveillance networks. The algorithm is theoretically founded on the concept of minimum volume sets. Through application to real images from an example, simple closed-circuit television system and comparison with some existing algorithms, we show that it is possible to easily obtain high detection accuracy with low false alarm rates.

1. INTRODUCTION

An extensive network of multimodal surveillance systems is prevalent in many places in today's world. The London Underground and London Heathrow airport have more than 5000 cameras. Simultaneously monitoring multiple images becomes tedious and monotonous for human operators with typically short attention spans and cognitive limits on how many screens may be attentively observed simultaneously. The goals of current research in autonomous surveillance are to develop algorithms that attract the attention of a human operator in real-time based on end-user requirements, process information arriving from a multi-sensor environment at high rates, and use inexpensive standard components [1].

We propose the One-Class Neighbor Machine (OCNM) algorithm [2], run using a sliding window implementation, to autonomously detect the occurrence of an anomalous image in a sequence of images being captured by a visual surveillance network such as a CCTV system.

The OCNM algorithm had previously been applied to a sequence of images captured from a network of road traffic cameras on a Quebec highway [3], and used in an attempt to identify images depicting traffic congestions. However, in [3], the OCNM algorithm was applied in a block-based fashion, and the flags were only raised after-the-fact. This characteristic renders such an implementation useless when it comes to real-time intruder detection for surveillance purposes. Moreover, [3] was a work-in-progress, advocating promise over results [4]. Furthermore, [3] provided no comparison with any existing method. In this paper we apply OCNM in an online fashion, and present more mature results. Through comparisons with representative algorithms from two *families* of algorithms commonly used for novelty detection in image sequences, we demonstrate that our proposed algorithm not only achieves superior performance, but yields close-to 100% detection accuracy with low false alarm rates.

1.1 Outline of Paper

We motivate and describe our proposed OCNM algorithm in Section 2. Section 3 describes two related algorithms that we compare our proposed algorithm with. Section 4 presents experimental results on real images from an example CCTV surveillance system. Section 5 concludes.

2. AUTOMATED INTRUDER DETECTION ALGORITHM

2.1 Minimum Volume Sets

We expect that the set of *normal* (usual) images will constitute a high density region of the space spanned by the set of all images. With each image constituting a multidimensional data point, the densest regions of this multidimensional space should contain the vast majority of the arriving points. Estimating Minimum Volume Sets (MVSs) is a common approach for determining high-density regions in multidimensional spaces.

Assuming that the arriving data points are drawn from a generic and unknown underlying probability distribution P, minimum volume set G_β containing mass at least $\beta \in (0, 1)$, with respect to reference measure γ, is defined as:

$$G_\beta = \operatorname{argmin}\{\gamma(G) : P(G) \geq \beta\} \quad (1)$$

where G is a measurable set [5]. These sets are known in the MVS literature as density contour clusters.

Estimation of MVSs satisfying (1) allows the identification of high-density regions where the mass of the underlying probability distribution P is concentrated. Points lying outside these regions may then be declared anomalous.

2.2 The One-Class Neighbor Machine

The One-Class Neighbour Machine (OCNM) algorithm proposed by Muñoz and Moguerza provides an elegant means of estimating minimum volume sets [2]. The OCNM algorithm is a block-based procedure that provides a binary decision function indicating whether any point $\mathbf{x}_t$ is a member of the MVS or not. The algorithm requires the choice of a *sparsity measure*, which relaxes the density estimation problem by replacing the task of estimating the density function at each data point by a simpler measure that asymptotically preserves the order induced by the density function. Example choices for the sparsity measure include the kth nearest neighbour Euclidean distance and the average of the first k nearest-neighbour distances.

We have implemented the OCNM algorithm using the kth nearest-neighbour distance as the sparsity measure. The OCNM algorithm proceeds by sorting the values of the sparsity measure for the set of all points S, and subsequently identifies those points that lie inside the MVS as those having the smallest sparsity measure, up to a pre-specified fraction μ, of the total number of points in S.

We apply OCNM here in a sliding window fashion, with the window advancing by one when the next image arrives in the next timestep. The binary decision output of the algorithm output regarding the last point in the window (i.e. the most recently arriving image), is used to flag an anomaly in real-time. Varying the pre-specified fraction μ of outliers yields the Receiver Operating Characteristic (ROC) curve presented in Section 4. We are then able to compare the performance of OCNM with representative algorithms from two families of algorithms commonly used for novelty detection in image sequences. The results are discussed in Section 4.

3. RELATED WORK

3.1 Principal Component Analysis

The technique of Principal Component Analysis (PCA) may be used to separate the space occupied by set of input vectors into two disjoint subspaces, corresponding to normal and anomalous behaviour [4]. An anomaly may then be flagged in the timesteps where the magnitude of the projection onto the anomalous subspace, θ_t, exceeds a threshold.

Various approaches where moving objects are detected in video sequences directly using PCA have been proposed [6]. Wang et al. proposed a method which uses incremental two-dimensional PCA (2DPCA) to characterise objects, followed by maximum-likelihood estimation for tracking [7].

We apply PCA here in the following manner. We first verify using a scree plot [8] that the space is indeed overdetermined, and that the PCA subspace method of anomaly detection may be applied to this particular data set [4]. The number of components to be allocated to the normal and anomalous are then determined based on the *knee* in the scree plot [8,4]. We then decide on a window size, and evaluate the magnitude of the projection of the data points onto the anomalous subspace. A binary decision regarding the last point in the window is taken by comparing the magnitude of the projection for this point, with a threshold. The window is then advanced in the next timestep as the next data point arrives, and the process is repeated. Varying the threshold yields the Receiver Operating Characteristic (ROC) curve presented in Section 4.

3.2 Normalized Compression Distance-based Similarity Metric

Au et al. have presented an algorithm in [9] where a set of novel images are stored, and arriving images are compared to this set. A scene is considered anomalous when the maximum similarity between the given scene and all previously viewed scenes is below a given threshold. Similarity is measured using the Normalized Compression Distance (NCD) measure [10].

The NCD measure has been shown to be a versatile and broadly applicable tool for pattern analysis, and problem formulations based on it can be very general, parameter-free, robust to noise, and portable across applications and data formats [11]. Cohen et al. have proposed an information-theoretic algorithm based on NCD to track meaningful changes in image sequences [12]. Yahalom has developed a novel algorithm for web server Intrusion Detection Systems (IDS) using an NCD-based metric, which does not rely on signatures of past attacks [13].

4. EXPERIMENTS

4.1 Data

(a) Normal images at $t = 83$.

(b) Normal images at $t = 144$.

(c) Potentially anomalous images at $t = 30$.

(d) Potentially anomalous images at $t = 21$.

Fig. 1. Set of images obtained from four cameras in the the BRAC University CCTV surveillance system, corresponding to four different timesteps. Normal images are observed in two of the timesteps, while two show the occurrence of potential anomalies.

To test our proposed algorithms on real data, we collected image sequences from a set of four cameras from BRAC University's CCTV system. The raw data comprised of a video sequence in the AVI format. Still images in JPEG format were extracted from the videos at two-second intervals, and Haar wavelet decompositions with 128 coefficients were performed on them. The output of the four cameras was then concatenated to obtain one 512-dimensional row vector of input data corresponding to each timestep. The total data set consisted of 194 timesteps, of which 30 were manually identified as potential anomalous. Figure 1 shows pictures corresponding to four example timesteps. Two show regular (normal) scenarios and the other two show potential anomalies. The headlights of a car have just been turned on in Fig. 1(c)(bottom-right image), while Fig. 1(d) exhibits the more pronounced case of people arriving at the scene(bottom-right image). To be conservative, we identify both as potential anomalies that the operator may wish to be alerted to.

4.2 Results

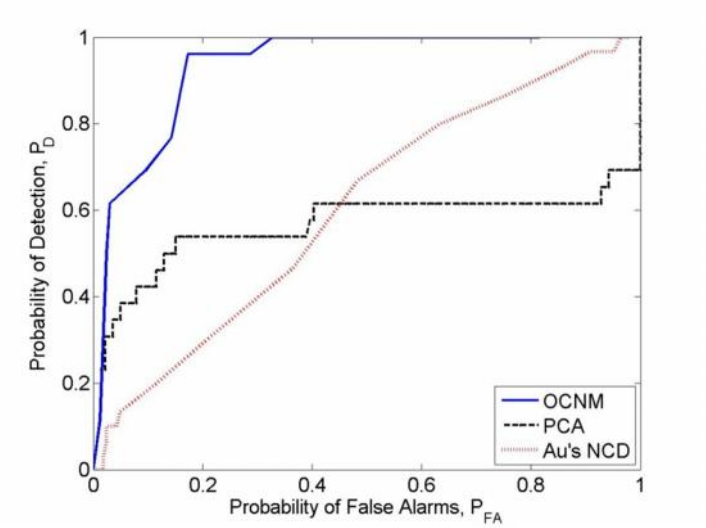

Fig. 2. ROC curves showing performances of proposed OCNM versus existing PCA and Au's NCD [9] algorithms. OCNM is seen to substantially outperform PCA and NCD.

Figure 2 compares the performances of OCNM with PCA and Au's NCD-based algorithm through receiver operating characteristics (ROC) curves, demonstrating the tradeoff between the Probability of False Alarms (P_{FA}) and the Probability of Detection (P_D). The curves were obtained by varying the anomaly detection thresholds for each algorithm. A window size of 30 was used. For OCNM, the nearest-neighbour parameter k was set to two. For PCA, four principal components are assigned to the normal subspace, while Au's NCD-based algorithm was run using her recommended settings [9]; these yielded the best results for PCA and NCD. It is evident from Fig. 2 that the performance of OCNM is substantially superior to those of PCA and NCD. Moreover, OCNM is easily able to achieve almost-perfect detection rates. The low performance of the NCD algorithm may be attributed to the fact that this

algorithm requires a significantly longer training period, and needs to maintain a significantly larger database of images to compare new arrivals against [9].

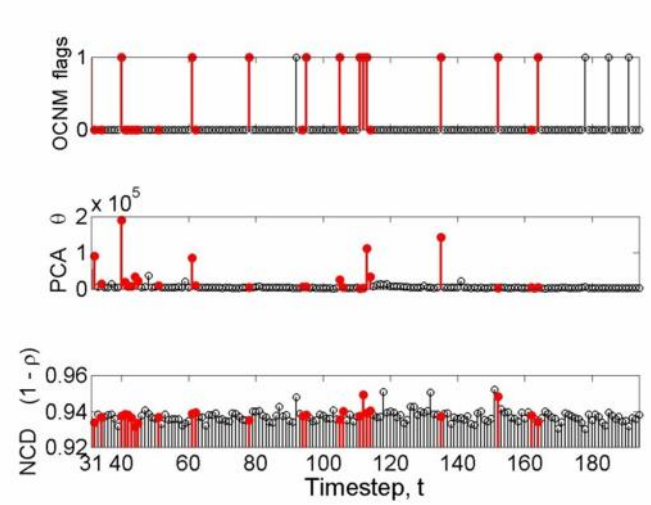

Fig. 3. Progression in the anomaly detection statistics for each algorithm. Top panel: Timesteps flagged by OCNM. Middle panel: Magnitude of projection onto the residual subspace, θ_t, for PCA. Bottom panel: $1-\rho_t$, where ρ_t is Au's NCD-based similarity metric [9]. The true anomalies are indicated as red stems with filled circles.

Figure 3(top panel) shows the timesteps that OCNM signals as anomalous, for the representative value of pre-specified fraction μ = 0.90 set to identify the 10% outliers. The location of the "true" anomalies, as we manually identified, are indicated as red stems with filled circles. Comparison with PCA presented in Fig. 3(Middle panel) and NCD presented in Fig. 3(Bottom panel), indicates that OCNM does the best job of isolating the identified anomalies, in agreement with the ROC curve from Fig. 2.

5. CONCLUSION

In this paper, we have presented a novel approach to performing real-time intruder detection in a surveillance system with inexpensive components. We have proposed the One-Class Neighbor Machine (OCNM) algorithm that is based on the theoretical concept of Minimum Volume Sets (MVSs). Through application to a set of real data from BRAC University's CCTV network, and comparison with two algorithms from two popular families of algorithms used for this purpose, we have demonstrated high detection rates and superior performance.

Our future work will focus primarily on integrating face detection algorithms to learn the characteristics of the regular visitors to the applicable premises [14]. In addition, we wish to investigate combined performance on multimedia sensor data.

REFERENCES

[1] M. Valera and S. Velastin, "Intelligent distributed surveillance systems: A review," *IEE Proc.-Vis., Image and Signal Process.*, vol. 152, pp. 192–204, Apr. 2005.

[2] A. Muñoz and J. Moguerza, "Estimation of high-density regions using one-class neighbor machines," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 28, no. 3, pp. 476–480, Mar. 2006.

[3] 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, Apr. 2007.

[4] T. Ahmed, S. Ahmed, S. 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.

[5] J. Einmal and D. Mason, "Generalized quantile processes," *Annals of Statistics*, vol. 20, no. 2, pp. 1062–1078, Jun. 1992.

[6] N. Verbeke and N. Vincent, "A PCA-based technique to detect moving objects," in *Image Analysis*, B. Ersbøll and K. Pedersen, Eds. Berlin/Heidelberg, Germany: Springer, Jul. 2007, vol. 3633/2005, pp. 641–650.

[7] T. Wang and I. G. amd P. Shi, "Object tracking using incremental 2DPCA learning and ML estimation," in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Process. (ICASSP)*, Honolulu, HI, USA, Apr 2007.

[8] A. Lakhina, K. Papagiannaki, M. Crovella, C. Diot, E. Kolaczyk, and N. Taft, "Structural analysis of network traffic flows," in *Proc. ACM SIGMETRICS*, New York, NY, Jun. 2004.

[9] C. Au, S. Skaff, and J. Clark, "Anomaly detection for video surveillance applications," in *Proc. IEEE Int. Conf. Pattern Recognition (ICPR)*, Hong Kong, Hong Kong, May 2006.

[10] M. Li, X. Chen, X. Li, B. Ma, and P. Vitanyi, "The similarity metric," *IEEE Trans. Information Theory*, vol. 50, no. 12, pp. 3250–3264, Dec 2004.

[11] E. Keogh, S. Lonardi, and C. Ratanamahatana, "Towards parameter-free data mining," in *Proc. ACM SIGKDD*, Seattle, WA, USA, Aug. 2004.

[12] A. Cohen, C. Bjornsson, S. Temple, G. Banker, and B. Roysam, "Automatic summarization of changes in biological image sequences using algorithmic information theory," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 31, pp. 1386–1403, Aug. 2009.

[13] S. Yahalom, "URI anomaly detection using similarity metrics," Master's thesis, Tel-Aviv University, Tel Aviv, Israel, May 2008.

[14] R. Chellappa, C. Wilson and S. Sirohey, "Human and machine recognition of faces: a survey," Proc. IEEE, vol. 83, pp. 705–741, May 1995.