Journal of Engineering and Applied Sciences 12 (Special Issue 12): 9376-9381, 2017
ISSN: 1816-949X

A Comparative Analysis of Machine Learning Based Anomaly Detection Techniques in Video Surveillance

Vijay A. Kotkar and V. Sucharita
Department of Computer Science and Engineering, K L University,
Vijayawada Andhra Pradesh (AP), India

Abstract: In recent years, video surveillance systems have been commonly adopted around the world because of security concerns and their low hardware cost. Anomaly detection is one of the research areas in the field of video surveillance. In this study, different existing cluster based, EM clustering and classification based anomaly detection techniques in video surveillance are discussed. The video surveillance system includes background modeling, object detection, object tracking, activity recognition and classification. Recently, the machine learning based anomaly detection techniques plays a major role in the classification of the events into normal and abnormal events. The new approaches like the combination of Convolution Neural Network (CNN) and Recurrent Neural Network (RNN) and cascade deep learning are the robust algorithms for large datasets.

Key words: Abnormal behavior, anomaly detection, event detection, suspicious activity, video surveillance, detection

INTRODUCTION

In India, Mumbai serial bomb blast in 1993, attack on parliament in 2001, attack on Taj Hotel Mumbai in 2008 and different antisocial activities attracted researcher towards the automatic video surveillance system. Now a days, it is found that the most of the public places like colleges, bus stops, railway stations, shopping malls, etc. are under surveillance of CCTV cameras. The video data is captured and it is useful to prevent and record the event for forensic evidence. The human can monitor such activities from the remote place but the monitoring of the videos 24/7 is the difficult task as if misses of few seconds of footage. Another issue of existing method is when the multiple cameras have to be monitoring at the same time, then it become tedious to watch the important event in the scenario. Hence, there is a need for the robust automatic video surveillance detection system.

A vision-based surveillance system can be a solution for an existing method. It preprocesses, segment and classifies the activity into normal and abnormal activity. A vision-based surveillance system can be a solution for manual monitoring method. It preprocesses, segment and classifies the activities into the normal and abnormal activity using defined algorithm. Numbers of algorithms has been developed in computer vision to process image and video. The field of image processing and computer vision will be one of the solutions to automate for monitoring the suspicious activity in the scene. The vision based systems are useful when the amount of data to be processed small but large data to be analyzed, machine learning and data mining techniques are useful.

The recent video surveillance has some problems. When human observed the video sequences, he perceives the video events as the high-level semantic concept but it is not possible for computer-based surveillance. The main difficulty in the video surveillance systems is in the conversion of low-level problems into high-level, meaningful activity classification (Chuang *et al*., 2009). The present video surveillance system is mostly human dependant where the content of data is the monitor for suspicious or abnormal activity. These systems can give evidence after an event has occurred. Hence, there is need of fast, reliable, efficient, robust approach to detect the activity before and after an occurrence of the causality. To develop such a system reliable, quick and environment independent algorithm are required. Before discussing the method to detect anomalies, next section explains the concept of the anomaly in detail.

Anomaly: Term anomaly is referring to as the something which differs from the standard. This term is also used to express irregularity, inconsistency, inconsistency, abnormality, etc.

Anomaly detection: Anomaly detection is finding the problem in the data pattern which is unexpected or standard. In recent year's anomaly has an application like

Corresponding Author: Vijay A.Kotkar, Department of Computer Science and Engineering, K L University, Vijayawada, Andhra Pradesh (AP), India

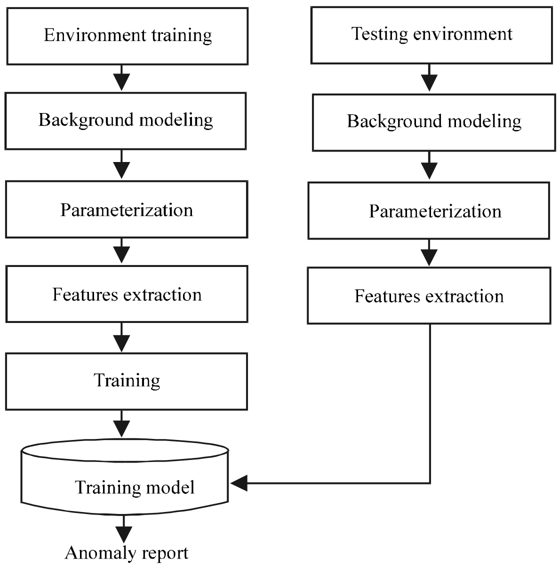

Fig. 1: Generalized methodology of anomaly detection

fall detection in health care domain, enemy detection, military vehicle detection in military surveillance, abandoned bag detection, suspicious activity detection in public surveillance, traffic jam detection, accident detection in traffic monitoring domain, etc. Anomaly detection translates the important and significant information in the actionable information, hence, it has importance in the computer vision domain (Agrawal and Agrawal, 2015).

Generalized block diagram of anomaly detection system: The generalized flow of the automatic anomaly detection system is as shown in Fig.1. The generalized block diagram consists of two essential parts, i.e., Training and testing. The background modeling is the basic step for any motion detection algorithms. The background model prepared as per environment. There are different types of anomalies discussed earlier such as crowd scene, fall detection, abandoned bag detection, traffic events, etc., so, anomalies required different parameterization consideration. Parameterization consist of preprocessing, segmentation techniques. Preprocessing is the step which processed the data which make data suitable for the further processing. The feature extraction step extracts the valuable information about the anomalous behavior or anomaly. The extracted features used for modeling the classification model. The testing environment is tested with the trained model to classify the activity into normal and abnormal.

MATERIALS AND METHODS

Anomaly detection using machine learning techniques: Machine learning and data mining is the grooming field in recent years. It has an ability to analyze a significant amount of data and leads to classifying the data into respective classes strongly. In anomaly detection, training databases are large and feature to be analyzes are more, so, utilization of proper machine learning methods will be the right choice.

In this study, different techniques of anomaly detection have been reviewed which mostly focused on machine learning techniques. Some of the machine learning techniques explained as follow:

Cluster-based: The cluster is the separation of the same data into different groups. The data in each group is similar to the other data in the same group and differ from other groups. Clustering techniques are unsupervised algorithm where algorithm detects the anomalies without prior knowledge. There is various clustering method explained below to detect anomalies in the video scene (Rao *et al*.,, 2011).

K-mean: K-mean clustering method, differentiate the number of data points into k-number of groups called the cluster. The value of k is user define value. The example of this approach is Network Data Mining (NDM) technique which uses the k-mean clustering algorithm to segregate the time intervals with normal and abnormal traffic in the training phase. The cluster centroid is taken as the threshold to label the new data.

K-medoids: Similar to the k-mean clustering another approach of clustering is k-medoids clustering. The only difference is the representation of the clusters. Unlike the k-clustering method, groups in the k-medoids are represented by the centric object in the cluster. It is more accurate than the k-mean because it provides good results in the presence of noise and outliers. This method detects network anomalies which contain unknown intrusion. It has been compared with various other clustering algorithms and has been finding out that when it comes to accuracy, it produces much better results than k-means (Agrawal and Agrawal, 2015).

EM clustering: The extension of the k means the method which is based on the mean of the clusters. This approach labeled the similar data into the similar group by calculating the mean of the cluster. In this method, the assigned label to the cluster according to the weight of probability functions. When compared to k means and k medoids, EM outperformed them and resulted in higher accuracy.

Hierarchical clustering: Hierarchical clustering is a method of cluster analysis which builds a hierarchy of clusters. Hierarchical clustering involves creating clusters

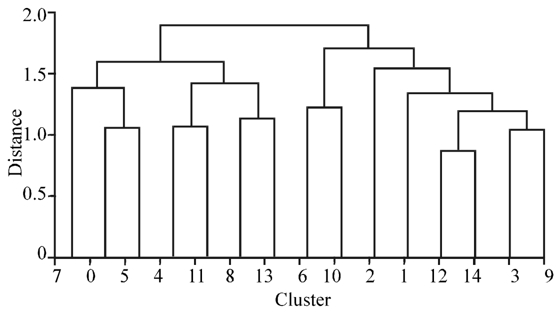

Fig. 2: Types of hierarchical clustering (Dendrogram)

that have a fixed ordering from top to bottom. All files and folders on the hard disk are organized in a hierarchy is one of the examples of this clustering.

Figure 2 shows that, the types of Hierarchical clustering, divisive and agglomerative in a divisive method, assign all of the observations to a single cluster and then partition the cluster to two least similar clusters. Finally, recursively on each cluster until there is one cluster for each observation.

Classification based: Classification is nothing but a problem of identifying the class of new instances on the source of a training set of data containing remarks whose category membership is recognized. The category can also be known as the class label. Various instances can fit into one or many of the class labels. In machine learning, classification is an example of supervised learning, in this learning where a training set of correctly-identified remarks is available. An algorithm that implements classification is called as a classifier. It is constructed to guess categorical labels or class label attribute. In anomaly detection, it will classify the data generally into two categories namely normal or abnormal. Following are standard machine learning technologies in anomaly detection.

Supervised: In this learning, all data is labeled and the algorithms are trained to expect the output from the input data. The process of this algorithm is learning from the training dataset can be thinking of as a teacher supervising the learning process. The algorithm makes predictions on the training data and is corrected by the teacher. If an acceptable level of performance is got, then stops the learning. Supervised learning problems can be further categorized into regression and classification problems. A classification is when the output variable is a category such as “black” or “pink” or “disease” and “no disease”. Regression is when the output variable is the actual value such as “age” or “weight” (Lane *et al*., 2016).

Unsupervised: In this learning, all data is unlabeled and the algorithms be trained to the inherent structure from the input data. This learning is called unsupervised because in this algorithm no correct answer and there is no teacher. Algorithms are left to their devises to discover and present the attractive structure in the data. Unsupervised learning can be further grouped into clustering and association problems. A problem is everywhere you want to find out the inherent groupings in the data such as grouping customers by purchasing behavior. In an association rule learning, trouble is where you want to discover rules that explain huge portions of your data such as people that buy P also tend to buy Q (Agrawal and Agrawal, 2015).

Semisupervised: In this learning, some data is labeled but most of the data is unlabeled and a fusion of supervised and unsupervised techniques can be used. Many actual machine learning problems fall into this area. This is because it can be costly or slow to label data as it may want to access domain experts. While unlabeled data is inexpensive and simple to collect and store. It uses unsupervised learning to find out and study the composition in the input variables and also use supervised learning to make best guess predictions for the unlabeled data, feed that data back into the supervised learning algorithm as training data and use the model to make predictions on new unseen data (Leeuwen *et al*., 2013).

Scenario based anomaly detection: The background scene plays the vital role for object detection. In the indoor environment, the light conditions are controllable while in outdoor the light condition changed frequently. So, background scene is most important factor for anomaly detection. The different environments and anomaly associated with them are explained in this study.

Indoor environment: There are many anomalies in the indoor environment such as fall detection anomalies, here in this anomaly incident of fall of more elderly peoples. Intrusion anomalies are in the smart home environment to detect entrance to a room and exit from a room in the home or office space. This is also used for control heating, ventilation, air conditioning and lighting systems which monitor the people’s well-being. Many individuals with cognitive and physical disabilities can lead independent lives in their homes for extended periods of time. These anomalies are used to perform automated health monitoring (Gunale and Mukherji, 2015).

Crowded environment: In the crowded scene, it is hard to define the anomalies. This is compounded by the discontinuity, sparseness, rarity of an event which limits the training parameter to train the system.

There are various anomaly examples are available for the crowded environment. Abandoned or unknown object detection, abnormal or suspicious behavior of people detection, intruder's detection in mobile obstacles (Borkar *et al*., 2013).

Divergences in dominant patterns are extracted by considering motion and appearance information for crowded scenes.

Traffic: Recently, in the field of video surveillance, the demand of accurate and robust visual-based algorithms increases rapidly for detection, tracking and recognition of objects such as pedestrian, vehicle and so on a robust and efficient anomaly detection algorithm in traffic surveillance system. Traffic anomaly detection using high-performance measurement systems offers the possibility of improving the speed of detection and enabling detection of important, short-lived anomalies.

Some examples of traffic based anomalies are the traffic jam, no entry vehicle detection, vehicle parking anomalies, accident detection, etc. (Kwon *et al*., 2013).

RESULTS AND DISCUSSION

This study briefly surveyed different machine learning based anomaly detection techniques in video surveillance such as Proximity (Prx) clustering for detecting abnormal activities, k-means, HMM, adjacent flow location estimation, sparse semi-nonnegative Matrix factorization and deep neural network methods for detecting anomalies in crowd scenes, local density method for maritime video surveillance, optical flow Based frequent pattern mining for identifying abnormal traffic events, Multivariate Exponentially Weighted Moving Average (MEWMA) for fall event detection. In a novel approach, i.e., combination of CNN and RNN is also used for detecting anomalies in different applications. Below Table 1 summarize different machine learning based anomaly detection techniques.

Table 1: Analysis of machine learnibg based anomaly detection techniques

Paper	Years	Anomaly	Methods	Advantages	Limitation	Research gap
Clustering based anomaly detection						
Unsupervised learning approach eventsin for abnormal event detection in video by surveillance revealing infrequent patterns (Sandhan *et al*., 2013)	2013	Abnormal activity	Proximity (Prx) clustering	Easy way to detect abnormal events	Some motion features are used	Analysis of video higher dimensional features space
Crowd Analysis with Target Tracking, k-means clustering and hidden markov models (Dhanachandra *et al*., 2015)	2012	Crowed scene	k-means and HMM	A dense crowed can not give the same detailed information	Work for small dataset and less crowd	To enhance the larger framework for dataset, larger crowd and group tracking scene
A comparative evaluation of anomaly detection algorithms for maritime video surveillance (Andersson *et al*., 2012)	2011	Maritime video surveillance	Local density technique	Detecting threats with some success	Tracks have minor variations	Coordinated threats using probabilistic relational models
Image segmentation using k-means algorithm and subtractive clustering algorithm	2015	Anomalous Images	k-means	Segmentation quality of image is very good	Partial Streching enhancement is required	To improve the quality of output image by using morphological operations clustering
Anomaly detection: A survey (Chandola *et al*., 2009)	2009	Satellite imaginary				
		Digit recognition Spectro-scopy Mammo-graphic image analysis video surveillance	Mixture of models Regression Bayesian network Neural network Clustering Nearest neighbor based technique	Used for motion detection and regions that appear abnormal on the static images	Large size of the input	Use of online anomaly detection techniques
Classification based anomaly detection						
A novel framework for anomaly detection in video surveillance using multi-feature extraction (Li and Li, 2016)	2016	Appearance anomaly, location anomaly and velocity anomaly	Normality sensitive hashing method anomalies	Separately detect local and global	Different kinds features are extracted of separately	Focus on new methods for instances extraction and efficiency
Anomalous event detection in traffic video surveillance based on temporal pattern analysis (Deepika *et al*., 2016)	2017	Abnormal traffic events	Optical flow based frequent pattern mining	Based on low level pixel features	Not extracting moving objects features	Integration of multiple camerasto incorporate advanced features
A simple strategy for fall event detection (Harrou *et al*., 2016)	2016	Fall events detection	Multivariate Eexponentially Weighted Moving Average (MEWMA)	Provide early alert mechanism	Classifier is not used	Use classifier to true distinguish between and false falls

Table 1: Continue

Paper	Year	Anomaly	Methods	Advantages	Limitation	Research gap
Real time abnormal crowed behavior detection based on adjacent flow location estimation (Wang *et al*., 2016)	2016	Abnormal crowed behavior detection	Adjacent, Flow location estimation	Effective for real time abnormal crowed behavior detection	Sometimes feature points less than a certain values	Uses in social public security
A bayesian ensemble for unsupervised anomaly detection (Yu and Parekh, 2016)	2016	Web properties	Bayesian classifier	Work on unsupervised anomaly detection	Some of the detectors gives correlated errors like dependence, posterior probabilities	To detect dependence among detectors and adjust the posterior probabilities accordingly
Learning to detect anomalies in video surveillance (Xiao *et al*., 2015)	2015	Crowd scene	Sparse Semi-nonnegative matrix factorization	Validating the effectiveness of the framework	Uses only unsupervised learning approach	Work on several benchmark video datasets
Deep learning based anomaly detection:						
Automatic soccer video event detection based on deep neural network combined CNN and RNN (Jiang *et al*., 2016)	2016	Soccer video events	Convolution Neural Network (CNN) Recurrent Neural Network (RNN)	Feature extraction algorithm is not	No suitable and effective dataset	Detection of common complex events
Deep-cascade: cascading 3D deep neural networks for fast anomaly detection and localization in crowded scenes (Sabokrou *et al*., 2017)	2016	Crowded scene	Deep neural network	Fast and reliable for anomaly detection	Detects the patches on their complexity and discriminative power	Work on large patches

CONCLUSION

In this study various machine learning techniques are described with examples that had been proposed in previous years. This study will de definitely useful for researchers to get basic idea about machine learning techniques to detect anomaly. Once the system is implemented then it can be modified for different type of anomalies. Every year it is found that behavior of the anomaly is changes. Hence, in future the generalized machine learning algorithm implementation is the basic need of tomorrow's world. The new approaches like deep learning are the robust algorithm for large dataset.

REFERENCES

Agrawal, S. and J. Agrawal, 2015. Survey on anomaly detection using data mining techniques. Proceedings of the 19th International Conference on Knowledge Based and Intelligent Information and Engineering Systems, September 7-9, 2015, Elsevier, Amsterdam, Netherlands, pp: 708-713.

Andersson, M., J. Rydell, S.L. Laurent, D. Prevost and F. Gustafsson, 2012. Crowd analysis with target tracking, K-means clustering and hidden Markov models. Proceedings of the 2012 15th International Conference on Information Fusion (FUSION), July 9-12, 2012, IEEE, Singapore, ISBN:978-1-4673-0417-7, pp: 1903-1910.

Borkar, A., M.S. Nagmode and D. Pimplaskar, 2013. Real time abandoned bag detection using OpenCV. Intl. J. Sci. Eng. Res., 4: 660-666.

Chandola, V., A. Banerjee and V. Kumar, 2009. Anomaly detection: A survey. ACM. Comput. Surv. CSUR., 41: 1-15.

Chuang, C.H., J.W. Hsieh, L.W. Tsai, S.Y. Chen and K.C. Fan, 2009. Carried object detection using ratio histogram and its application to suspicious event analysis. IEEE. Trans. Circuits Syst. Video Technol., 19: 911-916.

Deepika, R., A.V. Prasath, M. Indhumathi, A.P. Kumar and V. Vaidehi, 2017. Anomalous event detection in traffic video surveillance based on temporal pattern analysis. J. Comput., 12: 190-199.

Dhanachandra, N., K. Manglem and Y.J. Chanu, 2015. Image segmentation using K-means clustering algorithm and subtractive clustering algorithm. Procedia Comput. Sci., 54: 764-771.

Gunale, K.G. and P. Mukherji, 2015. Fall detection using k-nearest neighbor classification for patient monitoring. Proceedings of the International Conference on Information Processing (ICIP), December 16-19, 2015, IEEE, Pune, India, ISBN:978-1-4673-7758-4, pp: 520-524.

Harrou, F., N. Zerrouki, Y. Sun and A. Houacine, 2016. A simple strategy for fall events detection. Proceedings of the 2016 IEEE 14th International Conference on Industrial Informatics (INDIN), July 19-21, 2016, IEEE, Poitiers, France, ISBN:978-1-5090-2871-9, pp: 332-336.

Jiang, H., Y. Lu and J. Xue, 2016. Automatic soccer video event detection based on a Deep Neural Network Combined CNN and RNN. Proceedings of the 2016 IEEE 28th International Conference on Tools with Artificial Intelligence (ICTAI), November 6-8, 2016, IEEE, San Jose, California, USA., ISBN:978-1-5090-4459-7, pp: 490-494.

Kwon, E., S. Noh, M. Jeon and D. Shim, 2013. Scene modeling-based anomaly detection for intelligent transport system. Proceedings of the 2013 4th International Conference on Intelligent Systems Modelling and Simulation (ISMS), January 29-31, 2013, IEEE, Bangkok, Thailand, ISBN:978-1-4673-5653-4, pp: 252-257.

Lane, B., M. Poole, M. Camp and K.J. Murray, 2016. Using machine learning for advanced anomaly detection and classification. Proceedings of the 17th AMOS International Conference on Advanced Maui Optical and Space Surveillance Technologies, September 20-23, 2016, AMOS, Maui, Hawaii, USA., ISBN:978-1-5108-3288-6, pp: 1-6.

Leeuwen, V.C., A. Halma and K. Schutte, 2013. Anomalous human behavior detection: An adaptive approach. Proceedings of the SPIE Conference on Defense, Security and Sensing, May 23, 2013, SPIE, Bellingham, Washington, USA., pp: 874519-874519.

Li, Q. and W. Li, 2016. A novel framework for anomaly detection in video surveillance using multi-feature extraction. Proceedings of the 2016 9th International Symposium on Computational Intelligence and Design (ISCID) Vol. 1, December 10-11, 2016, IEEE, Hangzhou, China, ISBN:978-1-5090-3558-8, pp: 455-459.

Rao, K.H., G. Srinivas, A. Damodhar and M.V. Krishna, 2011. Implementation of anomaly detection technique using machine learning algorithms. Intl. J. Comput. Sci. Telecommun., 2: 25-31.

Sabokrou, M., M. Fayyaz, M. Fathy and R. Klette, 2017. Deep-cascade: Cascading 3d deep neural networks for fast anomaly detection and localization in crowded scenes. IEEE. Trans. Image Process., 26: 1992-2004.

Sandhan, T., T. Srivastava, A. Sethi and J.Y. Choi, 2013. Unsupervised learning approach for abnormal event detection in surveillance video by revealing infrequent patterns. Proceedings of the 2013 28th International Conference on Image and Vision Computing New Zealand (IVCNZ), November 27-29, 2013, IEEE, Wellington, New Zealand, ISBN:978-1-4799-0883-7, pp: 494-499.

Wang, G., H. Fu and Y. Liu, 2016. Real time abnormal crowd behavior detection based on adjacent flow location estimation. Proceedings of the 2016 4th International Conference on Cloud Computing and Intelligence Systems (CCIS), August 17-19, 2016, IEEE, Beijing, China, ISBN:978-1-5090-1256-5, pp: 476-479.

Xiao, T., C. Zhang and H. Zha, 2015. Learning to detect anomalies in surveillance video. IEEE. Signal Process. Lett., 22: 1477-1481.

Yu, E. and P. Parekh, 2016. A Bayesian ensemble for unsupervised anomaly detection. Cornell University, Ithaca, New York. https://arxiv.org/abs/1610.07677.