Techniques and Challenges in Building Intelligent Systems: Anomaly Detection in Camera Surveillance

Dinesh Kumar Saini, Dikshika Ahir and Amit Ganatra

Abstract Security is tedious, complex and tough job in today's digitized world. An attempt is made to study and propose an intelligent system for surveillance. Surveillance camera systems are used for monitoring and controlling the security. Anomaly detection techniques are proposed for designing the intelligent control system. In the paper challenges in detection and processing of anomaly in surveillance systems are discussed and analyzed. Major components related to an anomaly detection technique of camera control system are proposed in the paper. Surveillance data is generated through camera, and then this data is transmitted over the network to the storage. Processing is to be done on real time basis and if there is any anomaly detected, the system must produce an alert. This paper is an attempt to study soft computing approaches for anomaly detection.

Keywords Surveillance · Systems · Camera · Control · Anomaly · Detection

1 Introduction

Surveillance cameras are used extensively for security purposes. Access and control of these cameras through a remote computer over the web improves the security aspects of the system. The camera control system consists of a set of cameras located at different locations and the cameras are controlled remotely. Multimedia is

D.K. Saini (✉)
Faculty of Computer and Information Technology, Sohar University,
Sohar, Oman
e-mail: dinesh@soharuni.edu.om

D. Ahir · A. Ganatra
Charotar University of Science and Technology, Changa,
Gujarat, India
e-mail: 14pgce001@charusat.edu.in

A. Ganatra
e-mail: amitganatra.ce@charusat.ac.in

S.C. Satapathy and S. Das (eds.), *Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems: Volume 2*,
Smart Innovation, Systems and Technologies 51, DOI 10.1007/978-3-319-30927-9_2

the combination of different media like text, still images, audio, video, animation and graphics [1]. Generally multimedia content is bulky, so the media storage and the cost of transmission are noteworthy. To solve this, media are compressed in file for both streaming and storage. Streaming is a means of sending multimedia information over the internet so that the recipient plays it as it is being transmitted. Multimedia involves buffering mechanism (temporary storage). In that the limited segments of the streamed information is temporary stored for continuous play. Streaming avoids the copy and save/store an entire file. Without store entire file user can play data [2]. In the camera control systems anomaly detection can be used as one of the mechanism for building the intelligent system.

2 Anomaly Detection

Anomaly detection in data is the identification of patterns that do not match with normal behavior. And these anomalous patterns are also referred to as exceptions, outliers, novelties, noise, deviations, discordant observation in different application domain [3]. Anomaly detection in data is important because many times the detected anomalies translate the important, actionable information in many application domains. Here are some examples, in computer network is abnormal traffic pattern is found then it mean that sensitive information is transfer by hack computer to an unauthorized receiver [4].

An anomaly means something unusual, irregular or unexpected behavior that does not match to the normal behavior. Because of many kind of reasons anomalies could be occur in data. For example network intrusion, cyber intrusion, or terrorist activity and break down of a system.

Figure 1 shows a simple example of anomaly in two-dimension data set. In which R1 and R2 are two normal regions. The points which are outside normal region are considered as anomalies. Here point's a1, a2 and points in region a3 are anomalies.

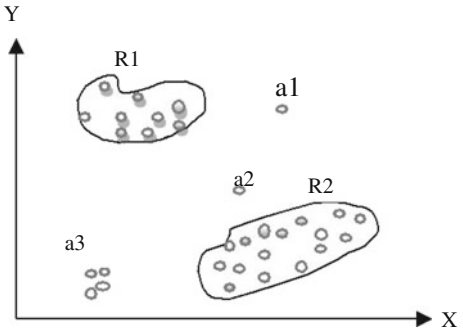

Fig. 1 Anomalies in a two-dimensional data set [5]

2.1 Challenges in Anomaly Detection

A straight forward approach to anomaly detection is defining a region that represents a normal behavior and remaining part that not belong to normal region declared as anomalies. But some factors make this approach very difficult [5].

- It's hard to define a region that comprehends all probable normal behavior. Because the boundary of anomalous and normal behavior is not much accurate. Thus an anomaly observation that situated close to the boundary may be normal or abnormal.
- While anomaly is aeries due to the malicious action, these malicious rivals often accommodate themselves to appear abnormal behavior as normal so the task of labeling normal behavior region becomes more difficult.
- By the time in various application domains, normal behavior is keep growing so the current conviction of normal behavior is may not be enough in future.
- Another challenge is, for different application domain the exact view of anomaly is dissimilar. For example, a small variation in normal reading might be diseases in medical domain. Whereas, in stock market domain small variation might be consider as normal. This makes it complex to apply a particular domain technique to another domain.
- When using recorded and real world datasets, the major issue is labeled data availability.

Sometimes noise is similar to anomaly and it is difficult to distinguish between noise and an anomaly because the data contains noise is analogous to actual anomalies hence it is hard to recognize and remove. Anomalies and noise removal are related to but both are two different things. Since the difference between noise and anomalies is lies in the interest of analyst. Noise can be refer as something unwanted and obstacle to data analyst. While anomalies are consider as something meaningful to data analyst.

3 Different Aspect of Anomaly Detection Issues

3.1 Input Data Nature

Input data nature is core aspect of Anomaly detection. In general the input consists of set of data instances which can call as sample, objects, record, point, vector, entity, pattern, event or case. And all data instance can be defined by a set of attributes. This attributes are also referred as variable, characteristics, feature, field or transmission. There are different types of attributes such are binary, categorical or continuous [5].

In choice of anomaly detection technique the characteristics of attributes have a major impact. For example, in statistical techniques the underlying model is

depends on whether the attributes data types is continuous or categorical. Likewise, in nearest-neighbor-based technique, the distance measure used in technique is determined by the characteristics of attributes.

There is another way of categorizing the input data. It is based on the relationship between the data instance. Mostly the anomaly detection technique deals with single point data. In point data there is no relationship among the data instance.

3.2 Data Labels

Data labels describe whether the data instance is normal or anomalous. Data labeling is expensive and usually it is done by human expert.

The systems are becoming extremely complex and dynamic and to understand the systems behavior it requires exploratory data analysis and descriptive modeling.

3.3 Types of Anomaly

3.3.1 Point Anomaly

Most common type of anomaly is point anomaly and has been focus on most of research. Point anomaly can be defined as an individual entity which is considered as abnormal with regards to other data. In Fig. 1 point a1, point a2 and points in region a3 are point anomalies as they are exterior to the normal region.

3.3.2 Contextual Anomaly

Contextual anomaly is also known as conditional anomaly. It can be defined as in some specific context if a data instance is anomalous then it is contextual anomaly. These types of anomalies are usually found out in spatial data and time series data.

3.3.3 Collective Anomaly

Collective anomaly can be defined as a set of related data instances which is anomalous with regard to remaining data in data set. Individual entities may not be anomalies by themselves in collective anomalies but their occurrence to gather is considered anomalous.

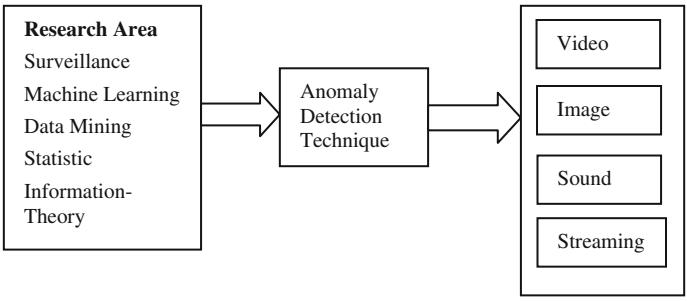

Fig. 2 Key component related to an anomaly detection technique of surveillance camera

4 Application Domain of Anomaly Detection

There are varieties of application domain for anomaly detection; such are network intrusion detection, industrial damage detection, machine learning, statistic, fraud detection, image processing, video surveillance, intrusion detection, medical science and public health. Figure 2 illustrates the component of camera control system associate with anomaly detection techniques [6]. In camera control system Input data for anomaly techniques are video data, image data, sound, or streaming. How this system work is described in next section.

5 Camera Control System

Figure 3 shows the basic block diagram for camera control system. Source in surveillance system is camera and the target is the entity or entities. The target consists of entities in which anomaly detection technique is used to find anomalies. Example of target can be crowds, road traffic, individuals, or network traffic. Data is taken from source and stored at server. From server streaming (streaming is transferring of data) of data is next part. Data can be type of text, image, voice, animation, or video. Streaming can be done in real-time/online or offline.

At server processing of data is done, this data can be recording or imaging. But this system is only focus on image and video part. Image processing is one part of this system. Processing of image is done by mathematical operations. At receiver side data preprocessing is done [7]. Data preprocessing includes editing, cleaning, modify, and feature extraction. Feature extraction is an essential preprocessing step. Feature extraction is used to reduce the required amount of resource to

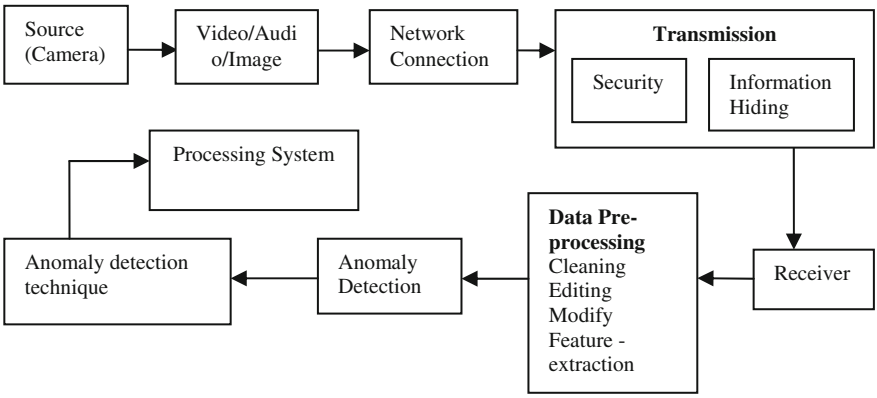

Fig. 3 Block diagram for camera control system an intelligent system

describe the large amount of data. It starts from initial set of calculated data and then it constructs resultant values. Feature extraction include edge detection, corner detection etc. From feature extraction the data is derived [8, 9].

Modeling and simulation predict the behavior of data that under what condition and in which way a part could fail and how it will behave. Soft computing technique is used in simulation and modeling. Soft computing techniques are statistical, mathematical, neural network, fuzzy logic, Bayesian, genetics. Soft computing techniques are statistical, mathematical, neural network, fuzzy logic, Bayesian, genetics.

6 Soft Computing Approaches and Learning

Various Soft computing techniques can be implemented in anomaly analysis. Those are Neural network, Artificial neural network, Fuzzy logic, Clustering, Decision tree, Genetic algorithm.

Fuzzy logic in anomaly detection can be used to manage ambiguity in normal verses abnormal determination. It can also be used in allocating a membership to a class which determines abnormal behavior. Artificial neural network is the mathematical model for machine learning. In which individual node are identified as neurons which are linked together in network [10]. Three layers are input, output and hidden. SVM (support vector machine) method is used in ANN as classification method to find linear separating in two dimensional planes between two classes of data.

6.1 Soft Computing Learning Methods

Learning methods in soft computing for anomaly detection are

1. Supervised learning,
2. Unsupervised learning
3. A priori knowledge application [11].

6.1.1 Supervised Learning

In supervised learning method an algorithm learns a model from training data (representative set of data). All these element of set is labeled with its class. Four methods are includes in supervised learning method for anomaly detection [11]:

1. Learn only normal events consisting from data.
2. Learn only an anomalous events consisting from data.
3. Learn both events.
4. Learn multiple classes of events.

Among this method 1 and method 2 lies in one-class classification problem. Method 3 lies in two-class classification problem. And method 4 is for multiclass problem.

1. **Learn normal events**

This is the most common approach for anomaly detection usually used in automated surveillance system. It trains an algorithm for normal event and then all the events which are outside the class are classify as anomalous. Benefit of this method is that it doesn't require data set from anomalous events. However, problem with this method is it may suffer from high rates of false positives because an event may be detected as anomalous which is not adequately represented in training data set.

2. **Learn anomalous events**

This is the least common approach in supervised learning method. Reason for avoidance is that there is a high risk in missed detection of abnormal events which are not fit into the learned pattern. Zhang et al. [1] used this method of learning for a system to retrieving anomalous events recorded in video surveillance.

3. **Learn normal and abnormal events**

This is a two-class approach. In this method normal and abnormal events are learned. The training data consist of the labeled examples of normal and anomalous events. This method can work well when the anomalous events are correctly defined and well characterize in the data set. Success to this approach is depending on the previous assumption of definition of anomalousness.

4. **Learn multiple classes of events**

This is multiple class approach in which behavior classification operation is performed. In this approach detection anomaly is found out by rules defined in initial classification. An issue to this approach is that only learned event can recognize reliably.

6.1.2 Unsupervised Learning

An unsupervised learning method involves normal and anomalous training data without labels. A simple assumption is made in this approach. The events which occur more frequently are declared as normal, and the events which occur rarely are declared as anomalous. Benefit of this method is that it doesn't require labeling of training data set. Unsupervised learning methods typically take clustering approach for anomaly detection [7]. In clustering approach, anomalies are detecting by distance of unobserved data points from closest cluster.

6.1.3 A Priori Modeling

There is no requirement of training data (labeled or unlabeled) in this approach. This method creates models or rules by applying external knowledge to domain for normal and anomalous classes. A key point to success of this technique is the use of external knowledge to given target. Precision and usefulness of knowledge to given domain is important part for designing proactive defense [12].

7 Classification of Anomaly Detection Techniques

Figure 4 shows the classification of anomaly detection techniques by classes. Main classes of anomaly detection are nearest neighbor based, classification based, clustering based, spectral, statistical, information theoretic [13]. Every technique has its own pros and cons. There are several anomaly detection techniques in variety of application domain but this paper only focus on those techniques which are used in video surveillance domain. Within surveillance domain there are different application areas like public area, land transport, maritime, under water, land transport, air. These techniques are used to identify abnormality in data.

Automated anomaly detection processor is proposed by Kraiman et al. [3] that use multi surveillance data and sensor data to identify and describe events and objects of military area. AADP use clustering algorithm SOM to training data set to classify new observation as normal or anomalous. AADP use Gaussian mixture model [5] and Bayesian analysis [5] for automate the anomaly detection.

Ye et al. [2] proposed a wireless video surveillance system for maximizing the quality of received video. In this system it uses the Gaussian mixture model to detect

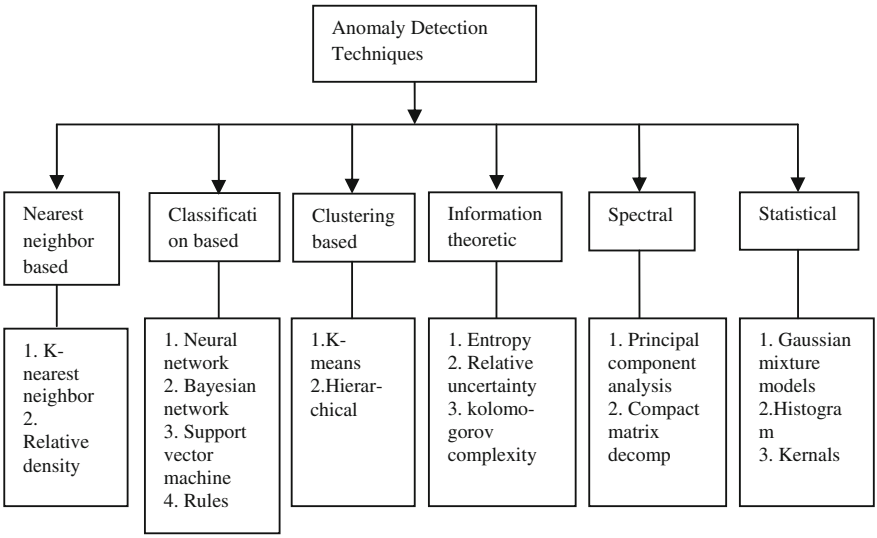

Fig. 4 Classification of anomaly detection techniques

abnormality. It is temporal learning process that models different condition of pixels at different position. Value of each Gaussian model is updated and the pixels which are not matching with any background model are detected and consider as anomaly.

8 Anomaly Detection Post Processing

Clustering and Aggregation is used for designing system level handling of false alarm. Aggregation can be used for analyzing flows of detected anomalies. After aggregation ranking can be done for the anomaly based on its severity. The post-processing mechanism allows constructing easy-to-interpret and easy-to-visualize ranked results, providing insights and explanations about the detected anomalies to the network operator. This allows us to prioritize its time and reduce its overall workload on the proposed system [14]. Post processing is an important issue that reduce lot of overhead in generating alert system.

9 Conclusion

Various Techniques are used in building Surveillance security systems. In this paper anomaly detection technique is used for detection of an abnormal behavior of the system to predict and generate alerts. Various soft computing approaches are

analyzed and propose to build Intelligent System. These proposed techniques can be used for designing proactive defense systems. In security surveillance camera control systems data is streamed and then analyzed on real time basis using various soft computing techniques which helps in classifying the anomalies. Various techniques like nearest neighbor, classification based, information theoretic clustering based, spectral and statistical are some of the techniques which can be used for anomaly classification in building the intelligent systems.

10 Limitation and Future Research Directions

In this paper we are proposing various techniques of anomaly detection but implementation on actual testbed is not carried out. Real testbed can set up and then all techniques can be implemented and comparison can be made which technique is more effective.

References

1. Zhang, C., Chen, W., Chen, X., Yang, L., Johnstone, J.: A multiple instance learning and relevance feedback framework for retrieving abnormal incidents in surveillance videos. J. Multimedia **5**(4), 310–321 (2010)
2. Ye, Y., Ci, S., Katsaggelos, A.K., Liu, Y., Qian, Y.: Wireless video surveillance: a survey. In: Access, IEEE, vol. 1, pp. 646–660 (2013). doi:10.1109/ACCESS.2013.2282613
3. Kraiman, J.B., Arouh, S.L., Michael, L.W.: Automated anomaly detection processor. In: Proceedings SPIE 4716, Enabling technology for Simulation Science VI, p. 128, 15 Jul 2002
4. Saini, D.K.: Security concerns of object oriented software architectures. Int. J. Comput. Appl. **40**(11), 41–48 (2012)
5. Chandola, V., Banerjee, A., Kumar, V.: Anomaly detection: a survey. ACM Comput. Survey **41**, 15 (2009)
6. Wang, Y.-K., Fan, C.-T., Cheng, K.-Y., Deng, P.S.: Real-time camera anomaly detection for real-world video surveillance. In: Proceedings of Machine Learning and Cybernetics (ICMLC) Conference IEEE, vol. 4, pp. 1520–1525, Jul 2011
7. Li, H., Achim, A., Bull, D.: Unsupervised video anomaly detection using feature clustering. IET Signal Proc. **6**, 521–533 (2012)
8. Maybury, M.: Information fusion and anomaly detection with uncalibrated cameras in video surveillance. In: Multimedia Information Extraction: Advances in Video, Audio, and Imagery Analysis for Search, Data Mining, Surveillance and Authoring, vol. 1, pp. 201–216. Wiley-IEEE Press (2011). doi:10.1002/9781118219546.ch13
9. Li, W., Mahadevan, V., Vasconcelos, N.: Anomaly detection and localization in crowded scenes. IEEE Trans. Pattern Anal. Mach. Intell. **36**(1), 18–32 (2014). doi:10.1109/TPAMI.2013.111
10. Xiao, T., Zhang, C., Zha, H.: Learning to detect anomalies in surveillance video. Signal Process. Lett. IEEE **22**(9), 1477–1481 (2015). doi:10.1109/LSP.2015.2410031
11. Nguyen, V., Dinh P., Duc-Son, P., Svetha, V.: Bayesian nonparametric approaches to abnormality detection in video surveillance. Ann. Data Sci. **2**(1), 21–41 (2015). doi:10.1007/s40745-015-0030-3

12. Saini, D.K., Saini, H.: Proactive cyber defense and reconfigurable framework for cyber security. Int. Rev. Comput. Softw. (IRCOS) **2**(2), 89–98 (2007) (Italy)
13. Steinwart, I., Hush, D.R., Scovel, H.: A classification framework for anomaly detection. J. Mach. Learn. Res. (2005)
14. Mazel, J., Casas, P., Fontugne, R., Fukuda, K., Owezarski, P.: Hunting attacks in the dark: clustering and correlation analysis for unsupervised anomaly detection. Int. J. Netw. Manage. **25**(5), 283–305 (2015)

http://www.springer.com/978-3-319-30926-2

Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems: Volume 2

Satapathy, S.C.; Das, S. (Eds.)
2016, XVI, 617 p. 254 illus., Hardcover
ISBN: 978-3-319-30926-2