Anomaly Detection for Intelligent Video Surveillance: A Survey

G.Gayathri, S.Giriprasad

IJCST Vol. 6, Issue 2, April – June 2015
ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

Abstract
Video anomaly detection plays a critical role for intelligent video surveillance. For an abnormal event detection spatial and temporal contents are considered. Using spatio-temporal video segmentation a new region based descriptor motion context is formed. The basic patch descriptor groups the neighbouring pair. Using dynamic patch grouping the same frames are merged. Then datasets are prepared and searched for best match. Dynamic threshold is determined. The datasets are compared with the original pattern. RGB colour variation can be used to improve the image quality.

Keywords
Anomaly Detection, Motion Context, Dynamic Threshold

I. Introduction
Video Surveillance is the monitoring of the behavior, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them. Through CCTV cameras or internet traffic or phone calls the movements are observed. As a result it is obtained through human intelligence agents and postal interception. The word surveillance comes from a French phrase for “watching over” (“sur” means “from above” and “veiller” means “to watch”), and is in contrast to more recent developments such as sousveillance. Surveillance is used for intelligence gathering, the prevention of crime, the protection of a process, person, group or object, or for the investigation of crime. This can be achieved by determining, observing and by reconstructing. Surveillance can be determined by increasing the chance of being caught, and by revealing the modus operandi and accomplishes. This requires a minimal level of invasiveness. Surveillance can detect by giving human operatives accurate and live situational awareness. Surveillance can help reconstruct an incident through the availability of footage for forensics experts, it again helped by video analytics. Surveillance can also influence subjective security if surveillance resources are visible or if the consequences of surveillance can be felt. In order to determine whether surveillance technology is actually improving surveillance, the effectiveness of surveillance must be expressed in terms of these higher purposes.

A. Anomaly Detection
Anomaly detection refers to the problem of finding patterns in data that do not conform to expected behavior. These non-conforming patterns are often referred to as anomalies, outliers, discordant observations, exceptions, aberrations, surprises, peculiarities or contaminants in different application domains. Of these, anomalies and outliers are two terms used most commonly in the context of anomaly detection; sometimes interchangeably. Anomaly detection finds extensive use in a wide variety of applications such as fraud detection for credit cards, insurance or health care, intrusion detection for cyber-security, fault detection in safety critical systems, and military surveillance for enemy activities. The importance of anomaly detection is due to the fact that anomalies in data translate to significant (and often critical) actionable information in a wide variety of application domains. For example, an anomalous traffic pattern in a computer network could mean that a hacked computer is sending out sensitive data to an unauthorized destination. An anomalous MRI image may indicate presence of malignant tumors. A variety of anomaly detection techniques have been developed in several research communities. Many of these techniques have been specifically developed for certain application domains, while others are more generic. This survey tries to provide a structured and comprehensive overview of the research on anomaly detection.

B. Anomalies
Anomalies are patterns in data that do not conform to a well defined notion of normal behavior. Fig. illustrates anomalies in a simple 2-dimensional data set. The data has two normal regions, $N_1$ and $N_2$, since most observations lie in these two regions. Points that are sufficiently far away from the regions, e.g., points $o_1$ and $o_2$, and points in region $o_3$, are anomalies.

Fig. 1: A Simple Example of Anomalies Using 2 Dimensional Dataset

The “interestingness” or real life relevance of anomalies is a key feature of anomaly detection. Anomaly detection is related to, but distinct from noise removal and noise accommodation both of which deal with unwanted noise in the data.

C. Types of Anomaly
An important aspect of an anomaly detection technique is the nature of the desired anomaly. Anomalies can be classified into following three categories:
1. Point anomalies
2. Contextual anomalies

II. Related Work

A. Anomaly Detection in Crowded Scenes
Anomaly detection is different for both crowded and non-crowded scenes. The popular method used is dense optical flow,
spatio-temporal gradients, PCA models, trajectory modeling. These approaches mainly focus on designing localized video representation that used for anomaly detection in crowded scenes. The representation should have three properties:

1. Jointly model appearance and dynamics of crowd patterns
2. Ability to detect temporal
3. Spatial abnormalities

DT-based models of normalcy is introduced over space and time. Four algorithms are used in this paper namely abnormality detection, mixture of dynamic textures, temporal abnormality detection and spatial abnormality detection. In abnormality detection two types of normalcy is used spatial and temporal. A situation that needs absolute capture of image is named as spatial.

The accuracy of abnormality detection can be improved by MDT. Mixture of dynamic textures takes a sample from a video sequence and look forward to a maximum likelihood collection of spatio-temporal video patches. It is done with the expectation maximization algorithm. Temporal abnormality detection is derived from background subtraction method. It relies on Gaussian mixture. In spatial abnormality detection two steps are done: center surround saliency detection and abnormality detection. Evaluation has two components: anomaly detection using frame level ground truth and anomaly localization using pixel level ground truth.

B. Chaotic Invariants of Lagrangian Particle Trajectories for Anomaly Detection in Crowded Scenes

Anomaly detection is done based on lagrangian particle dynamics and chaotic invariants. This outperforms the state of art and able to handle coherent and incoherent scenes. In a crowd the representation trajectories are calculated for which chaotic invariants are computed. For a crowd flow representation particle advection and representative trajectories are the two steps. In particle advection a video of crowd scene is divided into series of clips with respect to time and represented by matrix. Particle advection is performed to estimate the position of moving particles employing sub-pixel optical flow interpolation.

For each clip the system is again initiated. In representing the trajectories of an object, the image is divided by the moving particles and two clusters are formed. The anomaly detection is insensitive to the number of clusters. After the formation of clusters, the comprehensive model of scene through chaotic invariant dynamics is obtained. It is capable of handling coherent and incoherent scenes. It uses two features based on two chaotic invariants known as largest lyapunov exponent L and correlation dimension D. Based on the representative trajectories anomaly detection and localization is done. The localization of anomaly in terms of position and size.

C. Unsupervised Fast Anomaly Detection in Crowds

Representing the anomalies is not only problem for anomaly detection, making the crowded scene in normal state is also difficult. Because the presence of anomalies can turn the crowd into a confused state. So an unsupervised framework for anomaly detection and localization task is proposed. It uses attractive motion disorder descriptor to directly measure the overall intensities of anomalies. It neglects crowd’s abnormal behavior. This is done by the following steps 1) center surround saliency detection 2) attractive motion disorder descriptors 3) anomaly detection and localization. Motion disorder is measured by standard deviation of motion. Statistical distribution of visual saliency and motion vector matrix is analysed, by using this motion disorder is obtained. Localization of the detected anomalies is obtained using the spatial temporal saliency map. In this paper instead of modeling the normal states, the intensity of anomalies are modeled using attractive motion disorder.

D. Detecting Contextual Anomalies of Crowd Motion in Surveillance Video

Unsupervised anomaly detection aiming automatic mining anomaly behaviours without normal pattern training is mainly focussed. Point anomaly is used to detect an individual behavior instance. It proposes an unsupervised framework using hierarchical Bayesian models. Contextual anomalies are detected in crowded scenes by the following steps 1) motion representation and classification 2) grouping 3) context representation and anomaly detection. Crowd motion is captured by patch-based local motion representation. Non stationary parts are classified as spatio-temporal patches. All the patches are grouped. The pairwise distance between two patches is called martin distance. The crowd is differentiated into two groups of patches based on their movement and the neighbourhood motion. In this paper motion context of pedestrian is considered. So blob representation is used here. A blob grows based on the movement of the pedestrians. Hence the contextual anomalies are characterized by the blob size.

E. Nearest Neighbor Based Anomaly Detection Techniques

The concept of nearest neighbor analysis has been used in several anomaly detection techniques. Nearest neighbor based anomaly detection techniques require a distance or similarity measure defined between two data instances. Distance between two data instances can be computed in different ways. For continuous attributes, Euclidean distance is the correct one. For categorical attributes, simple matching coefficient is mostly used. For multivariate data instances, distance or similarity is usually computed for each attribute and then combined. The measures should be positive-definite and symmetric, but they need not to satisfy the triangle inequality. Nearest neighbor based anomaly detection techniques can be broadly grouped into two categories:

1. Techniques that use the distance of a data instance to its kth nearest neighbor as the anomaly score.
2. Techniques that compute the relative density of each data instance to compute its anomaly score.

Additionally there are some techniques that use the distance between data instances in a different manner to detect anomalies and will be briefly discussed later. Nearest neighbor anomaly detection technique is based on the following definition – The anomaly score of a data instance is defined as its distance to its kth nearest neighbor in a given data set. This basic technique has been applied to detect land mines from satellite ground and to detect shorted turns in the DC field windings of large synchronous turbine-generators. The first set of variants modify the above definition to obtain the anomaly score of a data instance. The second set of variants use different distance/similarity measures to handle different data types. The third set of variants focus on improving the efficiency of the basic techniques.

III. Conclusion

Various methods to detect the anomaly is analysed, considering various set of variants shows improved performance than the others. Blob representation can be efficiently used only in...
pedestrian detection. Representation trajectories can be varied according to the position and size. Anomaly localization using Frame level ground truth and pixel level ground truth shows good performance in crowded scenes.

References

G. Gayathri received her B.E degree in Electronics and communication Engineering from PRIST University, Thanjavur, Tamil Nadu, India. She is pursuing her M.E in Applied Electronics in Coimbatore Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India.

S. Giriprasad received his B.E degree in Electronics and Communication Engineering from Anna University, Chennai, Tamil Nadu, India. He has obtained M.E. in Embedded Systems Technologies from Anna University of Technology, Coimbatore, Tamil Nadu, India. Presently he is working as an Assistant Professor in the department of Electronics and Communication Engineering in Coimbatore Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India. He is pursuing Ph.D. Degree in Anna University, Chennai, Tamil Nadu, India. His present research interest are Computer Vision, Video Surveillance and Advanced Driver Assistance System.