Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 4027 - 4037
Received 20 January 2021; Accepted 08 February 2021.

A Comprehensive Study on Automated Anomaly Detection Techniques in Video Surveillance

P. Mangai Pannirselvam[1], M. Kalaiselvi Geetha[2], G. Kumaravelan[3]

Research Scholar, Department of Computer Science & Engineering, Annamalai University, Annamalainagar, Tamilnadu, India[1],

Professor, Department of Computer Science &Engineering,Annamalai University, Annamalainagar, Tamilnadu, India[2],

Assistant Professor, Department of Computer Science ,Pondicherry University, Puducherry, India[3]

[1]pannirselvammangai@gmail.com

[2]geesiv@gmail.com

[3]gkumaravelanpu@gmailcom

Abstract

Video surveillance systems are the most important aspect of security systems which are having wide range of applications in ourevery day life. In particular, it plays a significant role in remote monitoring of facilities in public and private premises. In this context, video surveillance refers to observing the scenes of improper human behaviours which are termed as real world anomalies. But, the traditional way of involving humans for real world anomaly detection isa time consuming process and involves various overheads. Thus, an automated anomaly detection in video surveillance using intelligent methods becomes an important area of research. This paper gives a comprehensive study on automated anomaly detection in video surveillance based on statistical, proximity, classification, reconstruction and prediction approaches with a special focus towards crime detection. In addition, this paper also highlights various benchmark datasets used in automated anomalydetection in video surveillance.

KeywordsVideo Surveillance, Crime Detection, Machine Learning, Anomaly Detection.

1 INTRODUCTION

With an inexorably developing needs of security for individuals and their properties, video surveillance has attracted a lot of concern in our day-to-day life. Video surveillance systems can adequately improve the safety and security for the administration and the control of public zone. More specifically, observation recordings can catch an assortment of real-world anomalies.Such anomalous events when detected, the authorities can be alerted to react to the situation quickly.Thus, an automated detection of anomalies becomes an important issue which has been studied in various application domains. This paper provides an overview of various approaches used for detecting the real world anomalies in video surveillance with respect to crime detection.

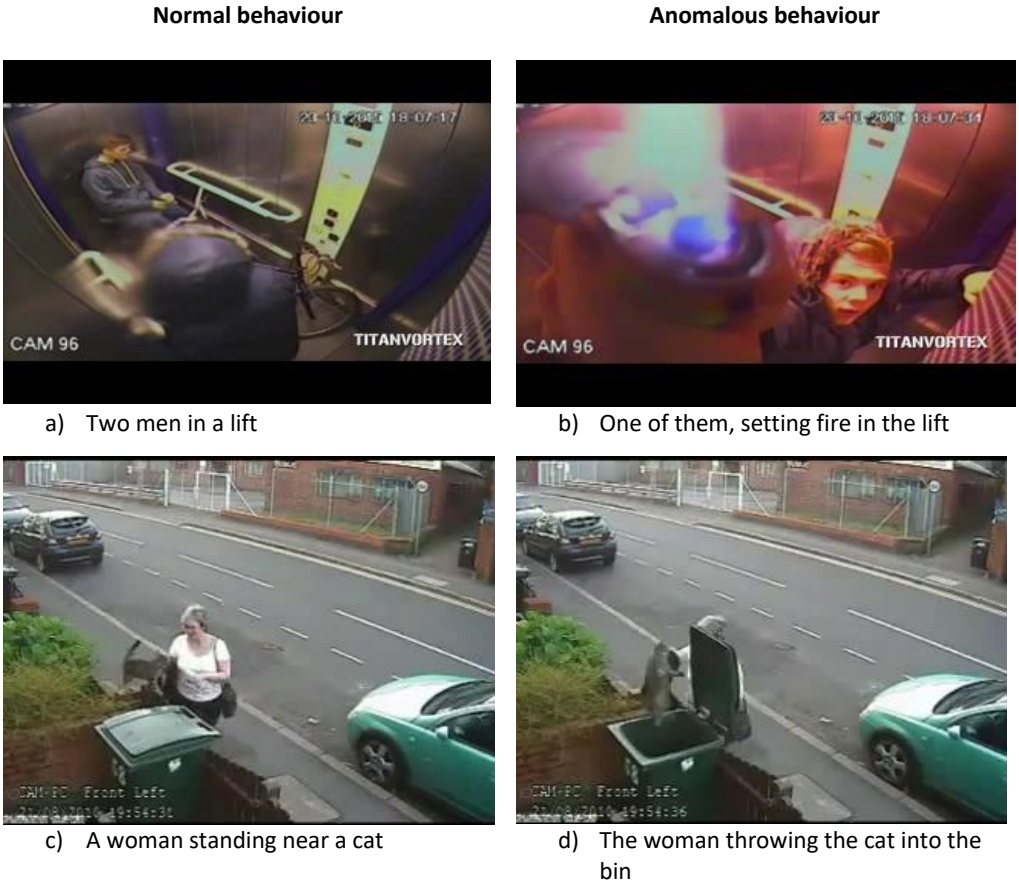
Anomalies, often called outliers, are the data points that do not comply with a normal behaviour notion. Detection of anomalies refers to detecting abnormal behaviour oroccurrences that do not stick to a normal behaviour. The significance of detectinganomalies lies in the fact that data anomalies translate into applicable/actionable knowledge across a broad range of application domains. With the complex systems having multiple components in perpetual motion that continuously redefine the "standard" behaviour, a new proactive approach is required todetect anomalous conduct [1].

Generally, surveillance cameras are progressively used in open areas to improve public safety, e.g. sidewalks, highways, stores, shopping centres, etc. Yet, law enforcement agency's surveillance capability has not kept pace. The consequence is that the use of surveillance cameras and an unworkable ratio of cameras to human monitors pose a conspicuous weakness.

Therefore, a simplistic solution to anomaly detection is to recognize a region reflecting normal behaviour and classify any finding that does not correspond to this normal region as an anomaly in the data. The automated

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 4027 - 4037
Received 20 January 2021; Accepted 08 February 2021.

identification and proper recognition of anything unknown as anomalous is a difficult problem that has been addressed in several different ways over the period of years. In particular, the recognition of anomalous incidents such as road accidents, robberies or other criminal activity playsa significant role in video surveillance.Figure1, depicts some of the examples for normal and anomalous behaviourcaputured in UCF-Crime Dataset. It also reveals that an anomalous eventsare usually seldom occur as compared with regular activities. Most of the existing techniques for detecting anomalies in video surveillance comprises various kinds of problem formulation factors such as existence of the data, accessibility towards the labelled data, type of anomalies to be observed, etc. In addition, conventional forms of data driven algorithms provides only sub-optimal results due to the higher dimensionality of data [2].



a) Two men in a lift

b) One of them, setting fire in the lift

c) A woman standing near a cat

d) The woman throwing the cat into the bin

Figure1. Normal and Anomalous behaviour capturedin UCF-Crime Dataset

Therefore, development of an intelligent computer vision algorithms for detecting anomalies automatically in surveillance videos is a pressing need to mitigate the loss of labour and time [3]. Meanwhile, the goal of any realistic anomaly detection system must be able to signal an occurrence in a timely manner that deviates regular patterns.
The main contribution of the paper is

- To provide a complete study about anomaly detection in video surveillance and its aspects.
- To explore the present contribution in automated anomaly detection of crime in video surveillance
- To discuss various datasets employed for real time anomaly detection.

With this detailed introduction of anomaly detection, the subsequent section2 explains the various taxonomies of anomaly detection.Section 3 explore the challenges in anomaly detection. Section 4explains theapproaches used for detecting anomalous behaviour of humans in surveillance videos. A brief description about the video datasets is surveyed in section 5, followed by conclusion.

1.1 Aspects of Anomaly Detection

A specific formulation of the problem is determined by several aspects such as the characteristics of the input data, the availability (or unavailability) of labels as well as the constraints and requirements induced by the application domain. In this section, the different aspects of anomaly detection problems are discussed.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 4027 - 4037
Received 20 January 2021; Accepted 08 February 2021.

1.1.1 Characteristics of Input Data

The essence of the input data is a significant component of any anomaly detection. One can see the input data as a set of features. The features can be of various types like categorical, binary or continuous. Each data could have either a single attribute or multiple attributes. In addition, the attributes of each data instance can be ofsimilar or different types. The existence of the attributes determines whether anomaly detection techniques are valid. Input data can also be classified depending on the datainstances relationship. Most of the present methods for detecting anomalies deal with recorddata where no relationship issupposed between data instances. The data instances are ordered linearly in sequence data. In spatial data, each instance of data is connected to their neighbouring instances. If spatial data has a temporal aspect, spatio-temporal data is handled by CNN and LSTM for feature extraction [4].

1.1.2 Data Labels

If the instance is normal or anomalous, the labels associated with the data instance denotes it. It should be mentioned that it is always prohibitively costly to collect labelled data which is reliable and reflective of all forms of behaviours. Labelling is often performed manually by a real human and often involves major effort to acquire the identified data set for the training. Moreover, the anomalous behaviour is always complex in nature e.g. new forms of anomalies that occur, for which no training data are labelled. Based on the availability of data labels, the anomaly detection methods can be used in any one of the following learningmodes.

1) Supervised Learning
2) Unsupervised Learning
3) Semi-Supervised Learning

Supervised learning suggests that the training data set is accessible for normal instances and anomaly with correct and representative labels. Semi-supervised learning assumes instances have been classified for just the usual class by training data. In unsupervised learning, detection of anomalies will assume that the whole set of data comprises the normal class and develops a model for normal data and considers deviations from the standard model as anomaly [4].

1.1.3 Types of Anomalies

In general, anomalies can be classified as point anomalies, contextual anomalies and collective anomalies. In point anomaly, the data instance deviates too far from the rest. A person running with a knife in a shopping mall can be termed as a point anomaly. In contextual anomaly, the data instance deviates with a specific circumstance, but not otherwise. In a school zone, if person drives his car faster as compared to others, it can be termed as contextual anomaly. In contrast, it is a normal behaviour in highways. In collective anomalies, a set of data instances concurrently cause deviations, but not individually. A group of people entering a shop can be termed as collective anomalies [5].

1.1.4 Output of Anomaly Detection

Several algorithms used for detecting anomalies output a score based on the anomalous level. These outputs can cover a range of data point dependent parameters. Binary mark specifies whether a data point is an exception. While some algorithms used for detecting anomaliesexplicitly return binary labels, anomaly scores can be represented by binary labels. Scoring based anomaly detection techniques permit the researcher to pick the most significant anomalies using a domain specific threshold. Techniques which provide the training samples with binary labels do not require analysts to take such a choice directly, although this can be managed indirectly by choosing parameters within eachstrategy [5].

2 TAXONOMIES OF ANOMALY DETECTION

This section decribes the various approaches adapted for detectinganomalies in surveillance videos.Figure2 depicts the general process of anomaly detection such as Pre-Processing, Feature Extraction, Anomaly detection Processing using learning techniques and classifying the output as anomalous or normal.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 4027 - 4037
Received 20 January 2021; Accepted 08 February 2021.

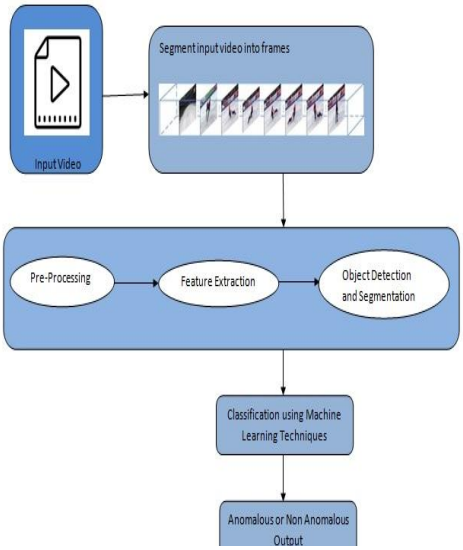


Figure2. Anomaly Detection Process

2.1 Classification of Anomaly Detection Approaches

Anomaly detection approaches can be grouped as Statistical based anomaly detection, Proximity-based anomaly detection, Classification, Reconstruction and Prediction based techniques[5]. Figure 3 depicts the methods used in the above mentioned approaches.

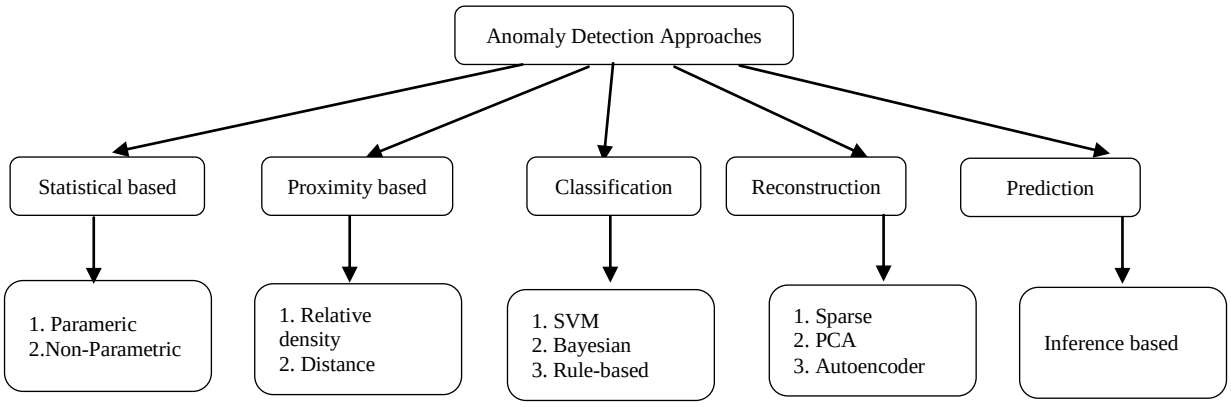


Figure 3.Classification of Anomaly Detection Approaches

2.1.1 Statistical based approach

The Statistical anomaly detection are based on probability distribution or pattern. Normal data instances are part of high probability regions where as anomalies are part of the low probability regions. A statistical model is tested for its fitness and a statistical inference is applied to unkown instances to determine whether it is fitting the model or not. Statistical based approaches can be grouped as Parametric methods and Non-Parametric methods. Parametric methods have the underlying distribution knowledge whereas the Non-parametric methods does not posses the knowledge of the distribution. Gaussian mixture modelsand regression modelsare best examples for Parametric techniques. Histograms and Kernel methods are examples for Non-parametric techniques.

GMM [6], [7] are formed by combining multivariate normal density components. Parameters are estimated using Expectation- Maximization (EM) algorithm which iteratively maximize the likelihood of the set. After obtaining maximum likelihood estimates,the probability density function is calculated for each class for a given data instance. Based on the probability the data instance is identified as normal if it has highest probability or anomalous if it has lowest probability. Regression model based approach [7] determines anomaly detection in two steps. Initially a regression model is fitted on the data instance. Later for each test instance, the residual for the test instance is used to decide the anomaly score. The residual is the part of the instance which is not clarified by the regression model. The magnitude of the residual is then used as the anomaly score for that test instance.

Histogram techniques partition the data instances into several bins based on the features extracted from them. The size of the bin is considered as an important aspect for anomaly detection. Histogram based anomaly detection

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 4027 - 4037
Received 20 January 2021; Accepted 08 February 2021.

approaches [8], [9], [10],[11],[12], [13] extracts the spatitemporal features from the given data instance. The extracted features are processed with Bag of words framework, where the features are represented as a fixed length vector using a histogram to reflect the frequency of different words. If the data instance does not occupy any bin , it is considered as anomalous. Kernel based approach involves kernel functions(Gaussian,Epanechnikov,etc) to estimate the probability density function. A data instance with low probability region is considered as anomalous.

2.1.2 Proximity based approach

The Proximty based methods detect the anomalies by the locality of the data points with the assumption that the normal data points lie in dense neighbourhood,whereas anomalous data pointslie in sparsely populated areas. Proximity based approach can be classified as Relative density based and Distance based. Relative density based approach [14] take into consideration the number of data points in the neighborhood. A data point is considered as anomalous ,if it lies in a neighborhood with low density. On the other case,if the data point lies in dense neighborhood,it is considered as normal. In distance based approach [15], [16] anomalies are identified by the distance of the relative points.A data instance is considered as anomalous,if its neighborhood does not have enough other points.

2.1.3 Classification based approach

The classification approach uses a set of labelled data instances called training data and these instances are used to learn a model. which is termed as classifer. Using the learned model, objects are then categorized as anomalous or non anomalous. Classification based methods can be categorized as one-class classification and multi-class classification. In one-class classification all the training data instance belong to a single label. In multi-class classification, all the training data instance belong to multiple labels.

One-class classification learns a discriminative boundary around the normal data instance.Support Vector Machines (SVM) are used for one-class classification[3], [5], [17], [18]. To classify the data instances, SVM tries to identify good decision boundaries in two stages. In the first stage, an instance is mapped to a new high dimemsional representation to express the decision boundary as a hyperplane. In the second stage, a good decision boundary is computed by maximizing the distance between the hyperplane and the closest data instances from each other.Multi-class classification using SVM [19]breaks down the classification problem into multiple binary-class classification problems. Neural network based multi-class classification [20], [21], [22] first trains the network on the normal data instance to learn the different classes, later each test instance is provided as an input to the neural network for determining the class to which it belongs.

Bayesian methods [23] estimates the posterior probabilityof class label from a set of normal class labels and the anomaly class labels for a given data instance with the assumption that the normal instances are generated by a known probability density function for a set of parameters.The smaller the probability of generating a new observation from the distribution the more anomalous the observation. Rule based classifiers learn rules that capture the normal behaviour . A test instance that does not satisfy such rule is treated as anomaly [24].

2.1.4 Reconstruction based approach

In Reconstruction based anomaly detection methods lower dimensional original data are considered as anomalies and the normal data is isolated from each other. The lower dimensional embeddings are taken back to original data space. This is called Reconstruction and exact nature of the data is found out. Anomaly Score is given based on Reconstruction error. Anomaly detection using Principal Component Analysis (PCA), Autoencoders andSparse techniquesare best examples of Reconstruction based methods.

PCA technique transforms correlated random variables into linear combinations of the orginal variables to express the data in lower dimension. PCA analyse the anomalies by computing its projection on the eigenvectors, along with reconstruction error. The data instance with higher reconstruction error is considered as anomalous [14]. Autoencoders encode data instances into a lower dimension representation, then decode or reconstruct the data instance back to the original representation. Autoencoders are trained mainly using the normal data instances.Anomalous data instances produces high reconstruction error [25], [26].Sparse techniques create a dictionary to encode all the normal data instances with a smaller reconstruction error[27].

2.1.5 Prediction based approach

The Prediction based approaches are based on inferences obtained from a series of data objects. Prediciton score is used to detect anomalies. LSTMs are capable of learning long time dependencies to make prediction regarding the future sequence of the data instance[21], [22], [28].

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 4027 - 4037
Received 20 January 2021; Accepted 08 February 2021.

3 CHALLENGES IN ANOMALY DETECTION

There are several research works contributed by the community for the automated anomaly detection. The contribution includes techniques such as listed below.

- Similarity comparison and finding dissimilarity frames
- Bi-directional prediction and anomaly score estimation based on sliding window
- Non parametric Bayesian regression model built upon Gaussian process priors
- Sparse coding technique
- Graph based self organizing map for data clustering
- Spatio Temporal texture model
- Convolutional autoencoders and Support vector machines
- Multiple instance learning method
- Sub trajectory model by segmenting the medium routes and modified Hausdorff distance
- Two stream fully convolutional neural network
- Ensemble random projection model
- Hierarchical temporal memory scheme

Although the contributed works address many of the challenges existing in the automated anomaly detection,still there are number of challenges which requires enormous efforts and research contributions to get addressed. The following issues and challenges are to be addressed.

- Computation and storage requirements for performing automated anomaly detection using Machine learning techniques.
- Issues in defining all unwanted events, real time model.
- One technique proposed for one dataset not suited for all.
- Cost and Training time of the Automated Anomaly systems.
- False detection, change in learned normal behaviour patterns.
- Low robustness and noisy environment.
- Finding suitable features during feature extraction process.

TABLE I
CRIME DETECTION METHODS AND LIMITATIONS

S. No	Anomalies Addressed	Method used	Limitations
1	Purse snatching, kidnapping and fighting	Object Segmentation And Motion Analysis Techniques - Distance Between Objects, Moving Velocity Of Objects And Area Of Objects Are Considered [16]	Unable to detect more complex crime - kidnapping, fighting.
2	Assault	Human Pose Track Detection [17]	No detection of additional features such as taking out a gun, run etc.
3	Fight	Motion Scale Invariant Feature Transform [18]	Computational overhead, Improvement required to detect real and simulated fight.
4	Aggressive behaviours	Extreme Acceleration Patterns are Estimated using Random Transform to the Power Spectrum of Consecutive Frames [31]	Time taking, relative actions detection not available.
5	Fight	BLOB Features Extraction [32]	Other better techniques are existing.
6	Violence	Local Spatio-Temporal Features with Bag-of-Words [9]	Should be tailored for difference set of violence.
7	Violence in crowd	Heuristic Behaviour Modelled into Equations and Heuristic Map generated [33]	Usage of Fixed size filters .
8	Violence in crowd	Usage of Violent Flow Descriptor[34]	Lack performance when used with larger vocabularies of STIP.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 4027 - 4037
Received 20 January 2021; Accepted 08 February 2021.

9	Violent behaviours	Usage of two Low Level Features (i) Local Histogram Of Oriented Gradient Descriptor And (ii) Local Histogram Of Optical Flow With Bag-Of-Words [10]	Low accuracy rate when texture and statistical features are included.
10	Kicking, pushing, punching	Usage of HOG Features [11]	Dimension of the feature vector is to be optimized to reduce the size for better operation.
11	Violence	Enhanced Local Spatio-Temporal Features With Bag-of-Words [12]	Complex scenarios not addressed.
12	Fight	Oriented Violent Flows [35]	Computation overhead
13	Fight	Improved Fisher Vector,Sliding window [36]	Unable to detect other anomalies apart from fight.

TABLE II
ACCURACY COMPARISION OF VARIOUS CRIME DETECTION TECHNIQUES

S. No	Title	Techniques	Datasets	Accuracy
1	Real-world Anomaly Detection in Surveillance Videos [3]	Deep Multiple Instance Ranking	UCF-Crime	75.44 (Without Constraints) 74.44 (With Constraints)
2	DEARESt: Deep Convolutional Aberrant Behaviour Detection in Real-world Scenarios [20]	VGG-19, Optical Flow combined with FlowNet, ANN	UCF-Crime (Subset)	76.66
3	CNN Features with Bi-Directional LSTM for Real-Time Anomaly Detection in Surveillance Networks [21]	CNN (Pretrained ResNet-50), BD-LSTM	UCF-Crime UCF-Crime2Local	85.53 89.05
4	Real-Time Anomaly Recognition Through CCTV Using Neural Networks [22]	CNN (Pretrained InceptionV3), LSTM	UCF-Crime	97.23
5	Real-time Surveillance based Crime Detection for Edge Devices [13]	Early Stopping Multiple Instance Ranking	UCF-Crime Peliculas	91.3 99.2
6	Deep Reinforcement Learning for Real-world Anomaly Detection in Surveillance Videos [37]	Deep Q Neural Network (DQN)	UCF-Crime	78.2

4 CRIME ANOMALY DETECTION

Feature extraction is the heart of the automated anomaly detection as the extracted features plays a significant role in determining the frames into normal or anomalous after applying the learning and detection. The features extracted are object based or trajectory based. It may also include low level STC or Pixel level extraction. Using neural algorithms automatic feature extraction can also be done [29].Since then computer vision has come a long way, in video surveillance the anomalies can be grouped as local anomalies and global anomalies. Global anomalies can exist in a frame or a portion of the video, without indicating where it has happened. Local anomalies typically occur within a concrete area of the scene [30]. A video can contain different types of visual anomalies, such as a car may unpredictably start making a turn, a person damaging a public property, a person climbing a closed fence, etc. Violence is one such phenomenon that needs to be identified and discussed. In this section, the existing feature

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 4027 - 4037
Received 20 January 2021; Accepted 08 February 2021.

extraction methods for detecting violent behaviour of humans in video surveillance are studied.

Table I summarizes the existing contributions of research community with respect to crime detection in video surveillance. There are lot of works available with regard to the automated anomaly detection. But the works with respect to crime detection in video surveillance is very limited. Most of the existing methods use Support Vector Machine(SVM) for classification of the anomalous and normal activity in crime detection. There are several works reported in specific to the crime detection as given in Table I.The following reported works listed in Table II employed deep learning techniques for feature extraction in the UCF-Crime dataset.

A Deep Multiple Instance Ranking Approach was proposed in [3] for the detection of anomaly in surveillance videos. It used bag of videos that contained anomalous and normal videos. Training labels were used at video level than at the clip levels. The approach proposed in [20], [21] and [22], utilized the idea of transfer learning for extracting appearance and motion features and [21],[22] employed recurrent neural networks (LSTM) for recognizing the anomalous behaviour. In [20] a two-way network was proposed to extract appearance and motion features distinctly from a video segment. Such features were concatenated to create a single vector function which was further used to recognize a violent/normal behaviour. Using VGG-19, the appearance features were extracted while the optical flows between successive frames were measured and was fed to FlowNet to extract motion features. Artificial Neural Network (ANN) was used for classification following convolution of features.

The proposed work in [21] included a framework for extracting spatio-temporal features with a pre-trained ResNet-50 architecture. The anomalous behaviour wasdetected and recognised by utilizing a multilayer BD-LSTM (Bidirectional Long Short Term Memory). The output of the BD-LSTM not only depends on the previous frames, but also on the future frames in the video sequence. The CNN and RNN with advanced object recognition pre trained model inceptionV3 was used in the proposed concept in [22].

4.1 Importance of Predicting Crime Anomaly

Although several contributions have been given for detecting the crime actions in video surveillance, there are very less works available on predicting the crime in video surveillance. Detecting crime anomaly saves the labour and time used for manpower to find out crimes. But real change would be predicting the crime before it happens. The work reported in [38] contributes early recognition of suspicious activity for crime prevention. In this work, the author proposed an action recognition framework for finding the suspicious activity interest point based 2D and 3D transformation approach.

5REAL-WORLD ANOMALOUS VIDEO DATASETS

This section briefs some of the famous real-world anomalous video datasets used for detecting the violent behaviour of humans. All the actions in the datasets were captured in controlled and uncontrolled environments. These datasets differ in the number of human subjects, background noise, appearance, pose variations, etc. and have been generally used for violence detection. Table III summarizes the type of anomalies in various datasets.

UCF-Crime is a large scale dataset with 950 anomalous and 950 normal untrimmed real-world surveillance videos. All the anomalous videos in this dataset are categorized to 13 real world anomalies such as Abuse, Arrest, Arson, Assault, Accident, Burglary, Explosion, Fighting, Robbery, Shooting, Stealing, Shoplifting and Vandalism.

TABLE III
REAL-WORLD ANOMALOUS DATASETS

S.No	Dataset	Anomalies
1	UCF- Crime	Abuse, Arrest, Arson, Assault, Accident, Burglary, Explosion, Fighting, Robbery, Shooting, Stealing, Shoplifting and Vandalism
2	UCF-Crime2Local	Arrest, Assault, Burglary, Robbery, Stealing and Vandalism
3	Hockey Fight	Fight
4	Violence Flows	Violence
5	Peliculas	Fight

UCF-Crime2Local dataset contains 300 real world videos which includes 100 anomalous and 200 normal videos. This dataset contains spatiotemporal annotations to a portion of the UCF-Crime dataset. The anomalous videos are

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 4027 - 4037
Received 20 January 2021; Accepted 08 February 2021.

categorized to six classes such as Arrest, Assault, Burglary, Robbery, Stealing and Vandalism. Hockey Fight contains 1000 real world videos with 500 violent videos and 500 normal videos. The violent videos have the fight scenes happening between two or more participants in the ice hockey rink. Violence Flowscontains 246 real-world videos of crowd violence and non-violence videos. It has 123 violence videos captured in streets, football stadiums, volley ball and ice hockey arenas and schools.Peliculascontains collections of fight scenes from Hollywood movies and some non-fight scenes from football games and other events. Out of 200 total videos, 100 of them are fight videos and 100 of them are non-fight videos.

6 CONCLUSION AND FUTURE DIRECTIONS

This paper includes a comprehensive study on the fundamentals of automated anomaly detection in video surveillance. Taxonomies and challenges in automated anomaly detection are explored. A survey onautomated crime detection in surveillance video is given. The popularly used datasets for crime detection in video surveillance has been presented. This study throws light on the aspects to be concentrated on future research.

The future research challenges includes addressing Computational and Storage complexities, Selecting appropriate features of the video for feature extraction, Choosing the right classifiers are paramount importance for better performance of the automated crime anomaly detection in surveillance videos. The recent techniques greatly employs Support Vector Machine for classification purposes. Advanced classifiers are to be employed for precisedanomaly detection. Methods to reduce errors on classifying the frames are to be improved. Most of the contribution in automated anomaly detection centers around only on detection. Extensive research in predicting or early identification of crime needs to be initiated. Optimization is another important area that needs attention to obtain benefits of reduced cost and time of automated anomaly detection.

REFERENCES

[1] Xu, X., Liu, H., & Yao, M. (2019). Recent progress of anomaly detection. Complexity, 2019, 1-11. https://doi.org/10.1155/2019/2686378

[2] Murphree, J. (2016). Machine learning anomaly detection in large systems. 2016 IEEE AUTOTESTCON. https://doi.org/10.1109/autest.2016.7589589

[3] Sultani, W., Chen, C., & Shah, M. (2018). Real-world anomaly detection in surveillance videos. 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition. https://doi.org/10.1109/cvpr.2018.00678

[4] Chalapathy, R., Khoa, N. L., & Chawla, S. (2020). Robust deep learning methods for anomaly detection. Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. https://doi.org/10.1145/3394486.3406704

[5] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection. ACM Computing Surveys, 41(3), 1-58. https://doi.org/10.1145/1541880.1541882

[6] Y. Li, W. Liu, and Q. Huang. (2017). Traffic anomaly detection based on imagedescriptor in videos. Multimedia Tools and Applications, 75(5), 2487–2505.https://doi.org/10.1007/s11042-015-2637-y .

[7] K. Cheng, Y. Chen, and W. Fang.(2015) . Gaussian process regression-based video anomaly detection and localization with hierarchical feature. IEEE Transactions on Image Processing. https://doi.org/10.1109/tip.2015.2479561 .

[8] Y. Zhang, H. Lu, L. Zhang, and X. Ruan. (2016). Combining motion and appearance cues for anomaly detection. Pattern Recognition, 51, 443–452.https://doi.org/10.1016/j.patcog.2015.09.005 .

[9] De Souza, F. D., Cha, G. C., Do Valle, E. A., & De A Araujo, A. (2010). Violence detection in video using spatio-temporal features. 2010 23rd SIBGRAPI Conference on Graphics, Patterns and Images. https://doi.org/10.1109/sibgrapi.2010.38

[10] Zhou, P., Ding, Q., Luo, H., & Hou, X. (2018). Violence detection in surveillance video using low-level features. PLOS ONE, 13(10), e0203668. https://doi.org/10.1371/journal.pone.0203668

[11] Roy, P. K., & Om, H. (2017). Suspicious and violent activity detection of humans using HOG features and SVM classifier in surveillance videos. Advances in Soft Computing and Machine Learning in Image Processing, 277-294. https://doi.org/10.1007/978-3-319-63754-9_13

[12] Souza, F., Valle, E., Chávez, G., & De A. Araújo, A. (2011). Color-aware local spatiotemporal features for action recognition. Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications, 248-255. https://doi.org/10.1007/978-3-642-25085-9_29

[13] Venkatesh, S., Anand, A., S., G., Ramakrishnan, A., &Vijayaraghavan, V. (2020). Real-time surveillance based crime detection for edge devices. Proceedings of the 15th International Joint Conference on Computer Vision, Imaging and Computer

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 4027 - 4037
Received 20 January 2021; Accepted 08 February 2021.

Graphics Theory and Applications. https://doi.org/10.5220/0008990108010809
[14] S. W. T. T. Liu, H. Y. T. Ngan, M. K. Ng, and S. J. Simske. (2018). Accumulated relative density outlier detection for large scale traffic data. Electronic imaging, 2018(9), 1–10.https://doi.org/10.2352/issn.2470-1173.2018.09.iriacv-239 .
[15] R. V. H. M. Colque, C. Caetano, M. T. L. de Andrade, and W. R.Schwartz. (2017). Histograms of optical flow orientation and magnitude andentropy to detect anomalous events in videos. IEEE Transactions onCircuits and Systems for Video Technology, 27(3), 673–682.
[16] Goya, K., Zhang, X., Kitayama, K., & Nagayama, I. (2009). A method for automatic detection of crimes for public security by using motion analysis. 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. https://doi.org/10.1109/iih-msp.2009.264
[17] Soares, P. G., Da Silva, A. B., & Pereira, L. F. (2019). An assault detection system based on human pose tracking for video surveillance. Anais Estendidos da Conference on Graphics, Patterns and Images (SIBGRAPI). https://doi.org/10.5753/sibgrapi.est.2019.8327
[18] Fu, E. Y., Leong, H. V., Ngai, G., & Chan, S. C. (2017). Automatic fight detection in surveillance videos. International Journal of Pervasive Computing and Communications, 13(2), 130-156. https://doi.org/10.1108/ijpcc-02-2017-0018
[19] Arunnehru, J., &Kalaiselvi Geetha, M. (2016). Difference intensity distance group pattern for recognizing actions in video using support vector machines. Pattern Recognition and Image Analysis, 26(4), 688-696. https://doi.org/10.1134/s1054661816040015
[20] Biradar, K., Dube, S., &Vipparthi, S. K. (2018). DEARESt: Deep Convolutional aberrant behavior detection in real-world scenarios. 2018 IEEE 13th International Conference on Industrial and Information Systems (ICIIS). https://doi.org/10.1109/iciinfs.2018.8721378
[21] Ullah, W., Ullah, A., Haq, I. U., Muhammad, K., Sajjad, M., &Baik, S. W. (2020). CNN features with Bi-directional LSTM for real-time anomaly detection in surveillance networks. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-020-09406-3
[22] Singh, V., Singh, S., & Gupta, P. (2020). Real-time anomaly recognition through CCTV using neural networks. Procedia Computer Science, 173, 254-263. https://doi.org/10.1016/j.procs.2020.06.030
[23] H. Mousavi, S. Mohammadi, A. Perina, R. Chellali, and V. Mur.Analyzingtracklets for the detection of abnormal crowd behavior. In WACV, 2015.https://doi.org/10.1109/wacv.2015.27 .
[24] V. Saligrama and Z. Chen. (2012). Video anomaly detection based on local statistical aggregates. In 2012 IEEE Conference on Computer Vision and Pattern Recognition,2112–2119.
[25] M. Hasan, J. Choi, J. Neumann, A. K. Roy-Chowdhury, and L. S.Davis. (2016). Learning temporal regularity in video sequences. CVPR.
[26] Yiru Zhao, Bing Deng, Chen Shen, Yao Liu, Hongtao Lu, Xian-Sheng Hua . (2017). Spatio-Temporal AutoEncoder for Video Anomaly Detection (2017). MM '17: Proceedings of the 25th ACM international conference on Multimedia. 1933–1941. https://doi.org/10.1145/3123266.3123451.
[27] B. Yu, Y. Liu, and Q. Sun. (2017). A content-adaptively sparse reconstructionmethod for abnormal events detection with low-rank property. IEEETransactions on Systems, Man, and Cybernetics: Systems, 47(4), 704–716.
[28] J. R. Medel and A. Savakis. (2016). Anomaly detection in video usingpredictive convolutional long short-term memory networks. arXivpreprint arXiv:1612.00390.
[29] Santhosh, K. K., Dogra, D. P., & Roy, P. P. (2017). Real-time moving object classification using DPMM for road traffic management in smart cities. 2017 IEEE Region 10 Symposium (TENSYMP). https://doi.org/10.1109/tenconspring.2017.8070028
[30] Santhosh, K. K., Dogra, D. P., & Roy, P. P. (2019). Temporal unknown incremental clustering model for analysis of traffic surveillance videos. IEEE Transactions on Intelligent Transportation Systems, 20(5), 1762-1773. https://doi.org/10.1109/tits.2018.2834958.
[31] Fast violence detection in video. (2014). Proceedings of the 9th International Conference on Computer Vision Theory and Applications. https://doi.org/10.5220/0004695104780485.
[32] Serrano Gracia, I., Deniz Suarez, O., Bueno Garcia, G., & Kim, T. (2015). Fast fight detection. PLOS ONE, 10(4), e0120448. https://doi.org/10.1371/journal.pone.0120448.
[33] Mohammadi, S., Perina, A., Kiani, H., &Murino, V. (2016). Angry crowds: Detecting violent events in videos. Computer Vision – ECCV 2016, 3-18. https://doi.org/10.1007/978-3-319-46478-7_1
[34] Hassner, T., Itcher, Y., &Kliper-Gross, O. (2012). Violent flows: Real-time detection of violent crowd behavior. 2012 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops. https://doi.org/10.1109/cvprw.2012.6239348

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 2, 2021, Pages. 4027 - 4037
Received 20 January 2021; Accepted 08 February 2021.

[35] Gao, Y., Liu, H., Sun, X., Wang, C., & Liu, Y. (2016). Violence detection using oriented violent flows. Image and Vision Computing, 48-49, 37-41. https://doi.org/10.1016/j.imavis.2016.01.006
[36] Bilinski, P., & Bremond, F. (2016). Human violence recognition and detection in surveillance videos. 2016 13th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). https://doi.org/10.1109/avss.2016.7738019
[37] Aberkane, S., &Elarbi, M. (2019). Deep reinforcement learning for real-world anomaly detection in surveillance videos. 2019 6th International Conference on Image and Signal Processing and their Applications (ISPA). https://doi.org/10.1109/ispa48434.2019.8966795
[38] Geetha, M. K., Arunnehru, J., & Geetha, A. (2018). Early recognition of suspicious activity for crime prevention. Computer Vision, 2139-2165. https://doi.org/10.4018/978-1-5225-5204-8.ch094