

Video Anomaly Localization and Detection using Markov-Modulated Poisson Process (MMPP)

S. Giriprasad*, S. Mohan**, S. Gokul***

Abstract: In Intelligent video surveillance application, the challenging part is video anomaly localization and detection for analyzing the anomalies in the sequence of video frames captured by a camera from a crowded scene. An anomaly can be detected by considering both the temporal and spatial contexts. In this paper, we propose a Markov-Modulated Poisson Process (MMPP) model for anomaly detection and classification. In addition, a discrete-time model with the poisson process comprise the superposition of normal behavior and the event behavior that may increase or decrease the number of counts observed. The event behavior is taken utilizing a Markov chain model in order to capture the idea of event persistence. After the anomaly detection, the genetic algorithm has been utilized in this paper to improve the classification accuracy. The efficiency of the proposed scheme on numerous video surveillance with different types of datasets are determined and the comparison between the proposed system and the existing work shows that the accuracy level is increased in the proposed work.

Keywords: Video Surveillance, Markov-Modulated Poisson Process (MMPP), Markov Chain Model, anomaly detection

1. INTRODUCTION

Video surveillance has been a part of important attention in both industry and academia. In recent times, anomaly detection for video surveillance has increased and a large number of surveillance cameras have been installed due to the reducing costs of video cameras and increasing demand to reduce the human effort of analyzing the large-scale video data in industry application. Many significant technologies have been established for intelligent surveillance, such as pedestrian detection, object tracking gait analysis, privacy protection, vehicle template recognition, iris recognition, face recognition, crowd counting and video summarization. Due to the features like cost effectiveness in the computer vision applications, it adds advantages to the camera technology and used to sequence the video frames automatically like video surveillance.

Most detection approaches utilize motion features such as texture information, image gradient, spatial-temporal volume or optical flow characteristics. These features consent to examine compressed video anomaly detection utilizing characteristics of individuals [13]. Some works in the analysis of anomaly detection usually assume that individuals can be identified and tracked in the video sequences. The inter-images inversely based on an optical flow computed and entropy image by a cluster method with a hierarchical optical flow estimation and this technique has vast computation load.

In this paper, the focus is on problems, where we are given a set of nominal training video samples. Based on these samples it is essential to define whether or not a test video contains an anomaly. Consider the anomalies in the

* Assistant Professor, Department of Electronics and Communication Engineering, Coimbatore Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India, *Email: toogiriprasad@yahoo.com*

** Professor, Department of Electronics and Communication Engineering, Coimbatore Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India.

*** Assistant Professor, Department of Electrical & Electronics Engineering, Coimbatore Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India.

motion attributes where the outliers occur in both usual and unusual patterns in different locations. These comprise anomalies such as illegal U-turns, sudden movements and irregular patterns that are dissimilar from the regular video events in a particular data set.

We focus on anomalies that have a novel hybrid model such as a Markov-Modulated Poisson Process (MMPP) model [17] for anomaly detection and classification using a neural network. Video surveillance abnormal event deduction using Genetic Algorithm (GA). The MMPP model is considered as a basic component in pattern recognition, signal processing, gesture and speech recognition, as well as applications for video surveillance anomaly detection.

Markov-Modulated Poisson Process (MMPP) model is designed to better handle numerous of the shortcomings not addressed in present classification systems. The motivation of this research is to provide a way of better detecting video surveillance anomaly for classification of the person's movement. This classification will be based on the neural network observations being linked and event retrieval using genetic algorithm. The goal of this research is to develop a more robust classification system than present standard MMPP and to speed up the anomaly search process, increase the video anomaly detection accuracy and identify a new model by looking at the links between video objects from the classification system.

The rest of the paper as follows: Section 2 summarizes the related work for video surveillance anomaly detection. In section 3, summarizes the problem statement about the anomaly detection and working process of Markov-Modulated Poisson Process (MMPP). In section 4 shows the simulation results and performance evaluation of the proposed work and Section 5 concludes this paper.

2. RELATED WORKS

A special sort of Intrusion Detection Systems (IDSs), called Anomaly Detection Systems, develop models based on normal network or system behavior, with the aim of detecting both known and unknown attacks [1] [11]. Anomaly detection systems face numerous issues, including, the ability to work in online mode, high rate of false alarm and scalability. A model-free methodology is based on the approach of types and Sanov's theorem and model-based methodology for traffic modeling using a Markov modulated process [2]. Utilizing these characterizations as a model, sequentially monitors the traffic and apply large decision theory and deviations. Several outlier detection techniques have been advanced specifically to certain application fields, while few methods are more generic [3] [12]. Some application methods are being researched in strict confidentiality, for example, research on terrorist activities and crime.

Machine learning techniques assist the development of anomaly detection algorithms that are non-parametric, adaptive to changes in the appearances of typical behavior in the appropriate network, and portable across applications. An intrusion detection technique based anomaly detection is proposed which is an advanced and accurate approach to protect data warehouse at target systems while moving across the networks beside the malicious activities [4].

The challenge of discovering little target in vast pictures lies in the description of the foundation clutter. The more homogeneous the foundation, the more recognizable an ordinary target will be from its experience. One approach to homogenize the foundation is to segment the picture into different areas, each of which is independently homogeneous, and after that to treat every area independently [5]. The target is unspecified (it is an abnormality), and different segmentation methodologies are utilized, including an adaptive hierarchical tree-based scheme.

The Evidence Feed Forward Hidden Markov Model provides observation to observation links, mathematical proofs of their learning of these parameters to enhance the likelihood of observations, standard HMMs in classification of both measurement data and visual action data, thus providing that the strong base for Evidence Feed Forward HMMs in classification of numerous types of problems [6].

A mathematical framework to jointly model associated activities with both context information and motion for anomaly detection and activity recognition. This is motivated from clarifications that activities correlated in time and

space rarely occurs autonomously and can serve as a framework for each other. The temporal and spatial distribution of various activities gives useful cues for the appreciating of these activities [7]. The generated labels and learned model are used to detect anomalies whose context patterns and motion deviate from the learned patterns.

The problem of detecting human behavioral anomalies in crowded surveillance environments is addressed in this paper. Inhuman behavior on the problem of detecting subtle anomalies in a behaviorally heterogeneous surveillance scene employs a novel unsupervised context-aware process and evaluate a method of utilizing scene context and social context to improve behavior analysis [8]. In a crowded scene the application of Mutual Information based social context permits the ability to prevent self-justifying groups and propagation anomalies in a social network.

Numerous dangers in this present reality can be identified with action of individuals on the web. The web surveillance method to prevent and predict attacks and to support in discovering suspects focused around data from the web [9]. Instead of, the measure of information on the web rapidly increases and drawn out to monitor numerous sites and time consuming. A novel technique to consequently monitor patterns and discover anomalies on the internet.

A novel framework[10] is developed for video anomaly detection and automatic human activity modeling without any manual labeling of the training dataset. The framework comprises of some key components and a compact activity representation technique which is established based on a stochastic sequence of spatialtemporal actions. A runtime accumulative anomaly measure is presented to detect abnormal activities. The natural grouping of activities is exposed over a novel clustering algorithm with unsupervised model selection, whereas usual human activities are predicted.

3. PROPOSED METHOD

3.1. Heterogeneous Face Descriptor (HFD)

A Markov-Modulated Poisson Process (MMPP) model based anomaly detection is providing a solution to various heterogeneous face recognition problems [16]. HFD started with sketch recognition utilizing to view sketches and has proceeded into different modalities such as near infrared (NIR). In this section, the heterogeneous face recognition process is described as follows:

In HFD frame extraction using basic patch descriptors such as Edge Orientation Histogram (EOH) and Multilayer Histogram of Optical Flow (MHOF) which will be used to partition the image into few parts of pixels then calculated the motion energy of every pixel. In Multi-scale Histogram of Optical Flow, which sanctuaries more temporal contextual information after the motion field is estimated. Quantize every pixel (x, y) in the MHOF [18] by using eq. 1

$$h(x, y) = \begin{cases} \text{round}\left(\frac{p\theta(x, y)}{2\Pi}\right) \bmod p & r(x, y) < T \\ \text{round}\left(\frac{p\theta(x, y)}{2\Pi}\right) \bmod p + p & r(x, y) \geq T \end{cases} \quad (1)$$

where $r(x, y)$ is the motion energy and $\theta(x, y)$ is the direction of motion vector at (x, y) .

For appearance feature, Edge Orientation Histogram (EOH) is used which filters the image using Sobel masks such as $[-1, 0, 1]$ and $d[-1, 0, 1]^T$ which makes the gradient image in x and y direction. Image patches containing more noise or background pixels, so they need to remove for robustness contingent on the subsequent two criteria

The foreground ratio can be found, by subtracting the background ratio using the following condition [18].

$$E(H) = -1 \sum_i H(i) \log(H(i)) \quad i = \{1, \dots, B\} \quad (2)$$

where the background model is used to generate the foreground mask.

The Entropy of the MHOF, which consider as the intersection of different objects [18].

$$E(H) = -1 \sum_i H(i) \log(H(i)), i = \{1, \dots, B\} \tag{3}$$

Where H is the feature vector MHOF of every patch, B is the feature dimension.

In HFD make pre-determined homographies from the camera’s image to the XY , ZY and XZ . A projected circle has two tangent points that describe the predictable camera center. These projections help as a simple representation of an else complex 4D (ZYZ and time) motion model. Fig. 1 shows a projected circle on the XY plane, with radius r , of an object o with detail to the camera center c .

Here the q angular translation of the circle center from c and the angular translation of the lower and upper tangents can be defined as $\xi_{upper} = \theta - a$ and $\xi_{lower} = \theta + a$ and where $a = \arcsin \frac{r}{d}$, the motion model of object, parameterized by time

$$f_c, o(t) = \bigcup_{\Pi=XY, XZ, YZ} \{ \theta(t, \pi) \pm \arcsin \frac{r(t, \pi)}{d(t, \pi)} \} \tag{4}$$

Where $r(t, \pi)$ and $\theta(t, \pi)$ are the distance of the circle center from c and $r(t, \pi)$ is the radius of the circle.

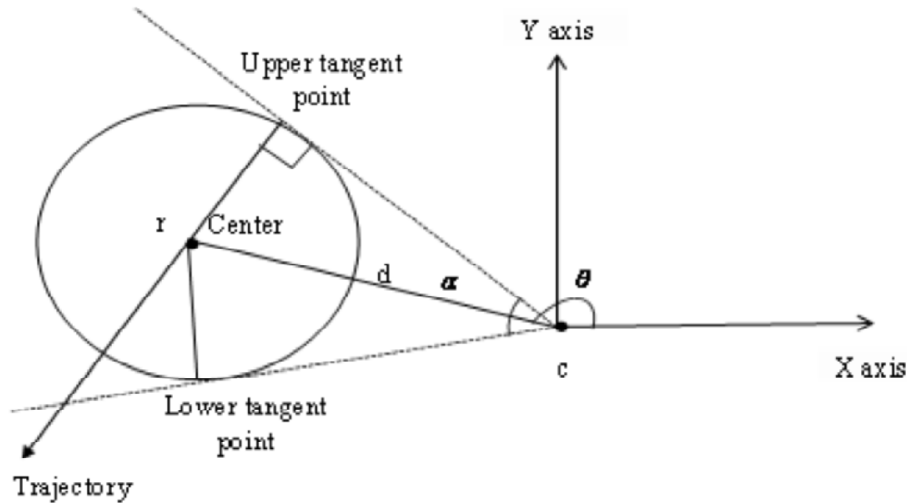


Figure 1: video projections

Consider a geometrical interpretation and ease computation of the positional uncertainties of a particular apriori distribution. For these resolutions, apply a method that makes the straight-line prediction paths. The positional uncertainty, which allows dissimilarity from the straight-line path, is shown by growing the radius of the circle linearly completed time as it moves beside the straight line.

Let one of the object be C_{obj} and be the successive positions of C_{obj} . Subsets of S_{hist} formed from consecutive elements are utilized to predict the speed and direction of C_{obj} . The first to k^{th} element would be appropriate to the first subset, the $(\eta + 1)^{th}$ to $(k + \eta)^{th}$ element to the second and so on.

Form a new set S_{pred} , Consisting of the predicted velocities of C_{obj}

$$S_{pred} = \{x_0, x_1, \dots, x_n\} \tag{5}$$

Where every $x_i = 0, \dots, n$ is a vector of direction and speed, h is the number of subsets formed from S_{hist} . Every

x_i is assigned a weight w_i and with all weights normalized so that $\sum_{i=0}^n \omega_i = 1$ the probability of perceiving a velocity v can be predictable as:

$$\Pr(v) = \sum_{i=0}^n w_i \prod_{j=1}^2 \frac{1}{\sqrt{2\pi\sigma_j}} e^{-\frac{1}{2} \frac{(v_j - x_{i,j})^2}{\sigma_j^2}} \quad (6)$$

Where j denotes the direction and speed component and σ_j^2 is the corresponding bandwidth.

The self-assurance interval, v_{\min}, v_{\max} that delivers a desired level of assurance p which is denoted as

$$p = \int_{v_{\min}}^{v_{\max}} pr(v)dv \quad (7)$$

The region of C_{obj} is computed using the v_{\min}, v_{\max} interval.

A Minimum Enclosing Circle (MEC) is created to enclose the predicted object into which object is moving.

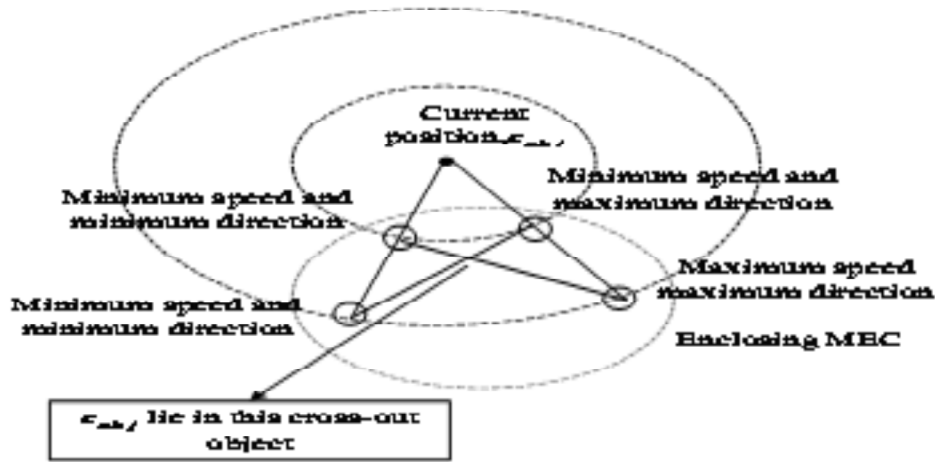


Figure 2: The predicted positions of C_{obj}

Fig. 2 denotes the next time instance, the region where the projected positions of C_{obj} lie is delimited by the curves of two concentric circles as displayed, with the four restricting corners of the region computed by the maximum and minimum speed, and the maximum and minimum direction, given by v_{\min}, v_{\max} . A MEC (red circles) can then be created to encompass the predicted object into which the object is moving.

3.2. Markov-Modulated Poisson Process (MMPP)

The framework of the proposed Markov-Modulated Poisson Process (MMPP) for DPG as shown in Fig.3

Dynamic Patch Grouping (DPG): DPG used to adaptively cluster similar patches and characterize every group as motion context utilizing the Heterogeneous Face Descriptor. DPG is only needed to handle a less number of units, thus is more effective. The DPG measured as a labeling procedure, in label $c \in \{1, \dots, c\}$ is assigned to each pixel. Let $\bar{y}_c = \{y_{ic}\}_{n \times 1}$ be a partitioning vector with $y_{ic} = 1$ if i belongs to the K^{th} segment and $y_{ic} = 0$. Otherwise Normalized cut Ncut is used for global optimization in DPG as defined in eq.8[18].

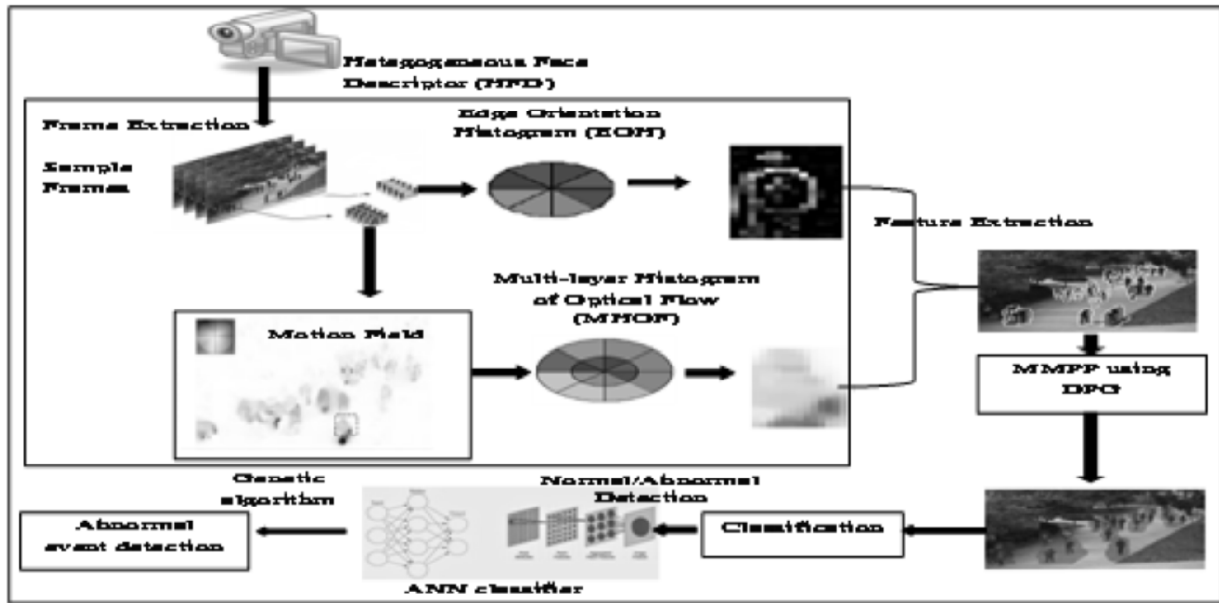


Figure 3: Markov-Modulated Poisson Process (MMPP)

$$N_{cut}(A, B) = \frac{cut(A, B)}{assoc(A, V)} + \frac{cut(A, B)}{assoc(B, V)} \tag{8}$$

Where $assoc(A, V) = \sum_{i \in A, j \in V^{s(i,j)}}$ is the total connection from the vertex set A, $cut(A, B) = \sum_{i \in A, j \in B^{s(i,j)}}$ is the cut value.

The empirical output of Dynamic Patch Grouping (DPG) display that the grouping of video anomaly events can be significantly under different video phases of the sample sequence videos. In view of such an observation, this study proposes a model whereby the intensity process of video anomaly event detection follows the MMPP and where the MMPP state is directed by a homogeneous Markov chain. Consider that the sample video for the anomaly detection is continuous except on finite points in time, and the intensity of anomalous events depends on the state of the person’s actions.

An MMPP, $\phi(t)$ is the passion process whose intensity $\lambda_X(t)$ varies according to a homogenous Markov process $X(t)$ with transition function $P_{ij}(t)$ for the finite state space $X = \{1, 2, \dots, I\}$. In other words, a Poisson process $\phi(t)$ is called MMPP if the conditional distribution $P(\phi|X)$ is equal to the distribution of a poisson process with the intensity function $\lambda_X(t)$ Particularly, the distribution of the MMPP can be denoted by

$$P(\phi(t)) = (m | X(t), t > 0) = \frac{(\int_0^t \lambda_{X(s)} ds)}{m!} \exp \left[-\int_0^t \lambda_{X(s)} ds \right] \tag{9}$$

Where p denotes the video transition rate $\psi(i, j)$

$$\psi(i, j) = \begin{cases} v(i, j), & i \neq j \\ -\sum_{j \neq i} v(i, j), & otherwise \end{cases} \tag{10}$$

Where $i, j \in X$ Since the Markov chain has a finite number of states, the Poisson intensity rate takes discrete values corresponding to each pixel. The intensity of the MMPP is

$$-a \sum_{n=1}^{\phi(t)} \gamma_n + \wedge k_1 t \quad (11)$$

Where t denotes martingale in a video sequence and $\wedge k_1 t$ denotes the occurrence of anomaly detection until time t .

In video surveillance application, assume an anomaly is an event that arises briefly, rarely and randomly. An anomaly causes a change in the video activity over the time period, and is detected in the $N(t)$. $N_A(t)$ is also a Poisson process rate is $\lambda_A(t)$ when there is a video anomalous event at time t otherwise 0. Determination of rare or random anomaly detection using a transition probability matrix M_A

$$A(t) = \begin{cases} 1 & \text{aneventisoccurringattimet} \\ 0 & \text{otherwise} \end{cases} \quad (12)$$

$$M_A = \begin{pmatrix} 1 - A_0 & A_1 \\ A_0 & 1 - A_1 \end{pmatrix} \quad (13)$$

Where $1/A_0$ is the expected time interval between normal and abnormal events and $1/A_1$ is the expected length of the abnormal event.

3.3. ANN with Genetic algorithm phase

A particular example, labeling i of a test or training dataset, the input layer of the ANN with Genetic algorithm phase using Markov-Modulated Poisson Process (MMPP) anomaly detected video frames receives the input vector T from training dataset. The input vector T created using below equation

$$T_i = t_{i,1} t_{i,2} \dots t_{i,n} \quad (14)$$

Here t_{ij} is the j th feature of i th instance of a test or training dataset. Total number of input neurons in input layer are equal to total features of a test or training dataset for anomaly detection. The output layer comprises the output neurons.

The input-output conversion in every hidden neuron is accomplished by a mathematical non linear activation function. The method of activation function is

$$Y_{i,k} = \left[1 + \exp \left(- \sum_{j=1}^N W_{j,k} * T_{i,j} - b_k \right) \right]^{-1} \quad (17)$$

Where b_k denotes the occurrence of anomaly activation function.

The output neurons obtain from an input using Equation 16

$$Z_i = (Y_{i,1}, Y_{i,2}, Y_{i,n}) \quad (18)$$

In genetic algorithm an archive of an ensemble of ANNs in terms of chromosomes of 1's and 0's as shown in Fig.4. In genetic algorithm, 1 denotes incorporation of resultant ANN and 0 denotes absence of resultant ANN in the formation of an ensemble [14] [15]. This phase is responsible for aggregating the predictions of ANNs base classifiers to get a final prediction of ensemble classifier archive the non-dominated ANN solutions. One chromosome of 1's and 0's from the archiving ensembles. Based upon the values of chromosome, equivalent ANNs predictions are combined to get a final prediction of the ensemble. The accurate video anomaly detection is obtained from the final Genetic algorithm results.

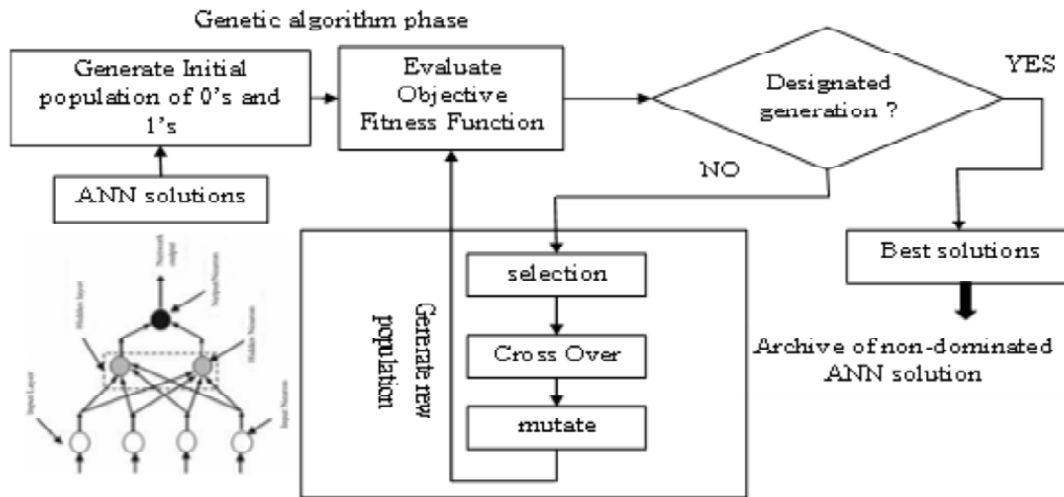


Figure 4: ANN with Genetic algorithm phase

4. SIMULATION RESULTS

This section presents the experimental results and discussion. The simulation model is implemented as a MATLAB application. It is used to perform in sample datasets which contains the both train and test data. Genetic algorithm parameter values are shown as Table.1 and video compression ratio as shown as Table.2.

4.1. Experiment Settings

Table 1
Parameter values of genetic algorithm

Total number of video frames	50
Population size	400, 600, 800
Number of generations	400, 600, 2000, 3000
Mutation rate	0.1
Sensitivity coefficient	1.0
Variability values	0.10, 0.15, 0.20, 0.25

Table 2
Compression ratio

	File Size (Bytes)														
Input Frame	5322	5274	5292	5319	5308	5283	5228	5196	5185	5209	5311	5343	5347	5356	5313
Output Frame	4964	4959	4950	4978	4954	4941	4884	4871	4843	4900	4985	5001	4994	5016	4982

Basically, train the algorithm on normal samples, then use these rules to find anomalies. To characterize the samples of normal or anomalies, the typical function was

$$\mu_{anomalies(x)} = D(x, normal) = \min\{d(x, s) : s \in normal\} \tag{17}$$

Which means the closer a vector x is to a point s , the less it is a anomalies sample.

The distance measure $d(x, s)$ as exposed in equation 17 utilized to describe the test data was the n -dimensional Euclidean distance.

$$d(x, s) = \sqrt{(x_1 - s_1)^2 + (x_2 - s_2)^2, \dots, + (x_n - s_n)^2} \tag{18}$$

The anomaly accurate prediction using below equation

$$Accuracy = \frac{TP + TN}{TP + FN + TN + FP} \quad (19)$$

Where TP is the True Positive, TN is the True Negatives, FP is the False Positives rate.

The ratio of frames that are abnormal and utilized for the ANN and GA training are measured by the subsequent equation

$$R = \frac{N_{abnormal}}{N_{normal} + N_{abnormal}} \quad (20)$$

Where N is the No. of frames, $N_{abnormal}$ is the number of abnormal frames and N_{normal} The number of normal frames.

The error rate is measured as following equation

$$ER = \frac{N_{FP} + N_{FN}}{N_{total}} \quad (21)$$

Where N is the No of frames, N_{FP} is denotes number of false positive frame and N_{FN} is denotes number of false negative frames.

$$Classifier Accuracy = \frac{Correctlyclassified}{Totalclassified} \quad (22)$$

4.2. Experimental Result

To compare the proposed MMPP approach with other methods, utilizing the same experimental setup and demonstrate the comparison results in Fig.5. Each of these is an anomalous activity detection algorithm that is accomplished of dealing with noisy data and low resolution. Fig.5 shows that the accuracy for various anomaly detection methods, where the proposed MMPP method is superior than the Hidden Markov Mode (HMM) method and MAP-based method by using the evaluation of 50 video frames. These approaches extract activity structure simply by computing local action-statistics, but are restricted by their capability to capture activity structure only able to some fixed region. MMPP provided the best account, existence able to resourcefully extract the

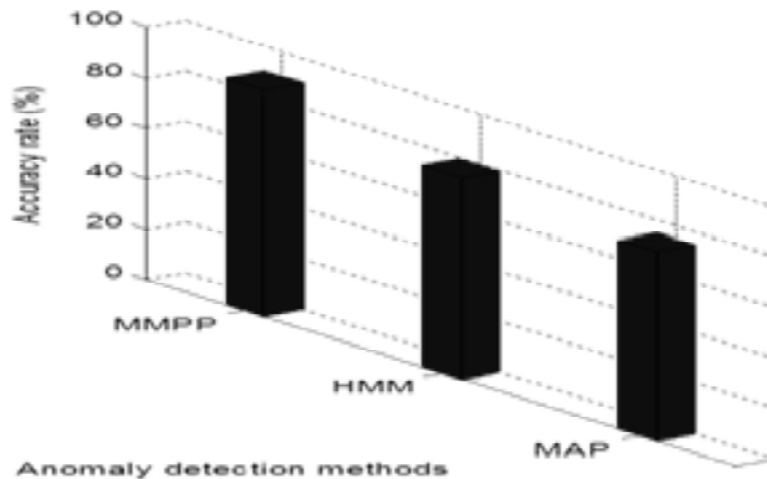


Figure 5: Anomaly Detection rate

adaptable length action subsequence of activity, constructing a more discriminating feature region, and resulting in theoretically better activity anomaly discovery and classification.

Fig.6 illustrates the anomaly detection for various state-of-the-art method true positive rates and the proposed approach. The results show that the MMPP score means better classification performance compared to HMM and MAP method.

Fig. 7 shows the classification accuracy of different type of algorithm. The accuracy rate utilizing different kind of video frames such as prototypical, temporal and spatial video frame. The proposed Machine learning techniques, like Artificial Neural Networks (ANN) and Genetic Algorithm (GA), have shown outstanding results in solving the lowering the false positives rate and accuracy concern on video anomaly detection systems. With the videos taken in this study, the Artificial Neural Networks (ANN) and Genetic Algorithm (GA) proved to have more abilities in refining accuracy and identifying anomaly from the presented video. They also show efficient capability to classify between normal and anomaly videos surveillance application. The predicted normal video frame and abnormal

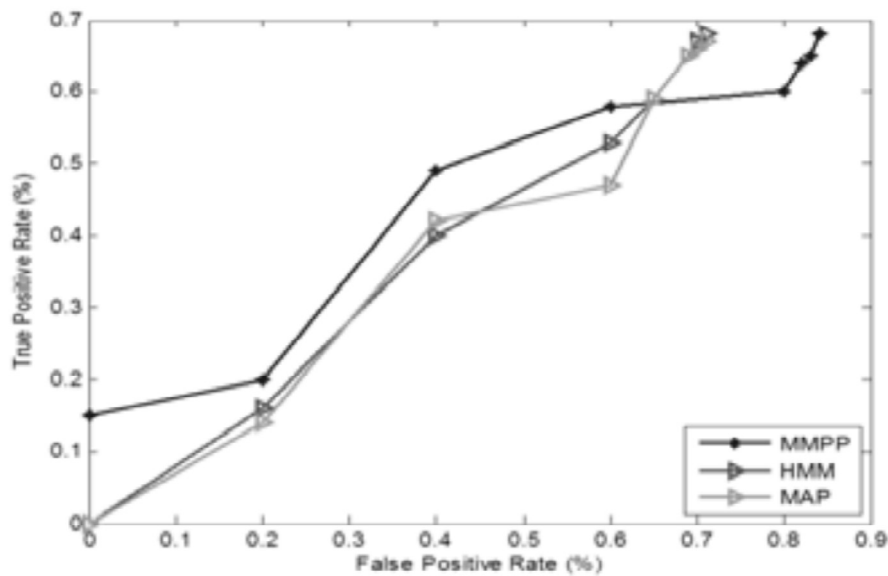


Figure 6: True positive rate

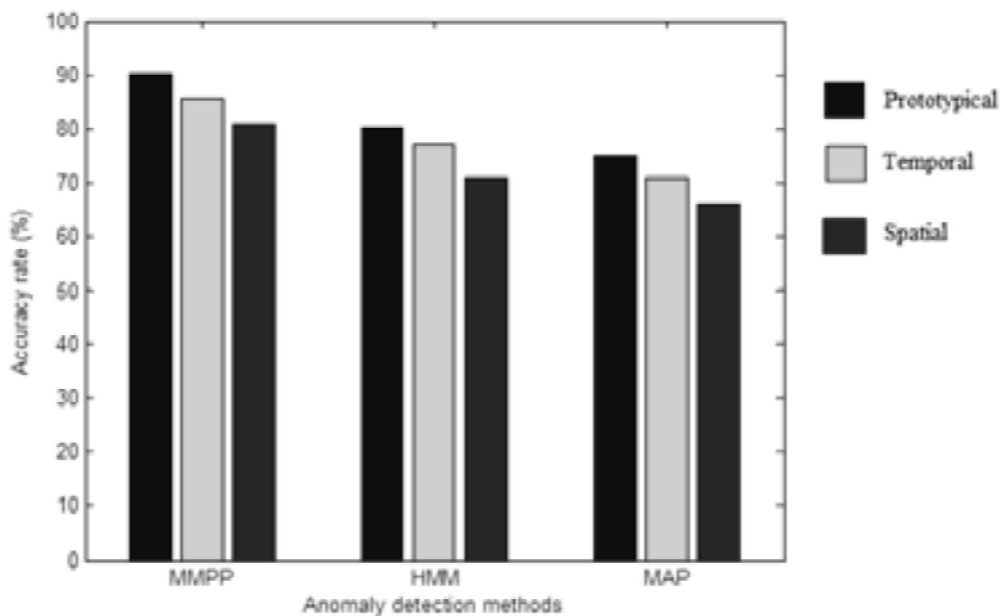


Figure 7: Accuracy rate



Fig. 8(a) normal video frame



8(b) abnormal video frame

video frames are shown in Fig.8 (a) and (b). Commonly happening anomalies include small carts, skaters, bikers, and persons walking crossways. It typically shown in Fig 8(b), the frame was shows that the truck was coming.

5. CONCLUSION

In this paper, a new approach has been formulated for efficient video surveillance anomaly detection and classification. The events are detected in the video sequence using Markov-Modulated Poisson Process (MMPP) model and the detected anomalies are classified using the neural network and anomaly event are accurately identified by using Genetic Algorithm (GA). The simulation results show the ability of the approach to detect video surveillance anomalies in an efficient way by having the lowest error rates on the given sample videos. The distance based techniques using Euclidean distance show they are more stable and less sensitive. The proposed algorithm provides robust and better demonstration of data. It was able to select weighty attributes which leads to progress the detection accuracy to 90.5%. This result displayed that the MMPP is efficient and reliable in video surveillance anomaly detection.

References

- [1] Rahul Jain, Tejpal Singh, AmitSinha, "A Survey On Network Attacks, Classification And Models For Anomaly-Based Network Intrusion Detection Systems", International journal of Engineering Research and Science and Technology (IJERST), 2319-5991, Vol. 2, No. 4, 2013.
- [2] Amjan.Shaik, S.V.AchutaRao, Hymavathi. Bhadriraju, Md.Reyaz, Nazeer. Shaik, "Assessing Deviations of Empirical Measures for Temporal Network Anomaly Detection: An Exercise", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 2 (3), 1327-1332, 2011.
- [3] Karanjit Singh, ShuchitaUpadhyaya, "Outlier Detection: Applications And Techniques", International Journal of Computer Science (IJCSI), Vol. 9, Issue 1, No 3, 2012.
- [4] Goverdhan Reddy Jidiga, P Sammulal, "Anomaly Detection Using Generic Machine Learning Approach With a Case Study of Awareness", International Journal of Modern Engineering Research (IJMER), Vol.3, Issue.2, pp1245-1252, 2013.
- [5] James Theiler and Lakshman Prasad, "Overlapping image segmentation for context-dependent anomaly detection", Algorithms and Technologies for Multispectral, Hyperspectral, and Ultraspectral Imagery, XVII, Vol 8048, 2011.
- [6] Michael Del Rose, Christian Wagner, Philip Frederick, "Evidence Feed Forward Hidden Markov Model: A New Type of Hidden Markov Model", International Journal of Artificial Intelligence & Applications (IJAA), Vol.2, No.1, 2011.
- [7] Yingying Zhu, Nandita M. Nayak, Amit K. Roy-Chowdhury, "Context-Aware Activity Recognition and Anomaly Detection in Video", IEEE, Journal Of Selected Topics In Signal Processing, Vol. 7, No. 1, 2013.
- [8] Michael J.V. Leach, Ed.P. Sparks, Neil M. Robertson, "Contextual anomaly detection in crowded surveillance scenes", Elsevier journal of Pattern Recognition Letters, 44, 71-79, 2014.
- [9] Henri Bouma, Stephan Raaijmakers, ArvidHalma, Harry Wedemeijer, "Anomaly detection for internet surveillance", Society of Photo-Optical Instrumentation Engineers (SPIE), Vol. 8408, 840807, 2012.
- [10] Xudong Zhu, Zhijing Liu, Juehui Zhang, "Human Activity Clustering for Online Anomaly Detection", Journal of Computers, Vol. 6, No. 6, 2011.

- [11] Jun-Yong Zhu, Wei-Shi Zheng, Jian-Huang Lai, Stan Z. Li, "Matching NIR Face to VIS Face Using Transduction", IEEE, Transactions On Information Forensics And Security, Vol. 9, No. 3, 2014.
- [12] Lei Qin, HichemSnoussi, FahedAbdallah, "Object Tracking Using Adaptive Covariance Descriptor and Clustering-Based Model Updating for Visual Surveillance", Sensors 14, 9380-9407, 2014.
- [13] Dongping Zhang, Yafei Lu, Xinghao Jiang, HuailiangPeng, "Abnormal Crowd Motion Detection with Hidden Markov Model", International Journal of Advancements in Computing Technology (IJACT), Vol.5,Number 8, 2013.
- [14] V.PreethaPallavi, V.Vaithyanathan, "Combined Artificial Neural Network and Genetic Algorithm for Cloud Classification", International Journal of Engineering and Technology (IJET), 0975-4024, Vol 5 No 2, 2013.
- [15] A.NishaJebaseeli, E.Kirubakaran, "Genetic Optimized Neural Network Algorithm to Improve Classification Accuracy for Opinion Mining of M-Learning Reviews", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 3, 2013.
- [16] Edward Clint A, Shiloah Elizabeth D, "Model Based Face Recognition Using Kernel Linear Discriminant Analysis", International Conference of ASAR, 17,9, 2014.
- [17] Alexander Ihler, Jon Hutchins, Padhraic Smyth, "Learning to detect events with Markov-modulated poisson processes" ACM Transactions on Knowledge Discovery from Data (TKDD), Vol.1, Issue 3, 2007.
- [18] Yang Cong, Junsong Yuan, Yandong Tang, "Video Anomaly Search in Crowded Scenes via Spatio-Temporal Motion Context", IEEE Transactions on Information Forensics and Security, Vol.8, Issue: 10, 2013.

