An Intelligent Suspicious Activity Detection Framework (ISADF) for Video Surveillance Systems

Dammalapati Neelima
Asst professor in Dept. of CSE
in JNTU Kakinada, AP, India.

Gera Jaideep
Full time Ph.D. Scholor of
Koneru Lakshmaiah University,
Vijayawada, AP, India.

Gera Indira Priyadharsani
Asst professor in Dept. of ECE
in Nalla Narsimha Reddy Engg
College, Hyderabad, AP, India.

ABSTRACT
Video Surveillance systems are playing vital role in ensuring the security at various public places like bus stops, railway stations, shopping malls, Airports etc. Suspicious activity recognition helps to prevent from threats and identify the causes after threat. Existing semi-automatic approaches depends on human intervention to detect the uncommon activities and suspicious behavior from video context. Due to these limitations they become non-intelligence, very slow and need more human observers. In this paper, to overcome these problems an Intelligent Suspicious Activity Detection Framework (ISADF) for Video data is proposed. This framework uses location dependent training data for intelligence and context (foreground) change information for suspicious activity detection. Experimental results show that ISADF is a high speed intelligent threat detection system than existing approaches.

Keywords: video Surveillance systems, self-learning approach, suspicious detection, data clustering, video processing.

1. INTRODUCTION
Video Surveillance system is a collection of video, electronic and wireless components to ensure the continuous or periodic video recording for monitoring the various important public locations. Due to the increased crime rate and instable incidents are happening around the world many organizations are deploying video surveillance systems at their locations with CCTV cameras. Now a day we can notice these cameras at various public locations like bus stops, shopping malls, holy places, streets, educational institutes, public meetings etc. The captured video data is useful to prevent the threat before crime and becoming a good forensic evidence to identify criminals after crime.

Conservative video surveillance systems can record what they see but they can't make sense what they are viewing. Hence In earlier days to monitor the intrusions from captured video data, organizations depend on human observers. These systems [1, 2] are very expensive, slow, complex and having less precision. Recent researches on surveillance systems made them as semi-automatic approaches [3, 4]. These semi-automatic approaches also required the human intervention greatly in suspicious activity detection from uncommon activities. Hence they need professional human observers for uncommon and suspicious activity notification, which makes them non-intelligent systems.

In this paper, to overcome these problems an Intelligent Suspicious Activity Detection Framework (ISADF) for Video data is proposed. This framework uses location dependent training data for intelligence and context (fore ground) change information for suspicious activity detection. The location dependent training data will gives the more accurate results than independent data. Self-training module of this framework will slowly reduce the human intervention by learning suspicious activity from past experience. Experimental results show that ISADF is a high speed and accurate intelligent threat detection system than existing approaches.

2. LITERATURE REVIEW
A recent study from IMS Research [5] predicted the world market for video content analysis (VCA) software will grow at an annual rate of over 40% from 2008 to 2013. Forecasts also indicate VCA market growth from roughly US$50 million in 2008 to US$140 million in 2012. A number of video surveillance systems have been proposed by various researchers for different types of video data monitoring.

Background subtraction from video data [6,7] was the most popular approach to extract static background image from video data to know the moving objects in foreground. Moeisund and Hilton proposed this approach for static back ground data extraction from moving video data. But this approach was suffering from same color of foreground extraction from background. CMS research people introduced Video Surveillance and Monitoring (VSAM) systems[8] for battlefield support. VSAM using multiple sensors enables one human observer can monitor many video frames at same location. These sensors only will identify the uncommon behavior from video data and redirect that information to human observer to identify the suspicious activity. The disadvantage of this approach is, it doesn't have the intelligence to detect suspicious activity from given video data. With the help of offline past learning data and behavior patterns Tao et [9] introduced the classification of normal behavior and abnormal behavior. This approach clusters the current data against many groups and identifies the cluster behavior pattern to identify the suspicious activity.

3. INTELLIGENT SUSPICIOUS ACTIVITY DETECTION FRAMEWORK (ISADF)
Intelligent Suspicious Activity Detection Framework (ISADF) contains mainly two parts as shown in Fig.1.

They are Video recording and Image extraction unit and Video Processing unit.

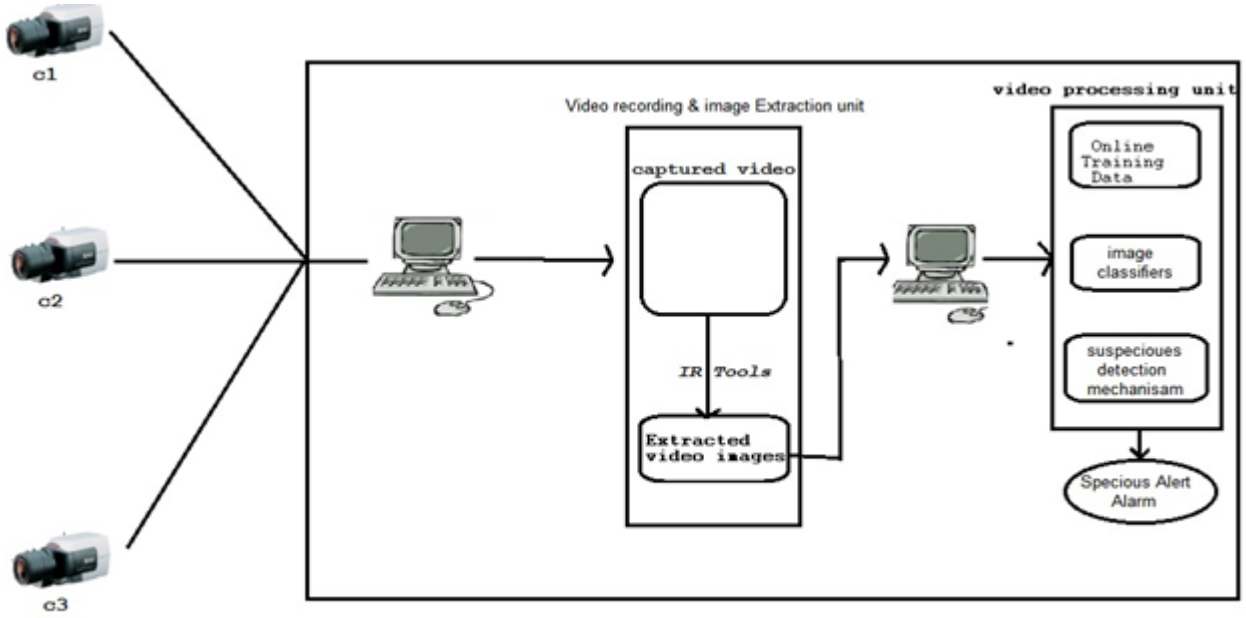

Fig.1. Intelligent Suspicious Activity Detection Framework

Video Recording and Image extraction unit

Video (CCTV) cameras can capture and transmit the video data to video recording and image extraction unit through the network. This unit stores the captured video data on video database for future processing. Image Retrieving tools from video data will extract the images and uploads to video processing unit.

Video Processing Unit (VPU): This unit plays a vital role in detecting the suspicious activity from the extracted image data. VPU contains three main components as shown in fig.1. they are i) Online Training data ii) Image Classifiers iii) Suspicious activity detection mechanism.

a)Image Classifiers: The initial operation in VPU is image background subtraction. In order to detect the moving object and motion Image classifiers will take all extracted images from image extraction unit. These image classifiers has to perform various operations like static back ground extraction, fore ground separation, noise removing from fore ground, Object identification, tracking human body, pose modeling and pose recognition, Motion detection.

From the given image to describe dynamic activities which are happening at that time, we have to separate static background of the image. Many researches were introduced various approaches for back ground extraction but we were used Massimo Piccardi [10] designed eight background separation and fore ground noisy detection techniques in this framework image classifiers. This technology can apply from simple approaches to complex approaches for scalable performance and accurate results under any circumstances. After separation of back ground, by subtracting it from real image the dynamic fore ground was identified and used for activity identification. By comparing the current frames (fore ground) with previous frames we can track the interested human object motion and eliminates the noisy.

b)Human Activity Identification: From the identified human objects extracting the behavior is very crucial and important to identify the human activity. As on this area is improved only for simple human behaviors like walking, sleeping, running, sitting etc. Previous activity recognition techniques are broadly classified into scene interpretation, holistic and action primitives and grammar approaches [6]. Scene interpretation techniques [11] are failed because they are domain dependent approaches means the input parameters and event detection rules of one domain could not useful for other domains. Holistic approaches identify human activities by using human body movements (dynamics) either at body level or parts level. Many research implementations were proposed for this holistic approach, but we selected the Vaswani and co implemented holistic approach [12] for ISADF frame work. This approach concerns on moving objects in 2D plane by the polygonal shaped objects and extracts object dynamics from the very low resolution images also.

c) Training data for suspicious activity detection: The above activity detection methods only identify the object models (human activities), not suspicious activities because they are non-intelligent. After recognizing the dynamic activity of an object it should be clarified whether it is suspicious or not. For this reason system needs the intelligence in the form of training data. Training data is classified into offline and online. Offline training data is static, which should never be updatable from the current knowledge. But online training data has some startup knowledge and will extend by the current data. In this system we are using online updatable training data which initially has some suspicious activity identification Knowledge.

d) Suspicious Activity Detection Mechanism: This mechanism contains SVM classifier and connected to training data for R/W operations .Initially Training data was collected from past suspicious activities and were processed by human observer. This person not only identified the suspicious activity but also given the environmental awareness and symptoms of suspicious activity on video data. Based on the given basic human intelligence (training data) SVM classifier [13] will learn and classifies the current data for activity detection and automatically extends the knowledge from present experience for future classification as shown in fig.2. SVM classifier will consider the present extracted frames

from image classifier and identifies the features with Gaussians method and clusters them as a frameset currf1 based on time periods. SVM will used to check whether the identified activity is suspicious or not. To determine the suspicious activity ISADF is following the Behavior Interception (BI) Algorithm as a part in SVM. This BI Algorithm will check the current frameset with past experience to identify the suspicious activity and returns the result to SVM as shown below:

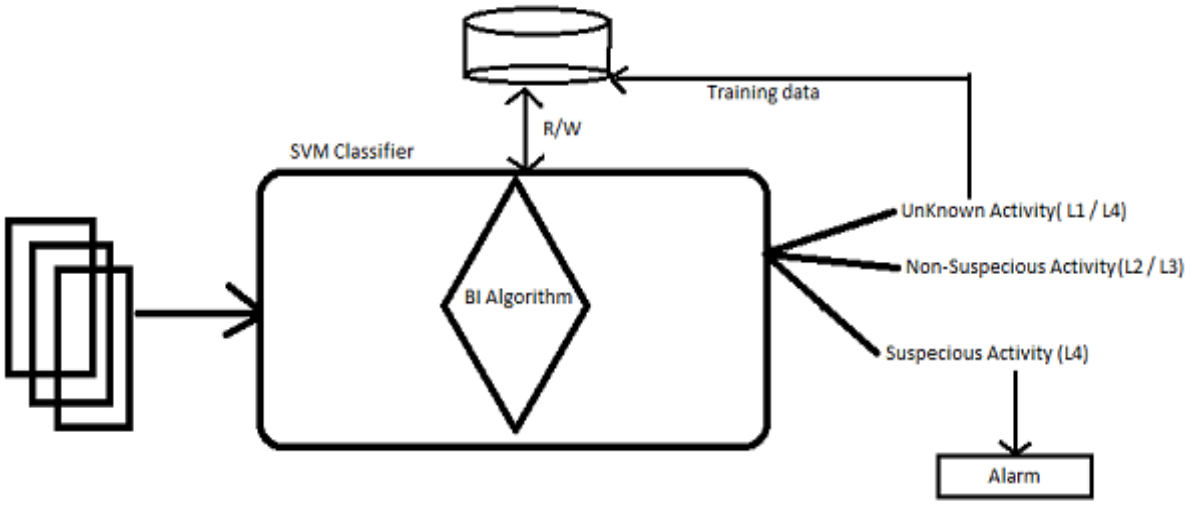

Fig.2. SVM and BI Algorithm for suspicious activity detection.

Behavior Interpretation (BI) Algorithm:

Input : currf1 and Training Data Clusters (TDC)

Output : Suspicious Activity, Common Activity, Un Identified Activity.

Begin:

If(currf1 not exists in TDC){ return Un Identified Activity; } // case1

else if (currf1 exists in TDC && non suspicious) {return Common Activity;} // case 2

else {return Suspicious Activity ; } // case3

End.

From the above algorithm the result may be in any of three cases. If the result is an unidentified activity (case1) our framework will learn the activity nature from human observer for future processing and updates the training data set with this new feature which makes our training data online. This unidentified activity may be a non or suspicious activity determines by human observer will results level1(normal) or level4 (suspicious). If the frameset data is available in TDC and it is not a suspicious according to TDC then the result is Common Activity (case2) and SVM will classify either level2(most common non-suspicious) or level3(uncommon non-suspicious) and discard the activity as a general activity. If the frameset data is available in TDC and it has the suspicious features in frame then BI returns the suspicious activity to SVM classifier. Then SVM will classify the level5 (suspicious) and returns and alert(/alarm) to responsible destination.

4. EXPERIMENTS

In order to identify the proposed framework performance we are introducing the ISADF scalability in this section. Experiments was done on Human Action data set named by KTH [15], which is widely used in video surveillance system experiments. This data set has many videos and contains the various human activities like walking, jagging, clapping, boxing, running, waving etc. Initially this video is segmented based on time slots and every segment has an unique subject for activity identification. KTH contains approximately 450 video segments and the frame size with 220x170 as shown in fig.3. From the above dataset our ISADF framework identified all human activities successfully with the help of training data and designed them as clusters based on pixel similarity and context configuration. We can observe some sample clusters done by ISADF for activity classification as shown in fig.4. After Clustering the input dataset our framework will identify the background and separates for activity recognition as shown in fig.5. After the SVM classifier will take the featured image data to identify the activity and behavior for suspicious detection. As mentioned in section3 it will classify the present frameset images with the help of training data to determine common or uncommon activity and defines the level of activity. The results of these experiments show that this framework is self-trainable and intelligent to detect suspicious activities from video data.

Fig.3. KTH dataset for human activity Classification.

Fig.4. Clustered dataset based on human activity

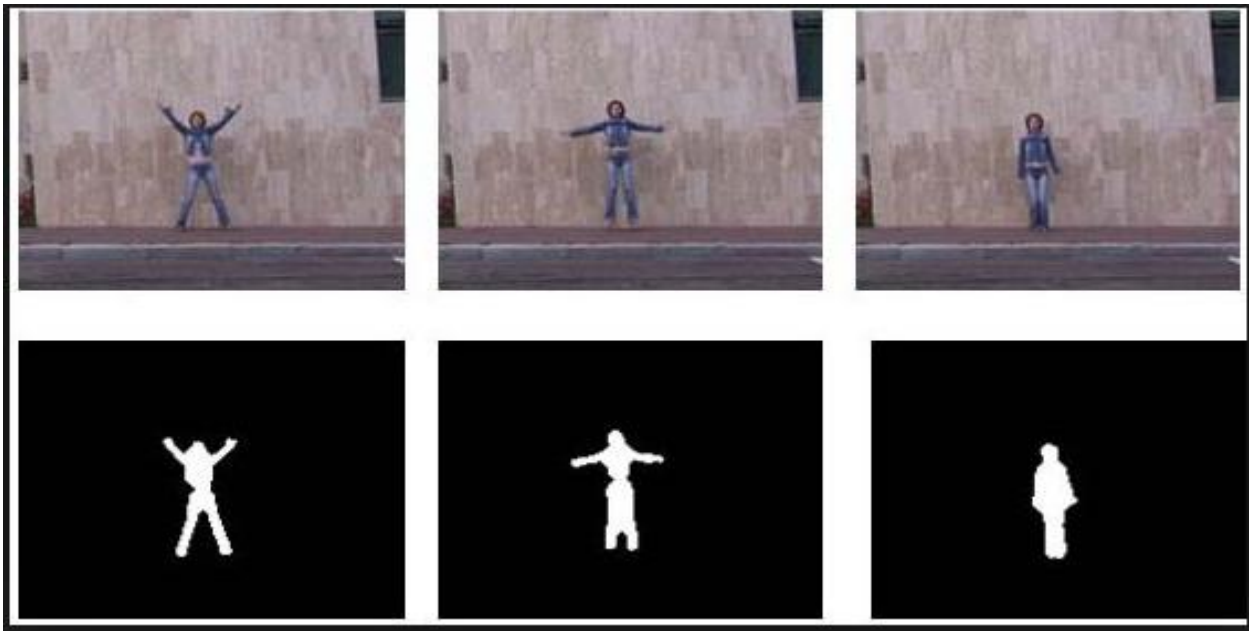

Fig.5. Human object region extraction for activity and behavior identification

5. CONCLUSION

According to present circumstances designing an automatic approach for detecting suspicious activity from video data for video surveillance systems is an important requirement. Unfortunately most existing approaches are hugely depending on human observers and there is no unified framework to meet this requirement. In this paper, we proposed a self-trainable, human activity and behavior detectable Intelligent Suspicious Activity Detection Framework (ISADF) for video surveillance systems. This framework contained video and extraction unit will extract the video data images as frameset and sends to video data processing unit for suspicious activity detection. Behavior Interpretation algorithm will compare the current activity against past experience to know whether activity is common, uncommon or unknown activity. BI Algorithm gives the activity type to SVM classifier to determine the level of activity ranges from 1 to 4. Experiments show that ISADF is able to process and identify the suspicious activities from KTH video data.

6. REFERENCES

[1] AACH, T. – KAUP, A.: "Statistical Model-Based Change Detection in Moving Video", Signal Processing, 31, pp. 165–180, 1993.

[2] BOJKOVIc, Z. – SAMcOVIc, A. – TURÁN, T:"Object Detection and Tracking in Video Surveillance Systems", COST 276 Workshop, Trondheim, Norvegia, pp. 113–116, May 25–26, 2005.

[3] R. Collins, Y. Tsin, J.R. Miller, and A. Lipton. Using a DEM to determine geospatial object trajectories. InProceedings of the 1998 DARPA Image Understanding Workshop, pages 115– 122, November 1998.

[4] Hae-Min Moon, Sumg Bum Pan:" A New Human Identification Method for Intelligent Video Surveillance System", 978-1-4244-7116-4/10, 2010 IEEE.

[5] http://www.imsresearch.com/research-areas.

[6] T.B Moelsund,A . Hilson, and V Kruger, " A Survey of Advances in vision based human motion capture and Analysis" Computer vision and image understanding special issue, vol-104,no 2-3,pp.90-126,2006.

[7] A. Mittal and D.Huttenlocher, "Scene modelling for wide area surveillance and image synthesis," in Proceedings IEEE conference on computer vision and pattern recognition ,2 ,pp. 160{167, (Hilton Head Isand, SC), June 2000.

[8]T. Kanade, R. Collins, A. Lipton, P. Anandan, and P. Burt. Cooperative multisensor video surveillance. In Proceedings of the 1997 DARPA Image Understanding Workshop, volume 1, pages 3–10, May 1997.

[9] " Incremental and adaptive normal behavior detection " by X.Tao and G. Shaogang from computer vision and understanding , vol. 111 , no. 1 ,pp 59-73, 2008.

[10] Massimo Piccardi, "Background subtraction techniques: a review", IEEE International Conference on Systems, man and cybernets 2004.

[11]" Multi Feature path modeling for video surveillance " by junejo, javed, shah in ICPR proceedings of the 17th International conference. VOL 2.PP. 716-719. vol2. 2004.

[12] A .Viswani , Roychowdary and challappa "activity recognition using the dynamics of the configuration of interaction objects" IEEE computer science society conference on, vol 2,pp 923-926.vol 2. 2004.

[13] HU.Yan Remote sensing image classification based on SVM classifier System Science, Engineering Design and Manufacturing Informatization (ICSEM), 2011 International Conference on (Volume:1) oct 2011.

[14] c.shuldt, laptev and capturo " Recognizing human actions : a local svm approach" in pattern reconization. ICPR proceedings of 17th international conference on vol 3,pp 32-36,2004.