JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

WEB INTERFACE FOR SUSPICIOUS ACTIVITY DETECTION FROM CCTV FOOTAGE

[1]Dasu Dasari, [2]Vijjeswarapu Anuhya Evangeline

[1]Assistant Professor, [2]B.Tech Student

[1]Department of Computer Science and Engineering

[1]Adikavi Nannaya University, Rajamahendravaram, India

Abstract: The escalation of anti-social activities has prompted a heightened emphasis on security measures. In response, numerous organizations have deployed Closed-Circuit Television (CCTV) systems to monitor individuals and their interactions continuously. In developed nations with sizable populations, each individual can be subjected to camera surveillance up to 30 times daily, resulting in a substantial accumulation of video data within defined time spans. For instance, video recording at 704x576 resolution and 25 frames per second yields an approximate daily data output of 20GB. However, manually scrutinizing this voluminous data for an abnormal event is a nearly unfeasible task due to the considerable human resources and sustained attention it necessitates. This challenge underscores the imperative to automate the monitoring process. Additionally, there is a crucial requirement to swiftly pinpoint the specific frame and segment containing unusual activities to expedite the identification of potential abnormalities. This study presents a solution by utilizing Convolutional Neural Network (CNN) algorithms. The approach involves converting video streams into individual frames and subjecting them to comprehensive analysis. By leveraging CNN, the system adeptly detects and categorizes individuals' activities, facilitating the identification of potentially suspicious behavior. The integration of CNN algorithms significantly enhances the accuracy of abnormal activity detection, making it an invaluable tool for ensuring public safety.

Index Terms **- Anti-Social Activities, Security, CCTV Footage, Abnormal Events, Surveillance, Convolutional Neural Network (CNN), Suspicious behavior, Public Safety.**

I. INTRODUCTION

The realm of person identification heavily relies on human facial features and behavioral patterns. Surveillance videos serve as a crucial wellspring of visual information, either in real-time or for retrospective examination. The modern trend of automation has significantly influenced the arena of video analytics, which encompasses diverse applications ranging from motion detection and human activity prediction to person and abnormal activity recognition. Among the techniques employed for person identification, face recognition and gait recognition stand out, with face recognition proving more versatile for automated person identification through surveillance videos. Face recognition not only predicts a person's identity but can also forecast their behavior based on head orientation. This paper introduces a methodology for detecting suspicious human activities through face recognition, particularly in contexts like examination halls. By delving into the intricate domain of video processing, this study addresses the intricate balance between computational efficiency and real-time surveillance demands. The proposed automatic suspicious activity detection system holds promise for minimizing malpractices, errors, and false alarms in educational institutions, presenting a sophisticated means to monitor and classify student activities during examinations. Through intelligent algorithms and real-time video analysis, the system identifies abnormal head motions, unauthorized student movements, and even inter-student interactions, offering a robust solution to maintain the integrity of examination environments.

II. SYSTEM ANALYSIS

Existing System: The current system operates by storing data in the form of records, necessitating continuous manual monitoring, which proves to be a labor-intensive task. Various detection techniques are employed to identify suspicious activities, albeit with limitations. Some researchers have attempted to develop models without leveraging established pre-trained models, resulting in the need to learn features from scratch. The drawbacks of this existing system include low accuracy in detection and high computational demands.

Disadvantages:

1. Low Accuracy: The existing system's reliance on detection techniques that are not well-optimized or based on established pre-trained models contributes to suboptimal accuracy in identifying suspicious activities. This can lead to both false positives and false negatives, undermining the system's reliability and effectiveness.
2. High Computation: The use of less refined or rudimentary detection methods in the existing system might result in high computational overhead. This can lead to slower processing times, delays in response, and potentially scalability issues when dealing with a larger volume of surveillance data.

Proposed System: In the proposed system, the focus shifts to enhancing the accuracy and efficiency of detecting anomalous behavior. To achieve this, Convolutional Neural Networks (CNNs) are employed, harnessing their capabilities for recognizing temporal patterns in video data. CNNs, which excel at extracting pertinent features from individual video frames, are identified as the optimal algorithm for this purpose. The key advantage lies in enabling CNNs to extract the necessary features from video frames, which is critical for accurate classification of anomalous activities.

Advantages:

1. High Accuracy: Leveraging CNNs for detecting suspicious activities can lead to significantly improved accuracy compared to traditional methods. CNNs are adept at learning complex patterns and features within visual data, enhancing the system's capability to accurately identify anomalies.
2. Effective Feature Extraction: The proposed system capitalizes on CNNs' ability to efficiently extract features from each frame of video data. This capability enhances the system's effectiveness in recognizing and classifying various types of suspicious behavior.
3. Temporal Data Recognition: By recognizing temporal patterns within video sequences, the proposed system can capture dynamic changes over time. This enables more nuanced and accurate identification of anomalous activities that might span multiple frames.
4. Efficient Classification: With the combination of accurate feature extraction and advanced classification capabilities, the proposed system can classify anomalous activities with a higher level of confidence, reducing the likelihood of false alarms and missed detections.

The proposed system adopts Convolutional Neural Networks (CNNs) to address the limitations of the existing system. By focusing on high accuracy, effective feature extraction, and temporal data recognition, the proposed system seeks to significantly enhance the detection of suspicious activities in surveillance videos, providing more reliable and efficient results.

III. System Architecture and Implementation

The proposed model encompasses a comprehensive approach to detect and analyze activities on websites and social media platforms. The step-by-step process of the model is as follows:

1. Data Collection: The process begins by extracting information from various websites and social media applications based on specific parameters. This data collection phase forms the foundation for subsequent analysis.
2. Preprocessing: The collected data undergoes preprocessing steps to ensure its suitability for analysis. This involves a series of actions such as noise removal, resizing, binary conversion, and grayscale conversion to enhance the quality and compatibility of the dataset.
3. Noise Removal: The input data, especially images and videos, undergo noise removal techniques using filters like average filters, median filters, Wiener filters, or Kalman filters. These filters effectively eliminate unwanted noise from the data.
4. Resizing: Image resizing is performed to adjust the total number of pixels, ensuring uniformity in the dataset. This step is particularly useful when managing variations in image dimensions.
5. Binary Conversion: Converting images into binary format involves representing each pixel with a binary value of 0 or 1. This simplifies the data representation and makes it suitable for certain types of analysis.
6. Grayscale Conversion: Grayscale conversion transforms images into grayscale representations, simplifying subsequent analysis processes while retaining crucial visual information.
7. Segmentation: Image segmentation involves the division of images into distinct segments or objects, facilitating more focused analysis. This step separates different components within the images for further processing.
8. Data Training: Both artificial and real-time data, including online news data, are compiled to create a training dataset. This dataset is then used to train machine learning classifiers, enabling them to recognize patterns and behaviors.
9. Feature Extraction: Feature extraction condenses the raw data into manageable groups, reducing dimensionality while retaining essential information. This is a crucial step in simplifying complex data for analysis.
10. Classification: Trained machine learning classifiers are used to classify and label groups of pixels or vectors within the data based on predefined rules. Classification identifies specific activities or patterns within the dataset.
11. Data Training (Social Media): Similar to the previous step, artificial and real-time social media data are gathered to form a training dataset. Machine learning classifiers are trained to detect specific activities in social media context.
12. Testing with Machine Learning: The developed system is tested using a separate dataset to evaluate its performance. Machine learning algorithms are applied to the testing dataset to accurately detect and classify activities.
13. Analysis: The accuracy and effectiveness of the proposed system are analyzed and compared to other existing systems. This analysis assesses the system's ability to identify and classify activities accurately.

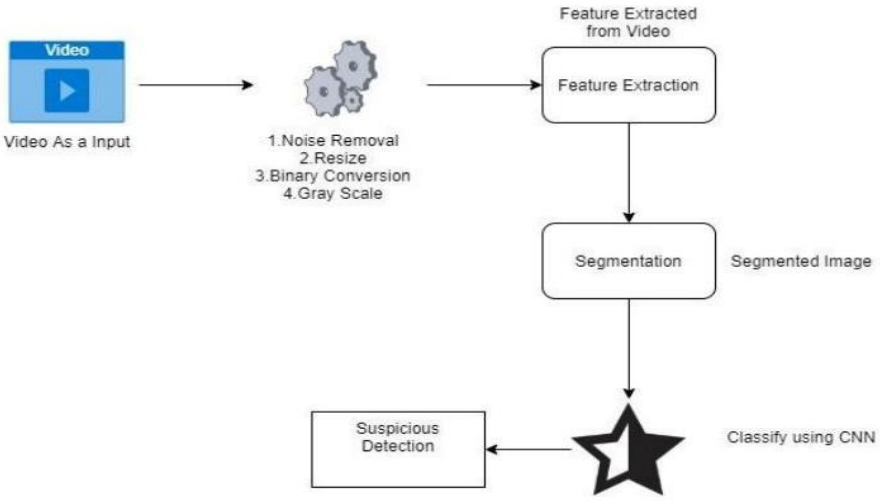

Fig.1 System Architecture

The proposed model integrates data collection, preprocessing, noise removal, segmentation, feature extraction, and machine learning classification to detect and analyze activities on websites and social media platforms. The combination of these steps enables the system to effectively identify and categorize various behaviors within the provided data, offering valuable insights and analysis.

In this project we need to detect person behavior as suspicious or not, now a day's everywhere CCTV cameras are installed which capture videos and store at centralized server and manually scanning those videos to detect suspicious activity from human required lots of human efforts and time. To overcome from such issue author is asking to automate such process using Machine Learning Algorithms.

To automate that process first we need to build training model using huge amount of images (all possible images which describe features of suspicious activities) and 'Convolution Neural Network' using TENSOR FLOW Python module.

Then we can upload any video and then application will extract frames from uploaded video and then that frame will be applied on train model to predict its class such as 'suspicious or normal'.

To implement above concept, we need to install python 3.5 version in 64-bit laptop. Once we install Python then we have to install tensorflow, numpy, scipy, opencv-python, pillow, matplotlib, h5py, keras using pip install command.

For training we used human images that cover their faces to perform suspicious activity and if any video contains person covering their faces then application will detect it as a suspicious activity.

IV. RESULTS

After implementing and deploying the proposed system for real-world criminal activity identification in surveillance videos, a comprehensive evaluation of the system's performance was conducted. The results of this evaluation provide insights into the effectiveness and efficiency of the system in detecting suspicious activities within surveillance footage.

Home Page:

Double click on 'run.bat' file from project folder to start project execution. We will get below Home Page. We can select and upload the video, Generate Frames and Detect Suspicious Activity Frame from this page.

a) Click on 'Upload CCTV Footage' button to upload video:

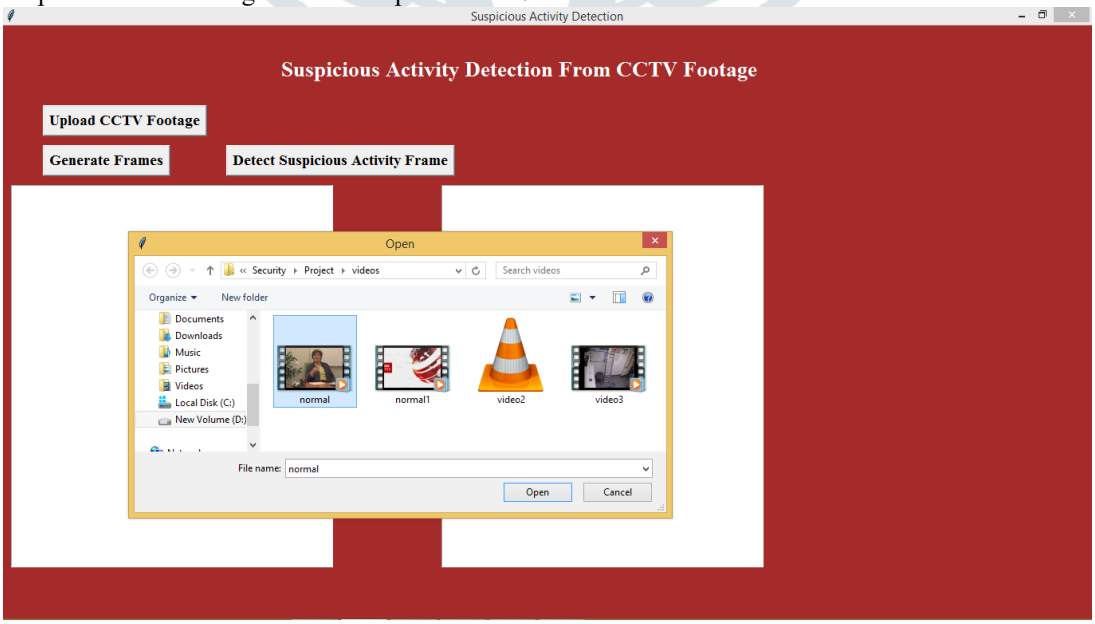

Fig.2 Select the Video

In above screen we can upload a video.

b) After uploading video click on 'Generate Frames' button to generate frames:

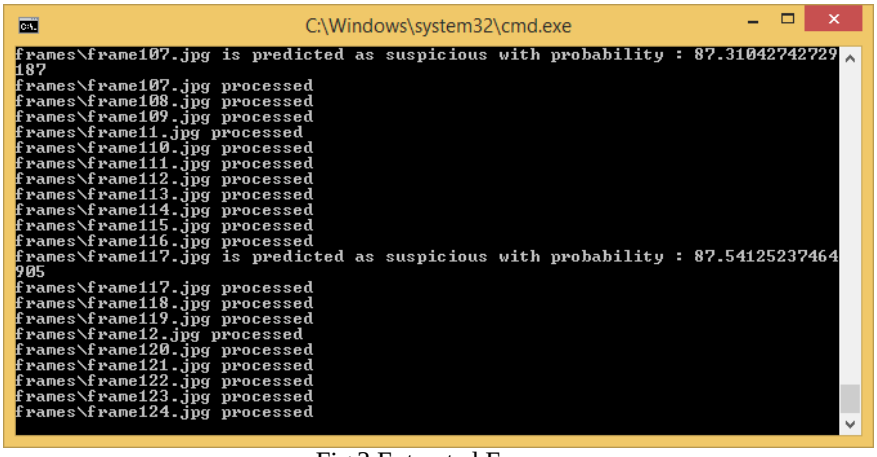

Fig.3 Extracted Frames

In above black screen we can see extracted frames are saving inside 'frames' folder frame no.

In this screen for uploaded video we can see suspicious activity found at farme117.jpg. After scanning all images, we will get below details screen in Fig4. Now in below screen we can see frame117 image from frames folder. Then we see frames folder below which has images from video.

Fig 4 Frame 117 with suspicious activity

In above screen frame117.jpg shows one image of a person with face covering.

c) Similarly we can see all frames details in below screen which has such activities by click on detect suspicious activity frame:

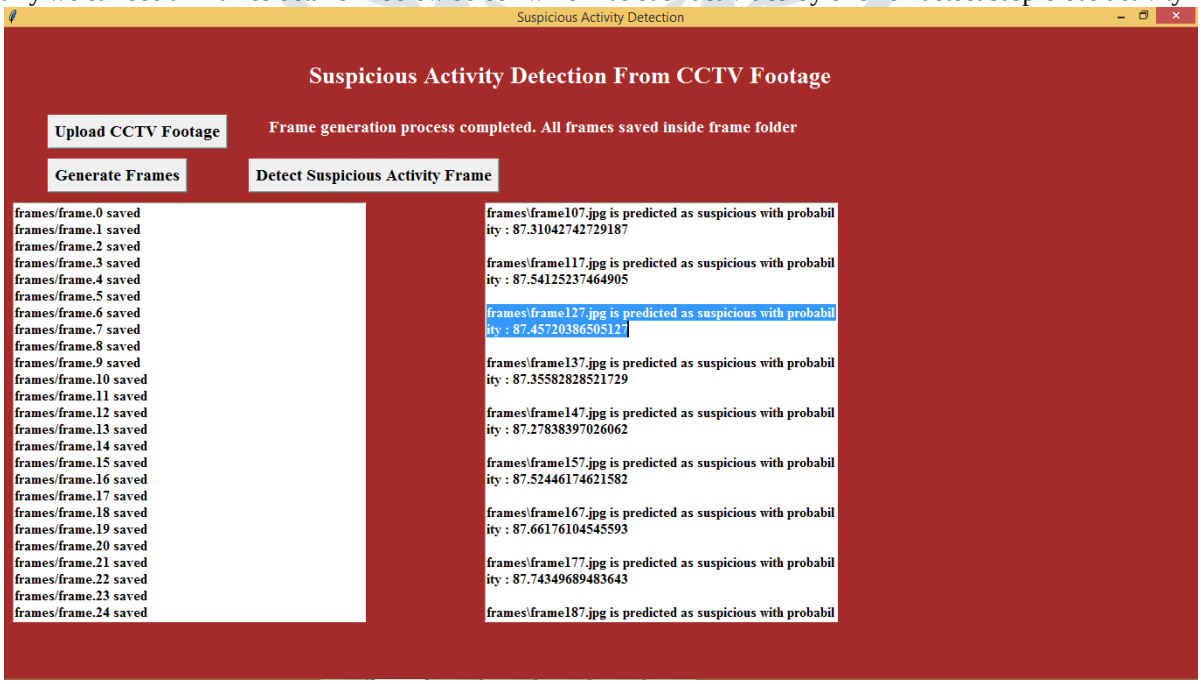

Fig.5 detected suspicious activity frame

In above screen in right text area we can see details of all frames which have such activities.

Note: You too can upload your own videos and check, but your videos must have person covering their faces or doing shop lifting robbery videos. Your videos must be like similar one which we used in this project.

V. CONCLUSION

In conclusion, the proposed system represents a significant advancement in the realm of crime detection through the application of machine learning to surveillance videos. With the escalating frequency of criminal activities in today's world, the development of such security systems has become paramount. This system's purpose lies in its capability to swiftly and accurately identify real-world criminal activities within surveillance footage. By addressing the pressing need for enhanced security measures, the proposed system contributes to public safety and law enforcement efforts.

The outcome of this research yields a solution capable of distinguishing between normal and anomalous actions captured in surveillance videos. Traditional approaches often suffered from lower accuracy rates in detecting abnormal behaviors, making accurate crime identification challenging. In response, this study introduces a novel approach by employing Convolutional Neural Networks (CNNs) to facilitate the identification of suspicious activities with improved efficiency.

By harnessing the power of CNNs, the proposed system aims to significantly enhance the accuracy and reliability of detecting anomalous actions. The integration of this advanced algorithm allows for the identification of subtle deviations from standard behaviors, enabling security personnel to respond promptly to potential threats. The utilization of CNNs marks a substantial departure from conventional methods and contributes to a more effective and robust crime detection mechanism.

As a result, the proposed system not only addresses the growing demand for improved security solutions but also offers a practical and efficient means to identify criminal activities in surveillance videos. By incorporating cutting-edge technology and innovative methodologies, this research contributes to the advancement of crime prevention strategies, ensuring a safer environment for communities and individuals alike.

REFERENCES

[1] System UFC Crime Dataset (Two classes anomalous and non-anomalous) 85% Vol-7 Issue-3 2021 IJARIIE-ISSN(O)-2395-4396 14261 www.ijariie.com 694

[2] Jefferson Ryan MEdel, Andreas Savakis, “Anomaly Detection in Video Using Predictive Convolutional Long Short-Term Memory Networks” under review.

[3] W. Luo, W. Liu, and S. Gao, “A revisit of sparse coding based anomaly detection in stacked RNN framework,” in The IEEE International Conference on Computer Vision (ICCV), Oct 2017

[4] Y. S. Chong and Y. H. Tay, “Abnormal event detection in videos using spatiotemporal auto-encoder,” in International Symposium on Neural Networks. Springer, 2017, pp. 189–196.

[5] J. R. Medel and A. Savakis, “Anomaly detection in video using predictive convolutional long short-term memory networks,” arXiv preprint arXiv:1612.00390, 2016.

[6] M. Hasan, J. Choi, J. Neumann, A. K. Roy-Chowdhury, and L. S. Davis, “Learning temporal regularity in video sequences,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 733–742.