Original Article

Suspicious Activity Detection Using Convolution Neural Network

S. A. Quadri [1], Komal S Katakdhond [2]

[1] Professor CSE Department, SECAB IET, Vijayapur, India

[2] PG Student, CSE Department, SECAB IET, Vijayapur, India.

DOI: 10.47750/pnr.2022.13.S01.151

Abstract

Video Surveillance plays a significant role in today's world. Various technologies have been utilized to implement the safety of life and property by installing high quality CCTV cameras. It is impossible to manually monitor each and every moment activity. Furthermore, in practical scenario the most unpredictable one is human behaviour and it is very difficult to find whether it is suspicious or normal. In this work the notion of Convolution Neural Network is used to detect suspicious or normal activity in an environment, and a system is proposed that sends an alert message to the corresponding authority, in case of predicting a suspicious activity.

Keywords: Convolution Neural Network, Anomaly, CCTV, Video Surveillance.

INTRODUCTION

Human activity recognition is valuable in variety of scenarios, and anomaly detection in security systems is one of among them. With the increasing demand for security, surveillance cameras have been widely set up as the infrastructure for video analysis. The videos/footages are captured and stored in memory devices. Several organizations have installed CCTVs cameras for continuous monitoring of individuals and their interactions. As an advanced nation, India which has 1380 million population, suppose, everyone is captured in a camera at least one time in a day, it will be mission impossible to manually monitor all activities and predict their behaviour.

One of the major challenges faced by surveillance video analysis is detecting abnormal activity which requires exhausting human efforts. Fortunately, such a tedious and cumbersome task can be recast as an anomaly detection problem which aims to detect unexpected actions or patterns. Anomaly detection varies from the traditional classification problem in the following aspects: 1) It is very difficult to list all possible negative illustrations. 2) It is a laborious job to collect adequate negative samples due to the rarity.

An automated activity recognition system is required to identify the basic day to day activities performed by a human being. It is challenging to achieve high-rate accuracy for recognition of these activities due to the complexity and diversity in human activities. Activity models required for identification and classification of human activities are constructed based on different approaches specific to the application. The activities of a human being can be generally categorized into normal activities or anomalous activities. A human being’s deviation from normal behaviour to abnormal causing harm to the surrounding or to himself is classified as an anomalous activity. To achieve anomaly detection, one of the most widespread methods is using the videos of normal events as training data to learn a model and then detecting the suspicious events which would do not fit in the learned model. For example, human pose guesstimate is used in applications including video surveillance, animal tracing and actions understanding, sign language recognition, advanced human-computer interaction, as well as marker less motion capturing.

In this paper, a methodology is proposed using CNN approach that classifies and detects suspicious activities in the ongoing or stored videos. The whole automated process will affirm safety and security of the premises under surveillance.

LITERATURE REVIEW

The domain of monitoring of the data acquired by image sensors has a wide spectrum. Several researchers have implemented various algorithms for image processing and detection of anomaly. There exists a vast literature review of several contributors in the field of camera surveillance. A brief of the same is presented below.

Joey et al. [1] proposed sparse coding approach for video processing. The methodology utilized labelled constructed anomaly detection method which has manifested better performance. An innovative neural network is proposed for anomaly detection which is also labelled as Anomaly Net by deeply accomplishing feature learning, sparse representation as well as dictionary learning in three joint neural processing blocks. Specifically, to learn improved features, the authors designed a motion fusion block accompanied by a feature transfer block to relish the benefits of eliminating background noisy, capturing motion and improving data insufficiency.

A suspicious activity is any observation of action that could state a person may be involved in a crime or is about to commit a certain criminality. Anomaly detection is the process detecting suspicious activity. Surveillance cameras are one of the best solutions to the issue of security in various places. Present-day system needs man power for monitoring the system as detecting and identifying criminal and abnormal activity is so challenging. Monika and Tejashri [2] proposed anomaly detection for video surveillance using concepts of recurrent neural network (RNN).

Jefferson and Andreas [3] worked on Predictive Convolutional Long Short-Term Memory Networks. They proposed a method that automates the detection of anomalous actions within long video series is challenging due to the uncertainty of how such events are defined. The authors tackled the problem by learning generative models that can discover anomalies in videos using restricted supervision. Projected end-to-end trainable complex Convolutional Long Short-Term Memory (Conv-LSTM) networks that are able to predict the development of a video sequence from a minor number of input frames.

Luo et al. [4] presented an efficient technique for identifying anomalies in videos. The Authors inspired by the capability of sparse coding based suspicious detection, projected a Temporally-coherent Sparse Coding (TSC) where they implement similar neighbouring frames be encoded with alike reconstruction coefficients. Then mapped the TSC with a distinct type of stacked Recurrent Neural Network (sRNN). The contributions of the paper are- i) proposed a TSC, which can be recorded to a sRNN which facilitates the parameter optimization and speed up the doubtful prediction. ii) Build a very huge dataset that is even larger than the summation of all existing dataset for finding anomalous activity.

Chong and Tay [5] presented an efficient technique for identifying anomalies in the videos. Recently applications of convolutional neural networks have shown possibilities of convolutional layers for object detection and recognition, specifically in images. Though, convolutional neural networks are supervised and have need of labels as learning signals. Authors as well as proposed a spatiotemporal architecture for suspicious detection in videos with crowded scenes.

Medel and A. Savakis [6] proposed end-to-end trainable complex Convolutional Long Short-Term Memory (Conv-LSTM) networks. These Conv-LSTM networks are capable to predict the evolution of a video sequence from a minor number of input frames. Consistency scores are derived from the renovation errors of a set of estimates with irregular video sequences yielding lower regularity scores as they separate further from the actual sequence over time. The models employ a composite structure and observe the special effects of conditioning in learning more meaningful representations.

Hasan et al. [7] the approach for the problem of anomaly detection by learning a generative model for consistent motion patterns using multiple resources with very restricted supervision. Specifically, paper contains two methods that are built upon the autoencoders for their capacity to work with little to no supervision. The first method is to leverage the conventional handcrafted spatio-temporal local features and then study the fully connected autoencoder. Secondly, construct a fully convolutional feed-forward autoencoder to learn together the local features and the classifiers as an end-to-end learning structure. The proposed model is able to capture the regularities from numerous datasets.

Sabokrou et al. [8] proposed the technique for actual time anomaly detection and localization in crowded scenes. Each video is well-defined as a set of non-overlapping cubic spots, and is explained using two local and global descriptors. The descriptors used here capture the video assets from different phases. By integrating simple and cost-effective Gaussian classifiers, we can distinguish normal events and anomalies in videos.

Lu et al. [9] proposed a method that is based on inherent redundancy of video structures. The authors proposed an effective sparse combination learning framework. It accomplishes decent performance in the detection phase deprived of compromising result quality. The short running time is fail-safe because the new method efficiently turns the original complex problem to one where only a few less in cost small-scale least square optimization steps are considered. The process scopes high detection rates on benchmark datasets when figuring on a usual desktop PC by using MATLAB programming.

Mousavi et al. [10] proposed a notion in which a fully unverified dynamic sparse coding methodology for spotting unusual events in videos based on online sparse re-constructability of query signals is proposed. Based on a perception that usual events in a video are mostly liked to be re-constructible from an event dictionary, whereas infrequent events are not, the algorithm works on a principled convex optimization formulation that permits both a sparse reconstruction code, and an online dictionary to be mutually inferred and modernized.

However, there exist several methods in which anomalies are detected for security applications [11-14], in our proposed model we have developed automated screening of videos, which finally classifies normal and suspensions activities. The system sounds an alarm if any suspicious activity is found.

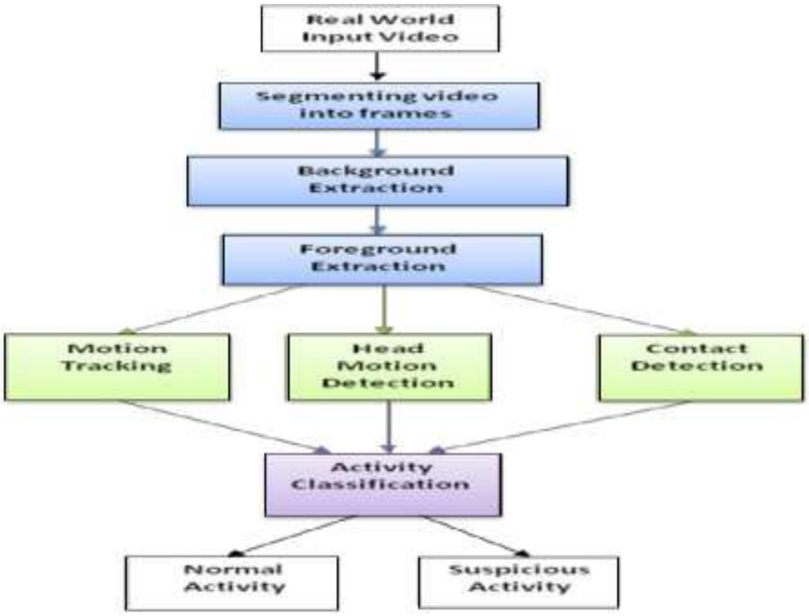
MATERIALS AND METHODS

1) Work flow model

Human behaviour and the human face are key factors in identifying a person. A critical source for these identifications is visual data. Surveillance footage offers this kind of visual data that may be watched in real time or recorded for later use. Even the field of video analytics is being impacted by the current "automation" movement. Applications for video analytics include human action prediction, motion recognition, person documentation, automobile counting, anomalous action recognition, crowd including, and many more.

Security and research are two major fields that use video processing. Such equipment keeps an eye on live videos using clever algorithms. A real-time system's design must consider a number of important elements, including time and computational complexity. The system that usages one algorithm including a relatively lesser period complexity, consuming a reduced amount of hardware properties then whichever produces respectable results resolve stand extra useful designed for period critical requests corresponding bank theft detection, patient specialist care system, noticing also writing doubtful actions by the railway place, etc. The flow of work is shown in the figure 1.

Figure 1: Suspicious activity detection Architecture



Considering a case of manual intensive care of exam hall that includes physical monitoring of exam hall, investigating videos that are stored through the episode. In terms of manpower requirements, monitoring an exam room is an extremely difficult undertaking. When used an "automated suspicious activity detection system," such a system decision not one assist popular identifying doubtful activity then as well in reducing it. Also, the probability based on error much smaller. The present structure feeling helps as per valuable surveillance structure since informative organizations.

The present study defines tool that analyses actual recordings of people in a testing environment and uses that information to classify whether or not their behaviour is suspicious. The advanced system categorises anomalous head movements, preventing reproduction. Additionally, it indicates when a pupil switches places with another student or leaves his spot. Finally, the system recognises student contact and stops students from transmitting accusatory information to one another. Our study has helped develop a system that can analyse real-time video of test rooms filled for students then categorise her behaviour just as doubtful or not.

The doubtful human action finding system goals into identify every student who pamper latest doubtful actions through the sequence based on examination. Every system mechanically senses doubtful actions also signals direction. This program will take its ideas from how the Visual Cortex function in the human brain. Processing of visual data from the external world is carried out through the visual cortex, a region of every human brain. Once every information collected after respectively layer has been integrated, image or visual move interpreted or classed. Similar to this, CNN uses a variety of filters that each collect data after the image, on the point of edges and numerous forms (vertical, horizontal, and round), which are combined into identify every image.

2 STEPS OF CNN

The Software requirements are Python, Django, MySQL and Wamp Server. The steps of CNN are listed below:

Step 1: Input is given as image / video.

Step 2: Then many different filters are applied to the input to create a feature map.

Step 3: Next a ReLU (Rectified Linear Unit) function is applied to increase non-linearity.

Step 4: Then applies a pooling layer to each and every feature map.

Step 5: The algorithm compresses the pooled images into one long vector.

Step 6: In next step, inputs the vector to the algorithm into a fully connected artificial neural network.

Step 7: Processes the features via the network. At the end fully connected layer delivers the “voting” of the classes.

Step 8: In this last step training is conducted through forward propagation and back propagation for numerous epochs. This repetition occurs until we have a well-defined neural network with trained weights and feature detectors.

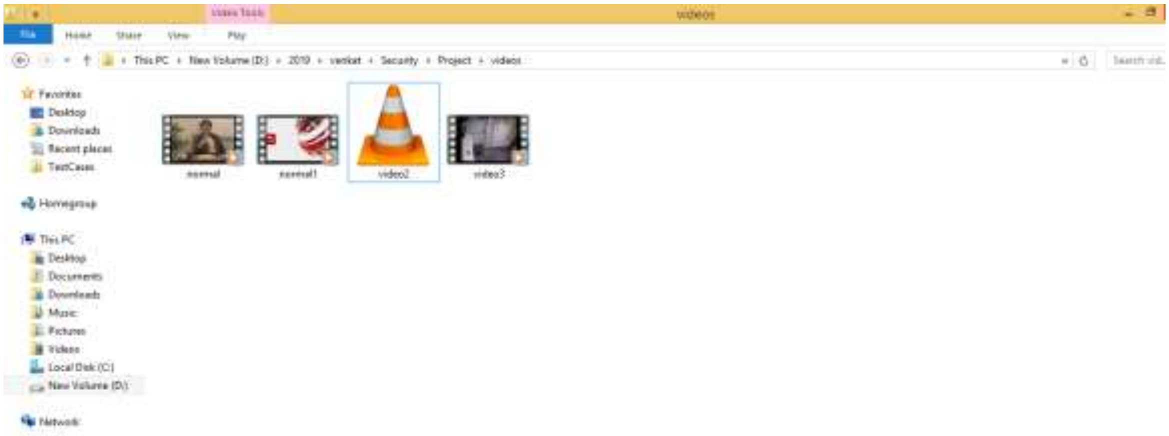
RESULTS AND DISCUSSION

Python 3.5 must be installed on a 64-bit laptop in order to put the above concept into practise. Will send the source code for this application. It is important to check the box labelled "Add path to system variable" while installing the software. This choice will show on either first or second installation screen. After installing the software, run the commands below. In the whole episode computer has to be online. These are nine commands that should be executed for installation. pip install tensor flow 2) pip install numpy 3) pip install scipy 4)pip install opencv-python 5)pip install pillow 6) pip install matplotlib7) pip install h5py 8) pip install keras 9) pip installs

The initial step in automating the procedure is to create a training model utilising a large number of photos (all images that could possibly identify aspects of suspicious activity) and using the Python library TENSOR FLOW, create a Convolution Neural Network. Then, after uploading any video, the application will take its frames and use those to train a model to determine the video's type, such as "suspect or normal."

Below are the sequence of all steps during execution. Two types of videos are fed, one with the normal images and other with the images whose faces are fully covered with masks. The fully covered faces are thought to be suspicious people.

Figure 2: Selection of images



Double click on ‘run. bat’ file from project folder to start project execution. We will get below screen.

Figure 3: Connect operating transmit CCTV Footage switch to transmit audio-visual

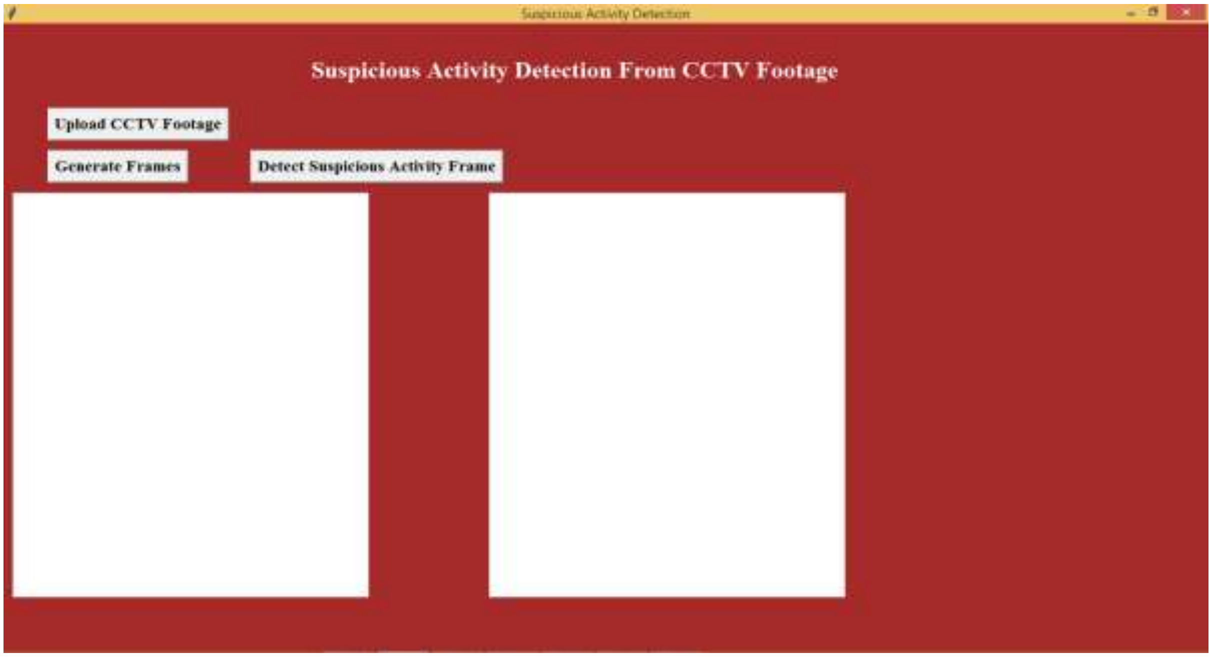

Suspicious Activity Detection
Suspicious Activity Detection From CCTV Footage
Upload CCTV Footage
Generate Frames
Detect Suspicious Activity Frame

Figure 4: Latest overhead screen, transferring unique ordinary video.

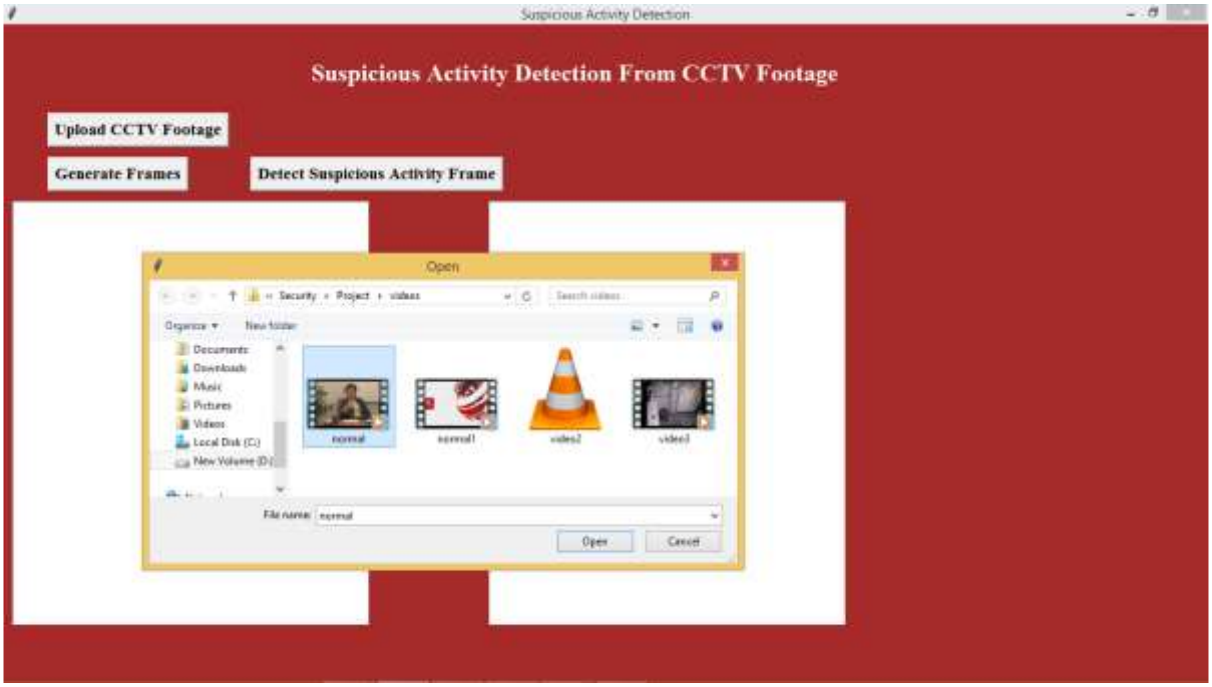
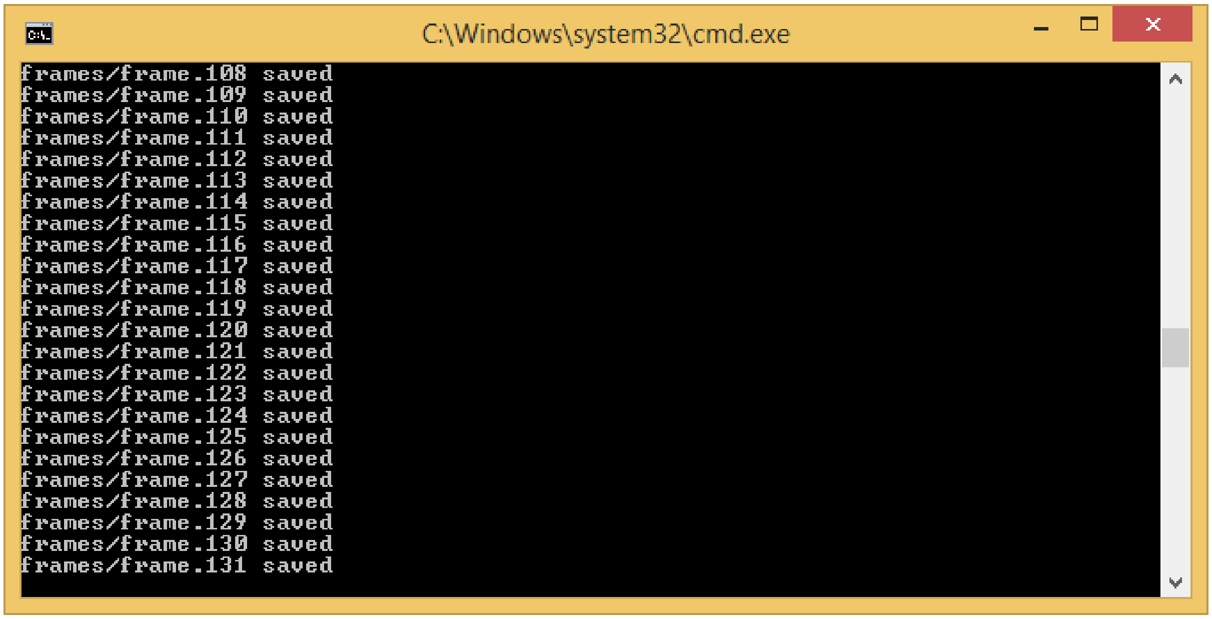


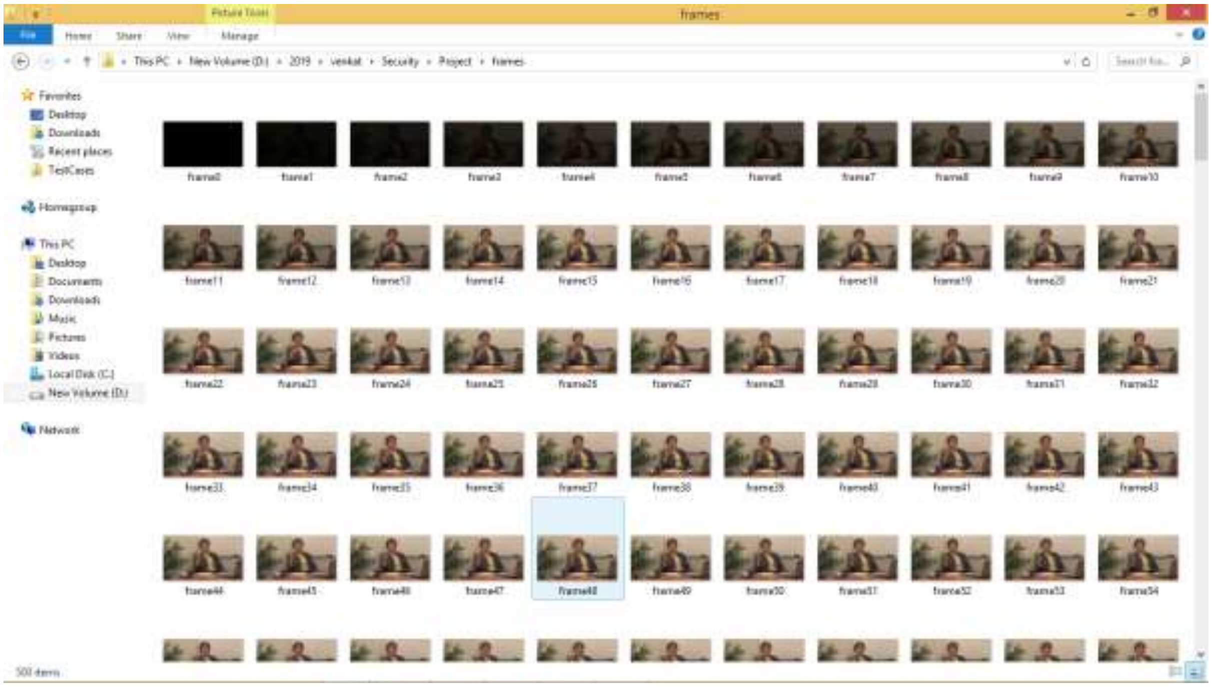
Figure 5: Saving the frames from Video



```
frames/frame.108 saved
frames/frame.109 saved
frames/frame.110 saved
frames/frame.111 saved
frames/frame.112 saved
frames/frame.113 saved
frames/frame.114 saved
frames/frame.115 saved
frames/frame.116 saved
frames/frame.117 saved
frames/frame.118 saved
frames/frame.119 saved
frames/frame.120 saved
frames/frame.121 saved
frames/frame.122 saved
frames/frame.123 saved
frames/frame.124 saved
frames/frame.125 saved
frames/frame.126 saved
frames/frame.127 saved
frames/frame.128 saved
frames/frame.129 saved
frames/frame.130 saved
frames/frame.131 saved
```

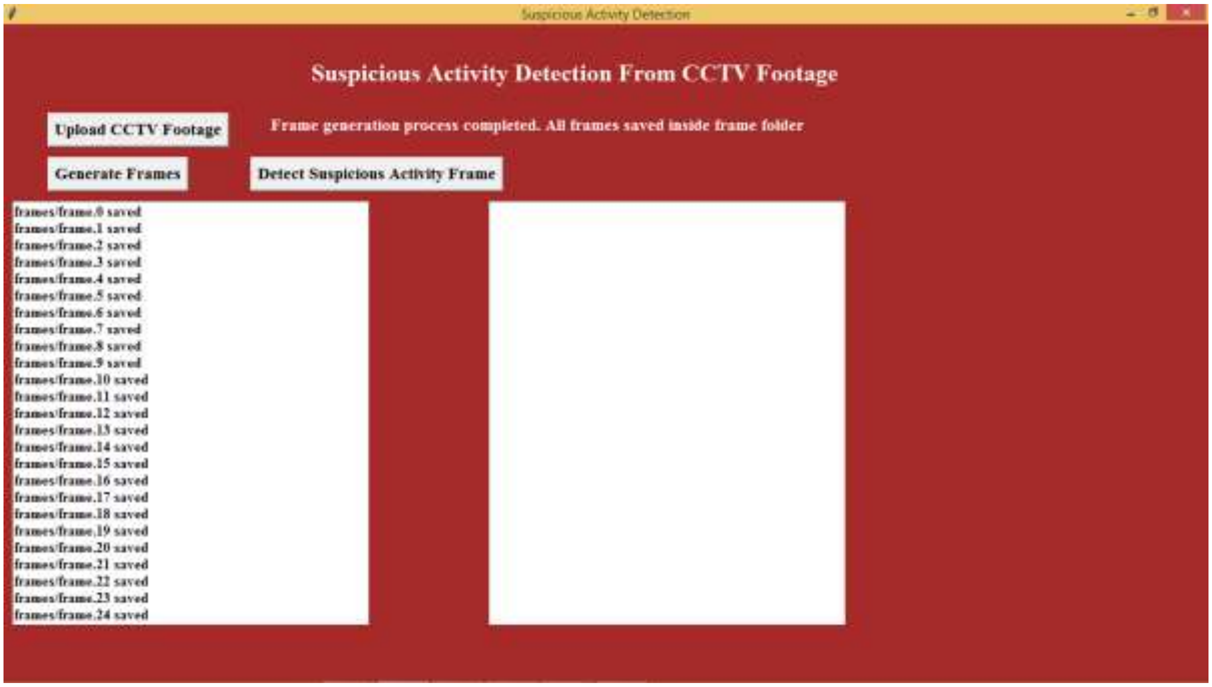
directly overhead black shelter we container get extracted frames be located good inside ‘frames’ file frame number.

Figure 6: Frame Mining



The above file shelter can realize all picture safter video pull out. Following frame mining, the screen desire be lower.

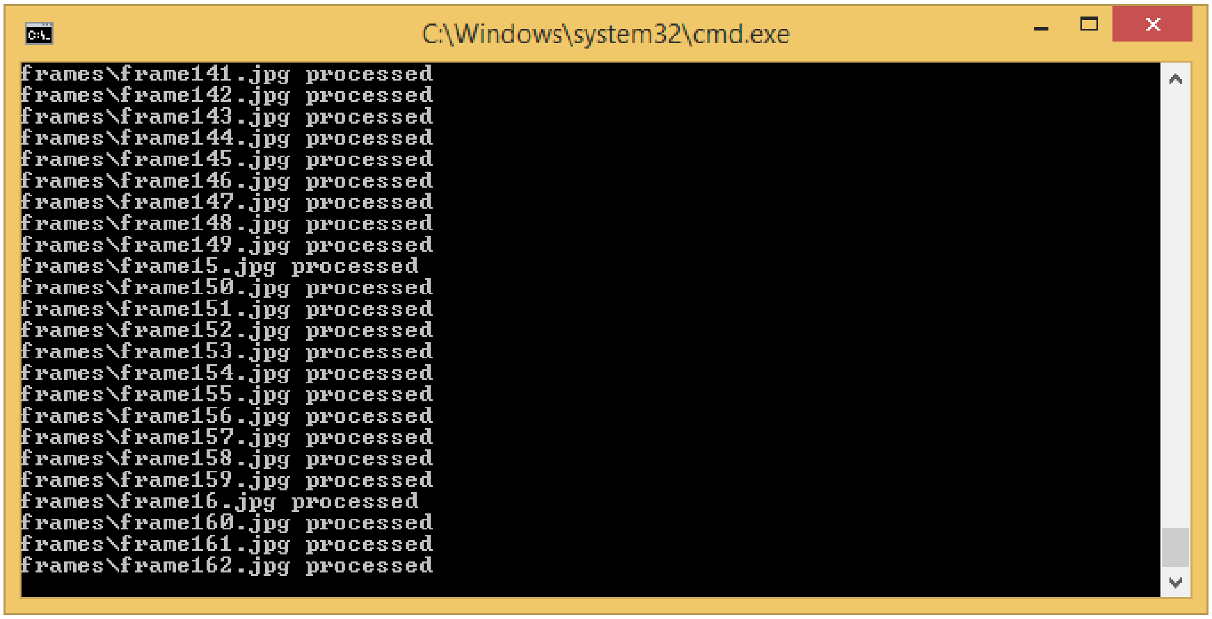
Figure 7: Frame saving


Suspicious Activity Detection
Suspicious Activity Detection From CCTV Footage
Upload CCTV Footage
Generate Frames
Detect Suspicious Activity Frame

Frame generation process completed. All frames saved inside frame folder

```
frames/frame.0 saved
frames/frame.1 saved
frames/frame.2 saved
frames/frame.3 saved
frames/frame.4 saved
frames/frame.5 saved
frames/frame.6 saved
frames/frame.7 saved
frames/frame.8 saved
frames/frame.9 saved
frames/frame.10 saved
frames/frame.11 saved
frames/frame.12 saved
frames/frame.13 saved
frames/frame.14 saved
frames/frame.15 saved
frames/frame.16 saved
frames/frame.17 saved
frames/frame.18 saved
frames/frame.19 saved
frames/frame.20 saved
frames/frame.21 saved
frames/frame.22 saved
frames/frame.23 saved
frames/frame.24 saved
```

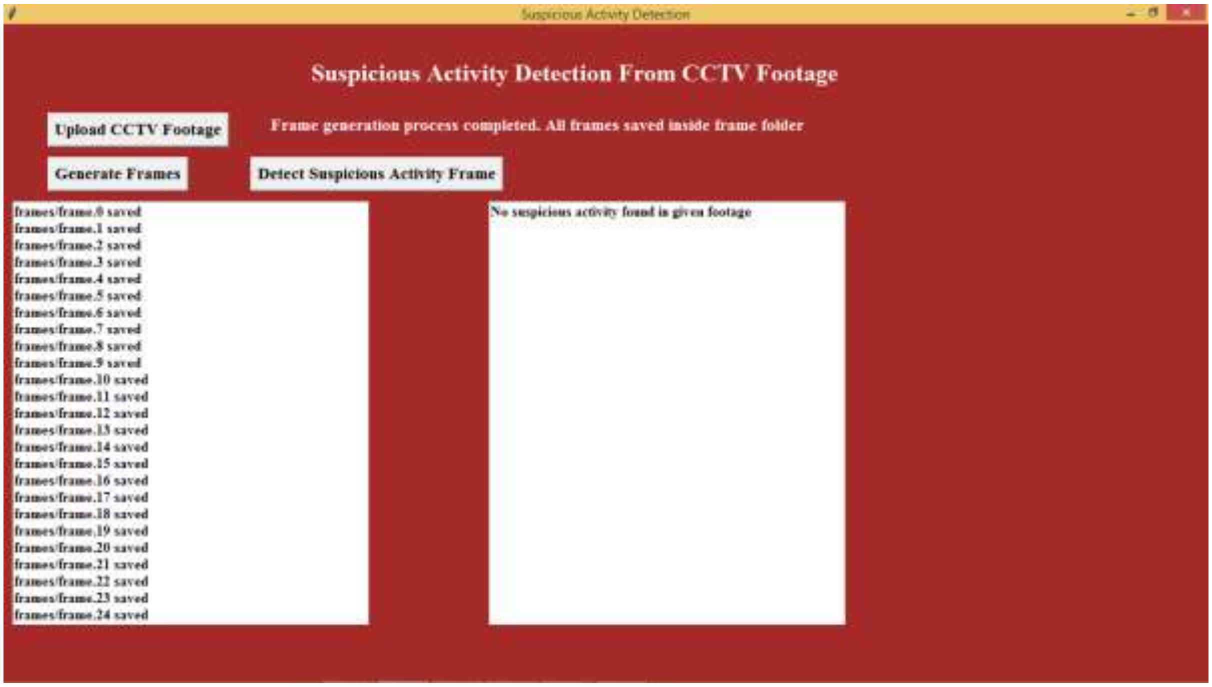
Figure 8: Frame Processing



```
frames\frame141.jpg processed
frames\frame142.jpg processed
frames\frame143.jpg processed
frames\frame144.jpg processed
frames\frame145.jpg processed
frames\frame146.jpg processed
frames\frame147.jpg processed
frames\frame148.jpg processed
frames\frame149.jpg processed
frames\frame15.jpg processed
frames\frame150.jpg processed
frames\frame151.jpg processed
frames\frame152.jpg processed
frames\frame153.jpg processed
frames\frame154.jpg processed
frames\frame155.jpg processed
frames\frame156.jpg processed
frames\frame157.jpg processed
frames\frame158.jpg processed
frames\frame159.jpg processed
frames\frame16.jpg processed
frames\frame160.jpg processed
frames\frame161.jpg processed
frames\frame162.jpg processed
```

Directly overhead black comfort opening can get meting out about respectively edge facing detect doubtful action.

Figure 9: Result showing that no suspicion



Suspicious Activity Detection
Suspicious Activity Detection From CCTV Footage
Upload CCTV Footage
Generate Frames
Detect Suspicious Activity Frame

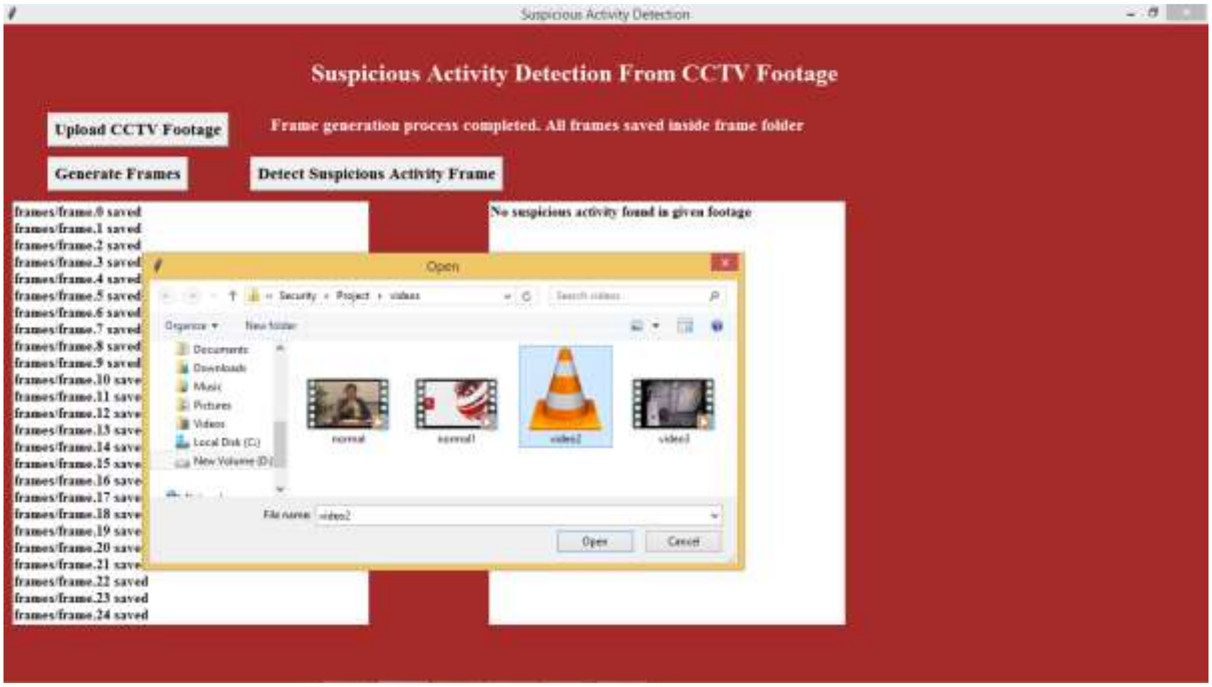
Frame generation process completed. All frames saved inside frame folder

```
frames/frame.0 saved
frames/frame.1 saved
frames/frame.2 saved
frames/frame.3 saved
frames/frame.4 saved
frames/frame.5 saved
frames/frame.6 saved
frames/frame.7 saved
frames/frame.8 saved
frames/frame.9 saved
frames/frame.10 saved
frames/frame.11 saved
frames/frame.12 saved
frames/frame.13 saved
frames/frame.14 saved
frames/frame.15 saved
frames/frame.16 saved
frames/frame.17 saved
frames/frame.18 saved
frames/frame.19 saved
frames/frame.20 saved
frames/frame.21 saved
frames/frame.22 saved
frames/frame.23 saved
frames/frame.24 saved
```

```
No suspicious activity found in given footage
```

The overhead screen can realize edges and finally detects that there is no suspension.

Figure 10: Next video is selected for processing



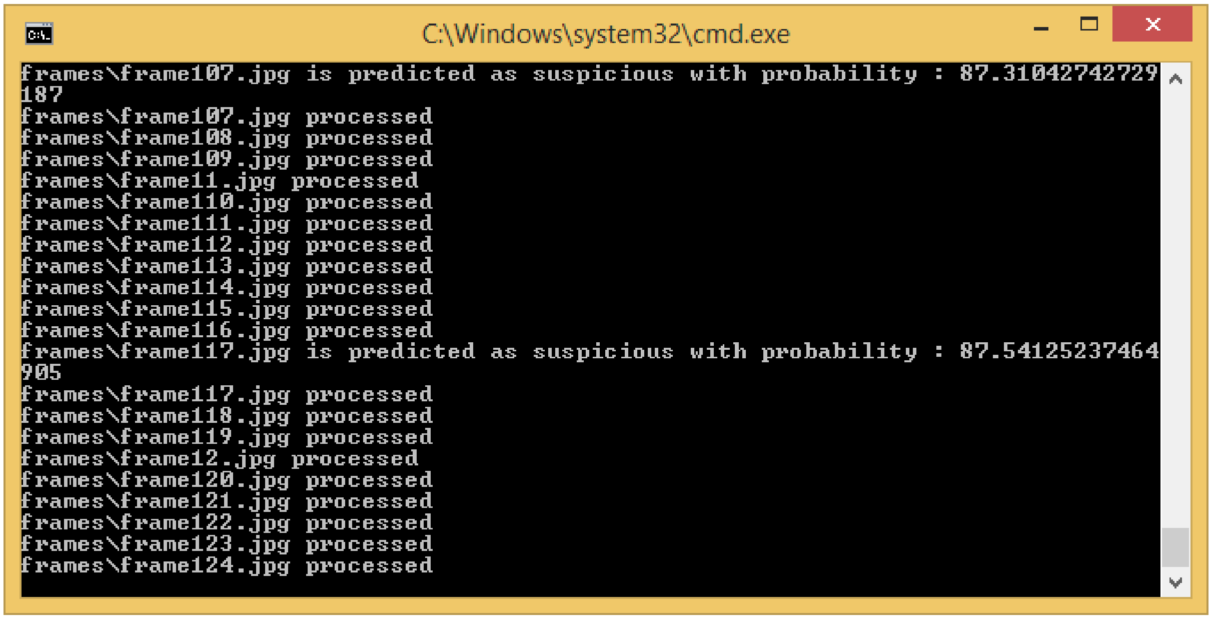
Frame generation process completed. All frames saved inside frame folder

```
frames/frame.0 saved
frames/frame.1 saved
frames/frame.2 saved
frames/frame.3 saved
frames/frame.4 saved
frames/frame.5 saved
frames/frame.6 saved
frames/frame.7 saved
frames/frame.8 saved
frames/frame.9 saved
frames/frame.10 save
frames/frame.11 save
frames/frame.12 save
frames/frame.13 save
frames/frame.14 save
frames/frame.15 save
frames/frame.16 save
frames/frame.17 save
frames/frame.18 save
frames/frame.19 save
frames/frame.20 save
frames/frame.21 save
frames/frame.22 saved
frames/frame.23 saved
frames/frame.24 saved
```

No suspicious activity found in given footage

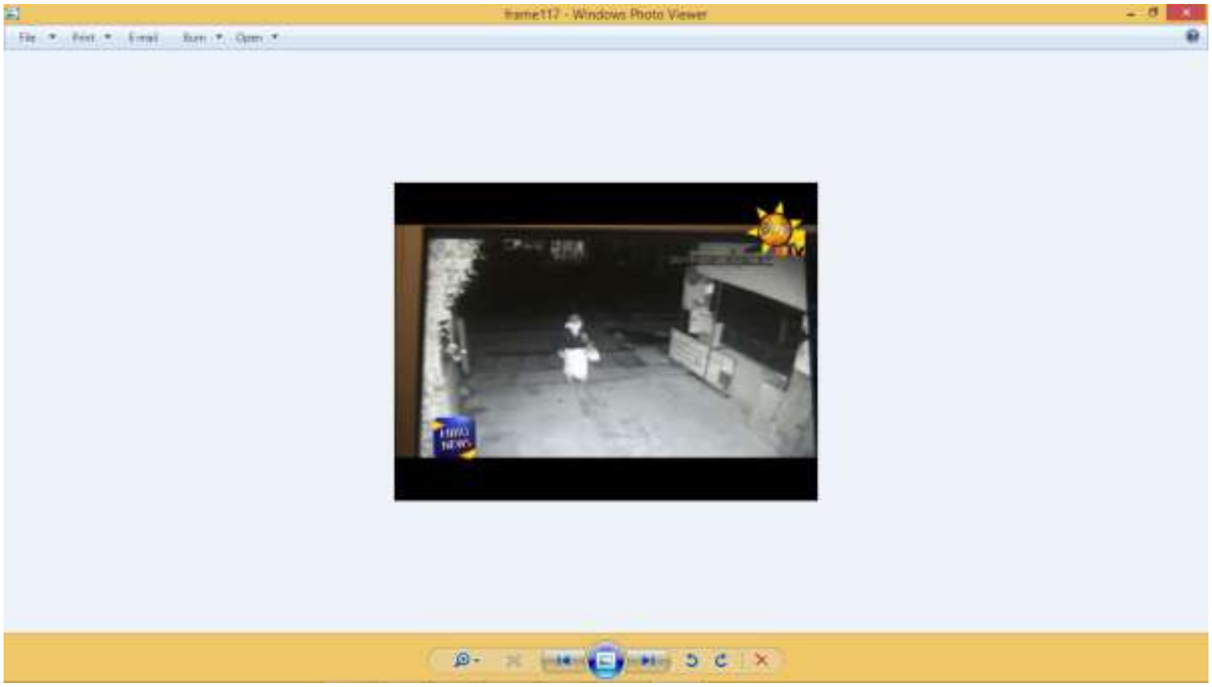
The above screen shows uploading of Video 2, selected or suspicious activity detection.

Figure 11: Frame Processing



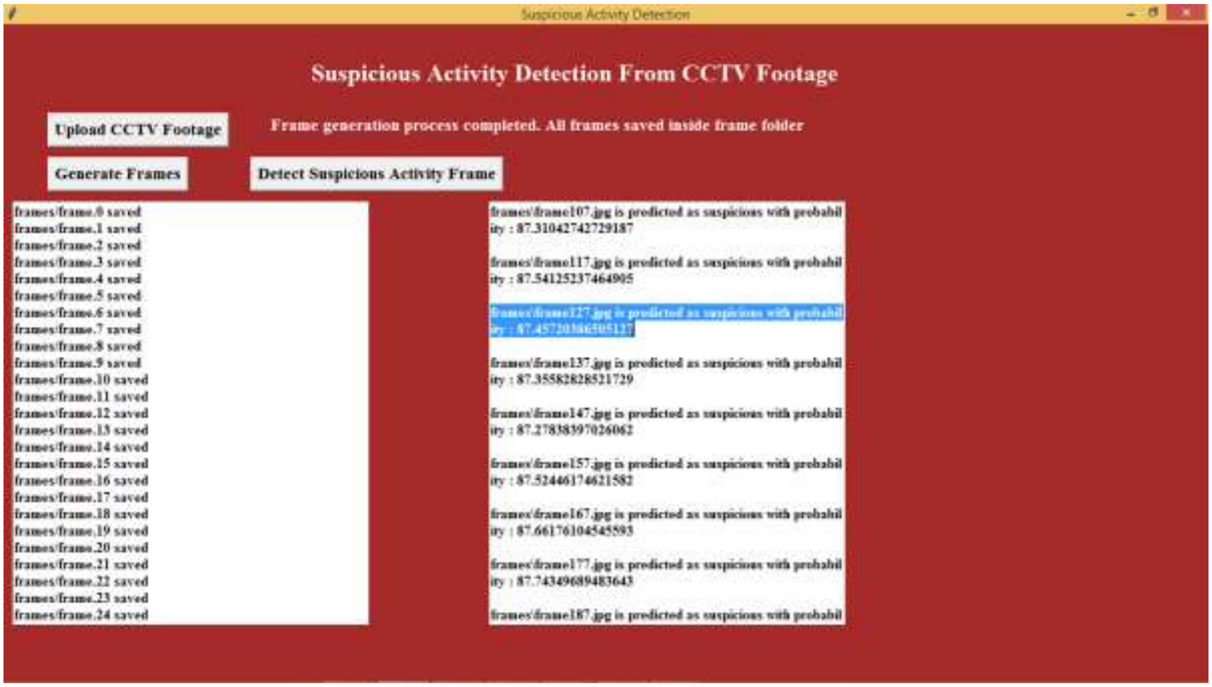
```
frames\frame107.jpg is predicted as suspicious with probability : 87.31042742729
187
frames\frame107.jpg processed
frames\frame108.jpg processed
frames\frame109.jpg processed
frames\frame11.jpg processed
frames\frame110.jpg processed
frames\frame111.jpg processed
frames\frame112.jpg processed
frames\frame113.jpg processed
frames\frame114.jpg processed
frames\frame115.jpg processed
frames\frame116.jpg processed
frames\frame117.jpg is predicted as suspicious with probability : 87.54125237464
905
frames\frame117.jpg processed
frames\frame118.jpg processed
frames\frame119.jpg processed
frames\frame12.jpg processed
frames\frame120.jpg processed
frames\frame121.jpg processed
frames\frame122.jpg processed
frames\frame123.jpg processed
frames\frame124.jpg processed
```

Figure 12: Suspicious video



This overhead screen frame 117 screening unique image about individual by look covering.

Figure 13: Detection of suspicious frame


Suspicious Activity Detection
Suspicious Activity Detection From CCTV Footage
Upload CCTV Footage
Generate Frames
Detect Suspicious Activity Frame

Frame generation process completed. All frames saved inside frame folder

```
frames/frame.0 saved
frames/frame.1 saved
frames/frame.2 saved
frames/frame.3 saved
frames/frame.4 saved
frames/frame.5 saved
frames/frame.6 saved
frames/frame.7 saved
frames/frame.8 saved
frames/frame.9 saved
frames/frame.10 saved
frames/frame.11 saved
frames/frame.12 saved
frames/frame.13 saved
frames/frame.14 saved
frames/frame.15 saved
frames/frame.16 saved
frames/frame.17 saved
frames/frame.18 saved
frames/frame.19 saved
frames/frame.20 saved
frames/frame.21 saved
frames/frame.22 saved
frames/frame.23 saved
frames/frame.24 saved
```

```
frames/frame107.jpg is predicted as suspicious with probabil
ity : 87.31042742729187

frames/frame117.jpg is predicted as suspicious with probabil
ity : 87.54125237464905

frames/frame127.jpg is predicted as suspicious with probabil
ity : 87.45720386505127

frames/frame137.jpg is predicted as suspicious with probabil
ity : 87.35582828521729

frames/frame147.jpg is predicted as suspicious with probabil
ity : 87.27838397026062

frames/frame157.jpg is predicted as suspicious with probabil
ity : 87.52446174621582

frames/frame167.jpg is predicted as suspicious with probabil
ity : 87.66176104545593

frames/frame177.jpg is predicted as suspicious with probabil
ity : 87.74349689483643

frames/frame187.jpg is predicted as suspicious with probabil
```

Thus, the system automatically detects the anomaly and alarm is raised on any such suspicious frame.

CONCLUSION

In this work, suspicious activity detection application is presented based on convolution neural network. The proposed model is successfully trained with CCTV footage instead of normal training datasets. Spatiotemporal analysis is implemented. The proposed system is a machine approach to detect real-world criminal activity identification in surveillance videos. The necessity to develop such a security system is increasing with the increasing number of crimes that are happening every day. The result of the proposed system is detection the anomaly. Manual process is substituted by intelligent automation process.

REFERENCES

1. Joey Tianyi Zhou, Jiawei Du, Hongyuan Zhu, Xi Peng, Rick Siow Mong Goh, (2019) “AnomalyNet: An Anomaly Detection Network for Video Surveillance”, IEEE Transactions on Information Forensics and Security, 1(1), pp. 99-105
2. Monika D. Rokade and Tejashri S. Bora, (2021)"Survey on Anomaly Detection for Video Surveillance" International Research Journal of Engineering and Technology(IRJET).
3. Jefferson Ryan Medel, Andreas Savakis, (2017), “Anomaly Detection in Video Using Predictive Convolutional Long Short-Term Memory Networks”.International Symposium on Neural Networks. Springer, pp. 189–196.
4. W. Luo, W. Liu, and S. Gao, (2017)“A revisit of sparse coding based anomaly detection in stacked rnn framework,” in The IEEE International Conference on Computer Vision (ICCV),
5. Y. S. Chong and Y. H. Tay, (2017)“Abnormal event detection in videos using spatiotemporal autoencoder,” in International Symposium on Neural Networks. Springer, pp. 189–196.
6. J. R. Medel and A. Savakis, (2016) “Anomaly detection in video using predictive convolutional long short-term memory networks,” arXiv preprint arXiv:1612.00390,
7. M. Hasan, J. Choi, J. Neumann, A. K. Roy-Chowdhury, and L. S. Davis, (2016) “Learning temporal regularity in video sequences,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), , pp. 733–742.
8. M. Sabokrou, M. Fathy, M. Hoseini, and R. Klette, (2015). “Real-time anomaly detection and localization in crowded scenes,” in The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops, June
9. C. Lu, J. Shi, and J. Jia, “Abnormal event detection at 150 fps in Matlab ,”(2013) Proceedings of the IEEE international conference on computer vision, , pp. 2720–2727.
10. H. Mousavi, M. Nabi, H. K. Galoogahi, A. Perina, and V. Murino, (2015)“Abnormality detection with improved histogram of oriented tracklets,” in International Conference on Image Analysis and Processing. Springer, pp. 722–732.
11. Monika D.Rokade, Dr. Yogesh Kumar Sharma, (2021) "MLIDS: A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset", International Conference on Emerging Smart Computing and Informatics (ESCI), IEEE.
12. S.A Quadri, Sadiq A Mulla (2020) "Crop-yield and Price Forecasting using Machine Learning" The International journal of analytical and experimental modal analysis,Volume XII, Issue VIII, 1731-1737
13. Ryan Dias, S. Abdulhayan, S.A. Quadri (2022) "Comparison of Machine Learning Algorithms for Localized GPS" Specialusis Ugdymas, Volume 1 Issue 43,5932-5944
14. Sumayya Fatima, S.A. Quadri (2022) "Malware Detection Using Cuckoo And ML Techniques" Science, Technology And Development Journal, 11(7) 165-170.
15. Agboola, Ridwan. (2013) "Analytical Interpretation Of Geomagnetic Field anomaly Along The Dip Equator." International Journal of Humanities, Arts, Medicine and Sciences (BEST: IJHAMS), 3 (3) 29-44
16. Nageswari P, Selvam M, Vanitha S, Babu M (2013) An empirical analysis of january anomaly in the Indian stock market. International Journal of Accounting and Financial Management Research. 3(1):177-86.
17. Patel, A. M., PATEL, A., & Patel, H. R. (2013). Comparative Analysis For Machine Learning Techniques Appliance On Anomaly Based Intrusion Detection System For Wlan. International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), 3(4), 77-86.