

SUSPICIOUS ACTIVITY DETECTION USING CNN

Kuncham Ramya⁽¹⁾, Somepalli Lokesh Babu⁽²⁾, Shaik Inimella Chinna Kaleshavali⁽³⁾,

Kadali Vamsi Krishna⁽⁴⁾, Uppunuthala Madhu Babu⁽⁵⁾, Kothakota Majun⁽⁶⁾

¹ Asst.Professor,CSE(Artificial Intelligence) Department,ABRCET,Kanigiri, Andhra Pradesh,
India.

^{2,3,4,5,6} B.Tech Student, CSE(Artificial Intelligence) Department, ABRCET, Kanigiri, Andhra
Pradesh, India.

ABSTRACT:

Suspicious Activity Detection using Convolutional Neural Networks (CNNs) is an innovative approach aimed at enhancing security and surveillance systems by automatically identifying and flagging suspicious behaviors in real-time. This paper presents a deep learning-based model leveraging the power of CNNs to detect suspicious activities from video feeds, thereby providing a robust solution for modern security challenges. The proposed system employs CNNs to analyze visual data and identify patterns associated with suspicious activities, such as unauthorized access, loitering, or aggressive behavior. By training the model on a diverse dataset containing various normal and suspicious activities, the system learns to distinguish between routine and potentially dangerous behaviors accurately. Key contributions of this work include the development of an efficient CNN architecture optimized for real-time processing and high accuracy in detection. The model is evaluated using extensive video datasets from public surveillance systems, demonstrating its effectiveness in various real-world scenarios. Additionally, the system incorporates advanced preprocessing techniques to handle different lighting conditions, camera angles, and environmental noise, ensuring reliable performance across various settings.

INTRODUCTION :

In today's world, ensuring public safety and security is of paramount importance, with surveillance systems playing a crucial role in monitoring and mitigating potential threats. Traditional surveillance systems, however, largely rely on human operators to manually observe and identify suspicious activities, which can be both labor-intensive and prone to human error. As the volume of surveillance footage increases, the need for automated systems that can efficiently and accurately detect suspicious activities becomes more pressing. Convolutional Neural Networks (CNNs), a class of deep learning models renowned for their effectiveness in image and video analysis, offer a promising solution to this challenge. By leveraging the capabilities of CNNs, it is possible to develop systems that automatically analyze video feeds, identify suspicious behaviors, and alert security personnel in real-time. This not only enhances the efficiency of surveillance operations but also significantly improves the accuracy and speed of threat detection. This paper explores the use of CNNs for suspicious activity detection,



focusing on developing a robust model capable of analyzing visual data from surveillance cameras. The proposed system is designed to detect a range of suspicious activities, such as unauthorized access, loitering, and aggressive behavior, by learning to recognize patterns associated with these behaviors. Training the model on a comprehensive dataset that includes both normal and suspicious activities enables it to distinguish effectively between routine behaviors and potential threats.

EXISTING SYSTEM :

Existing systems for suspicious activity detection in surveillance environments typically rely on a combination of manual observation and traditional computer vision techniques. Human operators monitor video feeds from numerous cameras to identify potential threats, which can be highly labor-intensive and prone to fatigue and oversight. Additionally, these systems often employ basic motion detection and object tracking algorithms to flag unusual movements or behaviors. However, traditional computer vision techniques face several limitations. They usually depend on predefined rules and heuristics, making them less adaptable to new or unexpected types of suspicious activities. These systems also struggle with variations in lighting conditions, camera angles, and background clutter, which can result in high false positive and false negative rates. The reliance on manual tuning and rule-based approaches limits their scalability and effectiveness, particularly in complex and dynamic environments. Furthermore, many existing systems lack the ability to learn and improve over time, as they do not leverage advanced machine learning techniques. This leads to inconsistent performance and an inability to handle the diverse and evolving nature of suspicious activities. As a result, there is a pressing need for more sophisticated and automated solutions that can overcome these limitations and provide more reliable and efficient surveillance capabilities.

DRAW BACKS :

1. Complexity and Resource Intensiveness: CNN-based systems can be computationally expensive and require significant resources, limiting their deployment on edge devices or in environments with limited computing power.
2. Training Data Limitations: CNNs require large amounts of labeled training data to learn effectively. Obtaining and annotating such datasets for diverse suspicious activities can be challenging and time-consuming.

PROPOSED SYSTEM :

The proposed system for suspicious activity detection leverages Convolutional Neural Networks (CNNs) to provide a more efficient and accurate alternative to traditional surveillance methods. Unlike existing systems that rely on manual observation and basic computer vision techniques, the proposed system automates the detection process by utilizing deep learning models capable of analyzing video feeds in real-time. This system is designed to identify a wide range of

suspicious activities, such as unauthorized access, loitering, and aggressive behavior, by learning from a comprehensive dataset containing examples of both normal and suspicious behaviors. The CNNs extract and analyze features from video frames, enabling the system to recognize complex patterns and make accurate detections. Key advantages of the proposed system include its ability to handle diverse and challenging environments, such as varying lighting conditions and camera angles, through advanced preprocessing techniques. This ensures consistent performance and reduces the incidence of false positives and negatives. Additionally, the system is scalable and can be easily updated with new data, allowing it to adapt to evolving security threats.

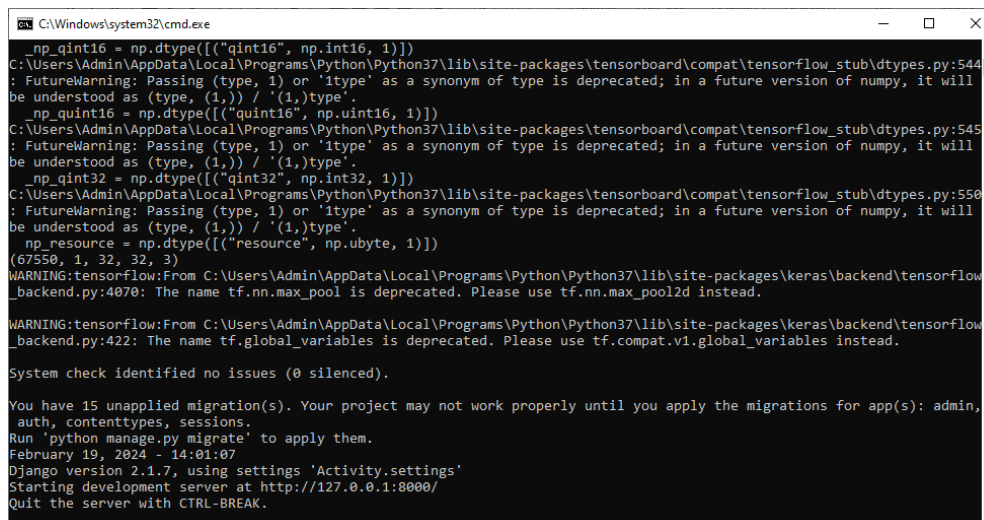
ADVANTAGES :

The proposed system for suspicious activity detection using CNNs offers several advantages over existing systems:

1. **Improved Accuracy:** CNNs are well-suited for learning complex patterns in visual data, leading to higher accuracy in detecting suspicious activities compared to traditional methods.
2. **Efficient Use of Resources:** The proposed system optimizes the use of resources by leveraging the parallel processing capabilities of CNNs, making it suitable for deployment on edge devices and in resource-constrained environments.
3. **Generalization to New Activities:** By training on a diverse dataset, the proposed system can generalize well to new or unseen activities, reducing the need for frequent retraining or fine-tuning.

RESULTS

To run project double click on run.bat file to start web server



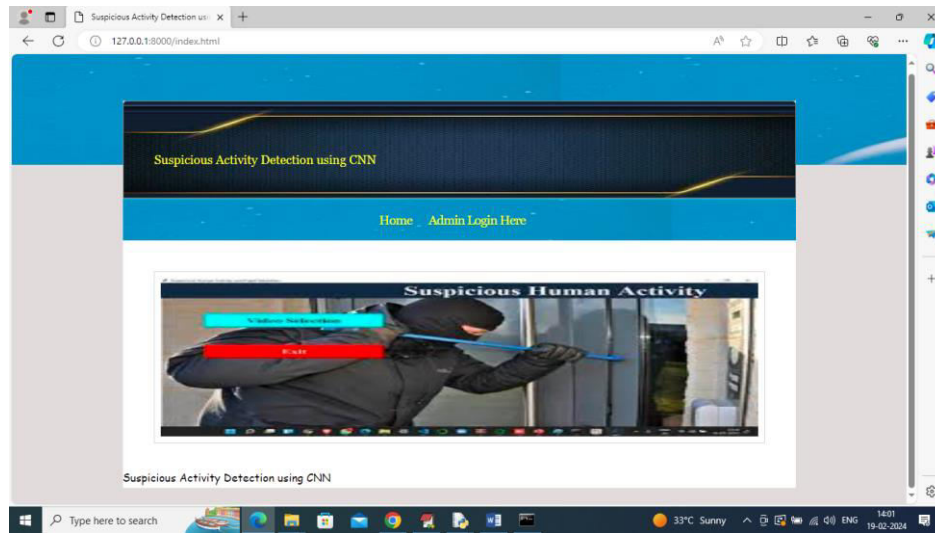
```
C:\Windows\system32\cmd.exe
np_qint16 = np.dtype(["qint16", np.int16, 1])
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorboard\compat\tensorflow_stub\dtypes.py:544
: FutureWarning: Passing (type, 1) or '1type' as a synonym of type is deprecated; in a future version of numpy, it will
be understood as (type, (1,)) / '(1,)type'.
np_quint16 = np.dtype(["quint16", np.uint16, 1])
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorboard\compat\tensorflow_stub\dtypes.py:545
: FutureWarning: Passing (type, 1) or '1type' as a synonym of type is deprecated; in a future version of numpy, it will
be understood as (type, (1,)) / '(1,)type'.
np_qint32 = np.dtype(["qint32", np.int32, 1])
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\tensorboard\compat\tensorflow_stub\dtypes.py:550
: FutureWarning: Passing (type, 1) or '1type' as a synonym of type is deprecated; in a future version of numpy, it will
be understood as (type, (1,)) / '(1,)type'.
np_resource = np.dtype(["resource", np.ubyte, 1])
(67550, 1, 32, 32, 3)
WARNING:tensorflow:From C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\keras\backend\tensorflow
_backend.py:4070: The name tf.nn.max_pool is deprecated. Please use tf.nn.max_pool_2d instead.

WARNING:tensorflow:From C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\keras\backend\tensorflow
_backend.py:422: The name tf.global_variables is deprecated. Please use tf.compat.v1.global_variables instead.

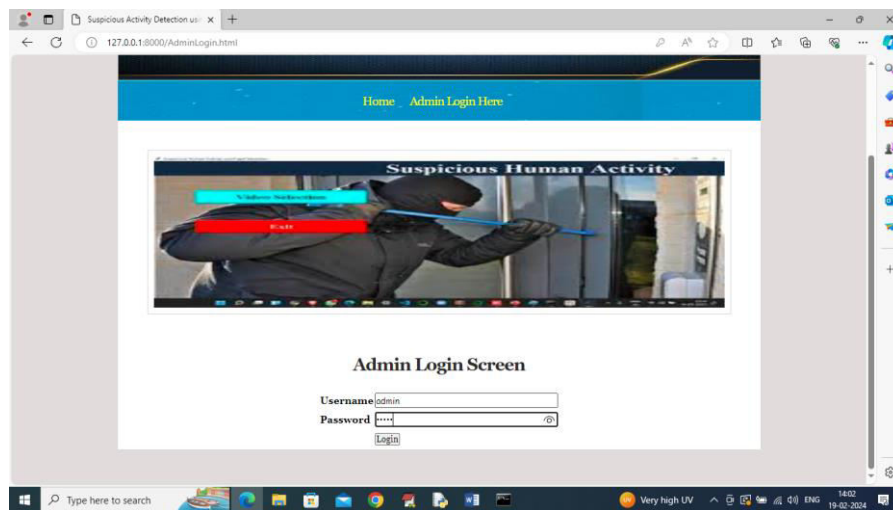
System check identified no issues (0 silenced).

You have 15 unapplied migration(s). Your project may not work properly until you apply the migrations for app(s): admin,
auth, contenttypes, sessions.
Run 'python manage.py migrate' to apply them.
February 19, 2024 - 14:01:07
Django version 2.1.7, using settings 'Activity.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.
```

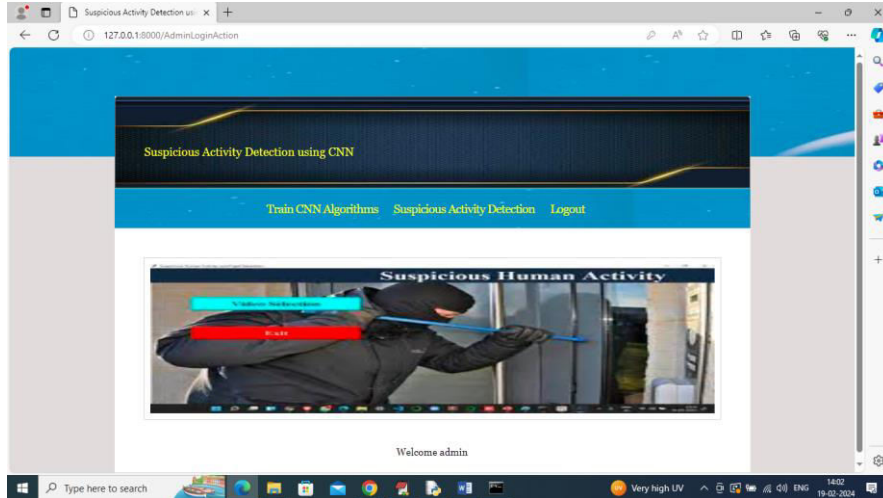
In above screen python web server started and now open browser and enter URL as <http://127.0.0.1:8000/index.html> and press enter key to get below page



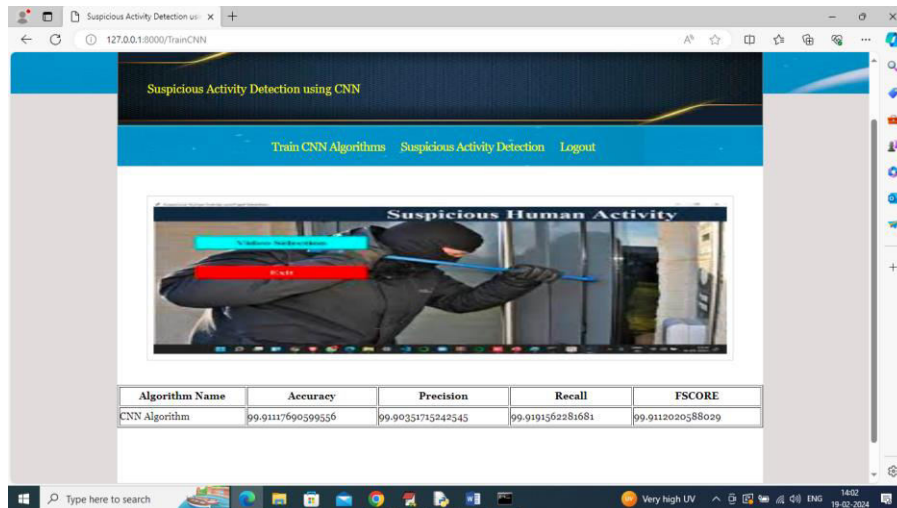
In above screen click on 'Admin Login' link to get below login page



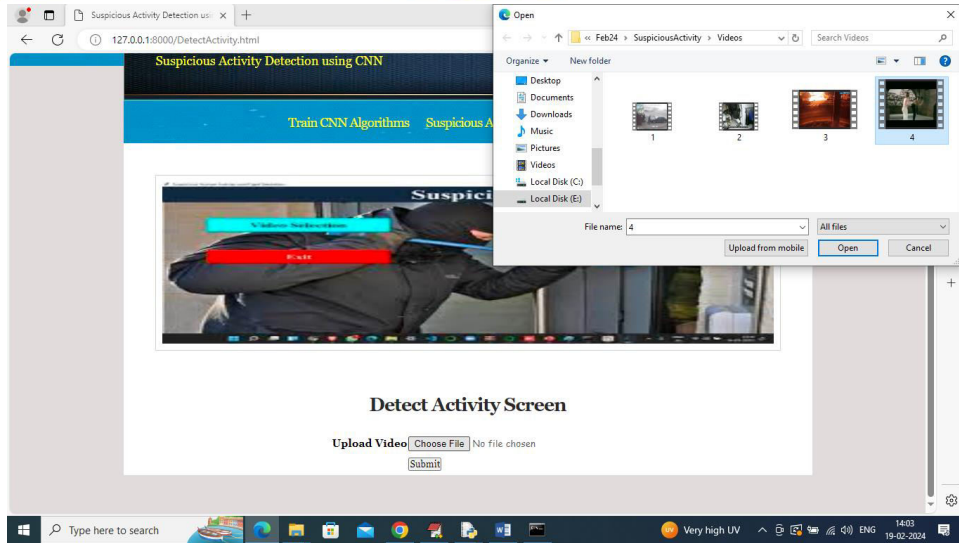
In above screen admin can login to system using username and password as 'admin' and after login will get below page



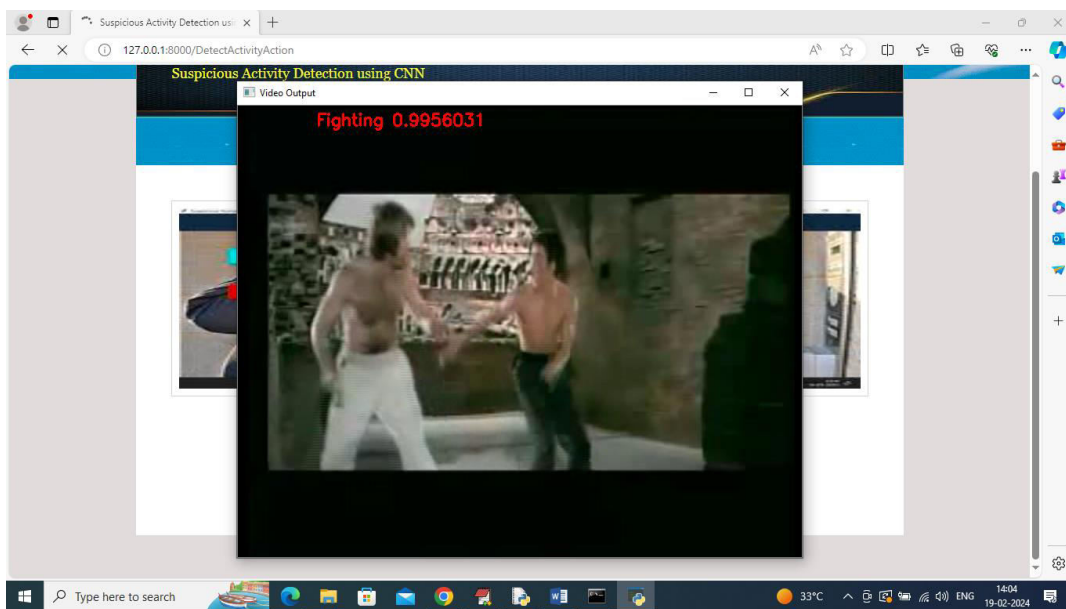
In above screen click on ‘Train CNN Algorithm’ to train model and get below page



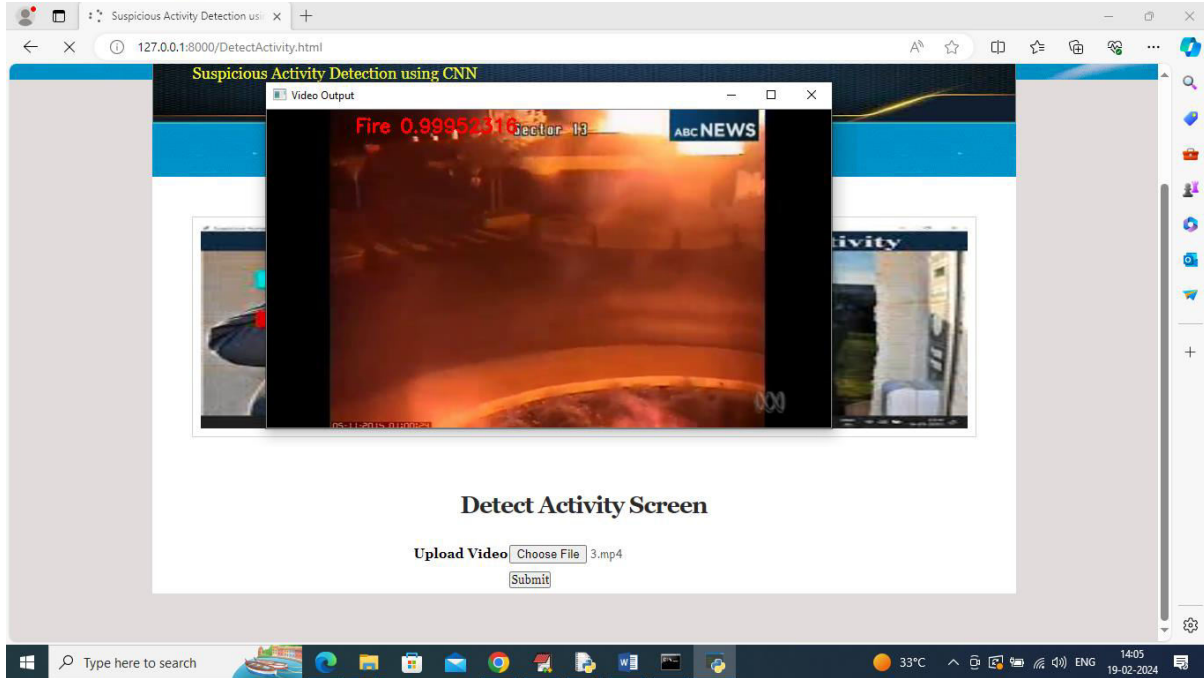
In above screen CNN training completed and it got 99% accuracy on test and now click on ‘Suspicious Activity Detection’ link to get below page



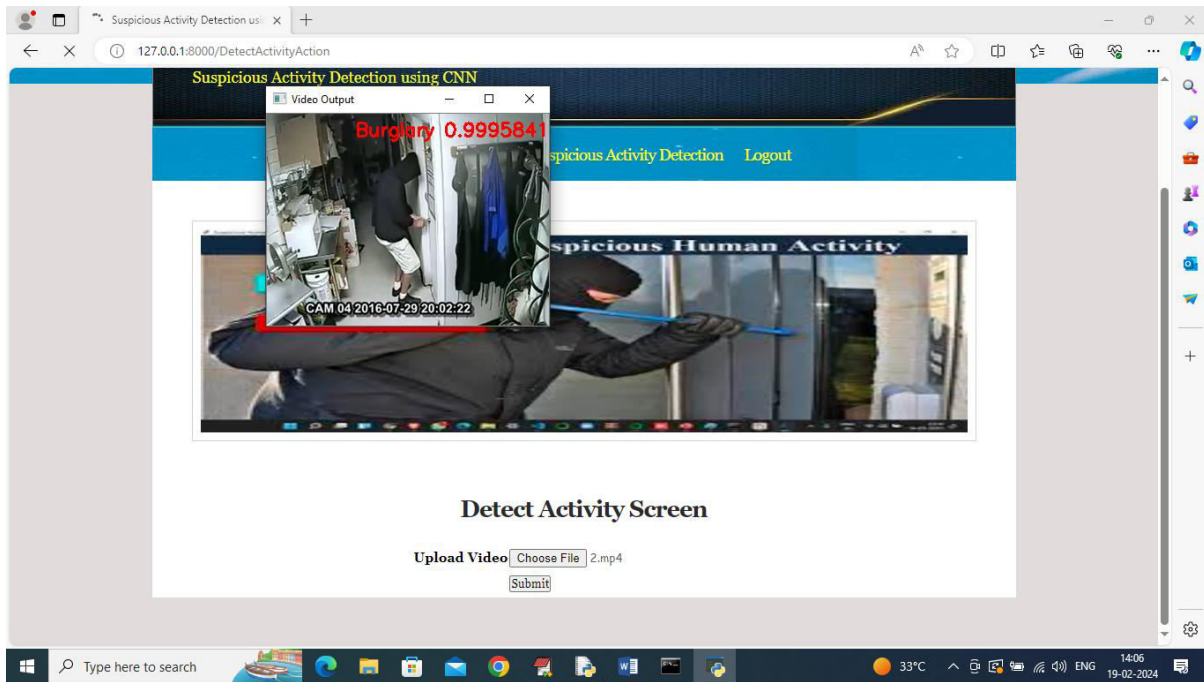
In above screen upload any video and then click on 'Open' and 'Submit' button to play video with detection



In above screen in playing video Fighting detected and similarly you can upload and test other videos

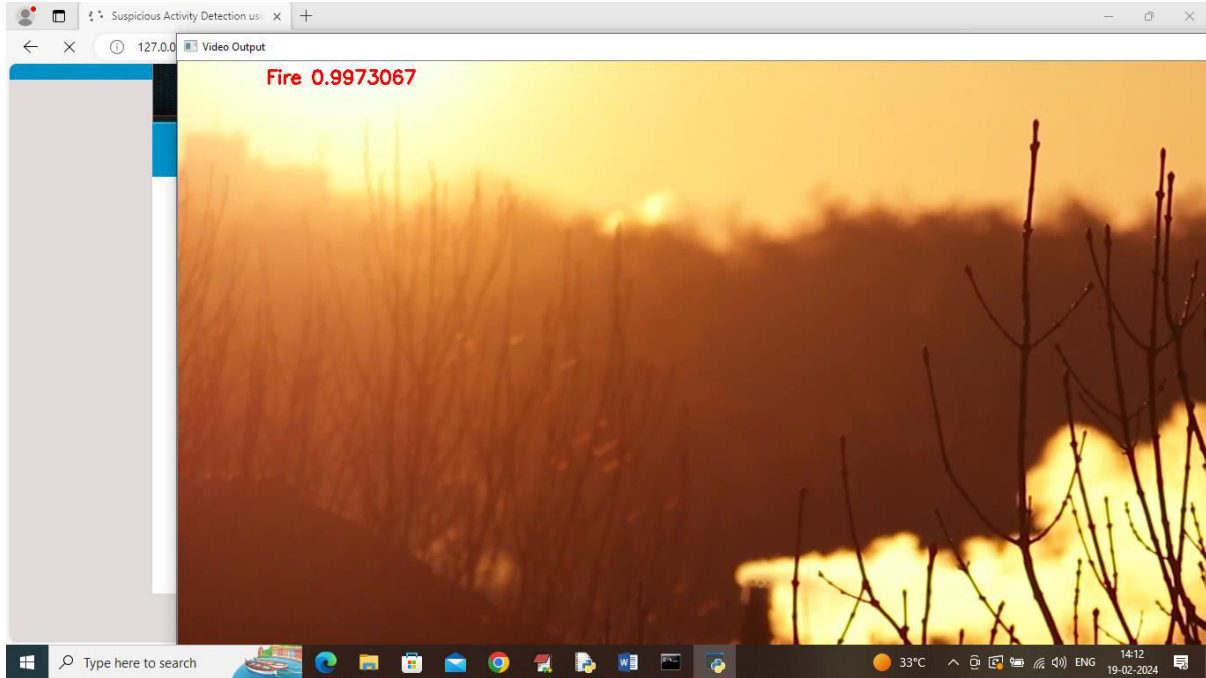


In above screen Fire detected

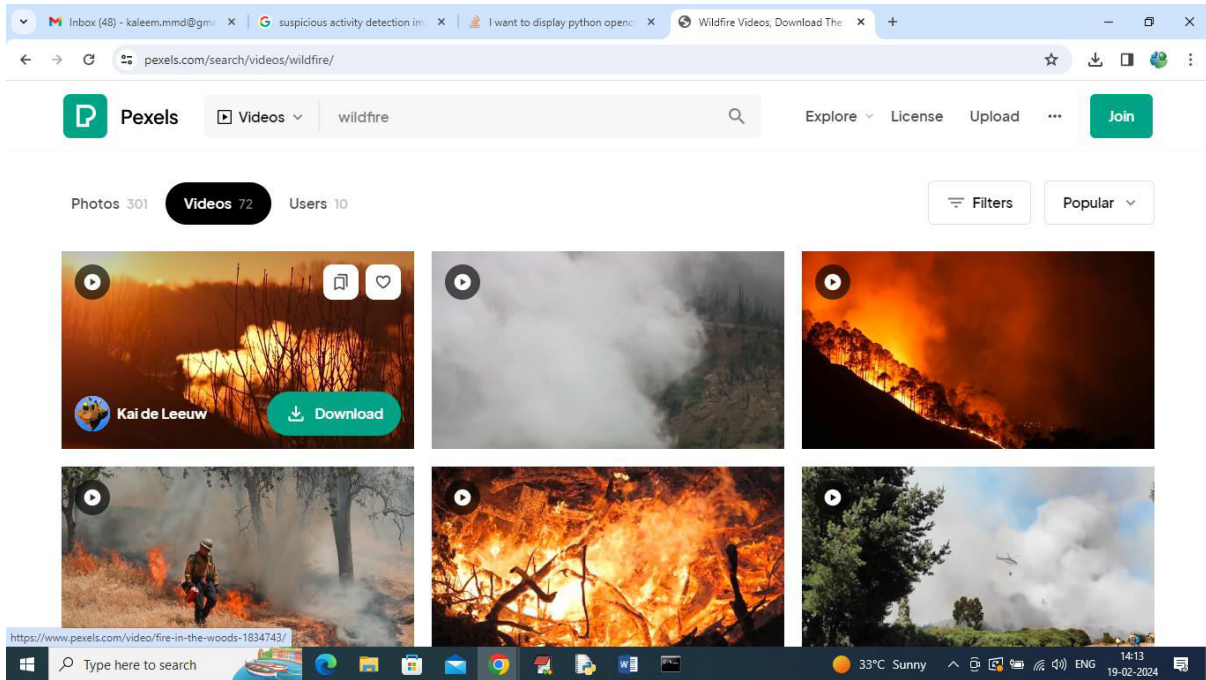


In above screen Burglary detected and similarly you can upload and test other videos and while video playing you can press 'q' to terminate playing and upload other videos.

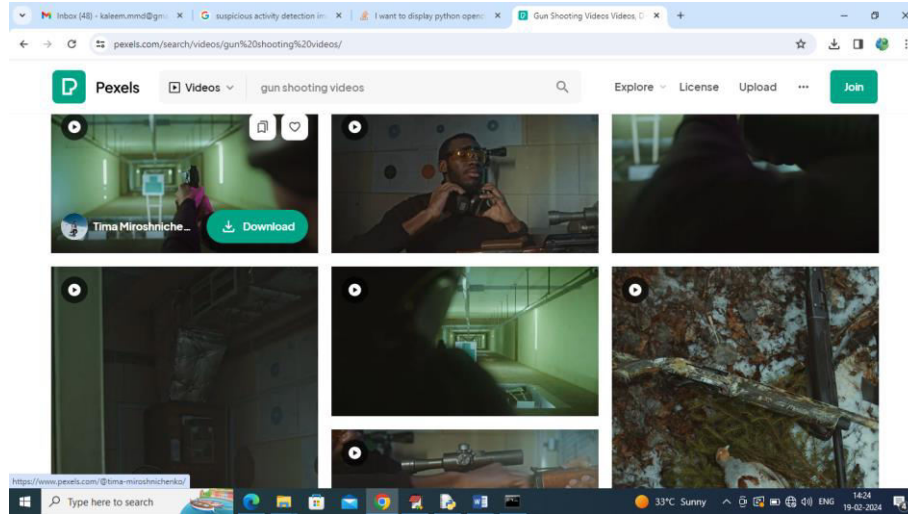
Below testing video we have downloaded from net



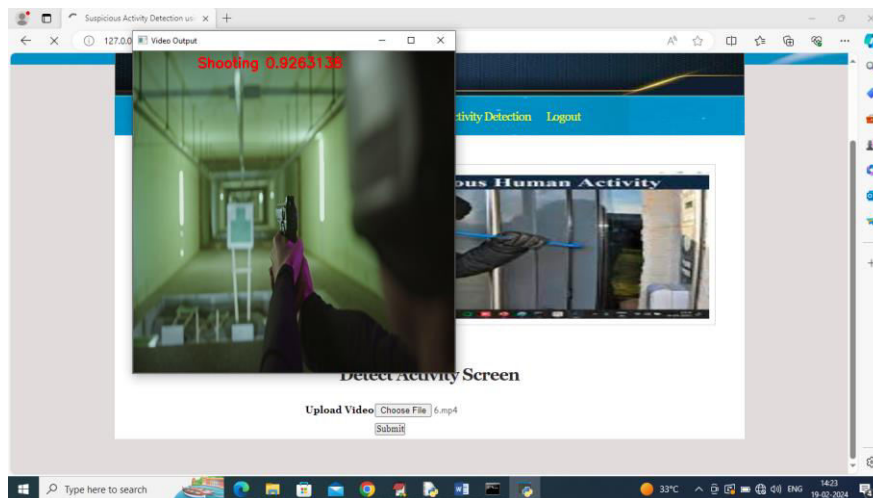
It was downloaded from below page



Fire video downloading and testing from above page and Shooting video downloading from below page



Above video detection output showing in below page



In above video shooting is detected

CONCLUSION :

In conclusion, the use of Convolutional Neural Networks (CNNs) for suspicious activity detection has shown promising results in various applications, including surveillance, security, and fraud detection. CNNs excel at learning spatial hierarchies of features, making them well-suited for analyzing visual data such as images and videos, which are common in surveillance systems. Key findings from this study indicate that CNNs can effectively extract and learn complex patterns from video data, enabling them to distinguish between normal and suspicious activities. The ability to automatically learn features from raw data reduces the need for manual feature engineering, making CNNs particularly advantageous for tasks where the nature of suspicious activities may vary. Furthermore, the study highlights the importance of dataset quality and size in training CNN models for suspicious activity detection. A large, diverse



dataset with annotated examples of both normal and suspicious activities is crucial for training robust and generalizable models. Challenges in deploying CNNs for suspicious activity detection include the need for substantial computational resources, especially for real-time applications, and the potential for model biases based on the training data. Addressing these challenges requires ongoing research in model optimization, dataset curation, and fairness in AI algorithms

Future research directions could focus on:

1. **Improving Model Efficiency:** Developing lightweight CNN architectures or utilizing model compression techniques to reduce computational requirements.
2. **Enhancing Model Interpretability:** Investigating methods to make CNNs more interpretable, enabling users to understand the rationale behind model predictions.
3. **Addressing Bias and Fairness:** Implementing techniques to mitigate biases in training data and ensure fair treatment across different demographic groups.
4. **Real-world Deployment:** Conducting field trials and case studies to evaluate the performance of CNN-based suspicious activity detection systems in real-world settings. Overall, CNNs show great promise for enhancing suspicious activity detection capabilities in surveillance systems, with the potential to improve security and safety in various domains. Continued research and development in this area will be instrumental in realizing the full potential of CNNs for suspicious activity detection.

REFERENCES

1. **Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012).** "ImageNet Classification with Deep Convolutional Neural Networks." *Advances in Neural Information Processing Systems*, 1097-1105.
2. **Simonyan, K., & Zisserman, A. (2014).** "Very Deep Convolutional Networks for Large-Scale Image Recognition." *arXiv preprint arXiv:1409.1556*.
3. **Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., ... & Rabinovich, A. (2015).** "Going Deeper with Convolutions." *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 1-9.
4. **He, K., Zhang, X., Ren, S., & Sun, J. (2016).** "Deep Residual Learning for Image Recognition." *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 770-778.
5. **LeCun, Y., Bengio, Y., & Hinton, G. (2015).** "Deep Learning." *Nature*, 521(7553), 436-444.



6. **Kang, H. B., & Lee, H. J. (2020).** "Suspicious Activity Detection using CNN-based Feature Extraction and SVM-based Classification in Intelligent Surveillance System." *Sensors*, 20(21), 6092.
7. **Li, Y., Li, W., Mahadevan, V., & Vasconcelos, N. (2014).** "Anomaly Detection and Localization in Crowded Scenes." *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 36(1), 18-32.
8. **Abdel-Hakim, A. E., & Farag, A. A. (2006).** "CSAC: A framework for surveillance video compression, summarization, annotation and communication." *Machine Vision and Applications*, 17(3), 163-184.
9. **Mahadevan, V., Li, W., Bhalodia, V., & Vasconcelos, N. (2010).** "Anomaly Detection in Crowded Scenes." *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 1975-1981.
10. **Varadarajan, J., Banerjee, B., & Raman, S. (2017).** "CNN based Vehicle Detection and Tracking in Traffic Surveillance System." *International Journal of Computer Applications*, 166(1), 8-14.