Deep Learning Approach for the Automatic Detection of Suspicious Human Activity

Aniket Tiwari[1], Aman Sharma[2], Vidhi Sethiya[3], Vandana Kate[4], Nisha Rathi[5]
Students, Department of Computer Science and Information Technology[1,2,3]
Project Guide, Department of Computer Science and Information Technology[4]
Project Incharge, Department of Computer Science and Information Technology[5]
Acropolis Institute of Technology and Research, Indore, Madhya Pradesh, India

Abstract: *The development of a security system that is totally automated, detects aberrant activity in real time, and provides a notification to the responsible authority with evidence. As a result, we devised a technique for examining and detecting suspicious human. This study presents one of the most important applications of human suspicious activity detection, known as "anomaly detection." Individual safety is a major problem in every community nowadays. The fundamental reason for this worry is the ever-increasing number of behaviours on campus that pose a hazard, such as mischief, fighting, and theft. A simple installation of a typical closed-circuit television (CCTV) system is insufficient since it requires a person to be vigilant and watch the cameras at all times, which is wasteful. This necessitates behaviour.*

Keywords: Machine Learning, Deep Learning, CNN (Convolutional Neural Network), and Suspicious Activity Detection.

I. INTRODUCTION

Identifying suspicious activity is critical for maintaining public safety, combating fraud, and lowering crime. Previous ways of detecting suspicious behaviour have depended on human observation, which may be costly, time- consuming, and error-prone. Advances in machine learning and computer vision have made it feasible to automate the process of detecting suspicious activity in video surveillance data in recent years. As a result, we suggest a fully automated approach to address this issue.

We propose a system whose primary goal is to detect suspicious activity on campus, identify people involved, and offer real-time alerts to higher authorities with evidence to aid in mischief reduction.

II. MOTIVATION

There are several potential motivations for undertaking a research project on suspicious activity detection. One primary motivation is the importance of public safety and the prevention of crime. By developing more accurate and reliable methods for detecting suspicious activities, we can improve security in various settings, including public spaces, educational institutions, and government facilities.

Another motivation for this project is the potential for technological advancement. With recent advances in machine learning and computer vision, there is a growing interest in applying these techniques to security and surveillance. Developing effective methods for suspicious activity detection could lead to innovations and improvements in the fields of computer vision and machine learning

III. LITERATURE REVIEW

Tejashri Subhash Bora1, Monika Dhananjay Rokade2 "Methodology for Human Suspicious Activity Detection"[1], Surveillance video analysis is a labour- intensive task that requires human efforts to detect abnormal activity. To achieve anomaly detection, one of the most common methods is using the videos of normal events as training data to learn a model and then detecting the suspicious events which do not fit in the learned model. Human pose estimation is used in applications such as video surveillance, animal tracing and actions understanding, sign language recognition, advanced human computer interaction, and marker less motion capturing. Neural networks are being used to overcome these problems. Anomalous human activity recognition from surveillance video is an active exploration part of image processing and computer visualization.

This paper proposes an innovative neural network for anomaly detection, AnomalyNet, which combines feature learning, sparse representation, and dictionary learning in three joint neural processing blocks. It automates the detection of anomalous actions within long video series by learning generative models that can detect anomalies in videos using restricted supervision. The research paper from Springer presented an efficient technique for identifying anomalies in videos using Temporally-coherent Sparse Coding (TSC) and a stacked Recurrent Neural Network (sRNN). The paper also proposed end-to-end trainable complex Convolutional Long Short-Term Memory (Conv- LSTM) networks, which are capable of predicting the evolution of a video sequence from a minor number of input frames. The approach for this problem is to leverage the conventional handcrafted spatio-temporal local features and then study the fully connected autoencoders.

Gaussian classifiers are used to distinguish normal events and anomalies in videos. CNN is an artificial neural network (ANN) that is used to learn spacial orders of features through back-propagation. We are using supervised learning and machine learning techniques such as Long short term Memory (LSTM), Advance Motion Detection (AMD) algorithm, SURF (Speed Up Robust Features), ANN (Artificial Neural Network), Gaussian Classifiers, and sparse auto-encoder.

J. indhumathi and M. balasubramanian, "Real time video based human suspicious activity recognition using deep learning"[2],This proposed system uses a deep learning approach to classify human activities such as normal, criminal, and suspicious activity in public environments. It outperforms the pre-trained model VGG16 in Kaggle/real- time video. CCTV surveillance is valuable when combined with image processing and object detection algorithms. Human activities are classified into three stages: normal activities, suspicious activities, and abnormal activities. Deep learning algorithms learn more about an image as it goes through several neural network layers. CNN/ConvNet is a category of deep neural networks. This paper proposes to use three CNN architectures, 2D-CNN, VGG16, and ResNet50, to detect and recognize suspicious activity using Kaggle data and real-time datasets. The system is developed

Using Python with Tensor Flow and the Keras deep learning library to build CNN in a Jupyter notebook environment.

Balbhim Lanke and Zarinabegam Mundargi, "Abnormal Acitivity Detection Using CNN Method" [3], This study employs neural networks to detect suspicious human behaviour in real-time CCTV video, which may be used to monitor places where robberies or shooting attacks are possible. Such as video monitoring and behaviour recognition, sign language identification, and sophisticated human-computer interaction, neural networks may be utilised to detect abnormal human activity in real-time CCTV footage. Intelligent video surveillance is required, with the ability to watch human behaviours in real time, identify them as normal or abnormal, and create an alarm. Pre-processing is an image data augmentation that suppresses undesired distortions or improves certain picture attributes. Feature extraction is the process of producing new features from existing ones in order to minimise the amount of features in a dataset.

Nandini. G1, Dr. B. Mathivanan2, Nantha Bala. R. S3, Poornima. P4, "Suspicious human activity detection"[4], An automated method of analysing video clips and coming to a wise conclusion about the actions in the video is human activity detection for video surveillance systems. It is accomplished by breaking up a video into frames and using the processed frames to analyse the people and their actions. In this study, the construction of a system that analyses video data to find suspicious human activity is discussed. Preprocessing, subtraction, background removal, face identification, person recognition, and pattern matching with the database are all part of the system. The training data set includes of images of various persons obtained from various perspectives. In order to identify the individual involved, the values created from the photos are compared to the information collected from the video frame and saved in a database.

S. A. Quadri 1, Komal S Katakdhond 2, "Suspicious Activity Detection Using Convolution Neural Network"[5], Convolution Neural Network (CNN) is utilised to detect suspicious or normal behaviour in an environment, and a system is presented to send an alarm message to the appropriate authority if a suspicious action is predicted. CNN collects data after the image, on the point of edges, and in a number of ways using a range of filters. Python, Django, MySQL, and Wamp Server are required software. This system may be utilised for time-sensitive requirements such as bank theft detection, patient specialised care system, detecting suspicious behaviours by the train station, and so on.

Dinesh Jackson Samuel R, Fenil E, Gunasekaran Manogaran, Vivekananda G.N, Thanjaivadivel T, Jeeva S, Ahilan A, “Real-time violence detection framework for football stadium comprising of big data analysis and deep learning through bidirectional LSTM”[6], To prevent violence at sporting events, a deep learning-based detection system has been proposed. Face detection, suspicious state detection, and anomaly detection are the three stages of the system. The trained model analyses the students' behavior to determine if they are suspicious. A Gaussian distribution is also used to detect unusual behavior. With an accuracy of 94.5%, the system is an effective solution for detecting potential violence. Using this real-time violence detection system, it is possible to create a safe environment for both players and spectators, thereby promoting peaceful sporting events.

Gurav, S. S., Godbole, B. B., & Sonale, M. S. “Improved accuracy of suspicious activity detection in surveillance video”[7], The review paper emphasises the importance of video surveillance analysis in modern society and investigates the various deep learning models, datasets, and algorithms used in this context. The majority of the papers reviewed in the paper rely on computer vision with various algorithms to analyse human behaviour from movies. Computer vision systems require extensive preprocessing to accurately analyse and comprehend the evolution of features in a scene series, including the extraction of trajectories and motion patterns. This crucial preprocessing step allows systems to recognise and interpret human behaviour from video surveillance footage.

The review paper emphasises the importance of video surveillance analysis in improving public safety and security, as well as the most recent advances in deep learning models, datasets, and algorithms for this purpose.

J. Sujanaa and S. Palanivel, “Real-time video based emotion recognition using convolutional neural network and transfer learning” [8], Transfer learning is a machine learning technique in which a previously trained model on a specific task is utilised as a starting point for a new, related task. In the instance of Srikanth et alwork,.’s they employed a pre- trained VGG16 model, a deep convolutional neural network, as a starting point for picture classification. The benefit of transfer learning is that it enables for more efficient use of computer resources and training data. The network can use the knowledge gained from the previous task by utilising a pre-trained model, and the improved model can more accurately categorise images in the new task. This strategy can considerably increase the model's performance and make it easier to solve more complicated situations.

C. Yeole, H. Singh, H. Waykole and A. Deshpande, “Deep Neural Network Approaches for Video Based Human Activity Recognition” [9], the use of deep neural networks for video-based human activity recognition is discussed in this research. The study presents novel activity identification algorithms and reviews tried and established ways to improve accuracy and capability in dealing with a variety of settings. Deep learning models have begun to deliver on their promises of feature learning, reaching cutting-edge outcomes for human activity recognition1. They can learn features automatically from raw sensor data and outperform models trained on hand-crafted domain-specific features. The research focuses on deep learning methodologies such as Convolution Neural Networks (CNN) and Recurrent Neural Networks (RNN), which are commonly utilized in deep learning architectures. The research also includes a mechanism for automatically detecting human activities in video sequences.

C. V. Amrutha, C. Jyotsna and J. Amudha, "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video,"[10], This research describes a two-part architecture for detecting and alerting authorities to suspicious activity in an academic setting using deep learning. The framework's first component employs deep learning techniques to detect potentially suspicious behaviour, while the second component is in charge of delivering an alarm message to the appropriate authority if such conduct is discovered. The strategy is meant to improve academic institution safety and security by swiftly identifying and responding to possible threats.

Gugale1, Abhiruchi Shendkar2, Arisha Chamadia3, Swati Patra4, Deepali Ahir5, "Human Suspicious Activity Detection using Deep Learning Rachana" [11], FastAI is a deep learning system built on PyTorch that is easy to use, very effective, and highly hackable and versatile. In addition to transfer learning, it provides discriminative learning rates, training, layer freezing, and optimum batch normalisation. The system is divided into two phases: deployment and training, with 80% of the data used for training and 20% for validation. Because of the increase in crime, research into suspicious activity detection has become critical. The CNN model was built with the ResNet architecture, and we tested it with the ResNet-18, ResNet-34, and ResNet-50 techniques. Each architecture's results were obtained.

Rajesh Kumar Tripathi, Anand Singh Jalal & Subhash Chand Agrawal “Suspicious human activity recognition” [12], Many researchers have also developed real-time intelligent surveillance systems, but the processing speed of the video frames is not as fast as needed, and no system has been developed that has 100% detection accuracy and 0% false detection rate for movies with complex backgrounds. Theft and the discovery of abandoned things the majority of the effort has gone into identifying abandoned objects in surveillance footage captured by stationary cameras. Detecting slips and falls Human form analysis, posture estimation analysis, and motion-based analysis have received the most attention in studies for detecting a single person's fall in indoor recordings.

Ahmed Mateen Buttar1, Mahnoor Bano1, Muhammad Azeem Akbar2, Amerah Alabrah3, Abdu H. Gumaei4 "Toward trustworthy human suspicious activity detection from surveillance videos using deep learning" [13], To extract information from video frames, a pre-trained Convolutional Neural Network (CNN) model is employed, which is subsequently processed using the Bi-directional long short-term memory (BD-LSTM) model. Hybrid Deep Learning models are used for testing and detecting suspicious activities in videos. The UCF-Crime dataset contains records of both common and unusual incidents, including 13 distinct anomalies such as fights, abuse, and snatching. ConvLSTM training, validation, and testing accuracy was more than or equal to 99.01 percent, 77.19 percent, and 88.73 percent, respectively, using the videos dataset. When training to detect human activity in video, LRCNN uses 100 epochs and achieves accuracy of 94.28%, 82.46%, and 91.55%.

The LRCNN models show the highest accuracy score on unseen data, which is 91.55% compared with other DL models, the ConvLSTM model attains 88.73% accuracy, and the GRU model achieves an 84.01% accuracy rate.

M. Adimoolam, N. M. Balamurugan, Karthi Govindharaju "Suspicious Actions Detection System Using Enhanced CNN and Surveillance Video" [14], the proposed ECNN algorithm is a serial function mechanism capable of detecting suspicious behaviour. For the detection steps, the GaussianBlur module from OpenCV's video capture read module is utilised. The experiment for detecting suspicious behaviour using the ECNN algorithm was launched, and the data was analysed using the SPSS application. The ECNN algorithm's average precision, accuracy, false-positive, and false-negative rates were 97.050%, 96.743%, 2.957%, and 2.927%, respectively. The findings of this experiment demonstrated that the proposed ECNN technique was novel, and that ECNN performance measures outperformed CNN performance metrics in general.

Bushra Yasmeen1 , Haslina Arshad2, Hameedur Rahman3 "Suspicious Activity Detection Using CCTV Surveillance Video" [15], Methodology We created a suspicious activity detection mechanism in this system utilising CCTV surveillance video. Suspicious Activity Detection Data Training Since they are unsophisticated, the following behaviour detection systems identify only object models (human activities), not suspicious behaviours. Conclusion In today's world, developing an automated method for detecting suspicious behaviour in videostreams and video cameras is a must. Unfortunately, most current methods rely primarily on social observation, and thus there is no cohesive structure to meet such demands. Suspicious Activity Monitoring Framework, a new trainable human activity and behaviour like an observable intellectual, is created for video cameras (ISADF). The video and extraction unit included in this system collects the video images as needed and sends them for suspected fraud analysis to both the video processing units.

Arroyo, R., Yebes, J.J., Bergasa, L.M., Daza, I.G. & Almazán, J. 2015, "Expert video-surveillance system for real-time detection of suspicious behaviors in shopping malls" [16], this paper proposes a comprehensive expert system for the real-time detection of potentially suspicious behaviors in shopping malls. It involves an image segmentation technique, followed by a blob fusion technique and a two-step tracking algorithm based on Kalman filtering and SVM kernels. The resultant trajectories of people obtained are processed by the expert video- surveillance system for analyzing human behaviors and identifying potential shopping mall alarm situations, as well as shop entry or exit of people, suspicious behaviors such as loitering and unattended cash desk situations. The publicly available CAVIAR dataset is used to test the proposed tracking method, which has a success near to 85% in occlusion situations. This method is comparable and more efficient than the most recent state-of-the-art works, and can effectively detect suspect behaviors in a shopping mall context.

This paper discusses the innovative algorithms implemented in a video-surveillance system for detecting suspicious behaviors in shopping malls, such as a new blob fusion technique, a novel tracking algorithm based on trajectories, and alarms. The tracking method consists of a two-step algorithm: LSAP and Kalman filter, followed by an image segmentation process, filtering foreground objects based on size and positional factors, grouping them by blob fusion algorithm, matching objects to track, and Occlusions between objects. The paper provides results and comparisons to corroborate the performance of the proposal.

III. PROBLEM DOMAIN

The problem domain of a project on suspicious activity detection is the detection of activities that may be considered suspicious or abnormal within a given environment. This can include various types of activities, such as

Such as mischief, theft, fighting, etc. The project aims to develop algorithms and techniques that can accurately detect such activities in video surveillance footage, potentially reducing the need for human surveillance and improving the effectiveness of security measures.

The problem domain also includes the challenges and limitations associated with suspicious activity detection. These may include issues related to data privacy, the need for real-time detection, and the need for robust and accurate algorithms that can operate effectively in a range of different environments.

Overall, the problem domain of a project on suspicious activity detection involves developing effective methods for detecting suspicious activities in various scenarios while also addressing the challenges and limitations associated with this task.

IV. PROBLEM DEFINITION

The problem definition of a project on suspicious activity detection is to develop algorithms and techniques that can accurately detect suspicious activities in video surveillance footage. The goal is to automate the process of suspicious activity detection and reduce the need for human surveillance, thereby improving the effectiveness and efficiency of security measures in various field.

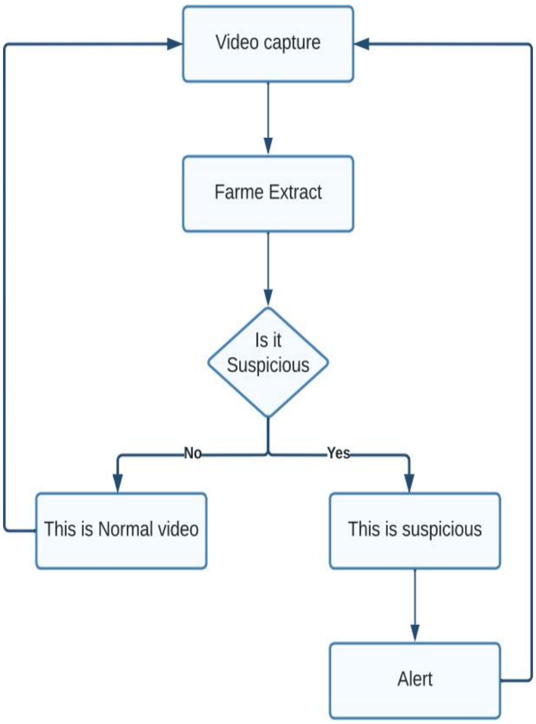
IV. REPRESENTATION AND SYSTEM DESIGN

The representation or system design of a project on suspicious activity detection can vary depending on the specific approach and techniques used. However, a general representation or system design may include the following components

1. Data Collection: Collecting data for suspicious activity detection typically involves setting up a video surveillance system to capture video footage of the relevant environment. This could be a public space, a commercial property, a residential neighborhood, or any other location where suspicious activities are expected to occur. The video footage is then used as input data for the suspicious activity detection algorithm.
2. Video data input: The system will take in video data from cameras or other sources to be analyzed for suspicious activities.
3. Data preprocessing: The system will preprocess the video data, which may include tasks such as video stabilization, noise reduction, and object detection.
4. Resizing: Image resizing is necessary when we need to increase or decrease the total number of pixels, whereas remapping can be done when we are adjusting for lens distortion or rotating an image.
5. Feature extraction: The system will extract features from the preprocessed data, such as object trajectories, motion patterns, and color histograms.
6. Suspicious activity detection: The system will compare the modeled activities to predefined rules or learned patterns to detect suspicious activities.
7. Alert generation: The system will generate alerts or notifications when suspicious activities are detected, which can be sent to security personnel or other relevant parties.

Overall, the representation or system design of a project on suspicious activity detection involves a combination of preprocessing, feature extraction, modeling, and detection techniques to accurately and efficiently detect suspicious activities in video surveillance footage.

DOI: 10.48175/568



VII. DATASET

The suggested model was trained and evaluated using the UCF Crime Dataset, which comprises 13 types of suspicious actions, as well as a normal class, including abuse, arson, assault, burglary, explosion, fighting, road accidents, robbery, shooting, shoplifting, theft, and vandalism. Several photographs were removed from all classes to ensure proportionality. The dataset is freely accessible on Kaggle and includes of footage collected from several CCTV cameras with diverse durations and frame rates.

A frequently used benchmark dataset for video-based activity recognition and anomaly detection in surveillance videos is the UCF Crime Dataset. It is suitable for developing and testing machine learning models because it has a lot of labelled data. However, it also presents a number of difficulties, including the varying lighting conditions, camera angles, and object appearances, the presence of occlusions, and the intricate relationships between people and objects.

Several methods, including data augmentation, transfer learning, and ensemble methods, have been suggested to address these difficulties. The UCF Crime Dataset has also been expanded recently to include more difficult situations, like videos with low resolution, videos taken in crowded places, and videos with multiple activities happening at once. Overall, the UCF Crime Dataset is a useful tool for academics and professionals developing video-based security and surveillance systems

The table shows the number of images per class in the UCF Crime Dataset.

CLASS NAME	NUMBER OF IMAGES
Stealing	1793
RoadAccidents	940
Shoplifting	994
Shooting	286
Fighting	988
Robbery	1660
Assault	415
NormalVideos	37911
Explosion	715
Arrest	1056

Abuse	764
Burglary	1581
Arson	977
Vandalism	546

Total number of Training Images	50662
Total number of Testing Images	22267

To display the UCF Crime Dataset visually. These images can assist readers in comprehending the nature of the activities captured in the dataset as well as providing context for the research.

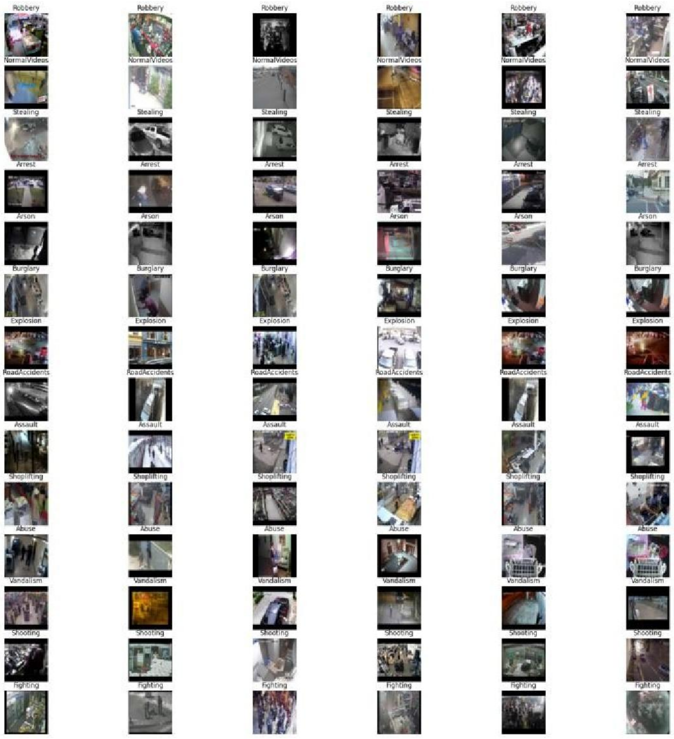


Fig 1.

The distribution of the UCF Crime Dataset into training and testing sets is depicted in Figure 2. In order to ensure that the model is trained on enough data while still having a sizeable amount of data for evaluation, the dataset was divided into 69.5% training data and 30.5% testing data.

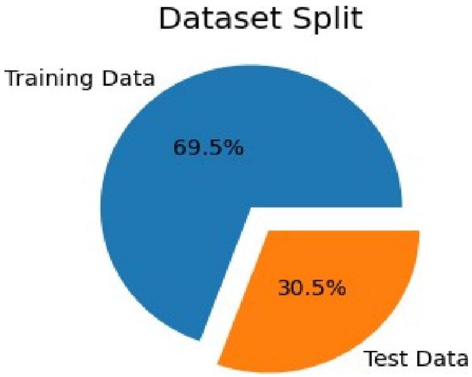


Fig 2.

Figure 3 shows the percentage of images that belong to each class in the UCF Crime Dataset and illustrates how the classes are distributed.

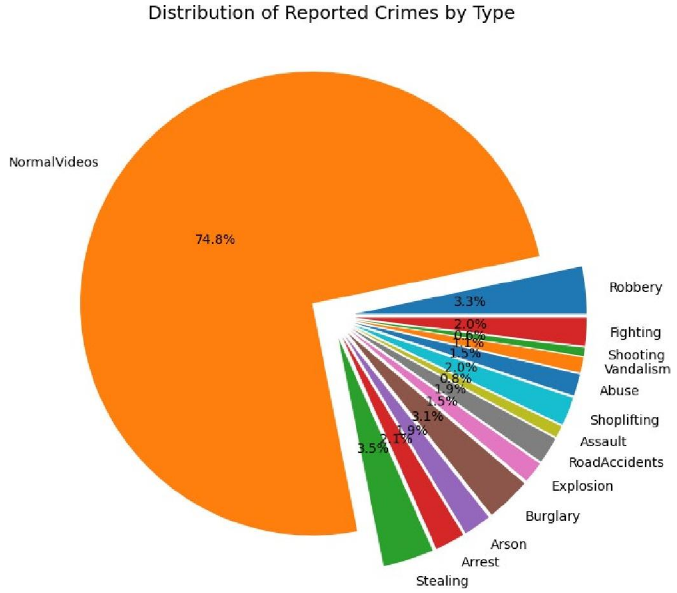


Fig 3

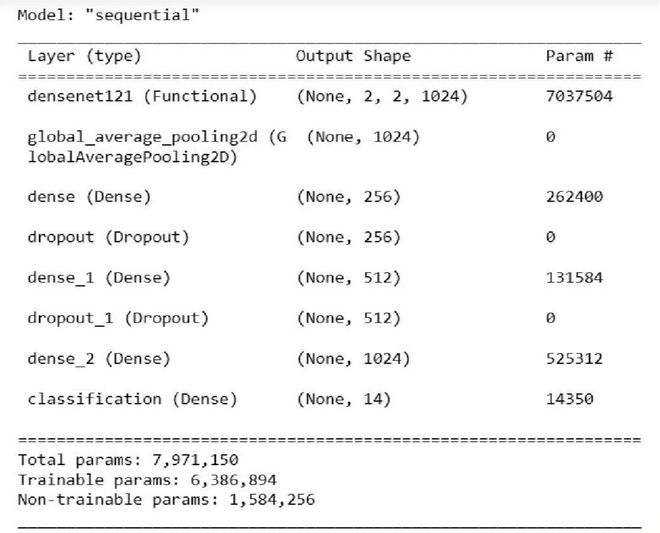
VIII. ALGORITHM DESIGN

Algorithm: Convolution Neural Network (CNN)

Step1: In the first step, we are using the transfer learning technique, which is densenet121, because the transfer learning technique involves using a pre-trained deep learning model as a starting point for a new task rather than training a model from scratch. One of the main advantages of using transfer learning is that it can significantly reduce the amount of data and computational resources required to train a new model.

DenseNet121 is a popular pre-trained deep learning model that has been trained on a large dataset of images (ImageNet) and has shown strong performance on a variety of image classification tasks. By using DenseNet121 as a starting point for your suspicious activity detection task, you can leverage the knowledge and feature representations that the model has learned from ImageNet and adapt them to your specific task. This can help you achieve better performance with less training data and training time compared to training a model from scratch.

Step2: In the initial layers of a convolutional neural network, the input image is convolved with a set of learnable filters to create a feature map.



```
Model: "sequential"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 densenet121 (Functional)    (None, 2, 2, 1024)        7037504

 global_average_pooling2d (G  (None, 1024)             0
 lobalAveragePooling2D)

 dense (Dense)               (None, 256)               262400

 dropout (Dropout)           (None, 256)               0

 dense_1 (Dense)             (None, 512)               131584

 dropout_1 (Dropout)         (None, 512)               0

 dense_2 (Dense)             (None, 1024)              525312

 classification (Dense)      (None, 14)                14350

=================================================================
Total params: 7,971,150
Trainable params: 6,386,894
Non-trainable params: 1,584,256
_________________________________________________________________
```

DOI: 10.48175/568

Step3: The model then adds a fully connected Dense() layer with 256 units and a ReLU activation function, followed by a Dropout() layer with a dropout rate of 0.2. Dropout is a regularization technique used to prevent overfitting by randomly dropping out some neurons during training.
Step4: The model adds another Dense() layer with 512 units and a ReLU activation function, followed by another Dropout () layer with a dropout rate of 0.2.
Step5: The model adds a final Dense () layer with 1024 units and a ReLU activation function.
Step6: Finally, the model adds an output Dense() layer with n units (where n is the number of classes in the dataset which is 14), a softmax activation function, and the name "classification."

IX. INNOVATIVE CONTENT

Traditionally, security camera footage has been monitored by human operators to detect suspicious behavior. However, this process can be slow, expensive, and prone to errors. With recent advancements in machine learning and computer vision, it is now possible to develop automated systems that can detect and identify anomalous behavior in real-time.

Our proposed system utilizes advanced machine-learning techniques to analyze surveillance footage and identify suspicious activities. When unusual behavior is detected, the system will immediately send a notification to the relevant authorities with evidence, including the video footage and information on the individuals involved. This allows for a faster response to potential security threats and increases the accuracy and reliability of surveillance systems.

Overall, our goal is to create a fully automated system that can detect suspicious activities and alert the authorities in real time, reducing the reliance on human operators and improving security measures

1. Advanced machine learning techniques: One area of innovation could be in the use of advanced machine learning techniques, such as deep learning, to improve the accuracy and efficiency of suspicious activity detection. Deep learning approaches, such as convolutional neural networks and recurrent neural networks, can learn complex patterns and relationships in video data, potentially leading to more effective detection of suspicious activities.
2. Real-time detection: Real-time detection of suspicious activities is a critical requirement for many security applications. Innovative content could focus on developing algorithms and techniques that can perform suspicious activity detection in real-time, potentially reducing response times and improving the effectiveness of security measures.
3. Anomaly detection: Anomaly detection techniques can be used to detect suspicious activities that deviate from normal behavior patterns. An innovative approach could be to use unsupervised machine learning techniques to learn normal behavior patterns from video footage, and then detect suspicious activities as those that deviate from these patterns.

X. CHALLENGES & OPPORTUNITIES

10.1 Challenges

- One of the main challenges in suspicious activity detection is dealing with the high variability and complexity of human behavior. This can lead to high false-positive rates and make it difficult to design accurate and robust algorithms.
- Another challenge is dealing with data imbalance, where there may be significantly more normal behavior instances than suspicious behavior instances in the dataset.

10.2 Opportunities

- Advances in machine learning and computer vision, such as the use of deep learning models and unsupervised learning techniques, have the potential to improve the accuracy and robustness of suspicious activity detection systems.
- The integration of multiple sources of data, such as audio, text, and social media, can also provide a more comprehensive view of suspicious activity and help reduce false positives.
- The use of real-time processing and edge computing can enable faster detection and response to suspicious activity, which is crucial in critical scenarios such as public safety and security.

DOI: 10.48175/568

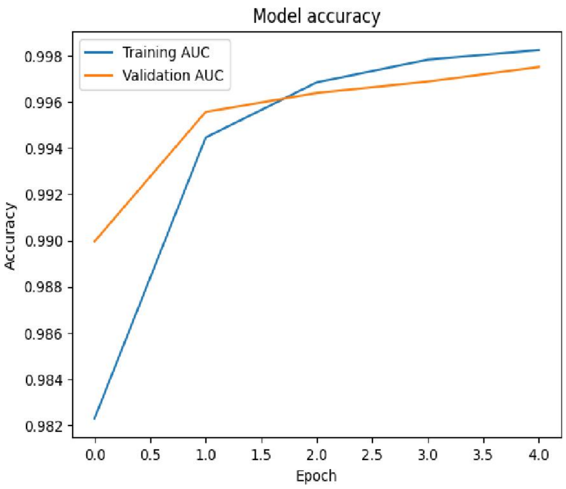
XI. RESULT AND ANALYSIS

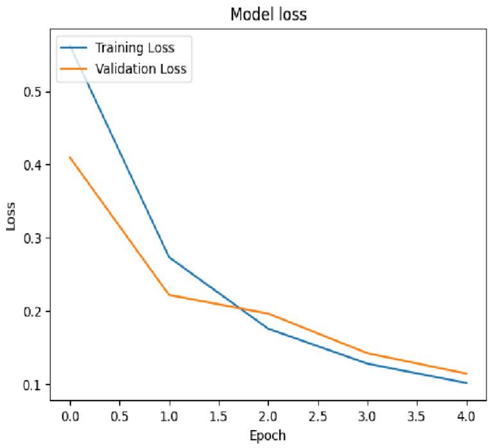
Our proposed machine learning model achieved an accuracy of 99% on the UFC Crime Dataset, which consists of 14 different classes of suspicious activity. The dataset was large, with a size of 12 GB, and included a diverse range of activities captured in surveillance footage. The high accuracy of our model demonstrates its effectiveness in detecting suspicious activities and its potential for real- world deployment.

To evaluate the performance of our model, we split the dataset into training and testing sets using a ratio of 70:30. We trained the model on the training set and evaluated its performance on the testing set. The accuracy was calculated as the percentage of correctly classified samples.

Our model was based on DenseNet121, a pre-trained deep learning model that has been shown to be effective for a variety of image classification tasks. We fine-tuned the model on our dataset using transfer learning, which enabled us to leverage the pre-trained model's knowledge and adapt it to our specific task. The model was trained using the Adam optimizer with a learning rate of 0.00003 and a batch size of 64.

Overall, the high accuracy achieved by our model demonstrates its potential for real-world deployment in surveillance systems for public safety and crime prevention. Further research could explore the use of multiple data sources and different model architectures to improve the performance of the system.





XII. FUTURE WORK

Suspicious activity detection using machine learning is a rapidly developing field, and there are many potential future directions for research and application. Here are some possible avenues for future work:

Improving the accuracy of existing models: Machine learning models can always be improved by tuning hyperparameters, adding more data, and refining the feature selection process.

- Developing new models: New types of machine learning algorithms can be developed and tested to improve the accuracy and efficiency of suspicious activity detection.
- Incorporating more data sources: Suspicious activity detection can be enhanced by incorporating additional data sources such as social media feeds, geolocation data, and financial transactions.
- Increasing automation: Machine learning algorithms can be used to automate the detection of suspicious activity, allowing for real-time monitoring and rapid response to potential threats.
- Reducing false positives: False positives can be reduced by improving the algorithms used to distinguish between normal and suspicious activity, and by incorporating more data sources to refine the detection process.
- Enhancing interpretability: Machine learning models can be made more interpretable by incorporating explainable AI techniques, enabling human analysts to better understand how the model is making decisions.
- Incorporating human feedback: Human analysts can provide feedback on suspicious activity alerts, allowing the machine learning algorithms to learn from these interactions and improve their accuracy over time.

XIII. CONCLUSION

Suspicious activity detection is a critical task for ensuring public safety, preventing fraud, and reducing crime. Advances in machine learning and computer vision have made it possible to automate the process of detecting suspicious activities in video surveillance footage. Different types of algorithms and techniques have been developed to detect suspicious activities in different scenarios. Despite the challenges, the future of suspicious activity detection looks promising, with new research directions focused on developing more robust and accurate algorithms and integrating multiple sources of data for more comprehensive detection.

XIV. ACKNOWLEDGMENT

We would be immensely grateful to Prof. Vandana Kate, my research project guide, and Prof. Nisha Rathi, my project in- charge, for their constant guidance, support, and encouragement throughout my project. Their invaluable insights and expertise have been instrumental in shaping my research and refining my ideas.

We would also like to express our heartfelt gratitude to the immensely talented professors from the "ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH" from whom we can learn deeply about Machine Learning

REFERENCES

[1]. Tejashri Subhash Bora1, Monika Dhananjay Rokade2 "Methodology for Human Suspicious Activity Detection"2021.

[2]. J. indhumathi and M. balasubramanian, "Real time video based human suspicious activity recognition using deep learning"2022.

[3]. Balbhim Lanke and Zarinabegam Mundargi, "Abnormal Acitivity Detection Using CNN Method"2022.

[4]. Nandini. G1, Dr. B. Mathivanan2, Nantha Bala. R. S3, Poornima. P4, "Suspicious human activity detection"2018.

[5]. S. A. Quadri 1, Komal S Katakdhond 2, "Suspicious Activity Detection Using Convolution Neural Network"2022.

[6]. Dinesh Jackson Samuel R, Fenil E, Gunasekaran Manogaran, Vivekananda G.N, Thanjaivadivel T, Jeeva S, Ahilan A, "Real-time violence detection framework for football stadium comprising of big data analysis and deep learning through bidirectional LSTM"

[7]. Gurav, S. S., Godbole, B. B., & Sonale, M. S. "Improved accuracy of suspicious activity detection in surveillance video"

[8]. J. Sujanaa and S. Palanivel, "Real-time video based emotion recognition using convolutional neural network and transfer learning"

[9]. C. Yeole, H. Singh, H. Waykole and A. Deshpande, "Deep Neural Network Approaches for Video Based Human Activity Recognition"

[10]. C. V. Amrutha, C. Jyotsna and J. Amudha, "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video"

[11]. Gugale1, Abhiruchi Shendkar2, Arisha Chamadia3, Swati Patra4, Deepali Ahir5, "Human Suspicious Activity Detection using Deep Learning Rachana"

[12]. Rajesh Kumar Tripathi, Anand Singh Jalal & Subhash Chand Agrawal "Suspicious human activity recognition"

[13]. Ahmed Mateen Buttar1 • Mahnoor Bano1 • Muhammad Azeem Akbar2 • Amerah Alabrah3 • Abdu H. Gumaei4 "Toward trustworthy human suspicious activity detection from surveillance videos using deep learning"

[14]. M. Adimoolam, N. M. Balamurugan, Karthi Govindharaju "Suspicious Actions Detection System Using Enhanced CNN and Surveillance Video"

[15]. Bushra Yasmeen1, Haslina Arshad2, Hameedur Rahman3 "Suspicious Activity Detection Using CCTV Surveillance Video"

[16]. Arroyo, R., Yebes, J.J., Bergasa, L.M., Daza, I.G. & Almazán, J. 2015, "Expert video-surveillance system for real-time detection of suspicious behaviors in shopping malls"