Deep Learning model for Anomaly Detection in Video Surveillance: A CNN Approach

Shrushti Thigale
Computer Engineering
Anantrao Pawar College of Engineering and Research
Pune, India
thigaleshrushti30@gmail.com

Prof. Jitendra Musale
Computer Engineering
Anantrao Pawar College of Engineering and Research
Pune, India
jitendra.musale@abmspcoerpune.org

Swapnil Shinde
Computer Engineering
Anantrao Pawar College of Engineering and Research
Pune, India
swappyshinde05@gmail.com

Swamini Deshmane
Computer Engineering
Anantrao Pawar College of Engineering and Research
Pune, India
deshmaneswamini@gmail.com

Harshad Kale
Computer Engineering
Anantrao Pawar College of Engineering and Research
Pune, India
harshadkale6111@gmail.com

Abstract: **Suspicious activity encompasses a broad concept relating to actions, behaviors, or occurrences that give rise to concerns regarding potential illegality, threat, or ethical violations. This term is commonly employed in various domains such as law enforcement, cybersecurity, and financial sectors. Detecting and addressing suspicious activity often involves vigilant observation, data analysis, and the use of technology to identify patterns that deviate from established norms. Individual and community awareness is essential for recognizing and reporting such activities, contributing to the overall maintenance of safety and security. Effectively managing and responding to suspicious activity requires a combination of proactive measures, investigative tools, and collaborative efforts to prevent potential risks from escalating. With the increasing demand for robust security solutions, video surveillance systems play a crucial role in monitoring and safeguarding public spaces. This study focuses on enhancing the capabilities of video surveillance applications by employing Convolutional Neural Network (CNN) algorithms for the detection of suspicious activities. The proposed system leverages the power of deep learning to analyze video streams and identify anomalous behaviors indicative of potential threats or security breaches. The CNN algorithm is trained on a diverse dataset to learn and recognize patterns associated with normal activities as well as those considered suspicious. The model's ability to discern complex spatial and temporal relationships in video frames enables it to provide accurate and timely alerts. Key aspects of the CNN algorithm include feature extraction, spatial hierarchies, and temporal dependencies, enabling the system to discern subtle nuances in human behavior that may go unnoticed by traditional surveillance methods. The model is designed to adapt to dynamic environments and varying lighting conditions, ensuring robust performance in real-world scenarios. In the evaluation phase, the proposed system demonstrates promising results in terms of accuracy, precision, and recall, outperforming conventional video surveillance methods.**

Keywords — ***Computer Vision, Player Detection, Player Tracking Basketball Videos, Object Detection, YOLO Algorithm.***

I. INTRODUCTION

Suspicious activity typically refers to a situation or behavior that raises concerns or doubts about the legality, safety, or ethical nature of an individual's actions. Suspicious activities may vary across different contexts, such as financial transactions, online behavior, physical movements, or interpersonal interactions. Identifying and reporting suspicious activity is crucial for maintaining security and preventing potential threats. In various sectors, including law enforcement, cybersecurity, and financial institutions, vigilance against suspicious activities is paramount. This could involve monitoring unusual patterns, unexpected behaviors, or transactions that deviate from established norms. Advanced technologies, surveillance systems, and analytical tools are often employed to detect and investigate suspicious activities. It is essential for individuals to be aware of their surroundings and be vigilant for signs of suspicious behavior. Reporting such activities to relevant authorities helps maintain public safety and prevents potential threats from escalating. Community awareness and collaboration play a key role in identifying and addressing suspicious activities effectively. Suspicious Activity is predicting the body part or joint locations of a person from an image or a video. This project will entail detecting suspicious human Activity from real-time CCTV footage using neural networks. Human suspicious Activity is one of the key problems in computer vision that has been studied for more than 15 years. It is important because of the sheer number of applications which can benefit from Activity detection. For example, human pose estimation is used in applications including video surveillance, animal tracking and behavior understanding, sign language detection, advanced human-computer interaction, and marker less motion capturing. Low cost depth sensors have limitations like limited to indoor use, and their low resolution and noisy depth information make it difficult to estimate human poses from depth images. Hence, we plan to use neural networks to overcome these problems. Suspicious human activity recognition from surveillance video is an active research area of image processing and computer vision. Through the visual surveillance, human activities can be monitored in sensitive and public areas such as bus stations, railway stations, airports, banks, shopping malls, school and colleges, parking lots, roads, etc. to prevent terrorism, theft, accidents and illegal parking, vandalism, fighting, chain snatching, crime and other suspicious activities. It is very difficult to watch public places continuously, therefore an intelligent video surveillance is required that can monitor the human activities in real-time and categorize them as usual and unusual activities; and can generate an alert. Mostly, of the research being carried out is on images and not videos. Also, none of the papers published tries to use CNNs to detect suspicious activities.

II. RELATED TECHNOLOGY

Machine Learning and Artificial Intelligence: Advanced machine learning algorithms and AI systems can be trained to recognize patterns of behavior indicative of suspicious activity across various datasets. These systems can continuously learn and adapt to new threats, enhancing their effectiveness over time.

Natural Language Processing (NLP): NLP techniques enable the analysis of text data, including social media posts, emails, and chat logs, to identify language patterns associated with criminal intent or malicious activities.

Anomaly Detection Systems: These systems use statistical methods and machine learning algorithms to identify deviations from normal behavior or expected patterns, flagging activities that may be suspicious or pose a security risk.

Mobile and IoT Device Monitoring: With the proliferation of mobile devices and IoT (Internet of Things) devices, monitoring solutions can track device activity and communications to detect anomalies or potential security breaches.

Blockchain Analytics: Beyond the use of blockchain for secure transactions, specialized analytics tools can analyze blockchain data to detect suspicious or fraudulent activities, such as money laundering or illicit transactions.

Thermal Imaging and Remote Sensing: Thermal imaging technology can detect anomalies in temperature patterns, which may indicate unusual activities or unauthorized access in physical spaces. Remote sensing technologies, including satellites and drones, can provide additional surveillance capabilities.

Quantum Cryptography: Quantum cryptography offers highly secure communication protocols that leverage the principles of quantum mechanics to detect eavesdropping attempts, ensuring the integrity and confidentiality of sensitive data.

Autonomous Security Systems: Autonomous robots equipped with sensors, cameras, and AI capabilities can patrol and monitor areas for suspicious behavior, providing real-time alerts and assistance to human security personnel.

Crowdsourcing and Community Reporting Platforms: Technology platforms that enable crowdsourcing of information or allow community members to report suspicious activities can serve as valuable tools for early detection and response to potential threats.

Privacy-Preserving Technologies: As concerns about privacy grow, technologies that enable effective surveillance without compromising individual privacy rights are becoming increasingly important. Techniques such as differential privacy and secure multi-party computation allow data to be analyzed while protecting sensitive information.

III. IMPORTANCE

1.Crime Prevention: Early detection of suspicious activity can help prevent criminal acts, including theft, fraud, cybercrime, and acts of violence. Proactive measures can deter criminals and disrupt their plans.

2.Security Enhancement: Recognizing suspicious behavior prompts the implementation of enhanced security measures. This may include improved surveillance, access controls, and cybersecurity protocols to protect against potential threats.

3.Risk Mitigation: Identifying and addressing suspicious activities is a key component of risk management. By understanding and mitigating potential risks early on, individuals and organizations can minimize the impact of adverse events.

4.Public Safety: Vigilance against suspicious activity contributes to overall public safety. Communities that actively report and address suspicious behavior create a safer environment for residents, businesses, and visitors. Preventing

5.Terrorism: In the context of national security, recognizing suspicious activities is crucial for preventing acts of terrorism. Early intervention can disrupt terrorist plans and protect the well-being of citizens.

6.Financial Integrity: Suspicious activity reports are vital in maintaining the integrity of financial systems. Identifying and reporting financial irregularities helps combat money laundering, fraud, and other financial crimes.

7.Cybersecurity Defense: In the digital age, identifying suspicious activities is paramount for defending against cyber threats. Timely detection allows for the implementation of cybersecurity measures to protect sensitive information and infrastructure.

8. Compliance with Regulations**:** Many industries are subject to regulations that require the identification and reporting of suspicious activities. Compliance with these regulations is essential for legal and ethical business practices.

9.Community Trust: Actively addressing suspicious activities builds trust within communities. When individuals feel secure and see that authorities take proactive measures, they are more likely to engage in reporting and cooperation.

10.Emergency Preparedness: Identifying suspicious behavior contributes to overall emergency preparedness. It enables authorities to anticipate and respond effectively to potential crises, minimizing the impact on public safety.

11.National Security: In the context of national security, recognizing and addressing suspicious activities is crucial for protecting a country's borders, infrastructure, and citizens from external threats.

IV. LITERATURE SURVEY

Sathyajit Loganathan, Gayashan Kariyawasam.[1] Suspicious activities are of a problem when it comes to the potential risk it brings to humans. With the increase in criminal activities in urban and suburban areas, it is necessary to detect them to be able to minimize such events. Early days surveillance was done manually by humans and were a tiring task as suspicious activities were uncommon compared to the usual activities. With the arrival of intelligent surveillance systems, various approaches were introduced in surveillance. We focus on analyzing two cases, those if ignored could lead to high risk of human lives, which are detecting potential gun-based crimes and detecting abandoned luggage on frames of surveillance footage. We present a deep neural network model that can detect handguns in images and a machine learning and computer vision pipeline that detects abandoned luggage so that we could identify potential gun-based crime and abandoned luggage situations in surveillance footage.

D. Mart´ınez,H.Loaiza, and E. Caicedo.[2] The proposed early detection algorithm is justified because the probability of success to control a criminal activity increases when the response time for generating a warning alarm is reduced. In this paper, a video-based representation model to describe suspicious behavior from elementary actions is proposed. Such behaviors allow detecting potential threats before suspects achieve physical contact with their potential victims. In the algorithm, a novel method to adjust the balance between the anticipation level to threats and the generation of false alerts is introduced.

Shriya Akella, Priyanka Abhang, Vinit Agrharkar, Dr. Reena Sonkusare.[3] There is a growing need for smart surveillance systems in public and private places to logically differentiate between normal and abnormal behaviour.This is not just important for the convenience of the people but also for their security. Understanding a video footage and classifying an activity as normal or suspicious especially in densely packed regions is possible and has been demonstrated in this paper. The proposed system makes use of the YOLOv3 algorithm for object detection. The COCO dataset, which is a large-scale object detection, segmentation and captioning dataset, has been used for training this model. The whole framework is made up of two parts.

UTKU GÖRKEM KETENCI 1 , TOLGA KURT1 , SELİM ÖNAL2 , CENK ERBİL2 , SİNAN AKTÜRKOGLU ˇ 2 , AND HANDE ŞERBAN İLHAN2[4]**.** Money laundering is the crucial mechanism utilized by criminals to inject proceeds of crime into the financial

system. The primary responsibility of the detection of suspicious activity related to money laundering is with the financial institutions. Most of the current systems in these institutions are rule-based and ineffective (over 90 % false positives). The available data science-based anti-money laundering (AML) models to replace the existing rule-based systems work on customer relationship management (CRM) features and time characteristics of transaction behaviour.Due to thousands of possible account features, customer features, and their combinations, it is challenging to perform feature engineering to achieve reasonable accuracy.

Shaaban Sahmoud, Hayder Safi [5]. With the huge widespread and usage of social media in our life, it becomes an effective tool to share our feeling, opinions and even our political orientations when there is civil unrest or protests. As a result, there are many tries from different formal and informal groups to affect on or reply to any political tweets or trends that rise on social media. The main purpose of these groups is to influence the general opinion to fit the intended goal by spreading fake posts, news and even hate speech. This paper introduces a set of first stage analyses automated methods that can be used to detect the effect of such groups called ”digital trolls”. We considered the recently occurred Iraq unrest and Iraqi people protest as a case study to analyze the activities of Twitter users and detect if there are any external groups try to influence the people’s opinions and orientations during the crisis. We gathered a new related dataset from Twitter that includes tweets and users’ information collected during the crisis.

David Acuna [6]. have discussed Real-Time Detection and Tracking of Basketball Players using Deep Neural Networks. In this paper, they presented a novel on-line multi detection and tracking framework that is able to accurately detect and track basketball players by just looking at broadcast videos. Their detection and tracking pipeline was composed by YOLOv2, a real-time state-of-the-art detector, and SORT a simple but accurate tracking by detection algorithm.

Jun liang Xing, Huizhou Ai, Liwei Liu and Shihong Lao [7]. has presented Multiple Player Tracking in Sports Video: A Dual-Mode Two-Way Bayesian Inference Approach With Progressive Observation Modeling .In this paper, they focus on the challenging problem of tracking multiple highly dynamic and highly interactive players in sports video. Facing the difficulties it presents, they propose a new algorithm that formulates the SOT problem and MOT problem in a unified dual-mode two-way Bayesian inference approach based on the observations that are built progressively. The proposed method obtains satisfactory tracking results on many typical real world sports videos.

Wenlin Yan, Xianxin Jiang, Ping Liu [8] have discussed A Review of Basketball Shooting Analysis Based on Artificial Intelligence. This article provides an overview of the current application status of artificial intelligence (AI) technology in basketball shooting analysis and discusses the main research topics in this field.

V. EXISTING SYSTEM

The Existing systems for managing suspicious activity vary across different sectors and industries. Here are some examples in various domains: Law Enforcement: Traditional law enforcement agencies rely on human intelligence, surveillance, and investigations to identify and address suspicious activities. Specialized units may use predictive policing models or profiling techniques to allocate resources based on historical data. Financial Institutions: Financial institutions employ transaction monitoring systems to detect anomalies in financial transactions, which may indicate money laundering, fraud, or other illicit activities. Compliance departments are responsible for ensuring adherence to regulatory requirements, conducting due diligence, and reporting suspicious transactions to relevant authorities.

VI. PROPOSED SYSTEM

The proposed system for managing suspicious activity involves the integration of advanced technologies and methodologies to enhance detection, analysis, and response to potential threats. This system aims to provide a comprehensive approach across various domains, such as cybersecurity, law enforcement, and financial sectors. Key components of the proposed system include:
Data Analytics and Machine Learning: Utilize sophisticated algorithms and machine learning models to analyze large datasets for patterns indicative of suspicious activity. Implement anomaly detection techniques to identify deviations from normal behavior or transaction patterns. Real-time Monitoring and Surveillance: Employ real-time monitoring systems to continuously observe activities across relevant platforms and networks. Integrate surveillance technologies, including video analytics and sensor networks, to enhance situational awareness.
Behavioral Analysis: Incorporate behavioral analysis tools to assess and understand user or entity behavior, identifying anomalies that may indicate potential threats. Use profiling techniques to create baseline behavior patterns for comparison.
Integration with Threat Intelligence: Integrate the system with external threat intelligence feeds to stay updated on emerging risks and known threat actors.
Enhance the system's ability to recognize patterns associated with previously identified threats.

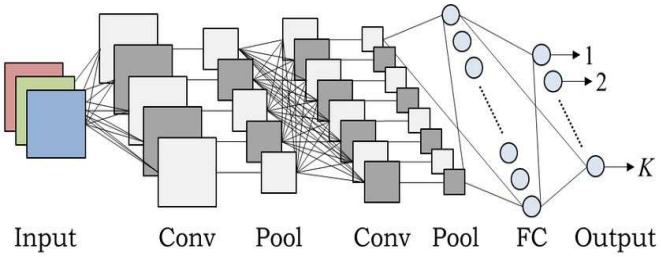


Fig 1: Diagram of Purposed System

VII. RESEARCH METHODOLOGY

Research methodology for studying suspicious activity typically involves a systematic and structured approach to collecting, analyzing, and interpreting data related to behavior or incidents that may raise concerns. Here's a general outline of a research methodology for studying suspicious activity:
1.Define the Research Objectives: Clearly articulate the goals and objectives of the research. What specific aspects of suspicious activity are you aiming to understand? Define the scope and purpose of the study.
2.Literature Review: Review existing literature on suspicious activity, crime prevention, security measures, and related topics. Understand the current state of knowledge, identify gaps, and build a theoretical framework for your research.
3.Formulate Research Questions or Hypotheses: Based on the literature review and research objectives, develop specific research questions or hypotheses that will guide your investigation.
4.Select a Research Design: Choose an appropriate research design that aligns with your objectives. Common designs may include observational studies, surveys, case studies, or a combination of methods.

5.Define the Population and Sampling Strategy: Identify the population or group under study. Develop a sampling strategy to select a representative subset if the population is too large. Ensure that the sample chosen is relevant to the research objectives.
6.Data Collection Methods: Determine the methods for collecting data. This could involve:
Observation: Systematically observing and documenting suspicious activities.
Surveys/Questionnaires: Gathering information from individuals or groups regarding their experiences or observations.
Interviews: Conducting one-on-one or group interviews with relevant stakeholders.
Document Analysis: Reviewing documents, reports, or records related to suspicious activities.
Develop Data Collection Instruments: If applicable, design and validate instruments such as surveys or interview guides. Ensure they align with the research questions and objectives.
Ethical Considerations: Address ethical considerations, including obtaining informed consent, ensuring participant anonymity and confidentiality, and adhering to ethical guidelines for research involving human subjects.
Pilot Testing: Conduct a pilot test of your data collection instruments to identify and address any issues with clarity, comprehensibility, or appropriateness.
Data Analysis: Choose appropriate analytical methods based on your research design. Common methods include statistical analysis, content analysis, thematic analysis, or qualitative coding.
Interpretation of Results: Interpret the findings in the context of your research questions or hypotheses. Discuss the implications and limitations of your results.
Conclusion and Recommendations: Summarize your findings, draw conclusions, and provide recommendations for future research or practical applications.
Documentation and Reporting: Document the entire research process, from design to findings. Prepare a comprehensive report or academic paper following established guidelines.
Peer Review and Validation: If applicable, subject your research to peer review for validation and feedback.
Dissemination of Results: Share your research findings through academic publications, conferences, or other relevant channels. This methodology provides a systematic framework for researching suspicious activity, ensuring rigor, validity, and ethical considerations throughout the process. The specific details of the methodology will depend on the nature of the suspicious activities under investigation and the resources available for the research.

VIII. SYSTEM ARCHITECTURE

Firstly we have to gather Image dataset. After data collection done then we prepare data using preprocessing. After preprocessing done we have to train dataset by using CNN algorithm. If training part done machine create model. We use train model for the testing and detect the output Suspicious activity or not.
1.Input as Dataset.
2.Preprocessing:- Data preprocessing is the concept of changing the raw data into a clean data set. The dataset is pre processed in order to check missing values, noisy data, and other inconsistencies before executing it to the algorithm. Data must be in a format appropriate for ML.
3.Feature Extraction:- Feature extraction refers to the process of transforming raw data into numerical features that can be processed while preserving the information in the original data set. It yields better results than applying machine learning directly to the raw data. 4.Classification by using CNN:- CNNs consist of a series of interconnected layers that process the input data. The first hidden layer of a CNN is usually a convolutional layer, which applies a set of filters to the input data to detect specific patterns. Detect the Suspicious Activity detect or not Convolutional Neural Networks specialized for applications in image & video recognition. CNN is mainly used in image analysis tasks like Image recognition, Object detection & Segmentation. There are Four types of layers in Convolutional Neural Networks:

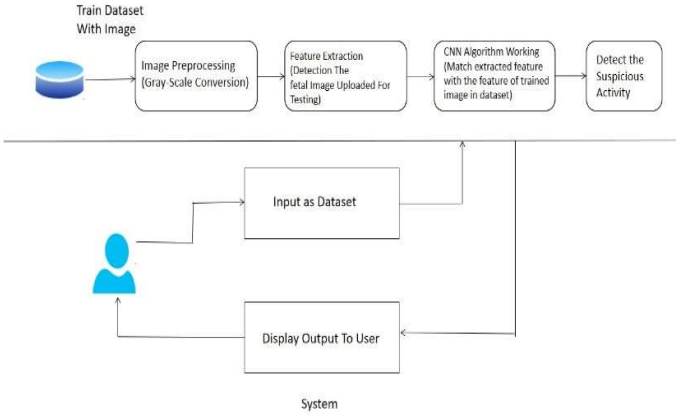


Fig 2: Diagram of System Architecture

Tools required are used to detect the activities:
1]JupyterLab: JupyterLab is an interactive development environment for working with notebooks, code, and data. It offers a flexible user interface for creating and editing Jupyter notebooks, text files, terminals, and custom components. It supports various programming languages including Python, R, Julia, and more.
2]Jupyter Notebook: Jupyter Notebook is an open-source web application that allows you to create and share documents that contain live code, equations, visualizations, and narrative text.It supports various programming languages, with Python being the most popular. Notebooks can be used for data cleaning and transformation, numerical simulation, statistical modeling, machine learning, and more.
3]Spyder: Spyder is an open-source integrated development environment (IDE) for scientific computing with Python.It provides tools for data exploration, analysis, and visualization, as well as development features like code debugging and profiling. Spyder's interface is designed to be user-friendly and efficient for scientific programming tasks.
4]PyCharm: PyCharm is a powerful IDE for Python development, designed by JetBrains.It offers intelligent code completion, code analysis, and debugging capabilities. PyCharm supports web development with Django, Flask, and other frameworks, as well as data science and scientific computing.
5]VSCode (Visual Studio Code): Visual Studio Code is a lightweight but powerful source code editor developed by Microsoft. It supports a wide range of programming languages and extensions, making it highly customizable for different development workflows. VSCode features include debugging, syntax highlighting, code snippets, and version control integration.

6]Glueviz (Glue): Glueviz is an open-source Python library and application for interactive data visualization.It allows users to explore relationships within and between datasets through linked visualizations. Glue is particularly useful for scientific data analysis and visualization tasks.
7]Orange 3 App (Orange): Orange is an open-source data visualization and analysis tool, particularly focused on machine learning and data mining tasks .It offers a visual programming interface for building data analysis workflows without requiring programming skills. Orange provides a wide range of data visualization techniques and machine learning algorithms.
8]RStudio: RStudio is an integrated development environment (IDE) for the R programming language. It provides tools for data analysis, visualization, and statistical computing. RStudio includes features such as code highlighting, debugging, and package management to support the development process in R.

IX. ADVANTAGES

1.Enhanced Security: Reporting suspicious activity can help prevent potential threats and enhance overall security in a community or organization.
2.Crime Prevention: Early reporting of suspicious activity can lead to the prevention of crimes before they occur, reducing the risk of harm to individuals and property.
3.Community Safety: Reporting suspicious activity fosters a sense of community responsibility and encourages individuals to look out for one another.
4.Law Enforcement Support: Reporting suspicious activity provides law enforcement with critical information that can help them investigate and respond to potential threats.
5. Timely Response: It allows law enforcement to respond promptly to situations that could pose a danger to public safety.

X. ALGORITHM

1.Convolutional Layer: In a typical neural network each input neuron is connected to the next hidden layer. In CNN, only a small region of the input layer neurons connect to the neuron hidden layer.
2.Pooling Layer: The pooling layer is used to reduce the dimensionality of the feature map. There will be multiple activation & pooling layers inside the hidden layer of the CNN.
3.Flatten: - Flattening is converting the data into a 1-dimensional array for inputting it to the next layer. We flatten the output of the convolutional layers to create a single long feature vector.
4.Fully-Connected layer: Fully Connected Layers form the last few layers in the network. The input to the fully connected layer is the output from the final Pooling or Convolutional Layer, which is flattened and then fed into the fully connected layer.
CNN Implementation Steps:
Step 1: Convolution Operation (Filter image)
Step 2(b): RELU Layer
Step 3: Pooling(Used max Pooling function)
Step 3: Flattening (Covert Matrix into 1D Array)
Step 4(b): Dense
Step 4(c): Optimizer
Step 4(d): Compile
Step 1: Convolution Operation (Filter Image): In this step, the algorithm applies convolutional filters to the input image. These filters are small matrices that slide over the image to detect local patterns or features. The result is a set of feature maps that highlight different image features.
Step 2(b): RELU Layer: After each convolution operation, a Rectified Linear Unit (RELU) activation function is applied element-wise to each feature map. RELU introduces non-linearity to the model by replacing negative values with zero while leaving positive values unchanged.
Step 3: Pooling (Used Max Pooling Function):Pooling reduces the dimensionality of each feature map while retaining the most important information. Max pooling is commonly used, where the maximum value in a small region of the feature map is retained, and the rest are discarded. This helps make the model more robust to variations in position and scale.
Step 3: Flattening (Convert Matrix into 1D Array):The flattened layer reshapes the 2D feature maps into a 1D array. This prepares the data for input into a traditional feedforward neural network.
Step 4(b): Dense: After flattening, one or more dense (fully connected) layers are added to the neural network. These layers are responsible for learning global patterns and making predictions based on the extracted features from the previous steps.
Step 4(c): Optimizer: The optimizer is a crucial component that adjusts the model's weights during training to minimize the loss function. Common optimizers include Stochastic Gradient Descent (SGD), Adam, or RMSprop.
Step 4(d): Compile: The compile step involves configuring the loss function, optimizer, and evaluation metrics for the model. The loss function quantifies how well the model is performing, the optimizer specifies how the model's weights are updated, and evaluation metrics define how the model's performance is measured during training and testing.

XI. MATHEMATICAL MODEL

Let S be the Whole system S= {I,P,O}

I-input

P-procedure

O-output

Input(I)

I={ videos, various types of video}

Where,

user upload videos -> get dataset videos as a input

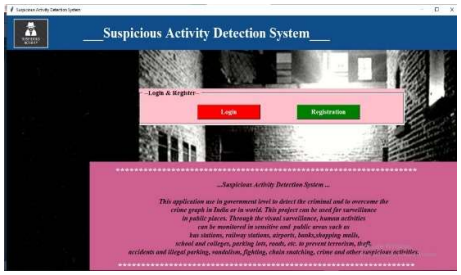
Procedure (P),

P={I, Apply CNN algorithm for preprocessing and classification}

Output(O)-

O={ get Message as a suspicious or not from video}

XII. RESULT



XIII. CONCLUSION

A system that analyzes CCTV footage in real-time to look for any suspicious activity would assist to improve security and require less human interaction. Human suspicious Activity has advanced significantly, allowing us to better support the countless applications that are made available by it. Additionally, research in allied domains, like activity tracking, can significantly increase its beneficial application in a number of fields. The suggested model for spotting suspicious activity during an exam in a classroom is built on a number of computer vision techniques, including the Viola Jones, related-Like Feature, and Ada Boost algorithms. As a result, the system for detecting various activities during an examination can be successfully implemented. Based on color and grid manipulation, the head direction and hand contact are determined, and the face is tracked using the practice data. This concept greatly aids educational institutions in reducing unusual or unfair behavior in the classroom. The suggested solution would undoubtedly provide excellent accuracy while using the fewest amount of computational resources. The system model serves as a foundation for developing and incorporating more activities to detect in addition to the one described here. Our research suggests experimenting with various architectures and comparing them in order to optimize faster predictions for guns as future work for this project. Due to time and resource constraints, we were only able to discuss the research as much as it is in this paper. This means that more work can be done to improve real-time gun detection. It might also be a good idea to conduct research on adding features other than surveillance footage to improve real-time detection .Further research in this area can advance the field as the abandoned luggage detection method suggested in this study does not address problems such as object identification in abrupt changes in illumination.

XI. FUTURE SCOPE

We have shown that adding time-frequency features, simplifies the feature selection process and improves the quality of the data science model. Time-frequency features such as mean, variance, Kurtosis, and skewness have been used for the first time in machine learning model training for suspicious transaction detection. Therefore, the feature engineering stage can be shortened by calculating the proposed time-frequency feature set. This potentially saves many person-months of modeling studies for the financial institutions. The proposed solution has been implemented in Python and the high-level of accuracy has been proven on real financial data. The generalized solution can easily be adapted to detect suspicious transactions in various organizations. An analysis of actual customer data indicates that time frequency features can distinguish between suspicious and clear cases, improving AUC and the efficiency of the transaction monitoring system. Among different time-frequency characteristics, Kurtosis provided the maximum differentiation in the model. The gains in accuracy and the capability of detecting money laundering cases that were not detectable before can save financial institutions from regularity fines and HR cost in the order of millions of USD. In this work, only a low complexity Fourier transform based approach is utilized for frequency domain analysis. As a future work, the time-frequency analysis can be accomplished with other types of linear and non-linear transform.

X. REFERENCESES

1] Miller, Z., Dickinson, B., and Hu, W. (2012). Gender prediction on twitter using stream algorithms with n-gram character features. International Journal of Intelligence Science, 2(04), 143.

2] Burger, J. D., Henderson, J., Kim, G., and Zarrella, G. (2011, July). Discriminating gender on Twitter. In Proceedings of the conference on empirical methods in natural language processing (pp. 1301-1309). Association for Computational Linguistics.

3] Verhoeven, B., Daelemans, W., and Plank, B. (2016). Twisty: a multilingual twitter stylometry corpus for gender and personality profiling. In Proceedings of the 10th Annual Conference on Language Resources and Evaluation (LREC 2016)/Calzolari, Nicoletta [edit.]; et al. (pp. 1-6)

4] Sumner, C., Byers, A., Boochever, R., and Park, G. J. (2012, December). Predicting dark triad personality traits from twitter usage and a linguistic analysis of tweets. In 2012 11th International Conference on Machine Learning and Applications (Vol. 2, pp. 386-393). IEEE.

5] Wald, R., Khoshgoftaar, T. M., Napolitano, A., and Sumner, C. (2012, December). Using Twitter content to predict psychopathy. In 2012 11th International Conference on Machine Learning and Applications (Vol. 2, pp. 394-401). IEEE.

6] Zheng, X., Han, J., and Sun, A. (2018). A survey of location prediction on twitter. IEEE Transactions on Knowledge and Data Engineering, 30(9), 1652-1671.

7] Lee, K., Ganti, R. K., Srivatsa, M., and Liu, L. (2014, December). When twitter meets foursquare: tweet location prediction using foursquare. In Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (pp. 198207). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

8] M. A. Villalobos and E. Silva, ''A statistical and machine learning model to detect money laundering: An application,'' Actuarial Sci. Dept. Anahuac Univ., Tech. Rep., 2017. [Online]. Available:

9] V. Jayasree and R. V. S. Balan, ''Money laundering regulatory risk evaluation using bitmap index-based decision tree,'' *J. Assoc. Arab Universities Basic Appl. Sci.*, vol. 23, no. 1, pp. 96–102, Jun. 2017.

10] M. B. Jamshidi, M. Gorjiankhanzad, A. Lalbakhsh, and S. Roshani, ''A novel multiobjective approach for detecting money laundering with a neuro-fuzzy technique,'' in *Proc. IEEE 16th Int. Conf. Netw., Sens. Control (ICNSC)*, May 2019, pp. 454–458.

11] Prof. Jitendra C. Musale, IJRASET52372"Hybrid Features Extraction for Emotion Detection using Deep Convolutional Neural Network", in International Journal for Research in Applied Science & Engineering Technology (International Peer Reviewed and Refereed Journal) Volume: 11 Issue: 05 | ,May- 2023 ISSN: 2321-9653 Pages 9

12] Prof. Jitendra C. Musale, "Design Of Conversion of Sign Language to Text", in Journal of Emerging Technology and Innovative Research (JETIR) JETIR2303334 Volume: 10 Issue: 03 |, March- 2023 ISSN: 2349-5162 www.jetir.org (ISSN-2349-5162) Pages 4