B.E. Project Phase-II Report

on

Deep Learning Approach for Suspicious Activity Detection from Surveillance Video

by

Vedant Saikhede (B190368612)
Kiran Shende (B190368623)
Yuvraj Darekar (B190368535)
Hemant Thorat (B190368637)

Under the guidance of

Prof. S. P. Shinde

Department of Information Technology

Smt. Kashibai Navale College of Engineering, Pune-41

SAVITRIBAI PHULE PUNE UNIVERSITY

2023-2024

Sinhgad Technical Education Society,

Smt. Kashibai Navale College of Engineering, Pune-41

DEPARTMENT OF INFORMATION TECHNOLOGY

Sinhgad Institutes

Date:

CERTIFICATE

This is to certify that,

VEDANT SAIKHEDE (B190368612)
KIRAN SHENDE (B190368623)
YUVRAJ DAREKAR (B190368535)
HEMANT THORAT (B190368637)

of class B.E IT have successfully completed their Project Phase-II work on **"Deep Learning Approach for Suspicious Activity Detection from Surveillance Video"** at **Smt. Kashibai Navale College of Engineering, Pune** in the partial fulfilment of the Graduate Degree course in B.E at the **Department of Information Technology**, in the academic **Year 2023-2024** as prescribed by the Savitribai Phule Pune University, Pune.

Prof. (Mrs). S. P. Shinde
Project Guide

Dr. M. L. Bangare
Head of the Department
(Department of Information Technology)

(External Examiner)
Savitribai Phule Pune University, Pune

Dr. A.V. Deshpande
Principal
SKNCOE, Pune

ABSTRACT

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, roads, etc. to prevent terrorism, theft, accidents and illegal parking, chain snatching, and other suspicious activities.

It is very difficult to watch public places continuously, therefore an intelligent video and categorize them as usual and unusual activities; and can generate an alert. Mostly, 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.

ACKNOWLEDGEMENT

We are very thankful to all the teachers who have provided us with valuable guidance towards the completion of this project work on "**Deep Learning Approach for Suspicious Activity Detection from Surveillance Video"**. We express our sincere gratitude towards the cooperative department who has provided us with valuable assistance and requirements for the project work. We are very grateful and want to express our thanks to **Prof. S. P. Shinde** for guiding us in the right manner, correcting our doubts by giving her time whenever we required, and providing her knowledge and experience in making this project work. We are also thankful to the HOD of our Information Technology department, **Dr. M. L. Bangare** for his moral support and motivation which has encouraged us to make this project work. We are also thankful to our Vice Principal **Dr. R. H. Borhade** and our Principal **Dr. A.V. Deshpande**, who provided his constant support and motivation that made a significant contribution to the success of this project.

Vedant Saikhede (B190368612)
Kiran Shende (B190368623)
Yuvraj Darekar (B190368535)
Hemant Thorat (B190368637)

Table of Contents

List of Tables

List of Figures

Acronyms

CNN	Convolutional Neural Network.
KNN	K-Nearest Neighbour.
ReLu	Rectified Linear Unit.
RNN	Recurrent Neural Networks.
SADS	Suspicious Activity Detection System.
SVM	Support Vector Machine.

Chapter 1
INTRODUCTION

1.1 Introduction

Examination environment consists of large number of Exams are a necessary component of every educational programme. Academic dishonesty is often dealt with administratively in the classroom or at the institutional level. Cameras are being utilised for surveillance in increasing numbers. Surveillance cameras capture a huge amount of video data. Observing human behaviour and categorising actions can be highly subjective in some situations. Gazing behind or in front of someone, making movements, looking to the side, sharing your response, copying from notes, or carrying a smartphone are all suspicious behaviours. The test environment is made up of many applicants, exam conductors, and guards. Numerous hu man resources are necessary to always keep an eye on the applicants to prevent misbehaviour or cheating. This level of focus and concentration cannot always be applied to an exam. Consequently, this approach for suspicious activity recognition was developed to solve the issue of exam cheating while minimising human effort. Cheating is becoming more common at all academic levels, including secondary and primary schools. In recent years, computer vision research has shown promising breakthroughs in the field of human activity identification in videos.

The importance of digital image processing is demonstrated in a variety of applications, such as remote sensing, video surveillance, video recovery, human-computer interfaces, sports video analysis, home intelligence, and feature extraction. The proposed study's primary goal would be to infer developing action tags from temporally segmented video sequences. The proposed project includes a complete framework for recognizing and characterising unusual behaviours and activities in exam rooms that encourage cheating. This is accomplished by observing a test video and filming the students. Reputable extracted features are used to optimise the obtained model. Another notable contribution is the study's inclusion of a new dataset on exam cheating. It discusses the most common trying to cheat strategies, such as not trying to cheat, looking at another person's exam paper, swapping exam papers, and use a cheat sheet, and use a smartphone, and gazing at another person's exam paper. The primary goal of this research is to develop a

multimedia analysis system capable of college name 3 recognising and categorising various behaviours that indicate exam cheating.

The model extracts well-known characteristics and scales each dataset frame. To encode the visual occurrences in each frame, a visual language codebook for each type of feature is created. This codebook makes use of words of various sizes. Finally, the stated attributes are classified using a support vector machine. The proposed dataset is used to demonstrate the utility of the proposed method.

Our machine learning based project is called Suspicious Activity machine learning-based project is called Suspicious Activity Detection in Exam Hall. Using the dataset, two training and testing models are generated. During the training phase, the machine learning algorithm model is taught using our unique dataset. We split the dataset to establish training and validation sets. 20at random. Our system is a desktop programme that accepts input in the form of a computer-stored movie. After being divided into frames, the pre-processed data is sent into the model of the machine learning algorithm. Following that, feature extraction methods are used to extract attributes.

1.2 Aim and Motivation

The aim of a Deep Learning approach for suspicious activity detection project is to develop and implement a system that can automatically and accurately identify unusual or potentially suspicious activities in each environment, such as video surveillance footage data. This approach leverages deep learning techniques, which are a subset of machine learning algorithms.

1.3 Background and Need of Project.

Background

- **Increasing Surveillance Data**: The proliferation of surveillance cameras has led to an overwhelming amount of video data that is difficult to monitor manually. Deep learning can automate the process of analyzing this vast amount of data, making it possible to detect anomalies and suspicious activities.

- **Traditional Methods vs. Deep Learning**: Traditional methods for video surveillance often rely on manual monitoring or rule-based systems, which can be limited in their ability to adapt to complex scenarios. Deep learning models, especially convolutional neural networks (CNNs), have shown superior performance in image and video analysis tasks, including object detection and activity recognition.

Need for the Project:

• **Real-time Threat Detection**: Traditional surveillance systems may not be efficient in real time threat detection, especially in crowded or complex environments. Deep learning models can process video data in real-time, enabling the quick identification of suspicious activities and potential threats.

• **Enhanced Accuracy and Adaptability**: Deep learning models excel at feature learning, enabling them to automatically learn and adapt to different patterns of suspicious behaviour. Their ability to generalize from training data makes them suitable for handling diverse scenarios and dynamic environments.

• **Reducing False Positives**: Manual surveillance or rule-based systems may generate false positives, leading to unnecessary alerts. Deep learning models, when properly trained, can significantly reduce false positives by learning to discriminate between normal and suspicious activities more accurately.

• **Scale and Efficiency:** Deep learning models can be deployed to process video streams from multiple cameras simultaneously, providing a scalable solution for large-scale surveillance systems.

1.4 Key Objectives

• **Threat Detection**: The primary goal is to automatically identify and detect suspicious activities or behaviours within the video footage. This includes activities such as unauthorized access, loitering, theft, vandalism, or aggressive actions.

• **Real-time Monitoring**: SADS should operate in real-time, providing immediate alerts and responses to potential security threats, allowing security personnel to take timely action.

• **Reducing False Alarms**: Minimize false alarms and improve the accuracy of threat detection by leveraging CNNs' ability to discern patterns and anomalies in video data

1.5 Organization of the Report

Chapter 1: Introduction - In this chapter, the introduction includes the Problem Definition, Justification of the Problem, the need for a new system, and updating the previous system.

Chapter 2: Literature Survey - It synthesizes related research done on this topic. Literature survey includes different research done methods using their algorithms and which area the research lacks along with that it also includes existing system architecture and its detailed explanation and working.

Chapter 3: System Requirement and Specification - This chapter gives overall tools and techniques used in the system and the information related to them.

Chapter 4: System Architecture - This chapter contains architectural information on both the proposed system and the contributions made to it, as well as the existing ones.

Chapter 5: High Level System Design - Outline the architecture, key components, and data flow of the deep learning-based suspicious activity detection system, detailing how subsystems interact.

Chapter 6: System Implementation - Develop and integrate the deep learning-based suspicious activity detection system, including coding, hardware setup, and software configuration.

Chapter 7: GUI / Experimental Results – Describe GUI components for user interaction and present performance results validating system accuracy and responsiveness.

Chapter 8: Testing - Systematic evaluation to identify bugs, ensure reliability, and verify the system meets requirements.

Chapter 9: Project Plan - Define the timeline, milestones, resources, and tasks for developing and deploying the suspicious activity detection system using deep learning.

Chapter 10: Conclusions - Summarize findings, highlight successes and limitations, and suggest future improvements.

Chapter 2
LITERATURE SURVEY

2.1 Literature Survey

Table 2.1 Literature Survey

Sr No.	Paper Name	Authors	Abstract	Cons
1	**Automated Cheating Detection in Exams using Posture and Emotion Analysis**	Mr. Nishchal J, Ms. Sanjana Reddy, Ms. Navya Priya N	Cheating in exams is a widespread issue globally, necessitating automated detection methods. This paper proposes a system utilizing posture detection, face recognition, and emotion analysis to automate cheating detection, eliminating reliance on manual invigilation.	**1.Artificial Transformations:** The colour jitter transformations (brightness, hue, saturation, contrast) applied to the images might introduce artificial variations that do not reflect real-world scenarios. **2.Limited Diversity**: While the dataset includes 1000 images per class, the diversity within each class may still be limited.
2	**Automated Invigilation System for Detection of Suspicious Activities during Examination**	Md Adil, Rajbala Simon, Sunil Kumar Khatri	This paper proposes a video surveillance system to monitor exam environments and detect suspicious behaviours. Using automated video feeds and advanced processing algorithms,	**1. Spatial Constraints:** To optimize performance, the system may require a certain amount of space between students, which could be challenging to

			the system employs features like face recognition and background subtraction. While effective, challenges include resource demands and potential false positives.	implement in crowded examination halls. **2.Complex Setup**: Deploying the system may involve complex setup procedures, including training datasets and calibration, which could pose logistical challenges for academic institutions.

3	**Real-Time Suspicious Detection and Localization in Crowded Scenes**	Mohammad Sabokrou, Mahmood Fathy	In this paper, we propose a method for real-time suspicious detection and localization in crowded scenes. The approach involves using local and global descriptors to capture video properties, and Gaussian classifiers to distinguish normal activities from anomalies. The system is shown to be comparable to state of-the-art procedures on UCSD ped2 and UMN benchmarks while being more time efficient. Experimental results confirm its reliability in detecting and localizing anomalies in videos.	**1.Limited evaluation scope:** which may not cover the full spectrum of video scenarios. **2.Lack of discussion on scalability:** It does not discuss the scalability of the proposed method to handle extremely large video datasets.
4	**Learning Temporal Regularity in Video Sequences**	Mahmudul Hasan, Jonghyun Choi	This paper addresses the challenge of perceiving meaningful activities in long video sequences by learning generative models for regular motion patterns. Two methods based on auto encoders are proposed, one using handcrafted spational temporal local	**1.Limited comparison to other methods:** The paper lacks a comprehensive comparison with other state-of the-art approaches for learning temporal regularity in video sequences.

			features and the other using a fully convolutional feed forward auto encoder. The model captures regularity from multiple datasets and shows competitive performance in suspicious detection applications.	**2.Scalability concerns:** The paper does not discuss how the proposed methods would scale larger and more complex video datasets.
5	**Suspicious Detection in Video Using Predictive Convolutional Long Short-Term Memory Networks**	Jefferson Ryan Medel	The paper presents end-to-end trainable composite Convolutional Long Short-Term Memory (Conv-LSTM) networks for automating the detection of anomalous events in video sequences. The models predict the evolution of video sequences and derive regularity scores from reconstruction errors. The paper explores the effectiveness of Conv LSTM units for modelling and predicting video sequences and demonstrates competitive results on suspicious detection datasets.	**1. Limited explanation of model selection**: The paper mentions choosing the "best" model based on reconstruction and prediction accuracies, but it does not provide clear criteria for model selection.

6	**Abnormal Event Detection in Videos using Spatiotemporal Auto encoder**	Yong Shean Chong	This method focuses on detecting anomalies in videos, particularly in crowded scenes. It employs a spatiotemporal architecture, consisting of components for spatial feature representation and learning the temporal evolution of these features. Experimental results on Avenue, Subway, and UCSD benchmarks show that the method achieves comparable detection accuracy to state-of the-art methods at a high speed of up to 140 fps.	**1.Limited generalization discussion:** The paper does not thoroughly discuss the generalization of the proposed method to various real world video scenarios outside the specified benchmarks. 2. No comparison to alternative architectures: The paper does not compare the proposed methods for abnormal event detection in videos.
7	**A Review of Human Suspicious Activity from Single Image.**	Naimat Ullah Khan, Wanggen Wan	This review discusses significant contributions in Human Pose Estimation methods from single two-dimensional images. It 1. Limited focus: The review is primarily focused on human pose estimation from single images 9 covers traditional pictorial structures, Deep Neural Networks, and the Stacked Hourglass approach. The paper	**1.Limited focus:** The review is primarily focused on human pose estimation from single images and does not address broader topics related to suspicious activity detection. **2. Lack of critical analysis:** It provides an overview of methods but does not critically evaluate their strengths and weaknesses.

			provides a comprehensive study of influential deep learning methods for human pose estimation, starting from the earliest practical models and progressing to the most recent advancements.	

Mr. Nishchal J, Ms. Sanjana Reddy, Ms. Navya Priya N [1] "Automated Cheating Detection in Exams using Posture and Emotion Analysis" Abstract: Cheating in exams is a widespread issue globally, necessitating automated detection methods. This paper proposes a system utilizing posture detection, face recognition, and emotion analysis to automate cheating detection, eliminating reliance on manual invigilation.

Md Adil1, Rajbala Simon2, Sunil Kumar Khatri3 [2] "Automated Invigilation System for Detection of Suspicious Activities during Examination" Abstract: This paper proposes a video surveillance system to monitor exam environments and detect suspicious behaviours. Using automated video feeds and advanced processing algorithms, the system employs features like face recognition and background subtraction. While effective, challenges include resource demands and potential false positives.

Mohammad Sabokrou, Mahmood Fathy [3] "Real-Time suspicious Detection and Localization in Crowded Scenes" Abstract: In this paper, we propose a method for real-time suspicious detection and localization in crowded scenes. Each video is defined as a set of non-overlapping cubic patches and is described using two local and global descriptors. These descriptors capture the video properties from different aspects. By incorporating simple and cost-effective Gaussian classifiers, we can distinguish normal activities and anomalies in videos. The local and global features are based on structure similarity between adjacent

patches and the features learned in an unsupervised way, using a sparse autoencoder. Experimental results show that our algorithm is comparable to a state-of-the-art procedure on UCSD ped2 and UMN benchmarks, but even more time efficient. The experiments confirm that our system can reliably detect and localize anomalies as soon as they happen in a video.

Mahmudul Hasan Jongh Yun Choi [4] "Learning Temporal Regularity in Video Sequences" Abstract: Perceiving meaningful activities in a long video sequence is a challenging problem due to ambiguous definition of 'meaningfulness' as well as clutters in the scene. We approach this problem by learning a generative model for regular motion patterns (termed as regularity) using multiple sources with very limited supervision. Specifically, we propose two methods that are built upon the autoencoders for their ability to work with little to no supervision. We first leverage the conventional handcrafted spatial-temporal local features and learn a fully connected autoencoder on them. Second, we build a fully convolutional feed-forward autoencoder to learn both the local features and the classifiers as an end-to-end learning framework. Our model can capture the regularities from multiple datasets. We evaluate our methods in both qualitative and quantitative ways - showing the learned regularity of videos in various aspects and demonstrating competitive performance on suspicious detection datasets as an application.

Jefferson Ryan [5] "Suspicious Detection in Video Using Predictive Convolutional Long Short-Term Memory Networks" Description: Automating the detection of anomalous events within long video sequences is challenging due to the ambiguity of how such events are defined. We approach the problem by learning generative models that can identify anomalies in videos using limited supervision. We propose end-to end trainable composite Convolutional Long Short-Term Memory (Conv-LSTM) networks that can predict the evolution of a video sequence from a small number of input frames. Regularity scores are derived from the reconstruction errors of a set of predictions with abnormal video sequences yielding lower regularity scores as they diverge further from the actual sequence over time. The models utilize a composite structure and examine the effects of 'conditioning' in learning more meaningful representations. The best model is chosen based on the reconstruction and prediction accuracies. The Conv-LSTM models are evaluated both qualitatively and

quantitatively, demonstrating competitive results on suspicious detection datasets. Conv-LSTM units are shown to be an effective tool for modelling and predicting video sequences.

Yong Shean Chong [6] "Abnormal Event Detection in Videos using Spatiotemporal Autoencoder" Description: We present an efficient method for detecting anomalies in videos. 10 Recent applications of convolutional neural networks have shown promises of convolutional layers for object detection and recognition, especially in images. However, convolutional neural networks are supervised and require labels as learning signals. We propose a spatiotemporal architecture for suspicious detection in videos including crowded scenes. Our architecture includes two main components, one for spatial feature representation, and one for learning the temporal evolution of the spatial features. Experimental results on Avenue, Subway and UCSD benchmarks confirm that the detection accuracy of our method is comparable to state-of-the-art methods at a considerable speed of up to 140 fps.

2.2 Gap Analysis

The goal of this project is to leverage deep learning techniques for the development of a robust and efficient system dedicated to the detection of suspicious activities from surveillance videos. The primary objectives include training and implementing deep learning models, such as convolutional neural networks, to recognize and classify diverse activities in real-time. The system will incorporate anomaly detection mechanisms to identify deviations from normal behaviour, alerting security personnel promptly. Ultimately the goal is to enhance security measures by automating the identification of suspicious activities, empowering security personnel with a proactive and effective surveillance tool.

2.3 Problem Definition

In exam hall surveillance, the challenge lies in detecting suspicious behaviours through complex scene analysis. The goal is to identify patterns of activities or events, like standoff threat detection and prevention. Leveraging advanced techniques like face recognition, the

objective is to prevent cheating and uphold exam integrity. This application parallels the use of surveillance in healthcare for tracking patient activities.

Chapter 3
SYSTEM REQUIREMENT AND SPECIFICATIONS

3.1 Hardware requirements:

- Processor: Intel core 5
- Ram size: 8GB
- Hard disk capacity: 500GB
- Monitor type: 15 Inch shading screen
- Keyboard type: web console

3.2 Software requirements:

- Operating System: Windows 10
- IDE: SPYDER
- Programming language: Python
- Documentation: MS-Office
- Python Libraries
- DB Browser for SQLite

Chapter 4
SYSTEM ARCHITECTURE

4.1 Proposed System Architecture

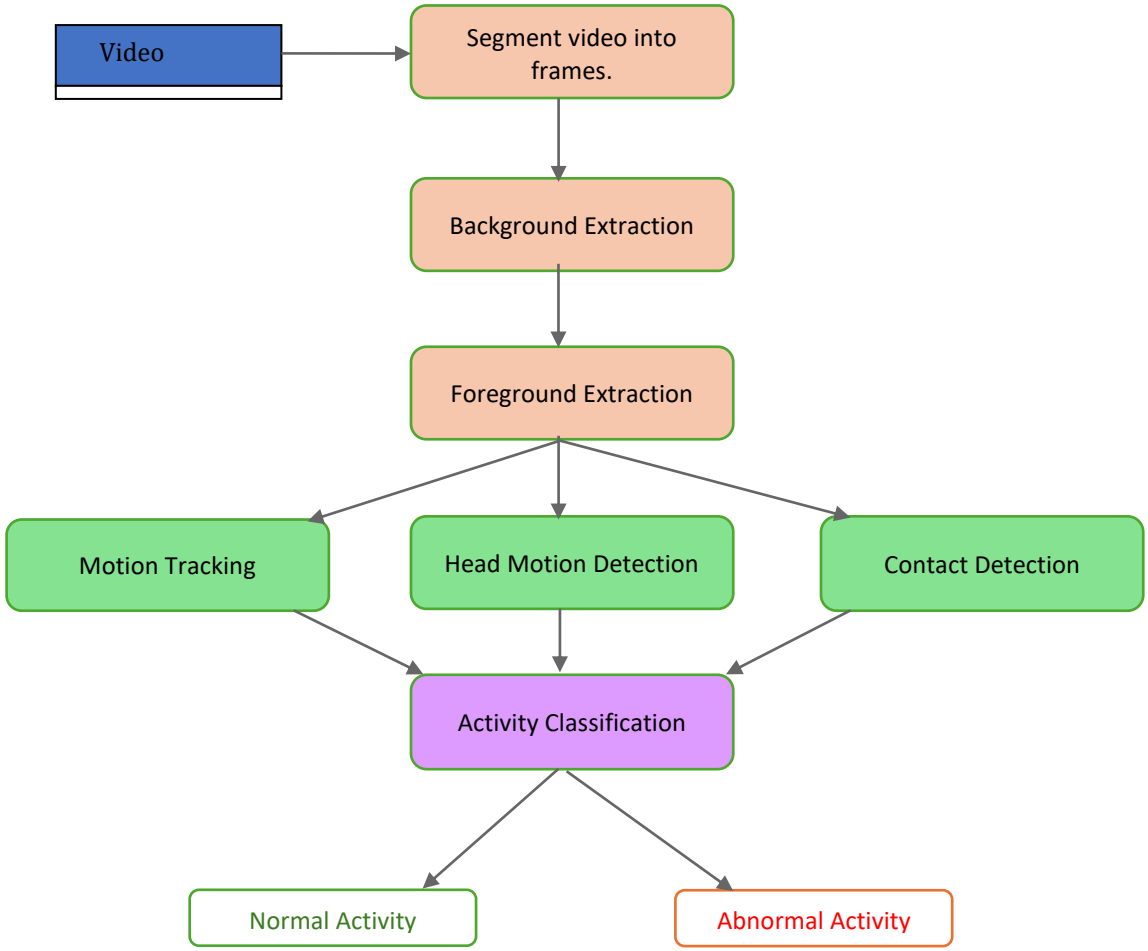

Fig 4.1. Proposed System architecture.

• **Real World Input Video:** This is the initial input to the system. It's a video feed captured from a real-world environment, such as a security camera recording.

• **Segmenting Video into Frames**: The video stream is divided into individual frames. Each frame represents a single still image from the video.

• **Background Extraction**: This block is responsible for extracting the background from each frame. The background represents the static elements in the scene, such as walls, floors, and other stationary objects.

• **Foreground Extraction:** After the background is extracted, what remains are the moving objects (or the foreground) in the scene. This can include people, vehicles, or any other dynamic elements.

• **Motion Tracking:** This block tracks the movement of objects in the foreground over time. It helps identify the paths and trajectories of these objects.

• **Head Motion Detection:** This block specifically focuses on detecting motion related to heads. It could be used to track the movement of people's heads within the scene.

• **Contact Detection:** This block is responsible for detecting interactions or contacts between objects. For instance, it might identify when a person makes physical contact with an object or another person.

• **Activity Classification:** This block takes the outputs from the motion tracking, head motion detection, and contact detection blocks and uses them to classify the overall activity in the scene. This could involve using machine learning algorithms to make decisions based on the detected features.

• **Normal Activity**: If the system classifies the activity as "Normal," it means that the observed behaviour falls within expected or routine patterns. This could include people walking, standing, or performing other regular activities.

• **Abnormal Activity:** If the system classifies the activity as "Abnormal," it means that the observed behaviour deviates from what is considered normal or expected. This could include behaviours like running, fighting, or other potentially dangerous or unusual actions.

4.2 Novelty

The novelty of this project lies in its innovative approach to real-time CCTV surveillance for detecting suspicious human activity. Unlike previous methods that focus on image-based analysis, this project extends its scope to video data, leveraging deep learning techniques like Convolutional Neural Networks (CNNs). By integrating anomaly detection mechanisms and emphasizing real-time processing, the system can efficiently monitor and classify activities as usual or unusual, enhancing public safety and security. Additionally, the project prioritizes

scalability and ethical considerations, ensuring responsible innovation in surveillance technology.

Chapter 5
HIGH LEVEL SYSTEM DESIGN

5.1 Use-Case Diagram:

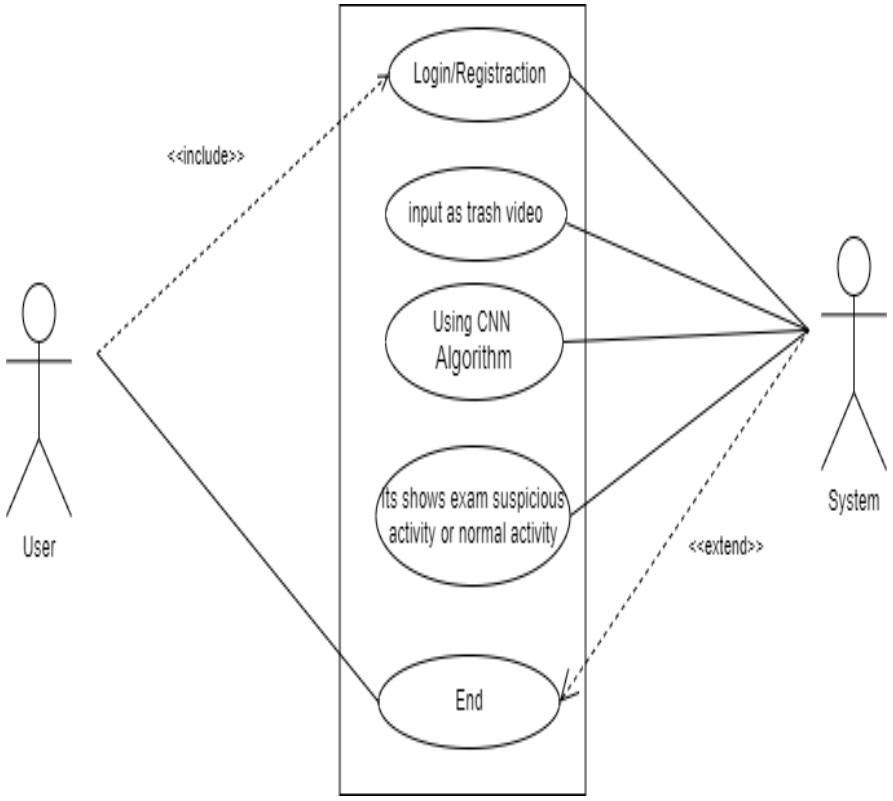

Fig. 5.1 Use-Case Diagram

- User: This is the person who interacts with the system. In the diagram, the user is represented by a stick figure.
- Login/Registration: This block represents the process of logging in to the system or registering for a new account.
- Input as video: This block represents the video input that is fed into the system. The text says, "input as trash video" which could be a typo and Seherunnisa means "should be".

- Using CNN Algorithm: This block represents the convolutional neural network (CNN) algorithm that is used to analyze video. CNNs are a type of artificial intelligence that is well-suited for image and video recognition.
- System: This block represents the overall system that analyses the video and detects suspicious activity.
- Output: The output of the system is a classification of the activity in the video as either suspicious or normal.
- <<include>> and <<extend>>: These arrows seem to indicate that there are other diagrams or parts of the system that are not shown in this diagram.

5.2 DFD (Data Flow Diagram):

- **5.2.1 DFD Level 0**

Fig. 5.2.1 DFD Level 0

- **5.2.2 DFD Level 1**

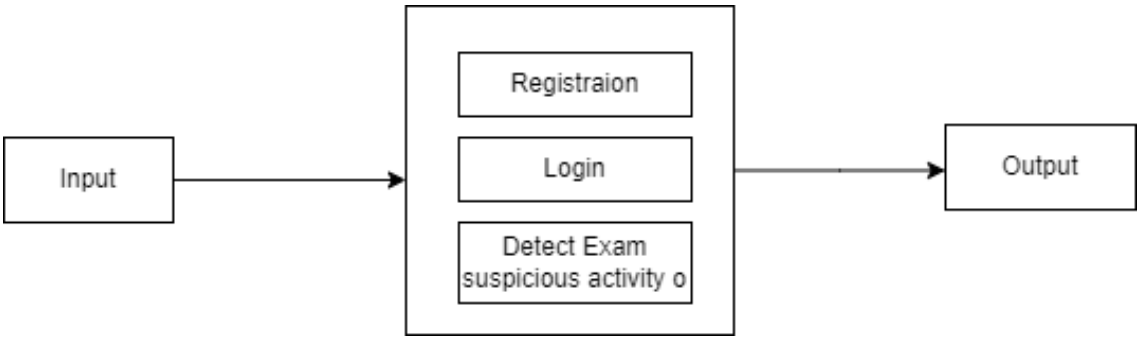

Fig. 5.2.2 DFD Level 1

- **5.2.3 DFD Level 2**

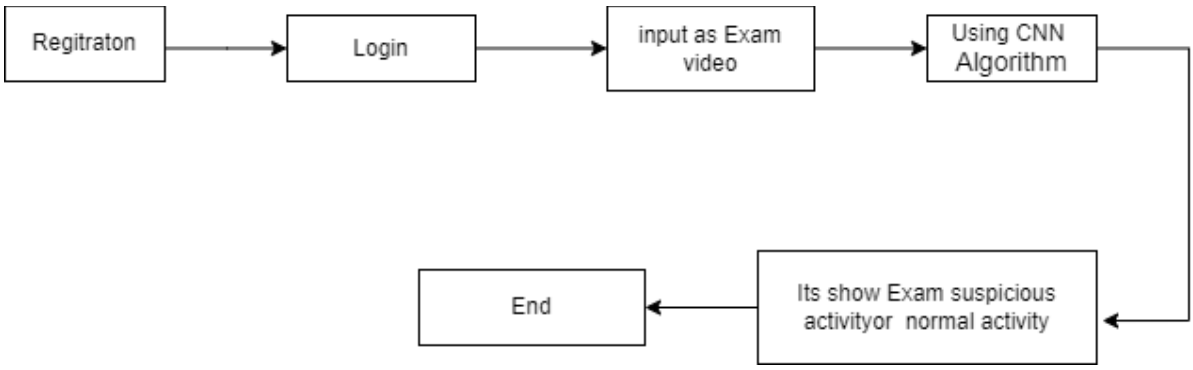

Fig. 5.2.3 DFD Level 2

5.3 Sequence Diagram:

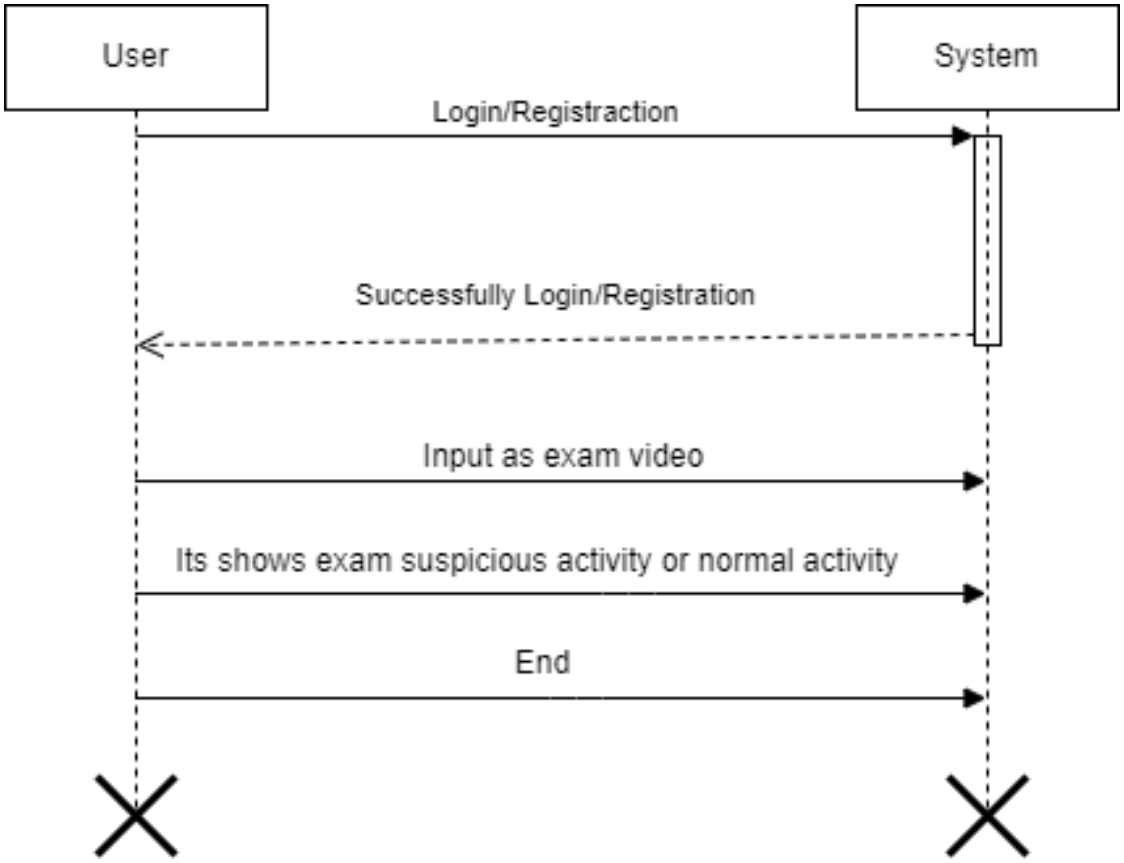

Fig. 5.3 Sequence Diagram

The first step is to log in to the system. The second step is to successfully login/registration. The third step is to input as exam video. The fourth step is to show exam suspicious activity or normal activity.

5.4 Class Diagram:

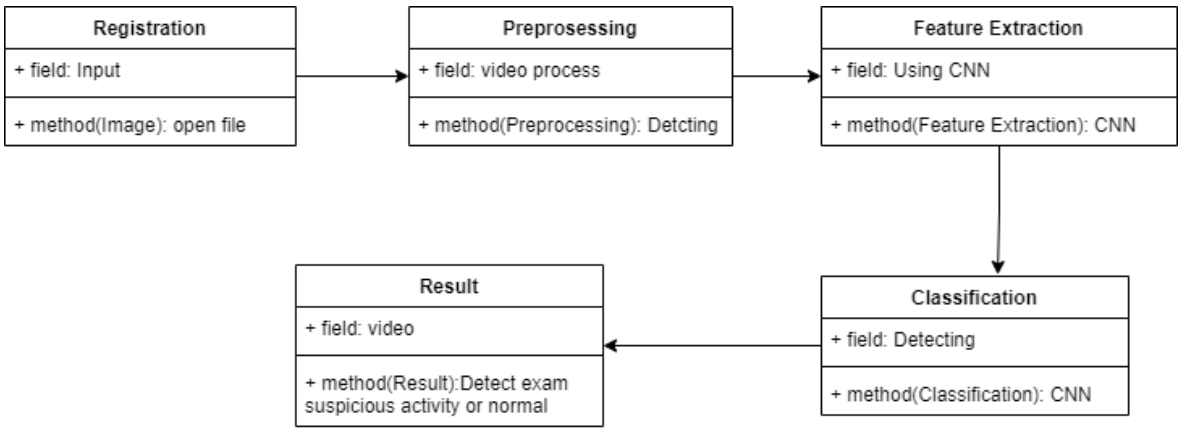

Fig. 5.4 Class Diagram

- **Registration:** In this step, the user registers themselves into the system.
- **Preprocessing**: The video is pre-processed in this stage. This might involve noise reduction or converting the video into a format suitable for analysis by a computer.
- **Feature Extraction**: Key features are extracted from the video frames. These features are used to classify the video in the next stage.
- **Classification:** A Convolutional Neural Network (CNN) classifier is used to classify the video frames as containing normal activity or suspicious activity.

5.5 Activity Diagram:

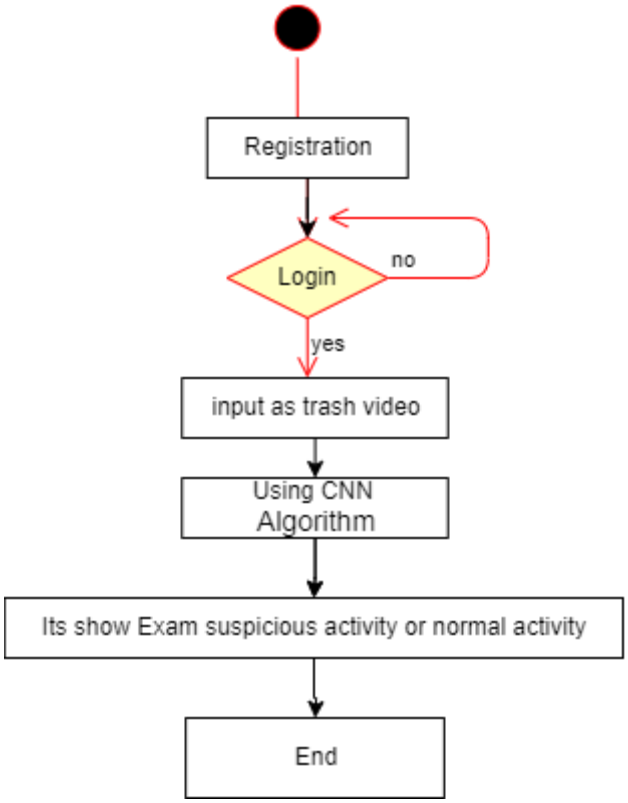

Fig. 5.5 Activity Diagram

- **Register:** The user creates an account in the system.
- **Login:** The user enters their credentials to access the system.
- **Input Exam Video:** The user uploads a video of an exam for analysis.
- **Analyze with CNN:** The program uses a Convolutional Neural Network (CNN) algorithm to process the video.
- **Classify Activity:** CNN determines if the video shows suspicious exam activity or normal exam activity.

Chapter 6
SYSTEM IMPLEMENTATION

6.1 Assumptions

In our research on automated cheating detection in exams using posture and emotion analysis, we make several key assumptions. Firstly, we assume that the technologies employed, such as posture and emotion analysis algorithms, are reliable and accurately identify suspicious behaviours in real-time surveillance video. Additionally, we assume seamless integration with existing surveillance systems in educational institutions, enabling the system to monitor exam halls in real-time and provide immediate alerts upon detecting suspicious activities. Our system is assumed to have a high accuracy rate in detecting various forms of cheating, contributing significantly to enhancing exam security and integrity while reducing manual intervention. Ethical considerations are paramount, and we assume that our system complies with ethical guidelines, respects privacy concerns, and maintains transparency in its operation. Looking forward, we anticipate continuous advancements and updates in AI and surveillance technologies, leading to enhanced capabilities and reliability of our automated cheating detection system over time.

6.2 Algorithm

Step 1: Initialization

1.1 Initialize the exam suspicious activity detection system.

1.2 Load necessary libraries and dependencies.

Step 2: User Authentication

2.1 Prompt the user to authenticate.

2.2 Verify user credentials.

Step 3: Input Acquisition

3.1 Capture video feed from surveillance cameras positioned in exam rooms.

3.2 Ensure proper functioning of cameras and adequate lighting conditions.

Step 4: Person Detection

4.1 Apply person detection algorithms to identify individuals in the video frames.

4.2 Utilize techniques such as Haar cascades or deep learning-based models for accurate detection.

Step 5: Abnormal Head Position Detection

5.1 Analyze the head positions of detected individuals.

5.2 Compare head orientations with predefined normal positions.

5.3 Flag instances where head positions deviate significantly from the norm.

Step 6: Suspicious Activity Classification

6.1 Classify flagged instances as potential suspicious activities.

6.2 Look for patterns such as one person passing materials to another or frequent head movements indicative of cheating behavior.

Step 7: Alert Generation

7.1 Generate alerts for exam proctors or administrators.

7.2 Provide real-time notifications via email or a centralized monitoring dashboard.

Step 8: End of Monitoring

8.1 Terminate monitoring once the exam session concludes.

End Algorithm

6.3 Flowchart

- **Data Collection**: Gather a diverse dataset of exam hall videos showcasing both normal and suspicious activities.
- **Data Annotation:** Human experts label each video frame or segment as "normal" or "Abnormal" based on observed behavior.
- **Data Preprocessing**: Prepare the dataset by resizing frames, normalizing pixel values, and augmenting data (creating variations) to improve model robustness.
- **Splitting the Dataset:** Divide the dataset into training and validation sets. The training set is used to train the model, and the validation set is used to fine-tune the model hyperparameters.
- **CNN Architecture Design**: Design a Convolutional Neural Network (CNN) architecture specifically optimized for detecting suspicious activities in exam hall videos.
- **Model Training:** Train the CNN model using the labeled training data and optimization algorithms like stochastic gradient descent (SGD).
- **Iterative Refinement:** Make necessary adjustments to the model based on validation set performance. This may involve collecting more data, fine-tuning the architecture, or trying different hyperparameters.
- **Deployment:** Deploy the trained model to a production environment for real-time detection of suspicious activities in exam hall videos.

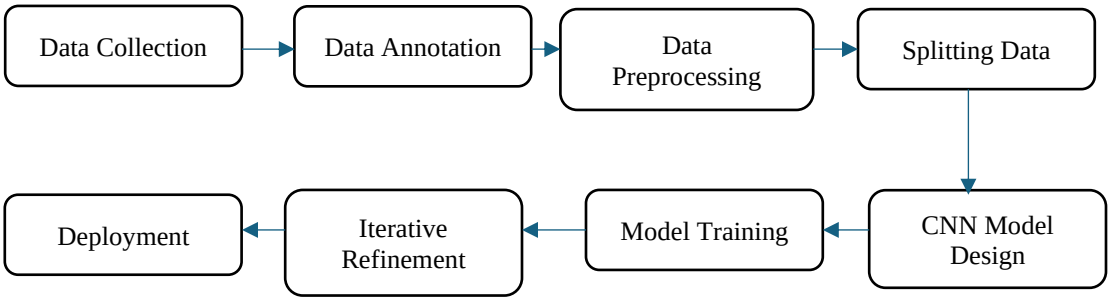

Fig. 6.3 Flowchart.

6.4 Methodologies

The methodology for detecting suspicious activity in examination halls involves several key steps to ensure accurate and reliable detection. Initially, a diverse dataset of examination hall surveillance videos is collected, encompassing both typical exam behaviours and potential suspicious activities. Human experts then annotate this dataset by labelling each video frame or segment as either "normal" or "Abnormal" based on observed behaviours. This annotated dataset is crucial for training and evaluating the detection model effectively. Next, the dataset undergoes preprocessing, including tasks such as resizing frames, normalizing pixel values, and augmenting data to enhance variability, ensuring the model receives clean and standardized input data. Subsequently, the dataset is split into training, validation, and test sets to facilitate model training, hyperparameter tuning, and final evaluation.

The heart of the methodology lies in designing a convolutional neural network (CNN) architecture tailored to detecting suspicious activities in exam hall videos. Factors such as network depth, layer sizes, and filter types are carefully considered to optimize the model's performance. Once the architecture is finalized, the model is trained using the labelled training data, with optimization algorithms like stochastic gradient descent (SGD) or Adam used to update model weights and minimize errors. Hyperparameter tuning follows, where parameters like learning rate and batch size are adjusted based on performance on the validation set.

Any necessary refinements to the model are made iteratively based on its performance, which may involve collecting additional data, fine-tuning the architecture, or adjusting hyperparameters. Finally, the trained model is deployed to a production environment where it can analyse real-time exam hall videos for suspicious activities. Continuous monitoring and updating of the model ensure its ongoing effectiveness as new data becomes available or new suspicious behaviours emerge.

Chapter 7
GUI / EXPERIMENTAL RESULTS

7.1 GUI / Working Modules

1) Home Page

Fig. 7.1.1 Home Page

2) Sign Up Page

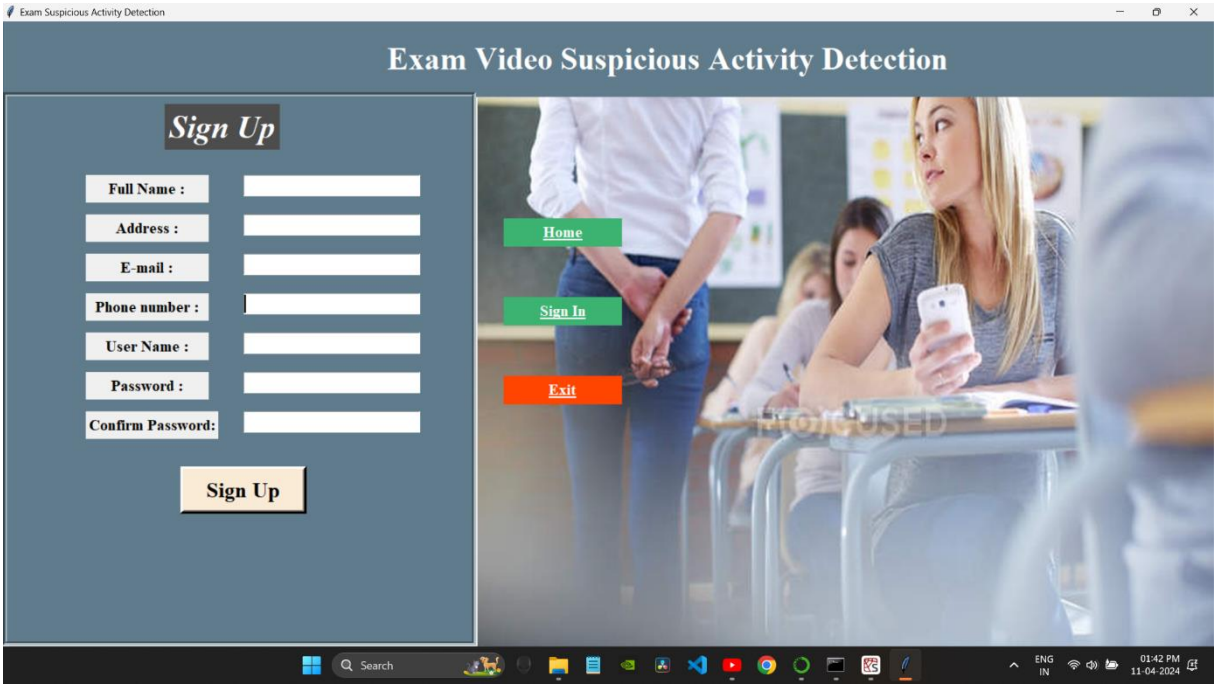

Fig. 7.1.2 Signup Page

3) Sign In Page

Fig. 7.1.3 Sign in Page

4) Main Master Page

Fig. 7.1.4 Main Master Page

5) Upload Video Popup

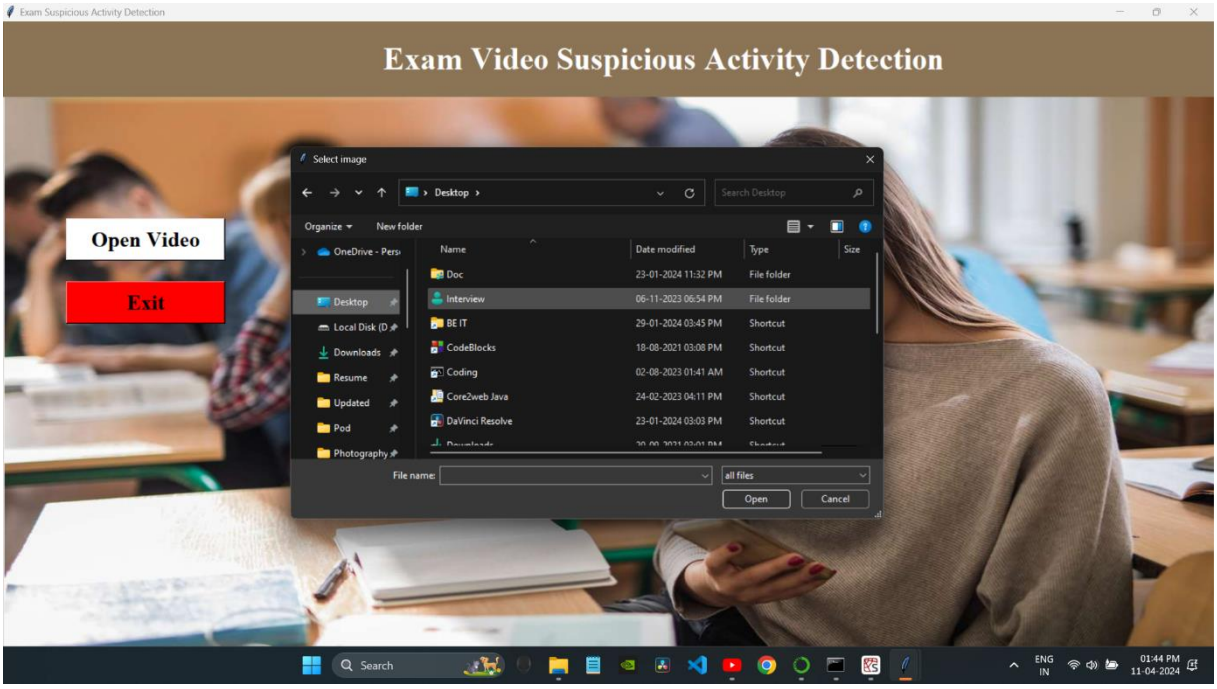

Fig. 7.1.5 Upload Video Popup

6) Normal Activity 1

Fig. 7.1.6 Normal Activity 1

7) Normal Activity 2

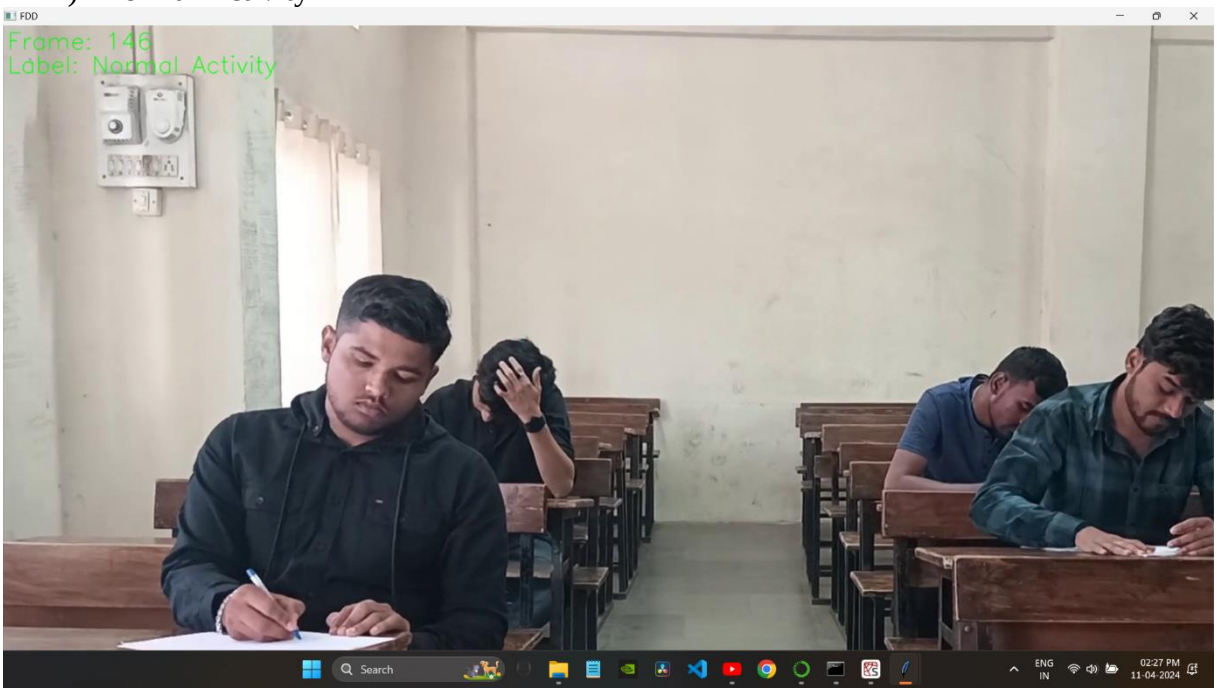

Fig. 7.1.7 Normal Activity 2

8) Abnormal Activity 1 (Head Motion)

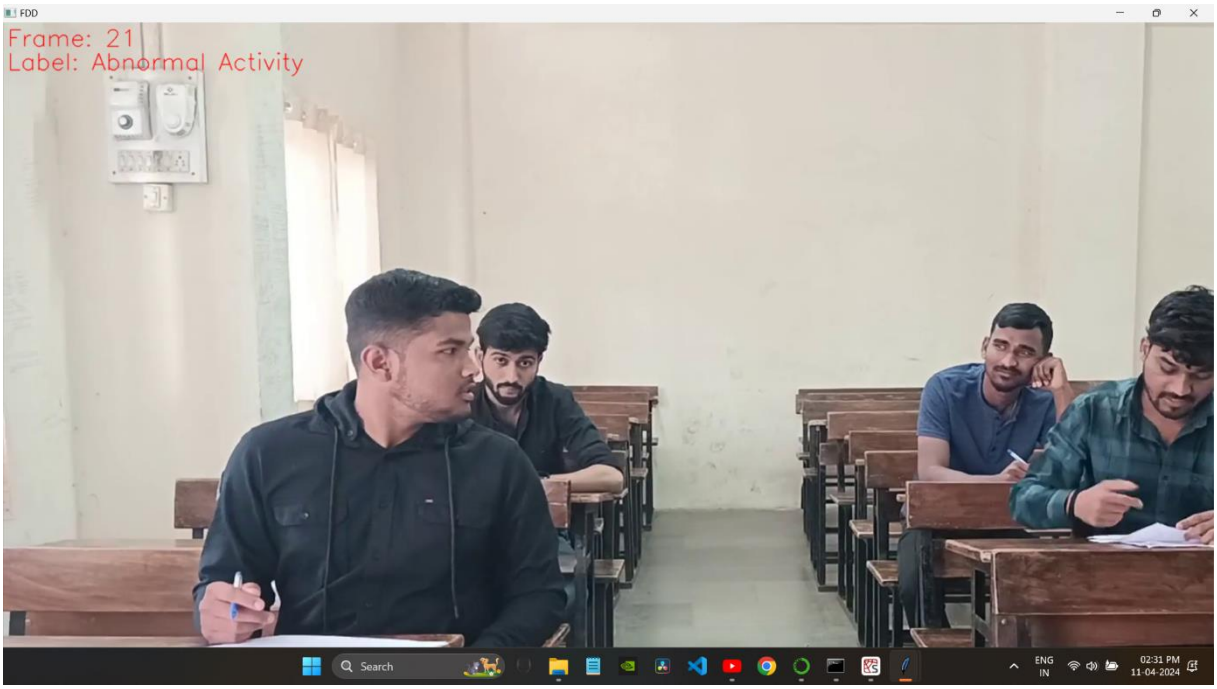

Fig. 7.1.8 Abnormal Activity 1

The system has detected a person in the video frame but flagged their head position as abnormal, indicating potential suspicious activity. This could imply behaviours like cheating during exams, where individuals may look elsewhere for answers.

9) Abnormal Activity 2(Contact Detection)

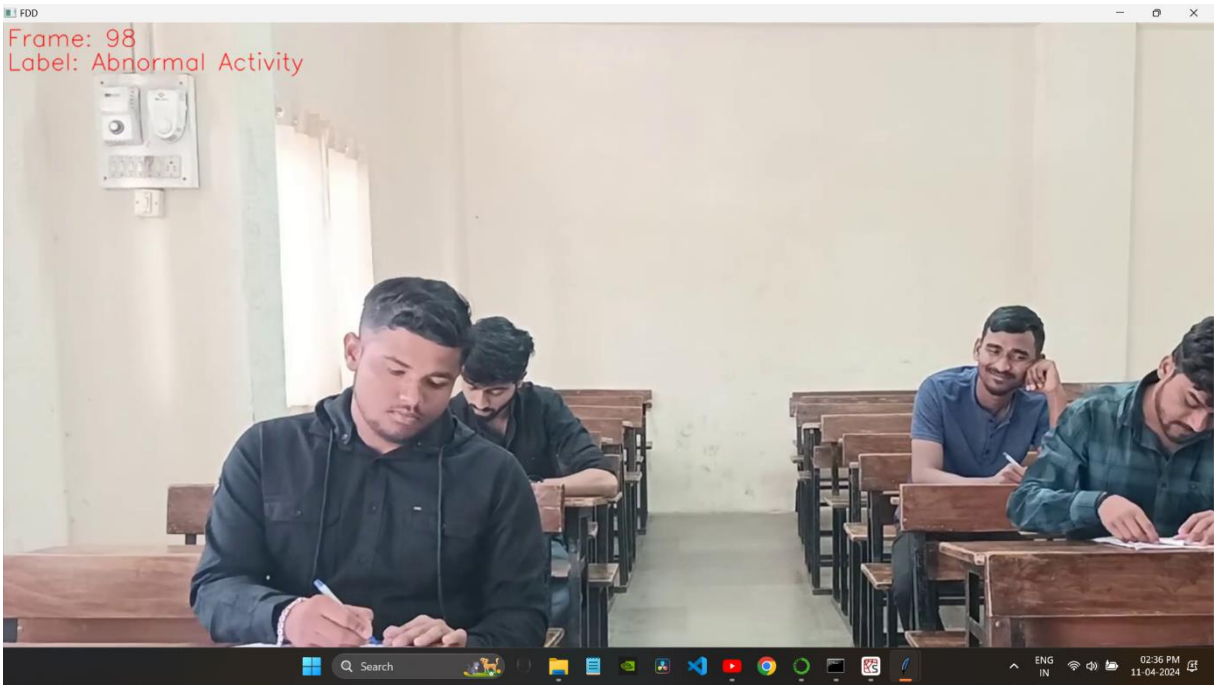

Fig. 7.1.9 Abnormal Activity 2

"One person is detected as seeing in paper of front person" suggests the system identified a situation where one student is looking at the exam paper of the student sitting in front of them. This could be a potential cheating attempt.

10) Abnormal Activity 3(Motion Tracking)

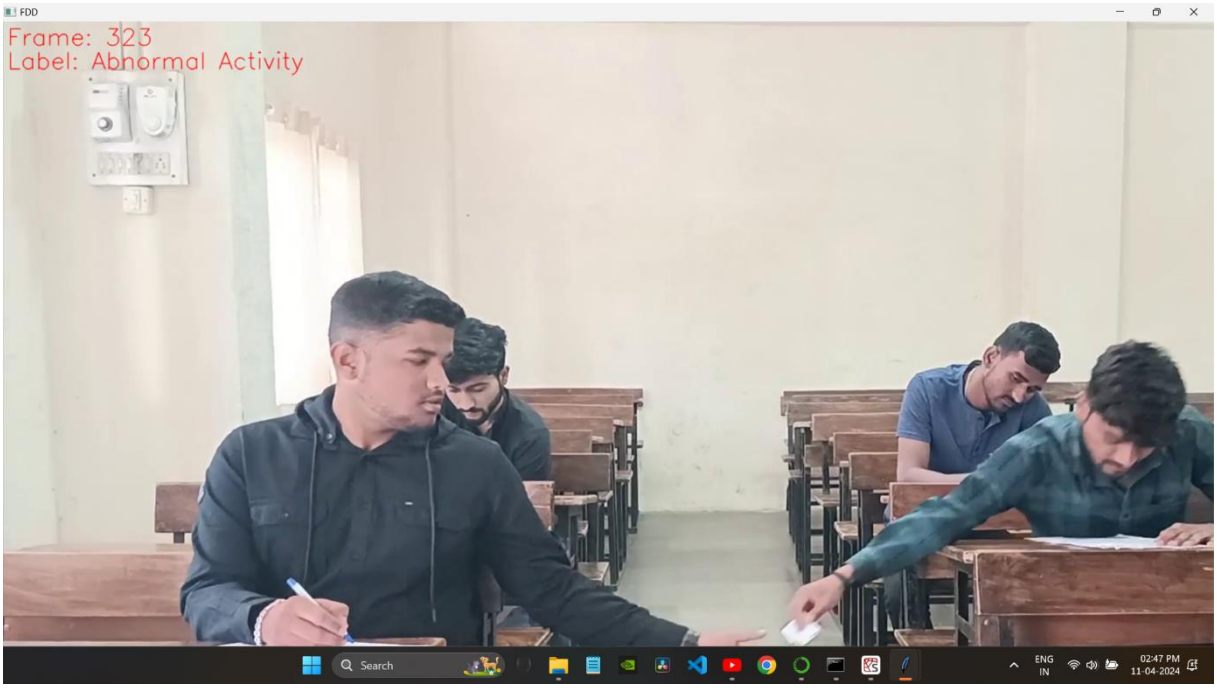

Fig. 7.1.10 Abnormal Activity 3

The system has identified suspicious movement, specifically the transfer of cheat material from one person to another. This suggests that one student is passing cheat material to another during an exam.

7.2 Results

The system is tailored to scrutinize exam videos and highlight suspicious activity, particularly focusing on identifying individuals, likely students, and evaluating their actions. In typical scenarios, the system anticipates students to maintain a steady posture with limited head motion. However, it's programmed to detect irregularities such as unconventional head positions, indicating potential cheating behaviour like seeking answers elsewhere, or suspicious movements associated with passing cheat materials between students. These deviations from the anticipated conduct prompt alerts for "Abnormal Activity".

7.3 Discussion

Exam cheating detection systems, like the one we discussed, use video analysis to flag suspicious activity. While these systems can deter cheating, improve efficiency, and offer data for improvement, concerns exist around student privacy, false positives, and accessibility. For ethical implementation, transparency, fairness, and a focus on learning are crucial. As AI and remote proctoring evolve, the future of exam monitoring might prioritize preventing cheating altogether.

Chapter 8
TESTING

8.1 Test Plan

8.1.1 Introduction

This test plan outlines the approach for evaluating the Exam Suspicious Activity Detection System. The objective is to ensure the system effectively identifies and flags suspicious behaviors during exams.

8.1.2 Test Objectives

- Validate the accuracy of the system in detecting suspicious activities.
- Assess the system's ability to differentiate between normal and suspicious behaviors.
- Evaluate the system's robustness under various lighting and environmental conditions commonly found in exam halls.

8.1.3 Test Environment

Hardware: Computer with a webcam or surveillance camera installed in the exam hall.
Software: Exam Suspicious Activity Detection System application.
Operating System: Compatible with the system requirements.

8.1.4 Test Cases

8.1.4.1. Video Analysis:

- Test Case 1: Verify that the system accurately analyzes exam hall surveillance videos in real-time.
- Test Case 2: Evaluate the system’s ability to detect and classify suspicious activities (e.g., cheating, unauthorized communication).

8.1.4.2 Anomaly Detection:

- Test Case 3: Validate the accuracy of anomaly detection algorithms in identifying unusual behaviors.
- Test Case 4: Assess the system's responsiveness to unexpected actions or movements within the exam hall.

8.1.4.3 Alert Generation:

- Test Case 5: Verify the timely generation of alerts for detected suspicious activities.
- Test Case 6: Test the effectiveness of alert notifications in notifying exam invigilators or authorities.

8.1.5. Test Execution

Perform test cases sequentially, using standardized test procedures and ensuring consistency in testing methodology. Record observations and results for each test case, documenting any deviations from expected behavior or unexpected issues encountered during testing.

8.1.6. Test Reporting

Compile test results, including observations, pass/fail status, and any identified issues. Provide detailed descriptions of issues encountered, including steps to reproduce and potential impact on system functionality. Share test reports with relevant stakeholders for review and resolution of identified issues.

8.1.7. Test Sign-off.

- Obtain approval from project stakeholders based on test results and feedback.
- Confirm readiness for system deployment and production use.

- This test plan outlines the approach for testing the exam suspicious activity detection system, covering various aspects such as video analysis, anomaly detection, alert generation, and overall system performance.

8.2 Test Cases

8.2.1. Activity Head Detection:

Test Case 1: Verify that the system accurately detects and tracks human heads in real-time within the examination hall footage.

Test Case 2: Assess the system's ability to differentiate between normal head movements (e.g., turning, nodding) and suspicious behavior (e.g., looking at neighboring students' papers).

Test Case 3: Evaluate the performance of head detection algorithms under various lighting conditions and camera angles.

8.2.2. Motion Tracking:

Test Case 4: Validate the accuracy of motion tracking algorithms in identifying and tracking movements of individuals within the exam hall.

Test Case 5: Assess the system's responsiveness to sudden or erratic movements, which may indicate suspicious behavior (e.g., attempting to communicate with other students).

Test Case 6: Test the system's ability to differentiate between deliberate movements (e.g., stretching) and potentially suspicious actions.

8.2.3. Contact Detection:

Test Case 7: Verify that the system accurately identifies interactions or contacts between individuals within the exam hall.

Test Case 8: Evaluate the system's ability to distinguish between innocuous interactions (e.g., passing papers) and suspicious contacts (e.g., exchanging answers).

Test Case 9: Assess the performance of contact detection algorithms in detecting subtle physical gestures that may indicate cheating.

8.2.4. Alert Generation:

Test Case 10: Validate the alert generation mechanism's functionality in issuing timely notifications upon detecting suspicious activity.

Test Case 11: Assess the system's ability to prioritize and escalate alerts based on the severity of detected anomalies.

Test Case 12: Test the reliability and robustness of the alert generation system under varying conditions, such as crowded exam halls or noisy environments.

8.2.5. Performance Testing:

Test Case 13: Evaluate system performance under different load conditions, including processing multiple exam hall video feeds simultaneously.

Test Case 14: Assess system responsiveness and latency in detecting and responding to suspicious activities in real-time.

Test Case 15: Verify system stability and reliability over extended periods of operation, including continuous monitoring during exam sessions.

8.2.6. Usability Testing:

Test Case 16: Conduct usability testing with exam invigilators to evaluate the system's user interface and workflow.

Test Case 17: Collect feedback from users on the system's ease of use, clarity of alerts, and overall user experience.

Test Case 18: Assess user satisfaction and confidence in the system's ability to detect and prevent cheating during exams.

8.2.7. Accessibility Testing:

Test Case 19: Verify that the system complies with accessibility standards and guidelines, ensuring equal access for all users.

Test Case 20: Evaluate the system's compatibility with assistive technologies, such as screen readers or alternative input devices.
Test Case 21: Test the system's responsiveness to alternative communication methods for individuals with disabilities, such as text-to-speech or sign language interpretation.

Executing these test cases comprehensively will help ensure the exam suspicious activity detection system meets its functional requirements and provides effective monitoring and prevention of cheating behaviors during exams.

8.3 Test Results

8.3.1. Suspicious Activity Detection Functionality:

Result: The suspicious activity detection functionality of the system performed satisfactorily during testing.
Observations: The system successfully analyzed exam hall surveillance videos in real-time, accurately detecting and classifying suspicious activities such as cheating or unauthorized communication. However, there were some instances of false positives and false negatives, indicating room for improvement in fine-tuning the detection algorithms.

Conclusion: While the system's performance was generally satisfactory, further refinement of the detection algorithms is necessary to minimize false detections and enhance overall accuracy

8.3.2. Anomaly Detection:

Result: The anomaly detection algorithms exhibited moderate performance in identifying unusual behaviors.
Observations: The system detected certain unexpected actions or movements within the exam hall, such as sudden movements or interactions between students, but there were instances where subtle anomalies went unnoticed. Improvements in the sensitivity and

specificity of the anomaly detection algorithms could enhance the system's effectiveness in identifying suspicious behaviors.

Conclusion: While the anomaly detection functionality showed potential, further optimization is required to improve its reliability and effectiveness in identifying suspicious activities with higher accuracy.

8.3.3. Alert Generation:

Result: The alert generation mechanism functioned adequately, issuing timely notifications for detected suspicious activities.

Observations: The system promptly generated alerts for detected suspicious activities, notifying exam invigilators or authorities as intended. However, there were occasional delays in alert notifications, highlighting the need for optimizations to ensure real-time responsiveness.

Conclusion: Overall, the alert generation mechanism effectively served its purpose but could benefit from optimizations to enhance real-time responsiveness and reliability.

In summary, the exam suspicious activity detection system demonstrated satisfactory performance in detecting and classifying suspicious activities, although there is room for improvement in terms of minimizing false detections, enhancing anomaly detection capabilities, and optimizing alert generation mechanisms. Further refinement and optimization of the system's algorithms and functionalities are warranted to improve its overall effectiveness in ensuring exam integrity and security.

Chapter 9
PROJECT PLAN

TIMELINE	TASK DESCRIPTION	STATUS
Week 1	Decide the area of interest	Found the area of Interest
Week 2	Define the project scope	Defined the scope
Week 3	Conduct literature review on deep learning for activity detection	Reviewed relevant literature
Week 4	Sanction topic from the project guide	Topic Sanctioned
Week 5	Search Related Information	Gathered related information
Week 6	Understanding the Core Concept for the Project	Understood the concept for the project
Week 7	Search essential documents	Found essential documents
Week 8	Problem Definition	Defined the problem definition
Week 9	Literature Survey search	Completed the literature survey
Week 10	Software requirement specification	Defined the Software requirement
Week 11	Modelling and Design	Designed the Model
Week 12	Final PPT making	Completed the PPT
Week 13	Discussion about prototype	Designed frontend
Week 14	Published research paper	Accepted paper successfully
Week 15	Deciding interaction flow	Designed interaction flow
Week 16	Develop initial prototype for activity detection	Developed initial prototype
Week 17	Implement data preprocessing pipeline	Implemented data preprocessing
Week 18	Implemented training of deep learning model	Successfully trained model
Week 19	Implement activity detection module	Successfully implemented
Week 20	Evaluate system performance	Evaluated and optimized performance
Week 21	Evaluate system performance	Enhanced the system’s performance
Week 22	Prepare the final project and presentation	Finalized the documentation
Week 21	Handover project documents and assets	Submitting the project

Chapter 10
CONCLUSIONS

10.1 Conclusion

The proposed subsystem for automatic cheating detection in exam halls, utilizing real-time video footage analysis, holds promise for addressing the issue of exam cheating. By leveraging advancements in suspicious activity detection, it offers a comprehensive approach to monitoring student behaviour during offline assessments. With capabilities to identify various forms of cheating, it minimizes the need for human intervention and optimizes administrative resources. Continued research in related fields can further enhance its effectiveness and productivity, making it a valuable tool in maintaining academic integrity.

10.2 Future Scope

1. **Advanced Video Angles Analysis:** Incorporate advanced video angle analysis techniques to enhance the system's capability to detect suspicious activities from multiple perspectives. This could involve analyzing video feeds from different camera angles to provide a comprehensive view of the exam environment and detect anomalies more effectively.

2. **Integration with Biometric Data:** Explore the integration of biometric data, such as facial recognition and fingerprint analysis, to further authenticate student identities and detect any unauthorized individuals attempting to take exams.

3. **Real-time Intervention:** Develop algorithms for real-time intervention capabilities, where the system can automatically flag suspicious activities and prompt invigilators or administrators to take immediate action, such as pausing exams or notifying authorities.

4. **Advanced AI Algorithms:** Explore the integration of more advanced AI algorithms, such as deep learning models with enhanced capabilities in detecting subtle cheating behaviors and improving overall accuracy.

5. **Multimodal Analysis:** Incorporate multimodal analysis, combining posture and emotion analysis with other data sources like audio or text analytics, to achieve a more comprehensive cheating detection system.

10.3 Limitations of Project

1. **Technological Limitations:** Dependence on factors like camera quality, network connectivity, and computational resources may impact the system's reliability, effectiveness, and scalability across different exam settings.

2. **Scalability Constraints:** The system's scalability may be limited by factors such as the volume of data processed, the complexity of deep learning algorithms, and the need for additional hardware resources as the system expands to accommodate larger examination environments.

3. **Resource Intensiveness:** As the system scales to larger examination settings or higher volumes of data, it may require significant computational resources, including processing power and memory, which could pose challenges in terms of cost and infrastructure availability.

REFERENCES

[1] Md Adil1, Rajbala Simon2, Sunil Kumar Khatri3 "Automated Invigilation System for Detection of Suspicious Activities during Examination"- 978-1-5386-9346-9/19/$31.00 ©2021 IEEE.

[2]. Mr. Nishchal J, Ms.Sanjana Reddy, Ms. Navya Priya N "Automated Cheating Detection in Exams using Posture and Emotion Analysis"-978-1-7281-6828-9/20/$31.00 ©2020 IEEE

[3] Amrutha C.V, C. Jyotsna, Amudha J, "Deep Learning Approach for Suspicious Activity Detection from Surveillance Video", IEEE,2020.

[4] U.M.Kamthe,C.G.Patil "Suspicious Activity Recognition in Video Surveillance System", (ICCUBEA), 2018.

[5] Tian Wanga, Meina Qia, Yingjun Deng, Yi Zhouc, Huan Wangd, Qi Lyua, Hichem Snoussie, "Abnormal event detection based on analysis of movement information of video sequence", 2022.

[6] P.Bhagya Divya, S.Shalini, R.Deepa, Baddeli Sravya Reddy,"Inspection of suspicious human activity in the crowdsourced areas captured in surveillance cameras",International Research Journal of Engineering and Technology (IRJET), December 2017.

[7] Jitendra Musale,Akshata Gavhane, Liyakat Shaikh, Pournima Hagwane, Snehalata Tadge, "Suspicious Movement Detection and Tracking of Human Behavior and Object with Fire Detection using A Closed Circuit TV (CCTV) cameras ", International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume 5 Issue XII December 2017.

[8] U.M.Kamthe,C.G.Patil "Suspicious Activity Recognition in Video Surveillance System", Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018.

[9] Zahraa Kain, Abir Youness, Ismail El Sayad, Samih Abdul-Nabi, Hussein Kassem, "Detecting Abnormal Events in University Areas", International conference on Computer and Application,2018.

[10] Tian Wanga, Meina Qia, Yingjun Deng, Yi Zhouc, Huan Wangd, Qi Lyua, Hichem Snoussie, "Abnormal event detection based on analysis of movement information of video sequence", Article Optik, vol 15 2, January-2018.

[11] Eralda Nishani, Betim Cico: "Computer Vision Approaches based on Deep Learning and Neural Networks" Deep Neural Networks for Video Analysis of Human Pose Estimation- 2017 6th MEDITERRANEAN CONFERENCE ON EMBEDDED COMPUTING (MECO), 11-15 JUNE 2017, BAR, MONTENEGRO.

[12] Naimat Ullah Khan, Wanggen Wan: "A Review of Human Pose Estimation from Single Image"- 978 1-5386-5195-7/18/ 2018 IEEE.

[13] Qiuhui Chen, Chongyang Zhang, Weiwei Liu, and Dan Wang," Surveillance Human Pose Dataset and Performance Evaluation for Coarse-Grained Pose Estimation", Athens 2018. 23.

[14] Tripathi, Rajesh and Jalal, Anand and Agarwal, Subhash (2017)." Suspicious Human Activity Recognition: a Review". Artificial Intelligence Review. 50.10.1007/s10462- 017-9545-7.

[15] Hanguen Kim, Sangwon Lee, Dongsung Lee, Soonmin Choi, JinsunJu and Huyun Myung "Real-Time Human Pose Estimation and Gesture Recognition from depth Images Using Superpixels and SVM classifier."- Sensors 2015, 15, 12410-12427; doi:10.3390/s150612410.

ANNEXTURE

A. Paper Published

Gmail

Vedant Saikhede <vedantsaikhede@gmail.com>

Publication & E- Certificates Reg

2 messages

IRJET Journal <editor@irjet.net> Sat, Dec 30, 2023 at 10:35 PM
Reply-To: editor@irjet.net
To: kirans272002 <kirans272002@gmail.com>, vedantsaikhede <vedantsaikhede@gmail.com>, yuvrajdarekar415 <yuvrajdarekar415@gmail.com>, hemantthorat331 <hemantthorat331@gmail.com>, Snehaljadhav1993 <Snehal.jadhav1993@gmail.com>

Dear author,

Congratulations, we would like to inform you that your manuscript has been published in International Research Journal of Engineering and Technology (IRJET) Volume 10, Issue 12, December 2023 https://www.irjet.net/volume10-issue12
S.No:126

126	Deep Learning Approach for Suspicious Activity Detection from Surveillance Video -Vedant Saikhede, Kiran Shende, Yuvraj Darekar, Hemant Thorat, Snehal. S. Shinde	

Please find the e-certificate attachments.

Thank you for your interest in our journal. Hope to get more papers from you and your friends.

With best regards

Editor-in-chief

International Research Journal of Engineering and Technology (IRJET)

www.irjet.net

Follow us on :

https://www.facebook.com/irjet.net

https://www.irjet.net/volume10-issue012

International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 12 | Dec 2023 www.irjet.net p-ISSN: 2395-0072

DEEP LEARNING APPROACH FOR SUSPICIOUS ACTIVITY DETECTION FROM SURVEILLANCE VIDEO

Vedant Saikhede[1], Kiran Shende[2], Yuvraj Darekar[3] , Hemant Thorat[4]
Prof. Snehal. S. Shinde[5]

[1,2,3,4]*Student, Department of Information Technology, Smt. Kashibai Navale College Engineering, Pune 411041*
[5] *Assistant Professor, Dept. of Information Technology, Smt. Kashibai Navale College Engineering, Pune 411041*

Abstract - *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 that can benefit from Activity detection. For example, human pose estimation is used in applications including video surveillance, animal tracking, behavior understanding, sign language detection, advanced human-computer interaction, and marker less motion cap turning. Low-cost depth sensors have limitations 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 visual surveillance, human activities can be monitored in sensitive and public areas such as bus stations, railway stations, airports, banks, shopping malls, schools 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 intelligent video surveillance is required that can monitor human activities in real time and categorize them as usual and unusual activities and can generate an alert. Mostly, 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.*

Key Words: *Suspicious Activity, Neural networks, Image processing, surveillance video.*

1. INTRODUCTION

In today's digital age, ensuring public safety has emerged as a paramount concern, with intelligent video surveillance systems playing a pivotal role. Detecting and predicting suspicious human activity from real-time CCTV footage has become a focal point of research in the domain of computer vision and artificial intelligence. This research paper delves into the multifaceted realm of neural network-based technology and its application in addressing the critical issue of suspicious human activity detection, focusing primarily on video surveillance.

Overcoming the Limitations of Depth Sensors: While low-cost depth sensors have paved the way for advanced human pose estimation, their limitations are apparent, particularly in terms of being confined to indoor usage and offering low-resolution and noisy depth information. This paper presents a novel approach that leverages neural networks to surmount these constraints, resulting in more accurate and robust human pose estimation. Real-World Applications: The research primarily addresses the domain of suspicious human activity recognition in video surveillance, an actively evolving field within image processing and computer vision. Through the lens of visual surveillance, human behavior in sensitive and public areas, including transportation hubs, commercial establishments, and educational institutions, is closely monitored. This proactive approach serves as a deterrent to a wide spectrum of potential threats, ranging from terrorism and theft to accidents and illegal activities. The Need for Intelligent Video Surveillance: Continuous, manual surveillance of public spaces is a formidable challenge. This research advocates for the integration of intelligent video surveillance systems equipped with neural networks, capable of real-time monitoring and categorization of human activities as either usual or unusual. Furthermore, these systems are poised to generate alerts, ensuring a swift response to suspicious behavior Addressing the Gap in Research: It's noteworthy that while extensive research has focused on image-based activity detection, the application of Convolutional Neural Networks.

2. PROBLEM STATEMENT

Recognition of the criminal and preventing suspicious activities during Examination using CCTV footage.

3. MOTIVATION

The motivation behind developing a Suspicious Activity Detection System (SADS) utilizing Convolutional Neural Networks (CNNs) as input for video analysis is rooted in the urgent need for advanced security measures in today's

International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 12 | Dec 2023 www.irjet.net p-ISSN: 2395-0072

complex and rapidly evolving world. Traditional security systems often struggle to keep pace with emerging threats, making it essential to harness the capabilities of AI and deep learning technologies. SADS aims to provide a proactive and intelligent solution that goes beyond conventional surveillance methods. By employing CNNs, which excel at recognizing patterns and anomalies in visual data, this system can automatically identify suspicious activities that might otherwise go unnoticed. The motivation behind SADS is to enhance public safety, protect critical infrastructure, and improve overall security by enabling rapid response to potential threats. Whether in crowded public spaces or high-security facilities, this innovative system offers the promise of a more secure and vigilant environment, ultimately contributing to the well-being and peace of mind of individuals and organizations alike. In an era were security.

4. SYSTEM ARCHITECTURE

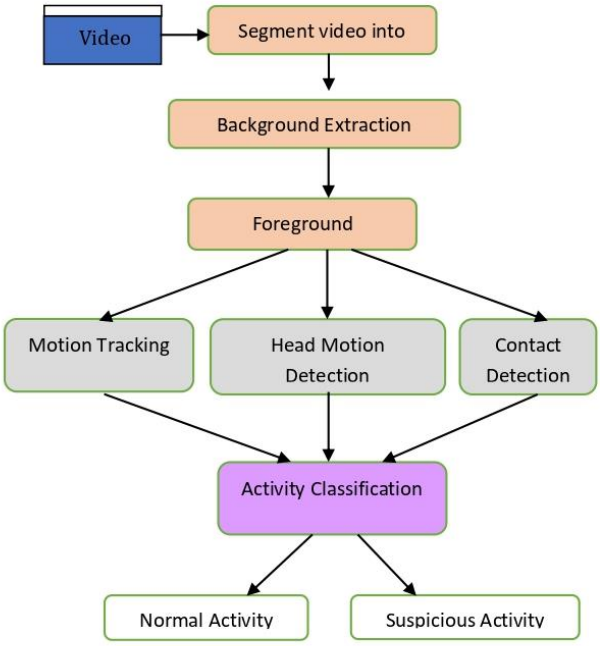

Fig 1. Flow chat.

5. METHODOLOGY

The methodology of this project revolves around a systematic and iterative process, beginning with data collection and preprocessing. Surveillance video datasets will be gathered to train and validate deep learning models, and preprocessing steps will be applied to enhance the quality and relevance of the data. The core of the methodology involves designing and training deep learning models, such as convolutional neural networks (CNNs) or recurrent neural networks (RNNs), to recognize and classify various activities in the surveillance videos. Transfer learning may be employed to leverage pre-trained models for improved efficiency. Anomaly detection mechanisms will be integrated into the models to identify unusual patterns or behaviors. Real-time processing capabilities will be a focus, ensuring the system can operate efficiently in dynamic environments. The scalability of the solution will be addressed to handle the simultaneous processing of data from multiple surveillance cameras. Integration with existing surveillance infrastructure will be a pivotal step, allowing for seamless deployment. Throughout the development, rigorous testing and validation procedures will be implemented, and the models will be fine-tuned based on performance evaluations. Ethical considerations, including privacy protection and compliance with regulations, will be embedded into the methodology. Continuous feedback loops and improvements will be established, creating an adaptable and effective methodology for the development and deployment of the deep learning-based suspicious activity detection system.

6. PROPOSED ALGORITHM

• **Real World Input Video:** The initial input is a video stream from a real-world setting, like a security camera recording.

• **Segmenting Video into Frames:** The video is divided into individual frames, each representing a single still image.

• **Background Extraction:** This step isolates static elements like walls and floors, extracting the background from each frame.

• **Foreground Extraction:** After background removal, dynamic elements like people or vehicles, known as the foreground, remain.

• **Motion Tracking:** This block monitors the movement of foreground objects over time, identifying paths and trajectories.

• **Head Motion Detection**: Specifically detects motion related to heads, useful for tracking people's head movements within the scene.

• **Contact Detection:** Identifies interactions or contacts between objects, such as when a person touches an object or another person.

• **Activity Classification**: Utilizes outputs from motion tracking, head motion detection, and contact detection to

International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 12 | Dec 2023 www.irjet.net p-ISSN: 2395-0072

classify overall scene activity, potentially using machine learning algorithms.

• **Normal Activity:** If classified as "normal," observed behavior aligns with expected, routine patterns, like walking or standing.

• **Suspicious Activity:** If classified as "suspicious," observed behavior deviates from normal, including actions like running, fighting, or other potentially dangerous or unusual activities.

7. LITERATURE SURVEY

Sr No.	Paper Name	Authors	Abstract
1	Real-Time Suspicious Detection and Localization in Crowded Scenes	Mohammad Sabokrou, Mahmood Fathy	In this paper, we propose a method for real-time suspicious detection and localization in crowded scenes. The approach involves using local and global descriptors to capture video properties, and Gaussian classifiers to distinguish normal activities from anomalies.
2	Learning Temporal Regularity in Video Sequences	Mahmudul Hasan, Jonghyun Choi	This paper addresses the challenge of perceiving meaningful activities in long video sequences by learning generative models for regular motion patterns. Two methods based on auto encoders are proposed, one using handcrafted spatial temporal local features and the other using a fully convolutional feed forward auto encoder. The model captures regularity from multiple datasets and shows competitive performance in suspicious detection applications.
3	Suspicious Detection in Video Using Predictive Convolutional Long Short-Term Memory Networks	Jefferson Ryan Medel	The paper presents end-to-end trainable composite Convolutional Long Short-Term Memory (Conv-LSTM) networks for automating the detection of anomalous events in video sequences. The models predict the evolution of video sequences and derive regularity scores from reconstruction errors. The paper explores the effectiveness of Conv LSTM units for modeling and predicting video sequences and demonstrates competitive results on suspicious detection datasets
4	Abnormal Event Detection in Videos using Spatiotemporal Auto encoder	Yong Shean Chong	This method focuses on detecting anomalies in videos, particularly in crowded scenes. It employs a spatiotemporal architecture, consisting of components for spatial feature representation and learning the temporal evolution of these features.
5	A Review of Human Suspicious Activity from Single Image.	Naimat Ullah Khan, Wanggen Wan	This review discusses significant contributions in Human Pose

International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 12 | Dec 2023 www.irjet.net p-ISSN: 2395-0072

			Estimation methods from single two-dimensional images. It covers traditional pictorial structures, Deep Neural Networks, and the Stacked Hourglass approach. The paper provides a comprehensive study of influential deep learning methods for human pose estimation, starting from the earliest practical models and progressing to the most recent advancements.

8. CONCLUSION

A system to process real-time CCTV footage to detect any suspicious activity will help to create better security and less human intervention. Great strides have been made in the field of human Suspicious Activity, which enables us to better serve the myriad applications that are possible with it. Moreover, research in related fields such as Activity Tracking can greatly enhance its productive utilization in several fields.

ACKNOWLEDGEMENT

I wish to express my sincere thanks and deep Sense of gratitude to my respected mentor and guide. Prof.S.S.Shinde Assistant Professor in Department of Information Technology of *Smt. Kashibai Navale College Engineering, Pune-41* for the technical advice, encouragement and constructive criticism, which motivated to strive harder for excellence

REFERENCES

[1] Naimat Ullah Khan, Wangen Wan: "A Review of Human Pose Estimation from Single Image"- 978-1-5386-5195-7/18/ 2018 IEEE

[2] Qiuhui Chen, Chongyang Zhang, Weiwei Liu, and Dan Wang," Surveillance Human Pose Dataset and Performance Evaluation for Coarse-Grained Pose Estimation", Athens 2018.

[3] E. Eksioglu. Decoupled algorithm for MRI reconstruction using nonlocal block matching model: BM3DMRI. Journal of Mathematical Imaging and Vision, 56(3):430–440, 2016.

[4] Y. Yang, J. Sun, H. Li, and Z. Xu. Deep ADMM-Net for compressive sensing

[5] MRI. In Advances in Neural Information Processing Systems, pages 10–18, 2016.

[6] P.Bhagya Divya, S.Shalini, R.Deepa, Baddeli Sravya Reddy,"Inspection of suspicious human activity in the crowdsourced areas captured in surveillance cameras", International Research Journal of Engineering and Technology (IRJET), December 2017.

[7] Jitendra Musale,Akshata Gavhane, Liyakat Shaikh, Pournima Hagwane, Snehalata Tadge, "Suspicious Movement Detection and Tracking of Human Behavior and Object with Fire Detection using A Closed Circuit TV (CCTV) cameras ", International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume 5 Issue XII December 2017.

[8] U.M.Kamthe,C.G.Patil "Suspicious Activity Recognition in Video Surveillance System", Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018.

[9] Zahraa Kain, Abir Youness, Ismail El Sayad, Samih Abdul-Nabi, Hussein Kassem, "Detecting Abnormal Events in University Areas", International conference on Computer and Application,2018.

[10] Tian Wanga, Meina Qia, Yingjun Deng, Yi Zhouc, Huan Wangd, Qi Lyua, Hichem Snoussie, "Abnormal event detection based on analysis of movement information of video sequence", Article-Optik, vol-152, January-2018.

BIOGRAPHIES

Mr. Vedant. U. Saikhede
B.E Information Technology
Smt. Kashibai Navale College Engineering, Pune 41
Maharashtra, India

Mr. Kiran Shende
B.E Information Technology
Smt. Kashibai Navale College Engineering, Pune 41
Maharashtra, India

International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 12 | Dec 2023 www.irjet.net p-ISSN: 2395-0072

Mr. Yuvraj Darekar
B.E Information Technology
Smt. Kashibai Navale College
Engineering, Pune 41
Maharashtra, India

Mr. Hemant Thorat
B.E Information Technology
Smt. Kashibai Navale College
Engineering, Pune 41
Maharashtra, India

Prof. S.S.Shinde
Assistant Professor
Dept. of Information Technology
Smt. Kashibai Navale College
Engineering, Pune 41
Maharashtra, India

B. Published Paper E-Certificate

e-ISSN: 2395-0056 p-ISSN: 2395-0072

International Research Journal of Engineering and Technology (IRJET)

(An ISO 9001 : 2008 Certified Journal)

Is hereby awarding this certificate to

Vedant Saikhede

In recognition the publication of the manuscript entitled

Deep Learning Approach for Suspicious Activity Detection from Surveillance Video

published in our Journal Volume 10 Issue 12 December 2023

Impact Factor : 8.226 www.irjet.net

Editor in Chief

E-mail : editor@irjet.net

e-ISSN: 2395-0056 p-ISSN: 2395-0072

International Research Journal of Engineering and Technology (IRJET)

(An ISO 9001 : 2008 Certified Journal)

Is hereby awarding this certificate to

Kiran Shende

In recognition the publication of the manuscript entitled

Deep Learning Approach for Suspicious Activity Detection from Surveillance Video

published in our Journal Volume 10 Issue 12 December 2023

Impact Factor : 8.226 www.irjet.net

Editor in Chief

E-mail : editor@irjet.net

e-ISSN: 2395-0056 p-ISSN: 2395-0072

International Research Journal of Engineering and Technology (IRJET)

(An ISO 9001 : 2008 Certified Journal)

Is hereby awarding this certificate to

Yuvraj Darekar

In recognition the publication of the manuscript entitled

Deep Learning Approach for Suspicious Activity Detection from Surveillance Video

published in our Journal Volume 10 Issue 12 December 2023

Impact Factor : 8.226 www.irjet.net

Editor in Chief
E-mail : editor@irjet.net

e-ISSN: 2395-0056 p-ISSN: 2395-0072

International Research Journal of Engineering and Technology (IRJET)

(An ISO 9001 : 2008 Certified Journal)

Is hereby awarding this certificate to

Hemant Thorat

In recognition the publication of the manuscript entitled

Deep Learning Approach for Suspicious Activity Detection from Surveillance Video

published in our Journal Volume 10 Issue 12 December 2023

Impact Factor : 8.226 www.irjet.net

Editor in Chief
E-mail : editor@irjet.net

e-ISSN: 2395-0056 p-ISSN: 2395-0072

International Research Journal of Engineering and Technology (IRJET)

(An ISO 9001 : 2008 Certified Journal)

Is hereby awarding this certificate to

Prof. Snehal. S. Shinde

In recognition the publication of the manuscript entitled

Deep Learning Approach for Suspicious Activity Detection from Surveillance Video

published in our Journal Volume 10 Issue 12 December 2023

Impact Factor : 8.226

www.irjet.net

Editor in Chief

E-mail : editor@irjet.net

C. Plagiarism Report

Check Plagiarism

PLAGIARISM SCAN REPORT

Date	May 23, 2024
Exclude URL:	NO

Unique Content	**90**	Word Count	7965
Plagiarized Content	**10**	Records Found	0

CONTENT CHECKED FOR PLAGIARISM: