A Model for Detecting Suspicious Behaviors during Examinations Using Deep Learning

Ori Silas Ene[1], Igwe Joseph Sunday[2], , Onu Sunday[3] Ituma Chinagorom[4]

Emewu, Benedict Mbanefo[5]

1 ,3 & 4 David Umahi Federal University of Health Science, Uburu, Ebonyi State, Nigeria

2 *Department Of Computer Science, Ebonyi State University, Abakaliki–Nigeria*

[1]ORCID ID: 0009000940632639

Summary: A Model for Detecting Suspicious Behaviors During Examinations Using Deep Learning focuses on building a smart system that can automatically monitor students and detect cheating-related actions during exams. Examination malpractice remains a serious challenge in educational institutions, as human invigilators may fail. This reduces the credibility in the examination process. To address this problem, the project will developed a deep learning model that uses Convolutional Neural Networks (CNN) to capture visual features from video frames and Long Short-Term Memory (LSTM) networks to analyze behavior patterns over time. The solution will be guided by two main methodologies: CRISP-DM, which structured the data mining process through phases; and OOADM, which will guide the system design using object-oriented principles. The system will be implemented using Python as the programming language and Django for database development and management. This model is expected to effectively identify suspicious behaviors with high accuracy.

Keywords: Frame, Image, Machine Learning, Digital Image and Deep Learnig

1. INTRODUCTION

Technology such as machine learning helps in solving a lot of problems across severalapplication domains, including entertainment, healthcare and surveillance . The interest in human activity monitoring, recognition and understanding through a surveillance system has increased over time and is gaining more attention as the concern for proactive information about safety and security grow [1]

[2] noted that video surveillance technology has developed rapidly in the recent years. The traditional method of students monitoring which includes an invigilator to monitor the examination hall is difficult and not very efficient. It is very challenging to differentiate between a normal behavior and an abnormal behavior, as the abnormal behavior in an examination hall includes many categories such as passing the paper, peeking into others paper, signaling to others etc. Video analytics technologies are now being widely proposed to examine videos to determine the behavior and data. The technology can not only be used in areas of examination hall but also in other fields like security surveillance and to determine dishonest behavior. Hence for an anomaly in examination system, there is a need to design a base/core for which the method differentiates the normal behavior actions and then classify them seeing other several actions which are not normal. However, constructing a structure that identifies the abnormal behavior is a challenging issue because of the standard of the video, dimension of territory, certain posture of students. The examination rooms are packed and dynamic which makes it difficult to part the student information. Backdrop due to continuous motion from various objects and scenes makes it difficult in the real time to recognize the activity that deviates from patterns which are normal.

[3] noted that the number of closed circuit television (CCTV) cameras mounted in public and private places has increased. This can be observed in academic institutions, entertainment centers, business environments, transportation systems, and health care center. Surveillance technology solutions are now being widely deployed to monitor people's activities and behaviors so that the related authority can be alerted when suspicious or abnormal activities are noticed. With such advancement in artificial intelligent technologies, it is believed that the fight against examination malpractices can be pushed further if computer vision and machine learning techniques are integrated into monitoring examinations.

The peril of examination malpractices has grown exponentially across all levels of study particularly at secondary and higher learning institutions in Nigeria over the past decades. Several existing approaches which include; creating photo albums that consist of true photographs of the prospective examination candidates during the registration. The album is used to validate candidates' examination cards before admitting the candidate into the examination hall. Also, the use of biometric devices to capture the biometric details of prospective examination candidates during regulatory bodies to various center's during examinations and reshuffling of invigilators from time to time, ensuring that only formally registered candidates sit for examinations, placing a ban on the use of gadgets such as mobile phones, calculators and other electronic devices have all been applied [4]

These approaches have however, not yielding the desired outcome because, in nearly every examination season, new and inventive ways of cheating are often being devised by these candidates.

This research article aims to model a system that can recognize suspicious activities or behaviors in the hall during examination using deep learning. The specific objectives of the study are:

i. Capture videos of examination scene, extract image frames from the videos, select frames with images of interest and perform segmentation on the selected frames.
ii. Extract features of interest from images.
iii. Train and test a classifier with the extracted features to predict whether activity is suspicious or normal.

2. PREVIOUS RELATED WORKS

[4]worked on automated cheating detecting using computer vision and CCTV footage using CNN(VGG-16) for feature extraction plus LSTM for behavior classification, the system had high accuracy, real time detection but was sensitive to environmental factors such as lighting and camera angles and highly computational demanding.

[5] proposed a suspicious activity in exams using OpenPose and CNN, the system detected object exchanges and was adaptable to controlled environments but had limited dataset, struggles with complex behaviours and requires predefined thresholds

[6]came up with a deep learning cheating detection in online examination, they employed CNN for visual analysis and the Gaussian-based DFT for speech detection and voting fusion, it was a multimodal approach but requires high quality cameras, and limited to predefined cheating behaviours.

[2] carried a survey on anomalous behavior detection in exam halls, they reviewed KNN,PA,HMM. SVM and deep learning, it was a comprehensive overview of techniques highlighting real time surveillance benefits but had no original method proposed and lacks empirical validation.

[7]proposed a real-time anomalous behavior detection using neural networks, the system had a continous monitoring capability adaptable to suspicious states but dependent on fixed cameras and limited to specific behaviors.
[8]proposed an automated proctoring using HOG features and KNN, it was simple in implementation and effective for basic posture analysis but failed to detect untrained suspicious actions and low in robustness.
[9] worked on deep learning for anomaly detection in surveillance videos, it was a multiple instance learning framework that was high in accuracy and robust in crowded scenes but required large labeled datasets and computationally intensive.
[10] proposed online exam proctoring using CNN and LSTM, the system was robust in temporal analysis but had privacy concerns.
[11] proposed a secured internet examination system based on video monitoring. The system has a camera at the client computer which captures the faces and the Posture of the student during the test at a random interval. The captured images which are stored on the server can be used to verify the student's identity whenever the need arises. The disadvantage of this system is that a configured to detect and report suspicious activities during an examination in real-time.
[12] proposed techniques for monitoring the comparability of examination standards. Techniques which have been employed by the examining boards and regulatory authorities, in England, over the fifty years were reviewed to ascertain if the technique were of a uniform standard
[13] noted that excessive human involvement in examination management is responsible for the prevalence of examination malpractices, hence proposed the use of automated test-taking, marking, and result in the printing system, as a solution for curbing examination malpractices for Africans.
[14] proposed a less costly, non-proctor alternative to promote academic honesty, using eight control procedures that enable faculty to increase the difficulty of cheating and thus reduce the likelihood of cheating by students. The major limitation of this system is that it does not support real-time detection of suspicious activities during an examination.
[15] proposed and designed a secured web-based online examination system using cryptography to ensure the integrity of interaction between the examinees system and the server.
In [16], the use of a wireless camera for online examination supervision was proposed as part of the continuing effort to continually tackle examination malpractices in computer-administered test environments especially in areas of candidate authentication and activities during an examination.
[17] proposed an e-learning tool called Moodle for monitoring the evaluation process of candidates in a computer-based examination. The tool automatically stores a log of all activities carried out by participants regardless of whether they are teachers or students during an online examination. The information logged is later audited and visualized with "Moodle Watcher" so that unauthorized and fraudulent activities during the examination can be detected. Fraudulent activities that can be detected in Moodle include (1) Sharing of access code amongst the various participants, allowing them to "tell each other the answers" during the exam: (2) able to access multiple accounts not belonging to the actual student which makes it possible for an exam to be taken in behalf of another candidate; (3) Access to blog posts with "copy-paste" from the blog posts. Though Moodle is a very good tool for monitoring educational progress, as a tool for evaluation, however, it has very serious security-related issues not yet corrected that may put the integrity of tests and examinations carried out on its platform in doubt.
[18] proposed a system able to detect and recognize suspicious activities such as peeping into the answer sheets of another candidate during examination. The system was focused on recognizing exchange of material between candidates. The

algorithm used includes background subtraction, edge detection algorithm, highest redundancy ratio, Gabor filter feature extraction, and ANN algorithms.

[19] conducted a study focused on candidate authentication to prevent malpractices. They proposed an embedded Zig Bee based communication system which uses a biometric fingerprint and webcam for verifying and authenticating candidates before access is granted into examination halls. This system could only prevent impersonation. But no other suspicious cases

3. METHODOLOGY

The methodology describes the process and steps used in developing the model for detecting suspicious behaviors during examinations using deep learning. The research adopted two main approaches: the CRISP-DM (Cross-Industry Standard Process for Data Mining) framework and the OOADM (Object-Oriented Analysis and Design Methodology).

CRISP-DM Framework

The CRISP-DM framework provides a structured way of building and deploying data mining and deep learning models. It was chosen because it helps in managing data-related tasks in stages and makes the process more organized. The six major phases of CRISP-DM applied in this research are:

1. Business Understanding
2. Data Understanding
3. Data Preparation
4. Modeling
5. Evaluation
6. Deployment

Object-Oriented Analysis and Design Methodology (OOADM)

The Object-Oriented Analysis and Design Methodology (OOADM) were used to design the structure of the system. This method makes it easy to divide the system into objects and show how they interact with each other. It also helps to understand how different parts of the system work together. The following steps were followed in applying OOADM:

1. **Object-Oriented Analysis (OOA)**

In this step, the problem was studied to find the main objects of the system, their features, and their roles. The important objects identified include:

i. Student**:** represents the person writing the exam. Attributes include ID, seat number, and behavior.
ii. Camera**:** captures video of the exam. Attributes include frame rate and resolution.
iii. Suspicious Behavior Detector: the deep learning model that checks for unusual actions. Attributes include accuracy, confidence level, and detection rules.

2. **Object-Oriented Design (OOD)**

This step explained how the objects connect and work together. It was represented with simple diagrams:

i. Use Case Diagram**:** shows how the invigilator uploads an exam video, clicks "Analyze," and receives analysis to know if cheating is detected.
ii. Class Diagram: describes the objects (Student, Camera, Detector, and Analysis) with their attributes and methods.
iii. Sequence Diagram**:** shows the order of actions

3. **Implementation Design**

In this step, the design was turned into real system modules. The system was implemented using Python programming language with libraries like TensorFlow**,** Keras**,** and OpenCV. Object-oriented programming principles such as encapsulation (hiding internal details) and inheritance (reusing code) were applied. This made the system easier to maintain, expand, and reuse.

System Analysis

System analysis is the process of studying the problem, understanding the user needs, and deciding what the new system should do. It helps to make sure the system is built in the right way and solves the problem of detecting suspicious behaviors during examinations. In this research, system analysis focused on finding the weaknesses of the current examination monitoring methods and describing how the new deep learning system will improve them.

Analysis of the Existing System

The existing system of examination monitoring works mainly through human invigilators who move around the examination hall to observe students and ensure that they follow the rules. The invigilators rely on their eyes and judgment to identify suspicious actions such as whispering, turning heads frequently, or exchanging materials. Whenever malpractice is suspected, the invigilator warns the student, seizes the illegal material, or reports the case for further action.

Although this method has been used for many years, it faces several challenges. Human invigilators can easily become tired or distracted, especially in large halls with many students. This makes it impossible to monitor every student at the same time, leaving gaps where some suspicious behaviors go unnoticed. In addition, monitoring is often subjective because what one invigilator sees as normal may be considered suspicious by another, which reduces consistency. The process is also stressful and time-consuming for the invigilators who must remain alert for long periods of time.

Weaknesses of the Existing system

The existing examination monitoring system, which depends mainly on human invigilators, has several weaknesses that reduce its effectiveness.

i. One major weakness is the problem of limited human attention. Invigilators are human beings, and they can become tired, distracted, or overwhelmed during long examination hours.
ii. Another weakness is the difficulty of handling large examination halls. In cases where hundreds of students are writing at the same time, one or two invigilators cannot carefully watch everyone. Some students may take advantage of this limitation to engage in malpractice without being noticed. The system is also highly subjective. What one invigilator may see as normal behavior could be judged as suspicious by another, which leads to inconsistency in reporting malpractice cases.
iii. This lack of evidence makes it hard to take disciplinary actions because the decision relies only on the word of the invigilator.
iv. The process is also stressful and time-consuming. Invigilators must move around the hall for long periods, staying alert throughout the examination. This creates physical and mental stress, and their efficiency decreases as the exam continues.

The weaknesses of the existing system show that relying only on human supervision is not enough. A more reliable, automated, and intelligent solution is needed to improve monitoring, reduce human error, and provide evidence-based detection of suspicious behaviors during examinations.

Analysis of the Proposed System

The proposed system introduces a deep learning-based solution for monitoring examinations and detecting suspicious student behaviors. Unlike the existing system that relies only on human invigilators, the new system uses computer vision and artificial intelligence to automatically analyze examination videos. The main goal of this system is to reduce human error, provide accurate monitoring, and supply evidence when malpractice occurs.

In the proposed system, the user uploads an examination video into the system. Once the video is uploaded, the user clicks on the Analyze button, and the deep learning model begins to process the video. The model examines the frames of the video to detect unusual behaviors such as frequent head turning, whispering gestures, looking at another student's script, or making hand signals. If the model finds suspicious behavior, the system

immediately raises an alert, which is displayed through the interface for the invigilator or examiner to review. This ensures that no suspicious activity goes unnoticed.

The proposed system also improves reliability because it can monitor all students at the same time without fatigue. Unlike human invigilators who may lose concentration, the system provides continuous and consistent analysis throughout the examination. Another advantage is that it creates a record of evidence since the alerts and analyzed video segments can be stored for future reference. This provides stronger support when handling reported cases of malpractice.

Block Diagram of the Proposed System

The block diagram of the proposed system shows the major parts of the system and how they work together to achieve the goal of detecting suspicious behaviors during examinations. A block diagram is very important because it gives a simple picture of the system and explains how information moves from one stage to another.

In the proposed system, the process starts with the input stage, where video data is collected either through surveillance cameras in the examination hall or from pre-recorded datasets. This data is then sent into the preprocessing stage, where the video is cleaned and prepared. At this stage, frames are extracted, unnecessary noise is removed, and the images are resized so that the deep learning model can easily understand them.

The next block is the feature extraction stage, where important details such as body movements, gestures, and facial directions are captured. These features help the system to differentiate between normal behaviors (such as writing or reading) and suspicious behaviors (such as looking around frequently, making hand signs, or exchanging items).

After feature extraction, the data enters the deep learning model. Here, a trained neural network (for example, CNN-LSTM) analyzes the features and classifies the behavior as either "normal" or "suspicious." This stage is the brain of the system because it makes the main decisions.

The output from the model is then passed to the decision-making and alert module. If suspicious behavior is detected, the system raises an alert that can be sent to the examiner or stored in the system log for later review. If the behavior is normal, the system continues monitoring without interruption.

Finally, the output stage shows the results in a user-friendly interface. This may include a notification, visual highlighting of the detected behavior, or a report summary of suspicious actions during the examination. The block diagram makes it clear how all these stages are linked together in a step-by-step flow, ensuring that the system works smoothly to reduce examination malpractice and improve supervision accuracy.

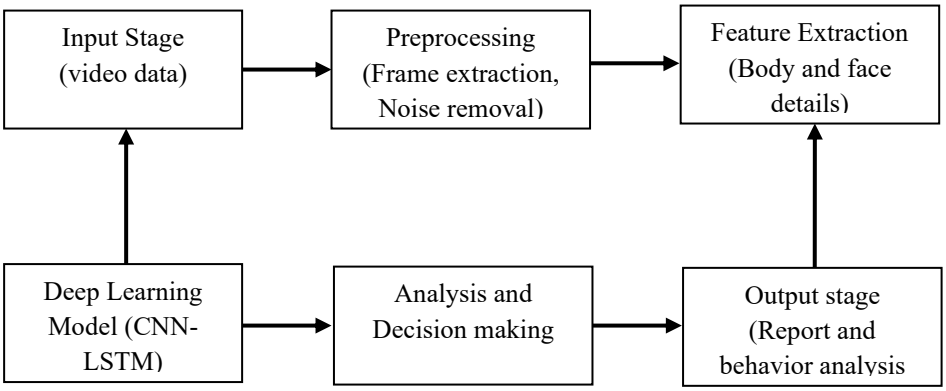

Figure 1: Block Diagram of the Proposed System

Figure 1 explains step-by-step process where each stage depends on the one before it to ensure accurate results. It begins with the input stage, where video data is collected from either a live camera feed or pre-recorded sources. This raw video is then passed to the preprocessing stage, which prepares the data by cleaning it, extracting individual frames, and removing noise or unnecessary information that could reduce accuracy. After preprocessing, the feature extraction stage focuses on identifying important details such as body movements, facial patterns, and hand gestures that will help the system understand human activities. These extracted features are then sent into a deep learning model that combines Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. The CNN is responsible for identifying spatial features like shapes and positions, while the LSTM captures time-based patterns such as continuous movements and gestures across frames. Once the model processes this information, the decision and analysis module interprets the results and determines whether the detected activity is normal, suspicious, or requires attention. At the final stage, the output is presented in a clear form, either as detailed reports that can be used for further action. This continuous flow makes the system reliable, intelligent, and effective in analyzing human behavior from video data.

Integration of Deep Learning Model

The integration of Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) into the system is very important because it allows the system to learn from both images and sequences of data in a smart way. CNN and LSTM work together, and each one plays a different but complementary role.

The CNN is mainly used to process images and video frames. It can detect shapes, facial features, gestures, and body movements from the raw data. For example, when a user uploads a video or live stream, the CNN is responsible for breaking down the frames and identifying important features such as suspicious hand signs, objects, or facial expressions that may show unusual behavior.

The LSTM, on the other hand, deals with time-based patterns and sequences. Instead of just looking at one image or one frame, LSTM looks at how the actions change over time. This makes it possible for the system to understand continuous behavior, such as a sequence of suspicious movements, repeated dangerous words in messages, or continuous abnormal activity on the platform.

When CNN and LSTM are integrated, the CNN first extracts features from the input data, and then these features are sent to the LSTM. The LSTM uses its memory ability to analyze the order of events and the relationship between them. This combined approach makes the system more powerful because it does not only detect what is happening at one moment but also understands how the activity develops over time.

Finally, after CNN and LSTM finish their analysis, the results are sent to the decision-making module. If the model detects suspicious or terrorist-related behavior, the system prepares a detailed report for security personnel. This integration ensures that the system can detect both visual patterns and behavioral trends, making it more accurate and reliable compared to using a single model alone. Integrating CNN and LSTM improves the system's intelligence by allowing it to recognize images, understand behavior over time, and generate useful reports that can help in preventing terrorist activities on social media.

The integration of Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) forms the core of the proposed system because both models handle different aspects of the data. CNN focuses on extracting visual features from images and video frames, while LSTM specializes in analyzing sequential patterns across time. When combined, they give the system a deeper understanding of suspicious actions, behaviors, or events. Step-by-step integration process:

i. Input Data Collection
ii. Preprocessing
iii. Feature Extraction with CNN

iv. Temporal Analysis with LSTM
v. Integration of CNN and LSTM
vi. Decision-Making Module
vii. Output Stage

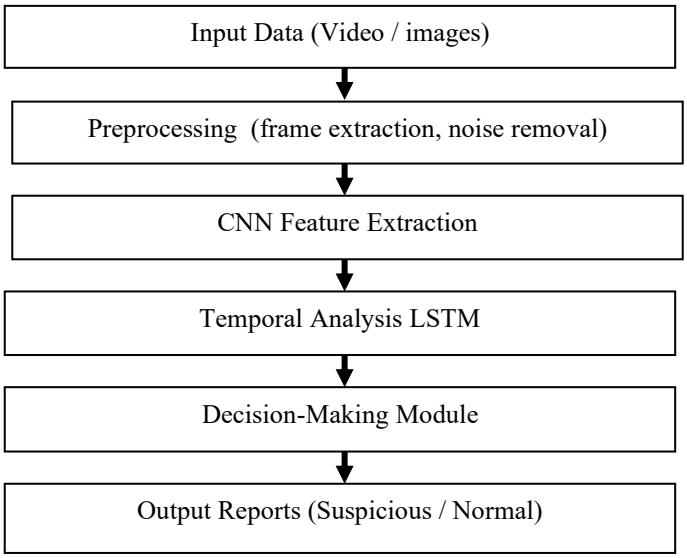

Figure 2: Block Diagram of Integration of CNN and LSTM

Figure 2 is the block diagram that shows how CNN and LSTM are combined to process input data step by step, from raw video to final reports.

3.3 Architecture Diagram of the Proposed System

The proposed system is designed with a 2-tier architecture to keep it simple, structured, and efficient. The two tiers are:

1. Client Tier (Front-End)
2. Server Tier (Back-End)

In the Client Tier, the system receives input from users or devices such as mobile phones, computers, or cameras. This tier is responsible for capturing the video or image data and sending it to the server for processing. It also displays the final results, such as recognized actions, decision-making reports, or activity classifications. The client tier acts as the interface between the user and the system.

The Server Tier is the core part of the system where all processing takes place. Once the client sends the input, the server handles the following tasks:

i. Preprocessing: Cleans and organizes the raw video or image data into frames.
ii. Feature Extraction: Identifies important patterns like human posture, gestures, and movements.
iii. Deep Learning Model (CNN + LSTM): The CNN extracts spatial features from images, while the LSTM learns the time sequence of movements. This combination makes the system accurate in understanding human actions.
iv. Decision-Making Module: After the deep learning analysis, this module interprets the recognized activity and generates a detailed report for the client tier to display.

The client then receives the processed results from the server and presents them in a simple and understandable format.

This 2-tier architecture makes the system faster and easier to maintain because the tasks are divided clearly between the client and the server. The client focuses on interaction and display, while the server handles the heavy processing and decision-making.

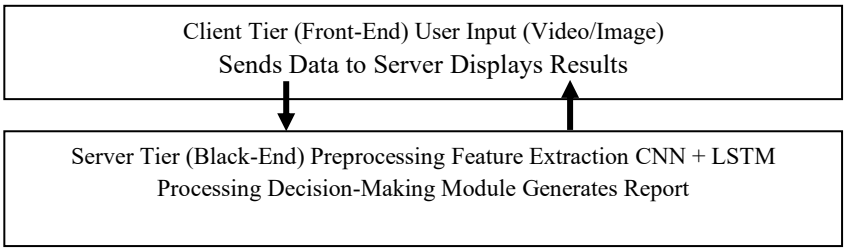

Figure 3: Architecture of the Proposed System

Here is the 2-tier architecture diagram of the proposed system showing the Client Tier (Front-End) and the Server Tier (Back-End) with their respective roles

4. SYSTEM DESIGN

Main Menu Design

The Main Menu Design is the central hub of the proposed system where users can access different features. It is simple, user-friendly, and arranged in a way that makes navigation easy. When the system is launched, the user is welcomed with the main menu, which provides options such as uploading data, running the deep learning model, checking decision-making results, and viewing reports. Administrators can also use the main menu to manage users and control system settings.

The design is structured like a dashboard, where each option is clearly shown with buttons or icons. This helps users, even those with little technical knowledge, to move from one feature to another without difficulty. The goal of the main menu is to make the system easy to use, reduce errors, and ensure that the user can quickly perform tasks.

Running the Model on VS Code

The deep learning model (CNN and LSTM) that powers the system is run inside Visual Studio Code (VS Code). The process is simple and works as follows:

i. Environment Setup:
ii. Loading the Code:
iii. Running the Model:
iv. Connecting with the Main Menu:
4. Viewing Results:

In this way, the main menu acts as a control center, while the deep learning model runs in the background through VS Code integration, ensuring smooth interaction between users and the system.

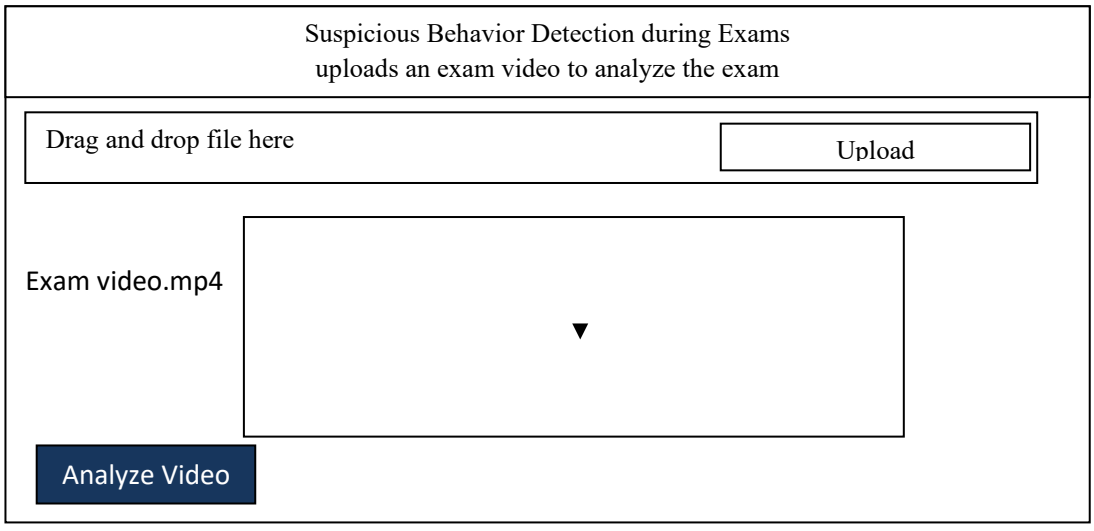

Figure 4: Main Menu Design

Figure 4 is the main menu design that enable a user to upload a video of the exam and click on analyze video button while the model uses the video to analyze the examination

5. SUMMARY

Summary

The proposed system introduces a deep learning-based approach for monitoring examinations and detecting suspicious student behaviors. Unlike the existing method that depends mainly on human invigilators, this proposed system will make use of computer vision and artificial intelligence to automatically analyze examination videos. The main aim is to reduce human error, increase accuracy in monitoring, and provide reliable evidence whenever malpractice is detected.

REFERENCES

1. Agwi. U. C., Irhebhude, M. E., Ogwueleka, F. N. Video surveillance in examination monitoring. *Security and Privacy,* e!44.https:/, doi.org/TO.1002/spy2.144, (2020)
2. Charara, N., Jarkass, I., Sokhn, M., Mugellini, E., Khaled, O. A. Adabev: Automatic detection of abnormal behaviour in video-surveillance. *In International Conference on* (2012)
3. Borges, P. V. K., Conci, N., Cavallaro, A. Video-based human behavior understanding: A survey. *IEEE transactions on circuits and systems for video technology,* 23(11), 1993-2008. (2013).
4. Navale, M., From Manual to Automated: A Computer Vision Based Solution for Exam heating Detection. *LIRID Journal.* (2024).
5. Moyo, R., et al. (2024). A video-based Detector for Suspicious Activity in Examination with OpenPose.*LIRID Journal.*
6. Ogbu, N. H. (2016) A Model Of University Examination Monitoring System. *Journal ofComputer Science and Engineering (IJRDO)* 2(7), 54 -63
7. Devi. G. S., Reddy, P. P., Kumar, G. S., Chaitanya, V. Multiple View Surveillance using Image Registration. International Journal of Computer Applications, 93(2), 27-32. (2014)
8. Desai, N., Pathari, K., Raut, J., Solavande, V. Online Surveillance for Exam. *International Journal of recent trends in Engineering and Research* 4(3), 331-336, (2018).
9. Kuna, S., Real Time Object Detection and Recognition using deep learning methods. International Journal for Research in Applied Science and Engineering Technology, 8(6),58-64. Lai, T.Y., (2020).
10. Atabong T. A. , Okpala M. C., Abondem A. L., &Essombe, C. E. (2010) Eliminating Examination Malpractice in Africa with Automated Test Taking, Marking and Result Printing, *Tropical Journal Of Biomedical And Allied Sciences Research,* 4(1), 452-469.
11. Yu, Z..Xu, M., Gao, Z. *Biomedical image segmentation via constrained graph cuts.* (2011).
12. Kale, G. V., Patil, V. H. A study of vision based human motion recognition and analysis. *International Journal of Ambient Computing and Intelligence* (1JACI), 7(2), 75-92. (2016).
13. Castro, P. Computing Machinery, Intelligence and Undecidability. *JTheorComputSci,* 4(160), 1-4. (2017).
14. Mohammed, M., Khan, M. B., Bashier, E. B. M. *Machine learning: algorithms and applications.* Crc Press. 1-34, (2017).

15. CluskeyJr, G. R., Ehlen, C. R., &Raiborn, M. H.-(2011). Thwarting online exam cheating without proctor supervision. *Journal of Academic and Business Ethics,* 4(1), 1-7

16. Ayodele, T. O. Types of machine learning algorithms. *New advances in machine learning,* 3, 19-48. (2010).
17. Matos. R., Torrao, S., & Vieira, T. C. S. (2012). *Moodlewatcher: detection and prevention of fraud when using Moodle quizzes.* In Proceedings of INTED2012 Conference. 4997-5001
18. Gowsikhaa, D., &Abirami, S. (2012). Suspicious Human Activity Detection from SurveillanceVideos. *International Journal on Internet and Distributed Computing Systems,* 2(2).141-148
19. Anumolu, B., &Bharadwaj, N. (2013) An Online Examination System Using Wireless Security Application Madhu. *International Journal of Engineering Trends and Technology (LIETT)* 4(9), 3885-3887.