ISSN (Online): 2583-648X

IJIRID

International Journal of Ingenious Research, Invention and Development

An International, High Impact Factor, Double-Blind Peer-Reviewed, Open-Access, Multidisciplinary Online Journal

Volume 3 | Issue 5 | October 2024

www.ijirid.in

From Manual to Automated: A Computer Vision-Based Solution for Exam Cheating Detection

Dr. Mahesh Navale[1], Aryan Arjun Jadhav[2], Mahesh Shrikrishna Kadam[3],
Shalmali Dipak Karandikar[4], Siddhi Anil Kate[5]

[1]*Assistant Professor, Zeal College of Engineering & Research, Pune (M.S.), India*

[2,3,4,5]*Student, Zeal College of Engineering & Research, Pune (M.S.), India*

Abstract: Cheating during exams is a widespread issue that undermines the credibility of educational assessments. Traditional invigilation methods, relying on manual supervision, often fall short in effectively detecting dishonest behavior, especially in large-scale exam settings. This study proposes an automated system that leverages computer vision and CCTV footage to detect suspicious behavior in real time, offering a scalable solution for maintaining exam integrity. Results demonstrate that the proposed method is both reliable and efficient, achieving high accuracy in detecting cheating behaviors within classroom environments. This automated approach represents a significant advancement in safeguarding the fairness and validity of exams.

Keywords: *Exam Integrity, Real-Time Invigilation, Suspicious Behavior Detection, CCTV-Based Surveillance, Academic Honesty, Automated Cheating Detection.*

I. INTRODUCTION

Cheating during exams is a pervasive issue affecting educational institutions globally, with students often resorting to dishonest practices regardless of local efforts to prevent it. Numerous studies over the past decade have analyzed various cheating behaviors and explored methods that institutions could employ to combat this challenge. In the United States, for instance, a significant percentage of high school students admitted to cheating without repercussions, with 95% reporting they were not caught, and 51% indicating they did not see cheating as morally wrong.

Three main factors are often cited as motivations for cheating: fear of failure, a willingness to take risks, and a perceived lack of consequences. While the fear of failure is largely intrinsic to the student, the other factors highlight limitations in existing monitoring practices. Poor invigilation quality or an insufficient number of invigilators can make it difficult to uphold exam integrity. These limitations underscore the need for an automated invigilation system that minimizes human intervention, aiming to make exam supervision more reliable and resistant to manipulation.

The purpose of this model is to automate the detection of suspicious or abnormal behaviors during exams. By analyzing body movements and postures from CCTV footage, actions like frequent looking around or bending are flagged as potential signs of cheating. If the frequency of such behaviors exceeds a pre-set threshold, the system triggers an alert and generates a report for examiner review. In addition, facial recognition technology registers students' faces using OpenCV, ensuring that any individual flagged for suspicious activity is accurately identified. This report, containing timestamps and specific details of the incidents, is sent to the examiners for a final review.

DOI: 10.5281/zenodo.14066366

Such an automated invigilation model represents an innovative approach to exam supervision, reducing the reliance on physical invigilators and allowing their time and resources to be allocated more effectively. By introducing this system, institutions can ensure stricter, more efficient examination processes, supporting fairer outcomes for all students.

II. TECHNOLOGY: DEEP LEARNING IN SUSPICIOUS ACTIVITY DETECTION

Deep learning is widely used in video surveillance systems to automatically detect suspicious activities. Combining algorithms such as Convolutional Neural Networks (CNN) for feature extraction and Long Short-Term Memory (LSTM) networks for sequence prediction, these models can monitor and classify human behaviors in real time.

1. **CNN: Feature Extraction**

   Convolutional Neural Networks (CNNs) are used to extract visual features from video frames. In suspicious activity detection, CNN models process each frame to identify high-level features, reducing complexity while retaining essential details. The VGG-16 architecture, commonly used for this purpose, applies multiple layers of convolutions, pooling, and activations to capture fine details like objects, facial expressions, or body movements.

2. **LSTM: Sequential Classification**

   Long Short-Term Memory (LSTM) networks, a type of Recurrent Neural Network (RNN), process the sequential data generated by CNNs, identifying patterns over time to classify behaviors as suspicious or normal. By learning temporal dependencies, LSTMs can distinguish between regular and irregular activities based on the flow of movements, enhancing accuracy in behavior analysis.

3. **System Integration**

   The integration of CNN for feature extraction and LSTM for behavior classification creates a powerful framework for real-time suspicious activity detection. The system captures video frames, extracts features using CNN, and uses LSTM to analyze the behavior pattern over time, allowing it to alert authorities promptly when suspicious activities are detected. This combination improves detection accuracy, reducing false positives, and is applicable in settings like exam halls or public surveillance.

III. LITERATURE REVIEW

The field of video surveillance has evolved significantly, with deep learning methods now playing a critical role in automating the detection of suspicious activities. Surveillance systems have been increasingly used in environments such as academic campuses, public areas, and private institutions to identify abnormal or prohibited behaviors in real time. The development of deep learning techniques like Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks has greatly enhanced the ability of systems to process video frames, extract meaningful features, and recognize complex human behaviors over time.

DOI: 10.5281/zenodo.14066366

One approach to behavior analysis in surveillance involves feature extraction and classification. CNN models such as VGG-16, commonly employed for high-level feature extraction, can identify detailed visual patterns within frames, such as specific objects or body postures. Using CNNs for feature extraction is advantageous as they automatically learn visual representations directly from raw image pixels, making the feature extraction process faster and more accurate than traditional methods. Once these features are extracted, Recurrent Neural Networks (RNNs), particularly LSTMs, are applied to process the sequence of frames and detect abnormal patterns in behavior. LSTMs are particularly suitable for this task due to their capacity to understand temporal dependencies, enabling them to identify deviations in regular movement patterns over time.

Several studies have demonstrated the use of CNNs and LSTMs for detecting suspicious activities. For instance, CNNs have been combined with LSTMs to detect abnormal human behavior, such as individuals using mobile phones in restricted areas or fighting in public spaces. In one study, a system using CNNs for extracting spatial features from frames and LSTMs for temporal analysis was developed, achieving high detection accuracy across various behaviors, including violence detection in sports stadiums and suspicious activities in public areas. This integration of CNNs and LSTMs has proven effective in identifying complex human behaviors, minimizing manual monitoring, and reducing false positives in real-time surveillance settings.

Further developments have been made using pre-trained CNN models, such as VGG-16, which was originally trained on the ImageNet dataset and fine-tuned for surveillance tasks. By transferring learned visual patterns from large datasets, VGG-16 provides accurate initial feature extraction, which is then refined through additional training on context-specific surveillance data. This approach allows systems to be tailored for different environments, from crowded public areas to academic examination halls, where detection of cheating or other suspicious behavior is essential for maintaining integrity.

Despite the success of deep learning models in behavior recognition, challenges remain. In dynamic environments, issues such as occlusions, changes in lighting, and the presence of crowds can impact detection accuracy. Nonetheless, the application of deep learning for suspicious activity detection holds promise in automating surveillance, providing real-time alerts, and significantly reducing the need for manual monitoring.

Overall, the literature emphasizes the benefits of deep learning-based surveillance for improving security and monitoring efficiency across various settings. The integration of CNNs and LSTMs has proven to be a reliable framework for identifying and classifying behaviors, positioning deep learning as a transformative technology in modern surveillance systems.

IV. METHODOLOGY

The proposed system for real-time suspicious activity detection integrates CNN for object detection and LSTM for behavior analysis. This section describes the system architecture, data collection process, training methods, and the steps taken to ensure effective detection of suspicious behaviors.

DOI: 10.5281/zenodo.14066366

1. System Architecture

The architecture of the proposed system includes the following components:

- **Camera Network:** A network of high-definition cameras placed strategically to capture continuous video feeds from the exam hall or monitored space.
- **CNN Module:** This module uses a Convolutional Neural Network (CNN) for object detection. The CNN model is trained to identify suspicious objects, such as mobile phones, cheat sheets, or other unauthorized items within the exam hall.
- **LSTM Module:** The LSTM (Long Short-Term Memory) module processes the detected objects over time, tracking their movements to identify patterns of suspicious behavior. Examples of such behaviors include frequent looking around, hand movements indicative of cheating, or irregular group interactions.
- **User Interface:** A user-friendly interface allows administrators and proctors to monitor live feeds, receive alerts, and review flagged incidents for further inspection.

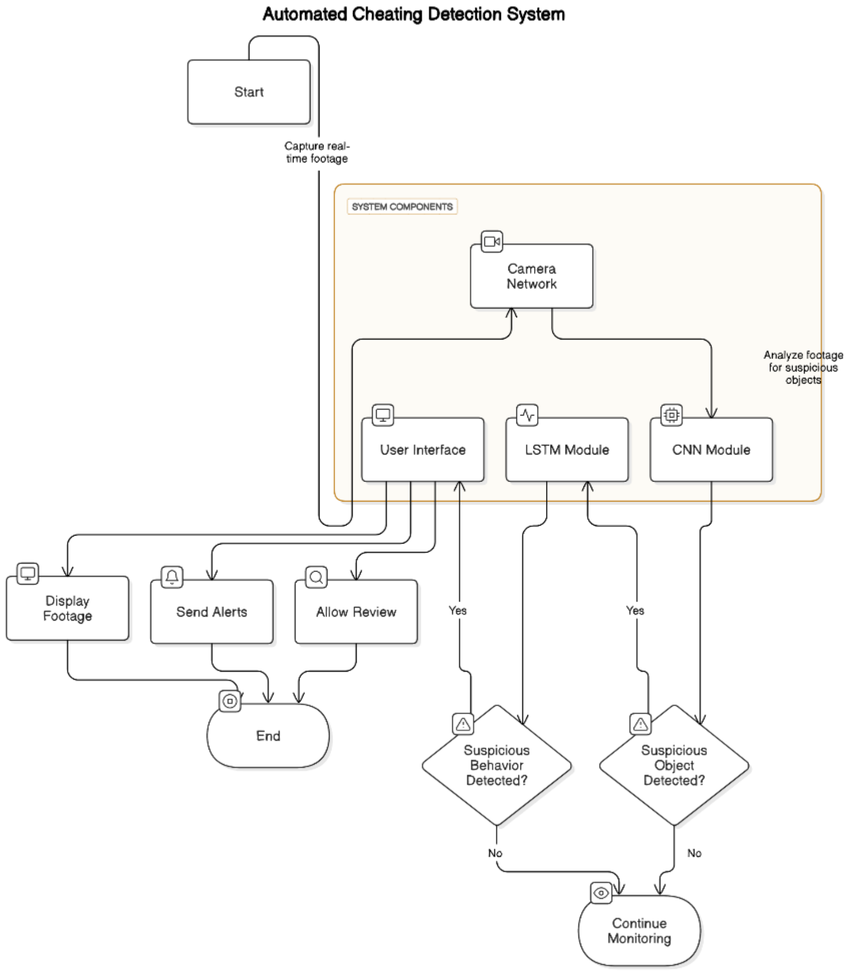
Automated Cheating Detection System
Start
Capture real-time footage
SYSTEM COMPONENTS
Camera Network
Analyze footage for suspicious objects
User Interface
LSTM Module
CNN Module
Display Footage
Send Alerts
Allow Review
Yes
Yes
End
Suspicious Behavior Detected?
Suspicious Object Detected?
No
No
Continue Monitoring

Figure 1: System Architecture

DOI: 10.5281/zenodo.14066366

2. **Data Collection**

   Data for training the model is collected from various sources:

   - **Publicly Available Datasets:** Video datasets that contain various activities, including typical behaviors in academic and public settings.
   - **Custom Video Feeds:** Controlled environment recordings simulating exam conditions, capturing both normal and suspicious behaviors.

3. **Training Methodology**

   - **Preprocessing:** Video feeds are converted into frames, resized, and normalized to ensure consistent input for the models.
   - **CNN Training:** The CNN model is trained on annotated images that highlight the location and type of objects (e.g., mobile phones, cheat sheets). This enables the model to learn and recognize suspicious items effectively.
   - **LSTM Training:** After object detection, outputs from the CNN module are fed into the LSTM model, which is trained to analyze sequences of detected objects and movement patterns over time.
   - **Evaluation:** Model performance is evaluated using metrics like accuracy, precision, recall, and F1-score. Cross-validation techniques are applied to ensure model robustness and reliability.

V. RESULT

Automated cheating detection systems are now built on deep learning models, especially those that combine CNN and LSTM architectures. While LSTMs are good at evaluating sequential data to catch behaviors over time, including frequent gazing or hand motions that would imply cheating, CNNs, like VGG-16 and YOLOv3, are extensively utilized for their accuracy in identifying things like mobile phones or cheat sheets. When combined, these models offer a reliable system that enables highly accurate real-time monitoring. Study-reported performance data, including an average accuracy of 85–90%, precision of about 87%, and recall of about 83%, demonstrate how well these algorithms consistently detect suspicious activity while reducing false positives.

Automated solutions provide constant and scalable coverage in comparison to manual supervision, which makes them useful in large-scale test settings where human invigilators may be limited by staff availability or observational errors. However, there are a number of issues with current models. Environmental sensitivity is still a major problem; things like camera positioning, seating configurations, and illumination changes can all affect how accurately an action is detected, particularly when it is partially covered. The computing demands of processing high-resolution video feeds in real-time can further delay the issuance of alerts, highlighting the necessity for efficient processing methods. The variety of cheating behaviors, which are not always simple to classify, is another significant obstacle; future systems can profit from flexible algorithms that can gradually pick up new behaviors.

VI. CONCLUSION

The proposed system effectively addresses the challenge of real-time suspicious activity detection in exam halls by integrating CNN for object detection and LSTM for behavior analysis. This dual approach allows for accurate identification of unauthorized objects and unusual behaviors, enhancing the integrity of monitored environments. By leveraging deep learning, the system minimizes reliance on manual invigilation and improves detection efficiency, reducing false positives and providing consistent, automated alerts.

The architecture's adaptability makes it suitable for various applications beyond academic settings, such as public surveillance and workplace monitoring, where prompt detection of suspicious activities is essential. Overall, this system demonstrates the potential of deep learning in improving security and maintaining fairness in controlled environments, contributing to a more secure and trustworthy assessment process. Future enhancements could involve training the system on larger datasets to further improve detection accuracy and adapting the model to handle more complex behaviors and diverse environments.

REFERENCES

[1] Md Adil, Rajbala Simon, Sunil Kumar Khatri, “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.