International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 05 | May 2026 www.irjet.net p-ISSN: 2395-0072

Performance Analysis of Machine Learning Models for Secure Online Examination Systems Using Face Detection

Supriya Koul Machama[1], Dr. Niresh Sharma[2]

[1]*Department of Computer Science, Sarvepalli Radhakrishnan University, Bhopal, Madhya Pradesh, India*
[2]*Professor, Department of Computer Science, Sarvepalli Radhakrishnan University, Bhopal, Madhya Pradesh, India*

Abstract - *The rapid expansion of online examination systems has introduced significant challenges in maintaining examination integrity and preventing unfair practices such as impersonation and unauthorized assistance. To address these concerns, automated monitoring approaches based on machine learning and computer vision have gained considerable attention. This paper evaluates the performance of multiple machine learning models for detecting suspicious behaviour in online examination environments using face detection-based features. The study considers Decision Tree, Logistic Regression, and Random Forest classifiers trained on behavioural indicators such as face presence, multiple face detection, and movement patterns. Model performance is assessed using standard evaluation metrics including accuracy, precision, and recall. The experimental analysis demonstrates that ensemble learning, particularly Random Forest, achieves superior performance compared to other models in identifying abnormal activities. The results confirm the suitability of machine learning techniques for enhancing the security and dependability of online proctoring systems.*

Key Words: Machine Learning, Online Examination Security, Face Detection, Random Forest, Performance Analysis

1. INTRODUCTION

The rapid growth of online education has led to the widespread use of online examination systems. While these systems provide flexibility and accessibility, they also introduce challenges related to maintaining fairness and preventing cheating.

Traditional monitoring methods are often insufficient to detect sophisticated cheating behaviours. Machine learning has emerged as a powerful tool for analyzing user behaviour and identifying anomalies in real time.

Face detection techniques such as the Viola–Jones algorithm [1] enable real-time monitoring of candidates, while machine learning models can classify behaviour as normal or suspicious [2][3]. However, selecting the most effective model for this task remains a challenge.

This paper presents a comparative analysis of different machine learning models for detecting suspicious activities in online examination systems. The study aims to identify the most accurate and reliable model for enhancing system security.

1.1 Literature Review

Recent advancements in online examination systems have led to increased research interest in ensuring security and academic integrity through automated monitoring techniques. Traditional invigilation methods are insufficient in remote environments, which has encouraged the adoption of artificial intelligence-based solutions.

In addition to face detection, OpenCV has been extensively used as a practical tool for implementing real-time video processing systems. It provides libraries for image processing, object detection, and tracking, making it suitable for developing automated proctoring systems. Machine learning techniques have also been widely applied in behavioural analysis and anomaly detection. Algorithms such as Decision Tree, Logistic Regression, and Random Forest have demonstrated effectiveness in classification problems involving structured behavioural data. Among these, ensemble methods like Random Forest are known to improve prediction accuracy by combining multiple decision trees and reducing overfitting.

Research in educational data mining has further highlighted the importance of analyzing user behaviour patterns to detect irregular activities in online learning environments. These approaches focus on identifying deviations from normal behaviour to flag potential violations during assessments. Despite significant progress, existing systems still face challenges such as false positives, limited real-time processing capability, and difficulty in handling complex cheating scenarios involving multiple behavioural cues. This creates a need for more robust and hybrid approaches that combine face detection with machine learning-based classification techniques for improved accuracy and reliability.

2. PROPOSED METHODOLOGY AND RESULTS ANALYSIS

The proposed system focuses on enhancing online examination security using machine learning-based behavioural classification integrated with face detection.

The implementation consists of two major components: face detection and machine learning-based classification.

Face detection is implemented using OpenCV's Haar Cascade classifier, which is based on the Viola–Jones framework. The system processes video frames in real time and identifies the number of faces present in each frame.

Machine learning models including Decision Tree, Logistic Regression, and Random Forest are trained to classify behavioural patterns. Among these, Random Forest is selected as a primary model due to its ability to handle complex data distributions and reduce overfitting. The feature set used for classification includes:

- Number of detected faces
- Duration of continuous face presence
- Frequency of movement or absence detection

A simulated dataset representing various examination scenarios is used for training and evaluation. The performance of different machine learning models was evaluated using accuracy, precision, and recall metrics under simulated examination conditions.
The results are shown in Table I.

Table -1: Performance Comparison of Models

Performance			
Model	Accuracy	Precision	Recall
Decision Tree	87%	85%	86%
Random Forest	92%	90%	91%
Logistic Regression	84%	82%	83%

The results indicate that Random Forest outperforms other models in all evaluation metrics, demonstrating its effectiveness in handling classification tasks involving behavioural data. Decision Tree provides moderate performance, while Logistic Regression shows comparatively lower accuracy due to its linear nature.

3. CONCLUSIONS

This study focused on enhancing the security of online examination systems through the integration of face detection and machine learning techniques. The proposed approach enables real-time monitoring of candidates by analysing behavioural patterns such as face presence, multiple face detection, and movement activity.

A comparative evaluation of Decision Tree, Logistic Regression, and Random Forest classifiers was conducted to assess their effectiveness in detecting suspicious behaviour. The experimental results demonstrate that the Random Forest model outperforms other models in terms of accuracy, precision, and recall. The integration of computer vision-based face detection with machine learning classification significantly improves the system's ability to identify potential malpractice during online examinations. This approach enhances the fairness, reliability, and overall security of digital assessment environments.

The proposed system is efficient and scalable, making it suitable for deployment in modern e-learning platforms and real-time online examination systems.

ACKNOWLEDGEMENT

The author would like to express sincere gratitude to the Department of Computer Science, Sarvepalli Radhakrishnan University, Bhopal, for providing guidance and support throughout this research work.

REFERENCES

[1] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), 2001.

[2] G. Bradski, "The OpenCV Library," Dr. Dobb's Journal of Software Tools, 2000.

[3] L. Breiman, "Random forests," Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.

[4] K. Choudhary et al., "AI-based online proctoring system," Proc. IEEE Conference on Emerging Technologies, 2020.

[5] S. Baker and I. Inventado, "Educational data mining and learning analytics," in Learning Analytics: From Research to Practice, 2014.

[6] W. Zhao et al., "Face recognition: A literature survey," ACM Computing Surveys, vol. 35, no. 4, pp. 399–458, 2003.